RIIGI INFOSÜSTEEMI AMET

INFOSÜSTEEMIDE KOLMEASTMELINE ETALONTURBE SÜSTEEM

ISKE

ISKE rakendusjuhendi lisa 1: Kataloogid B, M ja H

Versioon 8.06
November 2018

Sisukord

ISKE kataloogide versiooni 8.06 muutelugu

Lisatud tüüpmoodulid

B 1.18 Identiteedi- ja volituste haldus
B 3.213 Klient Windows 8 keskkonnas
B 3.407 Integreeritud süsteem
B 5.26 Teenustele suunatud struktuur
B 5.27 Tarkvaraarendus

Muudetud tüüpmoodulid

B 1.0 Infoturbe haldus
B 1.1 Organisatsioon
B 1.2 Personal
B 1.3 Hädaolukorraks valmisoleku kontseptsioon
B 1.4 Andmevarunduspoliitika
B 1.6 Viirusetõrje kontseptsioon
B 1.7 Krüptokontseptsioon
B 1.8 Turvaintsidentide käsitlus
B 1.9 Riist- ja tarkvara haldus
B 1.10 Tüüptarkvara
B 1.11 Väljasttellimine (Outsourcing)
B 1.12 Arhiveerimine
B 1.13 Infoturbe teadlikkus ja -koolitus
B 1.14 Turvapaikade ja muudatuste haldus
B 1.15 Andmete kustutamine ja hävitamine
B 1.17 Pilvteenuse kasutamine
B 2.1 Hooned
B 2.2 Elektrotehniline kaabeldus
B 2.3 Bürooruum
B 2.4 Serveriruum
B 2.5 Andmekandjate arhiiv
B 2.6 Tehnilise infrastruktuuri ruum
B 2.7 Kaitsekapid

B 2.8 Kaugtöökoht kodus
B 2.9 Arvutuskeskus
B 2.10 Mobiilne töökoht
B 2.11 Nõupidamis-, üritus- ja koolitusruumid
B 2.12 IT-kaabeldus
B 3.101 Server
B 3.102 Server Unixi all
B 3.107 Suurarvutid S/390 ja zSeries
B 3.109 Windows Server 2008
B 3.201 Klient
B 3.202 Autonoomne IT-süsteem
B 3.203 Sülearvuti
B 3.204 Klient Unixi all
B 3.208 Interneti-PC
B 3.210 Klient Windows all
B 3.211 Mac OS X-ga töötav klientsüsteem
B 3.212 Windows 7-ga töötav klientsüsteem
B 3.301 Turvalüüs (tulemüür)
B 3.302 Marsruuterid ja kommutaatorid
B 3.303 Salvestisüsteemid ja salvestivõrgud
B 3.304 Virtualiseerimine
B 3.305 Terminaliserver
B 3.401 Kodukeskjaam (PBX)
B 3.402 Faks
B 3.404 Mobiiltelefon
B 3.405 Nutitelefonid, tahvel- ja pihuarvutid
B 4.1 Heterogeensed võrgud
B 4.2 Võrgu- ja süsteemihaldus
B 4.3 Modem
B 4.4 Virtuaalne privaatvõrk (VPN)
B 4.5 IT-süsteemi kohtvõrguühendus ISDN kaudu
B 4.6 Traadita kohtvõrgud
B 4.7 IP-kõne (VOIP)
B 4.8 Bluetooth
B 5.2 Andmekandjatel toimuv andmevahetus
B 5.3 Rühmatarkvara
B 5.4 Veebiserver
B 5.5 Lotus Notes/Domino
B 5.6 Faksiserver
B 5.7 Andmebaasid
B 5.8 Kaugtöö
B 5.9 Novell eDirectory
B 5.12 Microsoft Exchange / Outlook
B 5.13 SAP süsteem
B 5.14 Mobiilsed andmekandjad
B 5.15 Üldine kataloogiteenus
B 5.16 Active Directory
B 5.17 Samba
B 5.18 DNS-server
B 5.19 Interneti kasutamine

B 5.20 OpenLDAP
B 5.21 Veebirakendused
B 5.22 Logimine
B 5.24 Veebiteenused
B 5.25 Rakendused
B 5.E2 ID-kaart/PKI

Lisatud meetmed

M 1.81 Integreeritud süsteemide füüsiline kaitse
M 2.559 Windows 8 soetamine
M 2.560 SOA-l põhineva need-to-share-kontseptsiooni integreerimine turbehaldusesse
M 2.561 Standardikohaste SOA-rakenduste ja konfiguratsioonide loomine
M 2.562 Integreeritud süsteemide kasutamise eeskirjad
M 2.563 Usaldusväärse tarne- ja logistikaketi ning pädeva tootja valimine integreeritud süsteemide jaoks
M 2.564 Integreeritud süsteemide soetamise kriteeriumid
M 2.565 Turbega seotud sündmuste protokollimine integreeritud süsteemides
M 2.566 Integreeritud süsteemi turvaline kasutusest kõrvaldamine
M 2.567 Usaldusväärsete arendustööriistade valik
M 2.568 Tarkvara testimisprotseduurid
M 2.569 Rollide ja vastutuse määratlemine tarkvaraarenduses
M 2.570 Protsessimudeli valik tarkvaraarenduse jaoks
M 2.571 Vastavusnõuete järgimine tarkvaraarenduse jaoks
M 2.572z Tööriistade soetamine tarkvaraarenduse jaoks
M 2.573 Kinnipidamine turvalisest protseduurist tarkvaraarenduses
M 2.574 Tarkvaraarenduse põhjalik dokumenteerimine
M 2.575 Tarkvara arenduskeskkonna korrapärane turvaaudit
M 2.576 Turvapoliitika koostamine kohalike võrkude kasutamisele
M 2.577 Sobiva krüpteerimismeetodi valik võrkudele
M 2.578 Kohaliku võrgu paigaldamine, konfigureerimine ja hooldamine kolmandate isikute poolt
M 2.579 Kohaliku võrgu regulaarsed auditid
M 2.580 Võrgukomponentide kasutuselt kõrvaldamine
M 2.581 Haldusvõrgu ehitus võrguhalduse jaoks
M 2.582 Võimalused haldusvõrgu loomiseks
M 2.583 Sobiva võrguhaldussüsteemi valik
M 2.584 Võrgu- ja süsteemihaldustööriista eeskirjadekohane kasutusest kõrvaldamine
M 2.585 Identiteedi ja volituste halduse kontseptsioon
M 2.586 Volituste andmine, muutmine ja äravõtmine
M 2.587 Identiteedi ja volituste halduse protsesside protseduur ja kontseptsioon
M 3.97 Projektimeeskonna koolitamine tarkvaraarenduse jaoks
M 3.98 Töötajate õpetamine, kuidas kasutada autentimisprotseduure ja -mehhanisme

M 4.471 Windows 8 uute turbefunktsioonide ülevaade
M 4.472 Andmete kokkuhoid Windows 8 puhul
M 4.473 XML-transpordikonteinerite pealtkuulamise kaitse SOA-s
M 4.474 Turvaaukude kaitse SOA Backend-rakendustes
M 4.475 Kaitse identiteeditеenuste teesklusrünnete vastu
M 4.476 WS-Notification-Subscription'i kaitse Broker'is
M 4.477 WS-Notification-Subscription'i kaitse
M 4.478 Võtmehaldus SOA-s
M 4.479 Poliitikate kaitse SOA-s
M 4.480 WS-Resource'i kaitse SOA-keskkondades
M 4.481 Ühendusevaba SOAP-suhtluse turvaline kasutamine
M 4.482 Integreeritud süsteemide funktsioonide riistvaraline teostamine
M 4.483 Krüptograafiliste protsessorite ja kaasprotsessorite (Trusted Platform Module) kasutamine integreeritud süsteemides
M 4.484 Salvesti kaitse integreeritud süsteemides
M 4.485 Turvaline operatsioonisüsteem integreeritud süsteemide jaoks
M 4.486z Integreeritud süsteemide vastupanuvõime külgkanalrünnete vastu
M 4.487z Urkimiskaitse (tuvastamine, takistamine, tõrje) integreeritud süsteemides
M 4.488 Mittekasutatavate liideste ja teenuste inaktiveerimine integreeritud süsteemides
M 4.489 Kaitstud ja autenditud buutimisprotsess integreeritud süsteemides
M 4.490 Seadmemoodulite funktsiooni automaatseire (BIST) integreeritud süsteemides
M 4.491 Silumisvõimaluste tõkestamine integreeritud süsteemides
M 4.492 Integreeritud veebiserveri turvaline konfiguratsioon ja kasutamine
M 4.493z Arenduskeskkonna valimine tarkvaraarenduse jaoks
M 4.494 Arenduskeskkonna turvaline kasutamine
M 4.495 Tarkvaraarenduse turvaline süsteemikujundus
M 4.496 Väljatöötatud tarkvara turvaline installeerimine
M 4.497 Võrguhaldussüsteemi turvaline installeerimine
M 4.498 Ainulogimisega pöörduse turvaline kasutamine
M 4.499 Identiteedi- ja volituste halduse süsteemide asjakohane valik
M 4.500 Identiteedi- ja volituste halduse süsteemide asjakohane kasutamine
M 4.501 Kiirgusturve
M 5.178 Infosüsteemis autentimislahendustele kehtivad nõuded ehk autentimisnormatiiv
M 6.160 Hädaolukorra ennetamise kava SOA-keskkondade jaoks
M 6.161 Liiasusega riistvarakomponendid teenustele suunatud arhitektuurides
M 6.162z Reageerimine krüpteerimismeetodi praktilise nõrgenemise korral
M 6.163 Integreeritud süsteemide taastamine
M 6.164 Valmisolek hädaolukorraks tarkvaraarenduses
M 6.165 Hädaolukorra plaani koostamine kohaliku võrgu tõrke puhuks
M 6.166 Valmisolek hädaolukorraks identiteedi- ja volituste halduse süsteemi puhul

Muudetud meetmed

M 1.10z Turvauksed ja -aknad
M 1.18 Valve- ja tuletõrjesignalisatsioon
M 1.26w Toite avariilülitid
M 1.28 Puhvertoiteallikas
M 1.49 Tehnilised ja organisatsioonilised nõuded arvutuskeskusele
M 1.80 Juurdepääsu kontrolli süsteem ja volituste haldus
M 2.1 IT kasutajate vastutuse ja reeglite kehtestamine
M 2.2 Ressursside haldamine
M 2.3 Andmekandjate haldus
M 2.4 Hooldus- ja remonditööde reeglid
M 2.5 Vastutuse ja ülesannete jaotamine
M 2.6 Sissepääsuõiguste andmine
M 2.7 Süsteemi ja võrgu pääsuõiguste andmine
M 2.8 IT-rakendustele ja andmetele pääsuõiguste andmine
M 2.9 Aktsepteerimata riist- ja tarkvara kasutuse keeld
M 2.10 Riistvara ja tarkvara inventuur
M 2.11 Paroolide kasutamise reeglid
M 2.12 IT-kasutajate nõustamine
M 2.13 Tundlike ressursside jäljetu hävitamine
M 2.14 Võtmete (ja kaartide) haldus
M 2.16 Välispersonali ja külastajate valve ja saatmine
M 2.17 Sisenemisreeglid ja reguleerimine
M 2.18z Kontrollringkäigud
M 2.20 Liinide kontroll
M 2.22z Paroolide deponeerimine
M 2.23z PC kasutamise juhised
M 2.24z IT-passi juurutamine
M 2.25 Süsteemi konfiguratsiooni dokumenteerimine
M 2.26z Süsteemiülema ja ta asetäitja määramine
M 2.28z Väline sidealase konsultatsiooni teenus
M 2.29 Kodukeskjaama (PBX) kasutamisjuhendid
M 2.30 Kasutajate ja kasutajarühmade määramise protseduurid
M 2.31 Volitatud kasutajate ja õiguste profiilide dokumenteerimine
M 2.32z Piiratud kasutajakeskkonna loomine
M 2.34 IT-süsteemi muutuste dokumenteerimine
M 2.35 Teabe hankimine turvaaukude kohta
M 2.37 Korrastatud töölaud
M 2.38 Administraatorirollide jagamine
M 2.39 Vastutus turvapoliitika rikkumise eest
M 2.40z Töötajate esinduse õigeaegne kaasamine
M 2.42 Võimalike suhtluspartnerite määramine
M 2.46 Krüpteerimise õige korraldus
M 2.62 Tarkvara vastuvõtuprotseduurid
M 2.64 Logifailide kontroll
M 2.65 IT-süsteemi kasutajate eraldatuse kontroll
M 2.66z Sertifikaatidega arvestamine IT soetamisel
M 2.73 Sobiva turvalüüsi (tulemüüri) põhistruktuuri väljavalimine
M 2.79 Vastutuste määramine tüüptarkvara alal

M 2.80 Tüüptarkvara nõuete kataloogi koostamine
M 2.81 Sobiva tüüptarkvaratoote eelvalimine
M 2.82 Tüüptarkvara testimisplaani väljatöötamine
M 2.83 Tüüptarkvara testimine
M 2.84 Tüüptarkvara installeerimisjuhendite otsustamine ja koostamine
M 2.85 Tüüptarkvara kinnitamine
M 2.86 Tarkvara tervikluse tagamine
M 2.87 Tüüptarkvara installeerimine ja konfigureerimine
M 2.88 Tüüptarkvara litsentsi- ja versioonihaldus
M 2.89 Tüüptarkvara deinstalleerimine
M 2.90 Kohaletoimetuse kontroll
M 2.95 Sobivate kaitsekappide soetamine
M 2.96 Kaitsekappide lukustamine
M 2.97 Õige koodlukuprotseduur
M 2.110 Andmeprivaatsuse suunised logimisprotseduurides
M 2.111 Juhendite käepärast hoidmine
M 2.112 Kodutööjaamade ja asutuse vahelise dokumentide ja andmekandjate transportimise reguleerimine
M 2.113 Kaugtöö reeglid
M 2.114 Infovool kaugtöötaja ja asutuse vahel
M 2.115 Kodutööjaama hooldus
M 2.116 Sidevahendite kasutamise reguleerimine
M 2.117 Kaugtöötajate pääsu reguleerimine
M 2.124 Sobiva andmebaasitarkvara valimine
M 2.125 Andmebaasi installeerimine ja konfigureerimine
M 2.126 Andmebaasi turvakontseptsioon
M 2.127 Tuletamise vältimine andmebaasis
M 2.128 Andmebaasisüsteemi pääsu reguleerimine
M 2.129 Andmebaasiinfo pääsu reguleerimine
M 2.130 Andmebaasi tervikluse tagamine
M 2.131 Haldusülesannete lahusus andmebaasisüsteemides
M 2.132 Andmebaasi kasutajate ja kasutajagruppide konfigureerimise reeglid
M 2.133 Andmebaasisüsteemi logifailide kontroll
M 2.134 Andmebaasipäringute suunised
M 2.135 Andmete turvaline teisaldus andmebaasi
M 2.137 Sobiva andmevarundussüsteemi hankimine
M 2.138 Struktureeritud andmetalletus
M 2.139 Olemasoleva võrgukeskkonna läbivaatus
M 2.140z Võrgu hetkeolukorra analüüsimine
M 2.141 Võrgukontseptsiooni väljatöötamine
M 2.142 Võrguplaani väljatöötamine
M 2.143 Võrguhalduse kontseptsiooni väljatöötamine
M 2.144 Sobiva võrguhaldusprotokolli valimine
M 2.145 Nõuded võrguhaldusinstrumendile
M 2.154 Viirusetõrje kontseptsiooni loomine
M 2.155 Potentsiaalselt viiruste poolt ohustatud IT-süsteemide tuvastamine
M 2.156 Sobiva viirusetõrjestrateegia valimine
M 2.157 Sobiva viiruseskanneri valimine
M 2.158 Viirusnakkustest teatamine
M 2.159 Viiruseskanneri värskendamine

M 2.160 Viirusetõrje eeskirjad
M 2.161 Krüptokontseptsiooni väljatöötamine
M 2.162 Krüptoprotseduuride ja -toodete vajaduse määramine
M 2.163 Krüptoprotseduure ja -tooteid mõjutavate tegurite määramine
M 2.164 Sobiva krüptoprotseduuri valimine
M 2.165 Sobiva krüptotoote valimine
M 2.166 Krüptomoodulite kasutamist reguleerivad sätted
M 2.167 Andmete kustutamiseks või hävitamiseks sobivate lahenduste valik
M 2.169 Süsteemihalduse strateegia väljatöötamine
M 2.170 Nõuded süsteemihaldussüsteemile
M 2.171 Sobiva süsteemihaldustoote valimine
M 2.173 Veebiserveri turbestrateegia väljatöötamine
M 2.177 Kolimise turve
M 2.190z Mobiilikogu sisseseadmine
M 2.192 Infoturbepoliitika koostamine
M 2.193 Infoturbeks sobiva organisatsioonilise struktuuri rajamine
M 2.195 Infoturbe kontseptsiooni loomine
M 2.197 Töötajate kaasamine turbeprotsessi
M 2.198 Personali teavitamine infoturbe küsimustest
M 2.200 Infoturbearuanded juhtkonnale ja hinnangud infoturbele
M 2.201 Infoturbe protsessi dokumenteerimine
M 2.204 Ebaturvalise võrkupääsu tõkestamine
M 2.207 Lotus Notesi/Domino turvakontseptsioon
M 2.213 Tehnilise infrastruktuuri hooldus
M 2.214 IT-kasutuse kontseptsioon
M 2.215 Tõrkekäsitlus
M 2.216 IT-komponentide kinnitamise protseduur
M 2.217 Teabe, rakenduste ja süsteemide hoolikas liigitamine ja käitlus
M 2.218 Andmekandjate ja IT-komponentide kaasavõtmise protseduurid
M 2.219 Infotöötluse pidev dokumenteerimine
M 2.220 Pääsu reguleerimise suunised
M 2.221 Muudatuste haldus
M 2.223 Tüüptarkvara kasutamise turvaeesmärgid
M 2.224 Trooja hobuste tõrje
M 2.225 Teabe, rakenduste ja IT-komponentide alaste vastutuste kinnistamine
M 2.226 Asutusevälise personali kasutamise protseduurid
M 2.229 Active Directory planeerimine
M 2.230 Active Directory halduse planeerimine
M 2.231 Windowsi grupipoliitika planeerimine
M 2.232 Windows CA-struktuuri plaaneerimine
M 2.242 Elektroonilise arhiveerimise eesmärkide määratlemine
M 2.243 Arhiveerimiskontseptsiooni väljatöötamine
M 2.244 Elektroonilise arhiveerimise tehniliste tegurite väljaselgitamine
M 2.245 Elektroonilise arhiveerimise õiguslike tegurite väljaselgitamine
M 2.246 Elektroonilise arhiveerimise organisatsiooniliste tegurite väljaselgitamine
M 2.250 Väljasttellimise strateegia määramine
M 2.251 Väljasttellimisprojektide turvanõuete spetsifitseerimine
M 2.252 Väljasttellitava teenuse sobiva tarnija valimine
M 2.253 Välise teenusepakkujaga sõlmitava lepingu koostamine
M 2.254 Väljast tellitud projektile infoturbekontseptsiooni loomine

M 2.255 Turvaline üleviimine väljast tellitud projektides
M 2.256 Infoturbe planeerimine ja käigushoidmine väljasttellimise tegevuste ajal
M 2.257 Arhiveerimis-andmekandja salvestusressursside seire
M 2.258 Dokumentide järjekindel indekseerimine arhiveerimisel
M 2.259z Üldise dokumendihaldussüsteemi kasutuselevõtt
M 2.260 Arhiveerimisprotseduuri regulaarne auditeerimine
M 2.261 Regulaarsed arhiivisüsteemide turu-uuringud
M 2.262 Arhiivisüsteemide kasutamise reguleerimine
M 2.263 Arhiveeritud andmeressursside regulaarne regenereerimine
M 2.264 Krüpteeritud andmete regulaarne regenereerimine arhiveerimisel
M 2.265z Digitaalallkirjade õige kasutamine arhiveerimisel
M 2.266 Arhiivisüsteemi tehniliste komponentide regulaarne asendamine
M 2.273 Turvalisust mõjutavate paikade ja värskenduste kiire paigaldamine
M 2.277z Kommutaatori funktsionaalne kirjeldus
M 2.280 Sobivate marsruuterite ja kommutaatorite ostmis- ja valimiskriteeriumid
M 2.303 Nutitelefonide, tahvel- ja pihuarvutite kasutamise strateegia määratlemine
M 2.306 Kahjudest teatamine
M 2.307 Väljasttellimissuhte nõuetekohane lõpetamine
M 2.312 Infoturbealase koolitus- ja teavitusprogrammi kavandamine
M 2.320 Serveri nõuetekohane kasutuselt kõrvaldamine
M 2.322 Klient-server-võrgu turvapoliitika kehtestamine
M 2.323 Kliendi korrakohane kasutuselt kõrvaldamine
M 2.324 Windows 7 kasutuselevõtu planeerimine
M 2.325 Windows 7 turvapoliitika kavandamine
M 2.326 Windows 7 grupeerimissuuniste planeerimine
M 2.327 Kaugpääsu turve Windows 7-s
M 2.330 Windows 7 turvapoliitika ja selle elluviimise regulaarne kontroll
M 2.334z Sobiva hoone valimine
M 2.335 Infoturbe eesmärkide ja strateegia kehtestamine
M 2.336 Koguvastutus infoturbe eest juhtkonna tasemel
M 2.337 Infoturbe integreerimine üleorganisatsioonilistesse tegevustesse ja protsessidesse
M 2.338z Sihtrühmakohase infoturbepoliitika koostamine
M 2.339z Ressursside ökonoomne kasutamine infoturbeks
M 2.340 Õiguslike raamtingimuste järgimine
M 2.354z Kõrge käideldavusega SAN-konfiguratsiooni kasutamine
M 2.364 Halduse planeerimine
M 2.365 Süsteemiseire planeerimine
M 2.366 Windows Serveri turvamallide kasutamine
M 2.367 Käskude ja skriptide kasutamine
M 2.368 Administratiivsete mallide kasutamine
M 2.369 Turvalisusega seotud hooldustööde regulaarne läbiviimine
M 2.370 Volituste haldamine
M 2.371 Kasutamata kasutajatunnuste organiseeritud desaktiveerimine ja kustutamine
M 2.374 IP-kõne krüpteerimise ulatus
M 2.376 Andmeside ja IP-kõne (VOIP) võrgu eraldamine
M 2.378z Süsteemiarendus
M 2.379z Tarkvaraarendus lõppkasutaja poolt

M 2.380 Erandite kooskõlastamine
M 2.381 Traadita kohtvõrgu kasutamise strateegia väljatöötamine
M 2.383 Sobiva traadita kohtvõrgu standardi valik
M 2.384 Sobiva traadita kohtvõrgu krüpteerimisviisi valik
M 2.385 Sobivate traadita kohtvõrgu komponentide valik
M 2.392 Virtualiseerimisserverite ja virtuaalsete IT-süsteemide modelleerimine
M 2.393 Infovahetuse reguleerimine
M 2.395 IT-kaabeldusele esitatavate nõuete analüüs
M 2.396z IT-kaabelduse dokumenteerimise ja märgistuse nõuded
M 2.397 Printerite, koopiamasinate ja multifunktsionaalsete seadmete kasutamise planeerimine
M 2.398 Printerite, koopiamasinate ja multifunktsionaalsete seadmete kasutusjuhised
M 2.399w Printerite, koopiamasinate ja multifunktsionaalsete seadmete soetamise ning väljavalimise kriteeriumid
M 2.400 Printerite, koopiamasinate ja multifunktsionaalsete seadmete turvaline kasutuselt kõrvaldamine
M 2.401 Mobiilsete andmekandjate ja seadmete kasutamine
M 2.402z Paroolide uuendamine
M 2.406 Kataloogiteenuste kasutamiseks sobivate komponentide valik
M 2.408z Kataloogiteenuste üleviimise planeerimine
M 2.412 Autentimise kaitse Active Directory kasutamisel
M 2.414 Domeenikontrollerite kaitse arvutiviiruste eest
M 2.420 Trusted VPN teenusepakkuja valimine
M 2.421 Turvapaikade ja muudatuste halduse planeerimine
M 2.422 Muudatustaotluste käsitlemine
M 2.423 Vastutusalade kindlaksmääramine turvapaikade ja muudatuste halduseks
M 2.424 Paikade ja muudatuste haldamise tööriistade turvapoliitika
M 2.425 Asjakohane turvapaikade ja muudatuste haldusinstrumentide valik
M 2.426 Turvapaikade ja muudatuste halduse integreerimine äriprotsessidesse
M 2.427 Muudatustaotluste kooskõlastamine
M 2.428z Skaleeritavus paikade ja muudatuste halduses
M 2.429z Muudatustaotluste tulemuste hindamine
M 2.431 Korrakohased protseduurid informatsiooni kustutamiseks või hävitamiseks
M 2.432z Eeskirjad informatsiooni kustutamiseks ja hävitamiseks
M 2.433w Ülevaade meetoditest andmete kustutamiseks ja hävitamiseks
M 2.434z Andmete kustutamiseks või hävitamiseks vajalike seadmete soetamine
M 2.435z Sobiva dokumendipurusti valik
M 2.436z Andmekandjate hävitamine välise teenusetarnija poolt
M 2.439 Nõuete halduse kontseptsioon ja organisatsioon
M 2.440 Windows 7 sobiva versiooni valimine
M 2.441 Uue tarkvara ühilduvuse kontroll koostööks Windows 7-ga
M 2.442 Windows 7 kasutamine kaasaskantavates arvutites
M 2.444 Virtuaalsete IT-süsteemide ressursside planeerimine
M 2.447 Virtuaalsete IT-süsteemide turvaline kasutamine
M 2.449z Konsooli kaudu virtuaalsetele IT-süsteemidele juurdepääsu minimaalne kasutamine
M 2.451 DNS-i kasutamise planeerimine

M 2.454 Rühmatarkvarasüsteemide turvalise kasutamise planeerimine
M 2.460 Väliste teenuste reguleeritud kasutamine
M 2.463z Bluetooth-lisaseadmete seadmekogu kasutamine
M 2.465 Terminaliserveri vajalike ressursside analüüs
M 2.468z Tarkvaralitsentsid terminaliserveri keskkonnas
M 2.470 Kodukeskjaama nõudlusanalüüsi läbiviimine
M 2.472 Kodukeskjaama (PBX) turvajuhendi koostamine
M 2.473 Kodukeskjaama (PBX) teenusepakkuja valimine
M 2.475 Lepingu koostamine väljast tellitava infoturbespetsialistiga
M 2.476 Interneti turvalise ühendamise kontseptsioon
M 2.477 Virtuaaltaristu planeerimine
M 2.480w Exchange'i ja Outlooki dokumentatsiooni kasutamine
M 2.482 Exchange'i süsteemide regulaarsed turvakontrollid
M 2.483 Exchange'i süsteemide turvaline kohandamine
M 2.489 Windows Server 2008 süsteemiseire planeerimine
M 2.490 Hyper-V-ga virtualiseerimise planeerimine
M 2.491 Windows Server 2008 rollide ja turvamallide kasutamine
M 2.494 Lotus Notesi/Domino keskkonna taristu jaoks komponentide valimine
M 2.495 Lotus Notesi/Domino komponentide kasutusest kõrvaldamine
M 2.498 Reageerimine hoiatus- ja veateadetele
M 2.499 Logimise planeerimine
M 2.500 IT-süsteemide logimine
M 2.501 Isikuandmete kaitse haldus
M 2.502 Isikuandmete kaitse vastutusalade kindlaksmääramine
M 2.504 Õigusalaste raamtingimuste kontrollimine ja isikuandmete töötlemise eelkontroll
M 2.509 Isikuandmete kaitse seadusele vastav kasutusse lubamine
M 2.526 Salvestisüsteemi käitamise planeerimine
M 2.529w Salvestisüsteemide modelleerimine
M 2.534 Pilvteenuse kasutamisstrateegia koostamine
M 2.535 Pilvteenuse kasutamise turvapoliitika koostamine
M 2.536 Tarbitavate pilvteenuste määratlemine teenuste tarbija poolt
M 2.537 Teenuste pilvteenusteks üleviimise turbe planeerimine
M 2.538 Pilvteenuste juurutamise turbe planeerimine
M 2.539 Pilvteenuste kasutamise turbekontseptsiooni koostamine
M 2.540 Pilvteenuste osutaja hoolikas valimine
M 2.541 Pilvteenuseosutajaga sõlmitava lepingu koostamine
M 2.542 Teenuste turvaline üleviimine pilvteenusteks
M 2.543 Pilvteenuste infoturbe tagamine igapäevatöös
M 2.544 Pilvteenuste kasutamise auditeerimine
M 2.555 Rakenduste autentimiskontseptsiooni koostamine
M 2.557 Infoturbealase koolitusprogrammi kontseptsioon
M 2.558 Töötajate mobiil- ja nutitelefonide ning tahvel- ja pihuarvutite infoturbe teadlikkuse suurendamine
M 2.E12 E-ID rakendusjuhiste järgimine
M 2.E13 Asutusesisesed reeglid ID-kaardi/PKI kasutamiseks
M 2.E14 Digitempli turvaline evitamine asutuses
M 2.E15 ID-kaardi või sarnase seadme PIN-ja PUK-koodide turvaline käitlemine
M 2.E16 Transpordikrüpto vormingute kasutuskeeld andmete säilitamiseks
M 2.E17 ID-kaardi või sarnase seadme kasutuskeeld tundmatute turvasätetega

keskkonnas
M 2.E18 ID-kaardi või digi-ID edasiandmiskeeld teisele isikule (tavakasutaja)
M 2.E19w ID-kaardi või digi-ID kaasavõtmiskohustus arvuti juurest lahkumisel
M 2.E20 ID-kaardi või digi-ID edasiandmiskeeld teisele isikule (administraator)
M 2.E21 Digitembeldussüsteemi tegevuse lõpetamine
M 2.E22 Krüptograafiliste algoritmide vahetatavuse nõue
M 3.1 Uute töötajate esmane juhendamine ja väljaõpe
M 3.2 Uute töötajate kohustamine eeskirju järgima
M 3.3 Asendamise korraldamine
M 3.4 Väljaõpe enne programmi tegelikku kasutamist
M 3.5 Turvameetmete koolitus
M 3.6 Reguleeritud protseduur töösuhete lõpetamiseks
M 3.7z Kontaktisik isiklikes küsimustes
M 3.8z Tööõhkkonda kahjustavate tegurite vältimine
M 3.9z Ergonoomiline töökoht
M 3.10 Usaldusväärse administraatori ja tema asetäitja valimine
M 3.11 Hooldus- ja halduspersonali väljaõpe
M 3.12 Töötajate teavitamine kodukeskjaama (PBX) signaalidest ja teadetest
M 3.13 Töötajate teavitamine kodukeskjaama (PBX) kasutusega seotud ohtudest
M 3.18 PC kasutajate väljalogimiskohustus
M 3.21 Kaugtöötajate turbealane koolitus
M 3.23w Sissejuhatus krüptograafia põhimõistetesse
M 3.26 Personali juhendamine IT-vahendite turvalise kasutamise kohta
M 3.27 Koolitus Active Directory haldamiseks
M 3.33z Personali taustakontroll
M 3.34 Arhiivisüsteemi haldamise koolitus
M 3.35 Arhiivisüsteemi kasutamise koolitus kasutajatele
M 3.38 Marsruuterite ja kommutaatorite koolitus administraatoritele
M 3.43 Turvalüüsi administraatorite koolitus
M 3.44 Juhtkonna teadlikkuse tõstmine infoturbe alal
M 3.45 IT-turbealaste koolituste sisu kavandamine
M 3.46 Kontaktisik turvalisuse alal
M 3.47z IT-turbealased tegevus- ja rollimängud
M 3.48z Koolitajate või koolitusfirmade valimine
M 3.49 Koolitus etalonturbe protseduuride alal
M 3.50z Personali valimine
M 3.51z Personali rakendamise ja kvalifitseerimise kontseptsioon
M 3.53w Sissejuhatus SAP süsteemidesse
M 3.54 Salvestisüsteemide administraatorite koolitus
M 3.55 Konfidentsiaalsuslepingud
M 3.56 IP-kõne administraatorite koolitus
M 3.58w Sissejuhatus traadita kohtvõrgu põhimõistetesse
M 3.63 Kasutajate koolitus autentimiseks kataloogiteenuste abil
M 3.64w Sissejuhatus Active Directory'sse
M 3.66w Turvapaikade ja muudatuste halduse põhimõisted
M 3.67 Töötajate koolitamine andmete kustutamise või hävitamise alal
M 3.68 Samba-serveri administraatorite koolitus
M 3.69w Sissejuhatus viirustest tulenevatesse ohtudesse
M 3.70w Sissejuhatus virtualiseerimisse
M 3.72w Virtualiseerimistehnika põhimõisted

M 3.73 DNS-serveri administraatorite koolitamine
M 3.74 Rühmatarkvarasüsteemide süsteemiarhitektuuri ja turbe koolitus administraatoritele
M 3.76 Rühmatarkvara ja meili kasutajate koolitus
M 3.83z Personaliga seotud turbefaktorite analüüs
M 3.84w Sissejuhatus Exchange'i süsteemidesse
M 3.89 Logimisprotsessi haldamise koolitus
M 3.90w Tsentraalse logimise põhitõed
M 3.93 Teavitus- ja koolitusprogrammide sihtrühmade analüüs
M 3.94 Õpitulemuste edukuse mõõtmine ja hindamine
M 3.95z Õppematerjali kinnistamine
M 3.96 Juhatuse tugi teavitusele ja koolitusele
M 3.E2 Töötajate koolitus ID-kaardi/PKI lahenduste kasutamise osas
M 4.1 IT-süsteemide paroolkaitse
M 4.3 Viirusetõrjeprogrammide kasutamine
M 4.4 Eemaldatavate andmekandjate draivipilude ja väliste andmekandjate nõuetele vastav kasutamine
M 4.7 Algparoolide muutmine
M 4.16 Konto- ja/või terminalipääsu piirangud
M 4.18 Monitori- ja ainukasutajarežiimi pääsu reguleerimine
M 4.19 Unixi süsteemifailide ja -kataloogide atribuutide jaotuse piirangud
M 4.20 Unixi kasutajafailide ja -kataloogide atribuutide jaotuse piirangud
M 4.21 Ülemaõiguste volitamatu võtu vältimine
M 4.25 Logimine Unix-süsteemis
M 4.29z Kaasaskantavatele IT-süsteemidele mõeldud krüpteerimistoote kasutamine
M 4.30 Rakendusprogrammide turvavahendite kasutamine
M 4.32 Andmekandjate füüsiline kustutamine enne ja pärast nende kasutamist
M 4.33 Viirustõrjeprogrammi kasutamine andmekandjate vahetamisel ja andmete edastamisel
M 4.34z Krüpteerimise, kontrollsummade ja digitaalallkirjade rakendamine
M 4.40 Arvuti mikrofoni volitamata kasutamise vältimine
M 4.41z Sobivate IT-süsteemide turvatoodete valimine
M 4.42z Turvafunktsioonide rakendamine IT-rakenduses
M 4.43z Automaatse ümbrikusüsteemiga faksiaparaat
M 4.47 Turvalüüsi operatsioonide logimine
M 4.56 Turvaline kustutus Windows operatsioonisüsteemides
M 4.63 Kaugtöökohaarvutite turvanõuded
M 4.64 Ülekantavate andmete kontrollimine enne edastamist/peidetud info kõrvaldamine
M 4.65 Uue riist- ja tarkvara testimine
M 4.72z Andmebaasi krüpteerimine
M 4.78 Konfiguratsioonimuudatuste hoolikas teostamine
M 4.80 Kaug-võrguhalduse turvalised pääsumehhanismid
M 4.81 Võrgutoimingute audit ja logimine
M 4.82 Võrgu aktiivkomponentide turvaline konfigureerimine
M 4.84 BIOSi turvamehhanismide kasutamine
M 4.85z Sobiv krüptomoodulite liideste disain
M 4.86 Krüptomoodulite kindel rollijaotus ja konfigureerimine
M 4.87z Krüptomoodulite füüsiline turve

M 4.88 Nõuded operatsioonisüsteemide turvalisusele krüptomoodulite kasutamise korral
M 4.90w Krüptoprotseduuride kasutamine ISO/OSI etalonmudeli eri kihtides
M 4.91 Süsteemihaldussüsteemi turvaline installeerimine
M 4.94 Veebiserveri failide turve
M 4.95 Minimaalne operatsioonisüsteem
M 4.99 Kaitse info muutmise eest pärast üleandmist
M 4.101 Tulemüürid ja krüpteerimine
M 4.107 Tootja ressursside kasutamine
M 4.109z Tööjaamade tarkvara reinstalleerimine
M 4.116 Lotus Notesi/Domino turvaline installimine
M 4.128 Lotus Notesi/Domino turvaline käitus
M 4.133z Sobivate autentimismehhanismide valimine
M 4.134z Sobivate andmevormingute valimine
M 4.135 Süsteemifailide pääsuõiguste andmise kitsendused
M 4.138 Windows Serveri konfigureerimine domeenikontrollerina
M 4.146 Windows'i klient-operatsioonisüsteemide turvaline käitus
M 4.147z EFS-i turvaline kasutamine Windows 'i keskkonnas
M 4.149 Windows'i faili- ja ühiskasutusõigused
M 4.151 Internet-PC turvaline installeerimine
M 4.152 Internet-PC turvaline käitus
M 4.168 Sobiva arhiivisüsteemi valimine
M 4.169 Sobiva arhiveerimis-andmekandja valimine
M 4.170 Dokumentide arhiveerimiseks sobivate andmevormingute valimine
M 4.171 Arhiivisüsteemi indeksiandmebaasi tervikluse kaitse
M 4.172 Arhiivipöörduste logimine
M 4.173 Arhiveerimise regulaarsed talitlus- ja taastetestid
M 4.177 Tarkvarapakettide tervikluse ja autentsuse tagamine
M 4.199 Ohtlike failivormingute vältimine
M 4.215 Turvakriitiliste z/OS-utiliitide kaitse
M 4.222 Turvaprokside õige konfigureerimine
M 4.223 Proksiserverite integreerimine turvalüüsi koostisesse
M 4.225z Logiserveri kasutamine turvalüüsis
M 4.226z Viirusskannerite integreerimine turvalüüsi koostisse
M 4.229 Nutitelefonide, tahvel- ja pihuarvutite turvaline kasutamine
M 4.244 Windowsi klientoperatsioonisüsteemide turvaline süsteemikonfiguratsioon
M 4.245 Windowsi Group Policy Objects alusseadistused
M 4.246 Süsteemiteenuste konfigureerimine Windows 7 keskkondades
M 4.247 Windowsi klientoperatsioonisüsteemide piiratud kasutajaõigused
M 4.248 Windowsi klientoperatsioonisüsteemide turvaline installimine
M 4.281 Windows Serveri turvaline installeerimine ja ettevalmistus
M 4.282 Windows Serveri IIS põhikomponentide turvaline konfiguratsioon
M 4.284 Teenuste rakendamine
M 4.301 Juurdepääsu piiramine printeritele, koopiamasinatele ja multifunktsionaalsetele seadmetele
M 4.303 Võrgutoega dokumendiskännerite kasutamine
M 4.304z Printerite haldamine
M 4.306z Paroolisalvestusvahenditega ümberkäimine
M 4.307 Kataloogiteenuste turvaline konfigureerimine

M 4.313 Turvaliste domeenikontrollerite kasutuse võimaldamine
M 4.314 Domeenide ja domeenikontrollerite turvaliste poliitikaseadistuste loomine
M 4.316 Active Directory infrastruktuuri monitooring
M 4.317z Windowsi kataloogiteenuste turvaline migratsioon
M 4.318 Active Directory turvaliste haldusmeetodite rakendamine
M 4.319 VPNi lõppseadmete turvaline installeerimine
M 4.321 VPNi turvaline käitamine
M 4.323z Sünkroniseerimine turvapaikade ja muudatuste halduse raames
M 4.324 Automaatsete uuendusmehhanismide konfiguratsioon turvapaikade ja muudatuste haldamisel
M 4.325 Likvideerimisele kuuluvate failide kustutamine
M 4.328 Samba serveri turvaline aluskonfiguratsioon
M 4.330 Samba serveri turvaline installeerimine
M 4.332 Samba serveri pääsuõiguste turvaline konfiguratsioon
M 4.333 Winbindi turvaline konfigureerimine Samba keskkonnas
M 4.334 SMB Message Signing ja Samba
M 4.336 Hulgilitsentslepinguga Windowsi süsteemide aktiveerimine alates Windows Server 2008-st
M 4.337z BitLockeri Drive Encryption kasutamine
M 4.338 Windows 7 failide ja registri virtualiseerimise kasutamine
M 4.339 Vahetavate andmekandjate volitamata kasutamise tõkestamine Windows 7-s
M 4.340 Windows kasutajakonto haldamise (UAC) kasutamine
M 4.341 Tervikluse kaitse
M 4.342z Last Access ajatempli aktiveerimine
M 4.343z Hulgilitsentsilepinguga Windowsi süsteemide reaktiveerimine alates Windows Server 2008-st
M 4.344 Windows 7 ja Windows Server 2008 süsteemi seire
M 4.345z Kaitse soovimatu infoäravoolu eest
M 4.346 Virtuaalsete IT-süsteemide turvaline konfigureerimine
M 4.347z Virtuaalsete IT-süsteemide snapshot'ide desaktiveerimine
M 4.349 Virtuaalse taristu turvaline kasutamine
M 4.351 Tsooniedastuse turve
M 4.354 DNS-serveri seire
M 4.356 Rühmatarkvarasüsteemide turvaline installeerimine
M 4.359w Veebiserveri koostisosade ülevaade
M 4.360 Veebiserveri turvaline konfiguratsioon
M 4.362 Bluetoothi turvaline konfigureerimine
M 4.363 Bluetooth-seadmete turvaline käitamine
M 4.365z Terminaliserveri kasutamine graafilise tulemüürina
M 4.371 Mac OS X-ga töötavate klientsüsteemide konfigureerimine
M 4.372 FileVaulti kasutamine Mac OS X-s
M 4.375z Sandbox 'i funktsioonide kasutamine Mac OS X-s
M 4.377z Mac OS X digisignatuuride kontrollimine
M 4.383 OpenLDAP turvaline installimine
M 4.384 OpenLDAP turvaline konfiguratsioon
M 4.392 Autentimine veebirakendustes
M 4.393 Sisestuste- ja väljastuste põhjalik valideerimine veebirakendustes ja veebiteenustes
M 4.395 Tõrkekäsitlus veebirakendustes ja veebiteenustes

M 4.397 Veebirakenduste turvet puudutavate sündmuste logimine
M 4.398 Veebirakenduste turvaline konfiguratsioon
M 4.399 Andmete ja sisu kontrollitud lisamine veebirakendustesse
M 4.401 Konfidentsiaalsete andmete kaitse veebirakendustes
M 4.402 Juurdepääsukontroll veebirakendustes
M 4.403 Päringuvõltsingu (CSRF, XSRF, Session Riding) tõkestamine
M 4.404 Veebirakenduste turvalise loogika kavandamine
M 4.406z Clickjacking-rünnete tõkestamine
M 4.408w Windows Server 2008 uute turbefunktsioonide ülevaade
M 4.409w Windows Server 2008 soetamine
M 4.410z Võrgu juurdepääsukaitse kasutamine Windowsis
M 4.411z DirectAccessi turvaline kasutamine Windowsis
M 4.414w Windows Server 2008 Active Directory uuenduste ülevaade
M 4.415z Biomeetriliste autentimisvõimaluste turvaline kasutamine Windowsis
M 4.417 Paikade haldus WSUS-iga alates Windows Server 2008-st
M 4.418 Windows Server 2008 kasutamise planeerimine
M 4.419z Rakenduste juhtimine AppLockeriga alates Windows 7-st
M 4.420 Windows 7 tegevuskeskuse turvaline kasutamine
M 4.421 Windows PowerShelli turve
M 4.422z BitLocker To Go kasutamine alates Windows 7-st
M 4.423 Kodugrupi funktsiooni kasutamine Windows 7-s
M 4.424z Vanemate tarkvarade turvaline kasutamine alates Windows 7-st
M 4.425 Vaulti ja Cardspace'i funktsiooni kasutamine Windows 7-s
M 4.426 Lotus Notesi/Domino keskkonna arhiveerimine
M 4.431 Logimise jaoks oluliste andmete valik ja töötlemine
M 4.432 Serveriteenuste turvaline konfiguratsioon
M 4.433z Serveriteenuste turvaline konfiguratsioon
M 4.434 Eraldiseisvate seadmete kasutamine
M 4.435z Isekrüpteerivad kõvakettad
M 4.447 SAN-Fabricu tervikluse tagamine
M 4.449z Tsoonide kontseptsiooni juurutamine
M 4.450 Veebiteenuste andmeside turve
M 4.451w Veebiteenuste värsked standardid
M 4.452 Veebiteenuse seire
M 4.453z Pääsmikuteenuse (Security Token Service) kasutamine
M 4.454 Veebiteenuste kaitsmine keelatud kasutuse eest
M 4.455 Volitamine veebiteenustes
M 4.456 Autentimine veebiteenustes
M 4.457 Teenusetarbijate turvaline lahutamine veebirakendustes ja veebiteenustes
M 4.458 Veebiteenuste kasutuselevõtu planeerimine
M 4.459 Krüpteeringu kasutamine pilvteenustes
M 4.462z Sissejuhatus pilveteenuse kasutamisse
M 4.463 Rakenduse turvaline installeerimine
M 4.464 Turbe tagamine rakenduste igapäevatöös
M 4.465 Mobiil- ja nutitelefonide ning tahvel- ja pihuarvutite kasutuselt kõrvaldamine
M 4.466 Viirusetõrjeprogrammide kasutamine nutitelefonides ning tahvel- ja pihuarvutites
M 4.E1 ID-kaardi/PKI lahenduste turvaline seadistamine

M 4.E2 ID-kaardi/PKI lahenduste turvaline seadistamine
M 4.E3 ID-kaardi, digi-ID ja mobiil-ID ning nende sertifikaatide õigeaegne uuendamine
M 4.E4 Juurdepääsutõendiga määratud signeerimisressursi seire ja uuendamine
M 4.E5 Nõuded ID-kaardi/PKI lahendusi kasutavale turvalisele autentimisele
M 4.E6 Keeld anda digiallkirja autentimisvõtmepaari ja PIN1-koodi kasutades
M 5.1 Tarbetute liinide kõrvaldamine või lühistamine ja maandamine
M 5.2 Võrgu sobiv topoloogia
M 5.3 Sidetehniliselt sobivad kaablitüübid
M 5.4 Kaabelduse dokumenteerimine ja märgistus
M 5.8 Võrgu regulaarne turvakontroll
M 5.13 Võrgu ühendusaparatuuri õige kasutamine
M 5.17 NFSi turvamehhanismid
M 5.33 Kaughoolduse turve
M 5.34z Ühekordsed paroolid
M 5.35 UUCP turvamehhanismid
M 5.45 Veebibrauserite turvaline kasutamine
M 5.52 Sidearvutite turvanõuded
M 5.54 Meili ülekoormuse ja spämmi tõrje
M 5.56 Meiliserveri turvaline kasutamine
M 5.57 Rühmatarkvara/meiliklientide turvaline konfiguratsioon
M 5.60 Sobiva magistraalvõrgutehnika valimine
M 5.61 Sobiv füüsiline segmenteerimine
M 5.62z Sobiv loogiline segmenteerimine
M 5.63z GnuPG või PGP kasutamine
M 5.64z Secure Shell (SSH)
M 5.66z SSL-i/TLS-i kasutamine kliendis
M 5.67z Ajatempliteenuse kasutamine
M 5.68z Krüpteerimisprotseduuride kasutamine võrgusuhtluses
M 5.76w Sobivate tunneldusprotokollide kasutamine VPN-süsteemis
M 5.77z Alamvõrkude rajamine
M 5.87 Leping kolmandate poolte võrkudega ühendamise kohta
M 5.88 Lepingud andmevahetuse kohta kolmandate pooltega
M 5.89 Turvalise kanali konfigureerimine Windowsis
M 5.90 IPSec'i protokolli kasutamine Windowsi keskkonnas
M 5.91 Interneti-PC personaalse tulemüüri installeerimine
M 5.93 Veebibrauseri turve Internet-PC kasutamisel
M 5.94 Meilikliendi turve Internet-PC kasutamisel
M 5.95 E-kaubanduse turve Internet-PC kasutamisel
M 5.98 Kulukate sissehelistusnumbrite kasutamise tõkestamine
M 5.100 Exchange'i süsteemi siseneva ja väljuva side kaitse
M 5.109z Meiliskanneri kasutamine meiliserveril
M 5.110z Meili kaitse SPHINXi (S/MIME) abil
M 5.115z Veebiserveri integreerimine turvalüüsi koostisse
M 5.118z DNS-serveri integreerimine turvalüüsi koostisse
M 5.121 Turvaline side mobiilseadme ja töökoha vahel
M 5.122 Sülearvuti turvaline ühendamine kohtvõrguga
M 5.123 Võrgusuhtluse kaitse Windowsis
M 5.124 Võrgupääsu korraldus nõupidamis-, ürituse- ja koolitusruumides
M 5.125 SAP-süsteemi siseneva ja väljuva side kaitse

M 5.142 IT-kaabelduse vastuvõtmine
M 5.143 Võrgu dokumentatsiooni pidev edasikirjutamine ja revisjon
M 5.144 IT-kaabelduse demonteerimine
M 5.145 Turvaline CUPSi kasutamine
M 5.147 Turvalise side tagamine kataloogiteenuste abil
M 5.149 Turvaline välisvõrguühendus IPSec-i abil
M 5.150 Penetratsioonitestide läbiviimine
M 5.152 Info ja ressursside vahetamine võrdõigusteenuste (p2p) kaudu
M 5.153 Võrgu planeerimine virtuaalsete taristute jaoks
M 5.154 Virtuaalse taristu võrgu turvaline konfiguratsioon
M 5.155z Interneti kasutamise andmekaitseaspektid
M 5.156z Twitteri turvaline kasutamine
M 5.157z Sotsiaalvõrgustike turvaline kasutamine
M 5.158z Veebimälu turvaline kasutamine
M 5.159w Veebiserveri protokollide ja sidestandardite ülevaade
M 5.163 Piirav õiguste jaotus terminaliserveritel
M 5.173z Lühi-URL-ide või QR-koodide kasutamine
M 5.175z XML-lüüsi kasutamine
M 5.176 Nutitelefonide, tahvel- ja pihuarvutite turvaline ühendamine asutuse võrguga
M 5.E1 Sertifikaatide õigeaegne peatamine
M 5.E2 Varem antud digiallkirjade õigeaegne ülesigneerimine
M 6.1 Käideldavusnõuete inventuur
M 6.16z Kindlustus
M 6.20 Varukoopia andmekandjate õige ladustus
M 6.21 Kasutatava tarkvara varukoopia
M 6.23 Käitumisreeglid arvutiviiruste esinemisel
M 6.24 Rikkejärgse buutimismeedia olemasolu
M 6.27 BIOS-süsteemi turvaline värskendamine
M 6.32 Regulaarne andmevarundus
M 6.33 Andmevarunduskontseptsiooni loomine
M 6.34 Andmevarunduse mõjutegurite määratlemine
M 6.35 Andmevarunduseks vajalike protseduuride määratlemine
M 6.36 Minimaalse andmevarunduse kontseptsiooni määratlemine
M 6.37 Andmevarunduse dokumenteerimine
M 6.39 Faksitoodete tarnijate loend asendushangeteks
M 6.41 Andmete taastamise harjutamine
M 6.43z Liiasusega Windowsi serverid
M 6.52 Võrgu aktiivkomponentide konfiguratsiooniandmete regulaarne varundamine
M 6.54 Protseduurid võrgu tervikluse kao puhuks
M 6.56 Andmevarundus krüptoprotseduuride kasutamisel
M 6.58 Turvaintsidentide käsitluse haldussüsteemi rajamine
M 6.59 Turvaintsidentide käsitlemise eest vastutavate isikute määramine
M 6.60 Turvaintsidentide käsitlusprotseduurid ja teavitamiskanalid
M 6.61 Turvaintsidentide käsitluse eskalatsioonistrateegia
M 6.62z Prioriteetide kindlaksmääramine turvaintsidentide käsitlemiseks
M 6.64 Turvaintsidentide likvideerimine
M 6.65 Asjassepuutuvate isikute teavitamine turvaintsidentidest
M 6.66 Turvaintsidentide järelhindamine

M 6.67z Turvaintsidentide avastamismeetmete rakendamine
M 6.68 Turvaintsidentide käsitluse süsteemi tõhususe testimine
M 6.74z Avariiarhiiv
M 6.76 Avariiplaani koostamine Windowsi süsteemi tõrke puhuks
M 6.78 Andmete varundamine Windowsi klientsüsteemides
M 6.81 Novell eDirectory andmete varundamine
M 6.83 Väljasttellimise avariiplaan
M 6.84 Süsteemi- ja arhiiviandmete regulaarne varundamine
M 6.91 Marsruuterite ja kommutaatorite andmete varundus ja taaste
M 6.92 Marsruuterite ja kommutaatorite hädaolukorraks valmisoleku plaan
M 6.94 Turvalüüside hädaolukorraks valmisoleku plaan
M 6.96 Serveri avariiplaan
M 6.99 Windows Serverite tähtsate süsteemikomponentide regulaarne varundus
M 6.103z Primaarkaabelduse liiasus
M 6.104z Hoone kaabelduse liiasus
M 6.105 Printerite, koopiamasinate ja multifunktsionaalsete seadmete hädaolukorraks valmisoleku plaan
M 6.106z Kataloogiteenuse hädaolukorraks valmisoleku plaani koostamine
M 6.107 Kataloogiteenuste andmevarundus
M 6.109 Virtuaalse privaatvõrgu (VPN) hädaolukorraks valmisoleku plaan
M 6.110 Kehtivusala ja hädaolukorrahalduse strateegia määratlemine
M 6.111 Hädaolukorrahalduse ja juhtkonnapoolse koguvastutuse võtmise poliitika
M 6.112 Sobiva hädaolukorrahalduse organisatsioonilise struktuuri rajamine
M 6.113 Hädaolukorrahalduse jaoks sobivate ressursside eraldamine
M 6.114 Hädaolukorraks valmisoleku kontseptsiooni koostamine
M 6.115 Kaastöötajate integreerimine hädaolukorra haldusprotsessi
M 6.116 Hädaolukorra halduse integreerimine üleorganisatsioonilistesse protseduuridesse ja protsessidesse
M 6.117 Testid ja valmisoleku harjutused
M 6.118 Hädaolukorra meetmete kontroll ja käigushoidmine
M 6.119 Hädaolukorra haldusprotsessi dokumentatsioon
M 6.120 Hädaolukorraks valmisoleku süsteemi kontroll ja juhtimine
M 6.121 Suuniste väljatöötamine turvaintsidentide käsitlemiseks
M 6.122 Turvaintsidendi defineerimine
M 6.123z Ekspertmeeskonna moodustamine turvaintsidentide käsitlemiseks
M 6.124z Turvaintsidentide käitlemise liideste kindlaksmääramine tõrgete ja vigade kõrvaldamiseks
M 6.125 Tsentraalse kontaktkoha sisseseadmine turvaintsidentide registreerimiseks
M 6.126w Sissejuhatus arvutipõhisesse kohtulikku juurdlusesse
M 6.127z Tõendite varundsusmeetmete kindlaksmääramine seoses turvaintsidendiga
M 6.128z Koolitus tõendusmaterjalide varundamise alal
M 6.129 Teenustoe töötajate koolitamine turvaintsidentide käsitlemise alal
M 6.130 Turvaintsidentide äratundmine ja mõistmine
M 6.131 Turvaintsidentide kvalifitseerimine ja hindamine
M 6.132 Turvaintsidentide mõju tõkestamine
M 6.133 Töökeskkonna taastamine pärast turvaintsidente
M 6.134 Turvaintsidentide dokumenteerimine
M 6.135 Samba serveri tähtsate süsteemikomponentide regulaarne varundamine

M 6.136 Hädaolukorraks valmisoleku plaani koostamine Samba serveri avarii puhuks
M 6.138 Hädaolukorraks valmisoleku plaani koostamine virtualiseerimiskomponentide tõrke puhuks
M 6.139 DNS-serveri avariiplaani koostamine
M 6.140 Hädaolukorra plaani koostamine rühmatarkvarasüsteemide avarii puhuks
M 6.141 Interneti kasutamise asendusprotseduurid
M 6.142z Redundantsete (ressurssi osaliselt või täielikult dubleerivate) terminaliserverite kasutamine
M 6.145 Kodukeskjaama (PBX) hädaolukorraks valmisolek
M 6.149 Andmevarundus Exchange'is
M 6.154 Veebiteenuste hädaolukordade haldamine
M 6.155 Pilvteenuse hädaolukorra kontseptsiooni koostamine
M 6.156 Organisatsioonisiseste andmevarunduste tegemine
M 6.157z Rakenduste liiasuse kontseptsiooni koostamine
M 6.158 Ettevalmistumine rakenduste hädaolukorraks
M 6.159 Nutitelefonide ning tahvel- ja pihuarvutite kaotuste ja varguste ennetamine
HG.1 Lisanõuded juhtmestuse kohandamisele
HG.6 Arvuti paroolkaitse rangemad reeglid
HG.14 Lisanõuded hädaolukorrajärgsele taasteplaanile
HG.19 Lisanõuded andmetaaste harjutamisele
HG.20 Taustauuring personali palkamisel
HG.23 Kahe erineva tootja kahjurvara- ja ründetuvastusprogrammi kasutamine
HG.28 Kõrge turbetaseme serveri kettatäitumise kaugindikatsioon
HG.33 Meiliaadresside asenduskorra regulaarseire
HG.34 Sülearvutite kasutuse regulaarseire
HG.37 Tarkvara tervikluskontroll igal installeerimisel
HG.38 Turvapaikade paigaldatuse regulaarseire
HG.39 Lisanõuded tarkvara vastuvõtuprotseduuridele
HG.40 CERT-EE teavitamine välismõjuga turvaintsidendist
HG.54 Regulaarse turvaauditi kohustus
HG.56 Lisanõuded muudatuste haldusele
HG.57 Muudatuste haldusinstrumentide pääsuõiguste määramine
HG.58 Lisanõuded turvakoolitusele
HG.59 Sagedasem turvameetmete läbivaatus
HG.60 Lisanõuded automaatsete uuendusmehhanismide konfigureerimisele
HG.62 Lisanõuded nõupidamisruumide võrguühendusele
HG.65 Mitmekordse nurjunud logimise automaatteavitus
HG.80z Pin-pad 'i kasutamine
HG.81 Krüptograafilisi detaile peitva vaheteegi kasutamine
HK.1 Varu-elektrigeneraatori nõue
HK.6 Edastmiseks genereeritud andmete kahes eksemplaris varukopeerimine
HK.7 Kahes eksemplaris varukopeerimine kodutööl
HK.8 Andmebaasi tervikliku varundamise nõue
HK.9 Varusidekanali nõue
HK.10 Lisanõuded personali asendamisele
HK.11 Serveriruumide ja kaitsekappide temperatuuriseire
HK.12 Arhiveerimisel kasutatavate andmekandjate taustauuring
HK.13 Arhiveerimisel kasutatavate andmekandjate regulaarkontroll

HK.14 Arhiivketta salvestusressursside kaugindikatsioon
HK.15 Lisanõuded arhiveerimisprotsessi auditeerimisele
HK.20 SAP'i klasterlahenduse kasutamine
HK.26 IP-kõne kesksеadmete dubleeritus
HK.29 Kaabelduse minimaalsuse nõue andmearhiivides
HK.30 Serveriruumi ja andmearhiivi eraldatuse nõue
HK.31 Kõrgkäideldavuse lisanõuded kaabelduse paigaldusele
HK.36 Käideldavusnõuete täidetuse regulaarseire
HK.37 Usaldusele toetuv deponeerimine (Escrow)
HK.38 Krüptograafiliste algoritmide kasutuskataloog
HS.11 Lisanõuded andmekandjate turvalisele kasutamisele
HS.17 Lisanõuded külastajate saatmisele
HS.34 Lisanõuded kolimise turbele
HS.39 Lisanõuded andmebaaside krüpteerimisele
HS.40 Juhtmeta klaviatuuri kasutuskeeld
HS.48 Kõrgkonfidentsiaalsuse lisanõuded IT kaabelduse paigaldusele
HS.51 Lisanõuded tundlike ressursside hävitamisele
HS.56 Paroolide taastamise/uuendamise lisanõuded
HS.60 Juuresolekunõue kõrgkonfidentsiaalsete dokumentide paljundamisel
HS.74 Piirangud IT süsteemide virtualiseerimisele
HS.75 Lisanõuded infovahetuse reguleerimisele
HS.76 Mobiilsete andmekandjate võimalik vältimine
HS.77 Kiirgusturve
HT.2 Süsteemi ja võrgu pääsuõiguste perioodiline seire
HT.4 Sagedasem tarkvara inventuur
HT.6 Esemeliste pääsuvahendite halduse seire
HT.7 Kasutajate ja nende profiilide perioodiline seire
HT.10 Andmebaasi kannete krüptoaheldamine
HT.11 Infoturbe regulaararuanded juhtkonnale
HT.13 Tulemüüri konfiguratsioonimuudatuste krüptoaheldamine
HT.14 Süsteemi tegevuslogide krüptoaheldamine
HT.23 Muudatuste eelnev turvajuhi poolne kinnitamine
HT.26 Serveriruumi ja andmearhiivi külastajate logiraamatu pidamine
HT.29 Kombineeritud autentimise nõue
HT.31 Arhiveerimisel kasutatavate andmekandjate regulaarkontroll
HT.34 Digiallkirja kasutamine
HT.47 Lisanõuded hooldustöödele ja remondile
HT.48 Lisanõuded krüptolahenduste võtmehaldusele
HT.49 Lisanõuded arhiveeritud andmete krüptoatribuutide regenereerimisele
HT.52 Lisanõuded krüptovahenditele
HT.53 Lisanõuded paroolisalvestusvahenditele
HT.54 Lisanõuded turvafunktsioonide rakendamisel
HT.55 Värske tarkvara kasutuskeeld
HT.60 Lisanõuded tarbetute liinide kõrvaldamisele
HT.63 Sülearvutite krüpteerimine
HT.65 Lisanõuded teisaldatavate andmekandjate kasutusele
HT.67 Pihuarvutite krüpteerimine

ISKE kataloogid

B1: Üldkomponendid
B 1.0 Infoturbe haldus
B 1.1 Organisatsioon
B 1.2 Personal
B 1.3 Hädaolukorraks valmisoleku kontseptsioon
B 1.4 Andmevarunduspoliitika
B 1.5 Andmekaitse
B 1.6 Viirusetõrje kontseptsioon
B 1.7 Krüptokontseptsioon
B 1.8 Turvaintsidentide käsitlus
B 1.9 Riist- ja tarkvara haldus
B 1.10 Tüüptarkvara
B 1.11 Väljasttellimine (Outsourcing)
B 1.12 Arhiveerimine
B 1.13 Infoturbe teadlikkus ja -koolitus
B 1.14 Turvapaikade ja muudatuste haldus
B 1.15 Andmete kustutamine ja hävitamine
B 1.16 Nõuete haldus
B 1.17 Pilvteenuse kasutamine
B 1.18 Identiteedi- ja volituste haldus

B2 Infrastruktuur
B 2.1 Hooned
B 2.2 Elektrotehniline kaabeldus
B 2.3 Bürooruum
B 2.4 Serveriruum
B 2.5 Andmekandjate arhiiv
B 2.6 Tehnilise infrastruktuuri ruum
B 2.7 Kaitsekapid
B 2.8 Kaugtöökoht kodus
B 2.9 Arvutuskeskus
B 2.10 Mobiilne töökoht
B 2.11 Nõupidamis-, üritus- ja koolitusruumid
B 2.12 IT-kaabeldus

B3 IT-süsteemid
B 3.101 Server
B 3.102 Server Unixi all
B 3.107 Suurarvutid S/390 ja zSeries
B 3.108 Windows Server 2003
B 3.109 Windows Server 2008
B 3.201 Klient
B 3.202 Autonoomne IT-süsteem
B 3.203 Sülearvuti
B 3.204 Klient Unixi all
B 3.208 Interneti-PC
B 3.209 Klient Windows XP all
B 3.210 Klient Windows all
B 3.211 Mac OS X-ga töötav klientsüsteem
B 3.212 Windows 7-ga töötav klientsüsteem
B 3.213 Klient Windows 8 keskkonnas
B 3.301 Turvalüüs (tulemüür)
B 3.302 Marsruuterid ja kommutaatorid
B 3.303 Salvestisüsteemid ja salvestivõrgud
B 3.304 Virtualiseerimine
B 3.305 Terminaliserver
B 3.401 Kodukeskjaam (PBX)
B 3.402 Faks
B 3.404 Mobiiltelefon
B 3.405 Nutitelefonid, tahvel- ja pihuarvutid
B 3.406 Printerid, koopiamasinad ja multifunktsionaalsed seadmed
B 3.407 Integreeritud süsteem

B4 Võrgud
B 4.1 Heterogeensed võrgud
B 4.2 Võrgu- ja süsteemihaldus
B 4.3 Modem
B 4.4 Virtuaalne privaatvõrk (VPN)
B 4.5 IT-süsteemi kohtvõrguühendus ISDN kaudu
B 4.6 Traadita kohtvõrgud
B 4.7 IP-kõne (VOIP)
B 4.8 Bluetooth

B5 Rakendused
B 5.2 Andmekandjatel toimuv andmevahetus
B 5.3 Rühmatarkvara
B 5.4 Veebiserver
B 5.5 Lotus Notes/Domino
B 5.6 Faksiserver
B 5.7 Andmebaasid
B 5.8 Kaugtöö
B 5.9 Novell eDirectory
B 5.12 Microsoft Exchange / Outlook
B 5.13 SAP süsteem
B 5.14 Mobiilsed andmekandjad
B 5.15 Üldine kataloogiteenus
B 5.16 Active Directory
B 5.17 Samba
B 5.18 DNS-server
B 5.19 Interneti kasutamine
B 5.20 OpenLDAP
B 5.21 Veebirakendused
B 5.22 Logimine
B 5.24 Veebiteenused
B 5.25 Rakendused
B 5.26 Teenustele suunatud struktuur
B 5.27 Tarkvaraarendus
B 5.E2 ID-kaart/PKI

B1: Üldkomponendid

Moodulite nimekiri

B 1.0 Infoturbe haldus

Tänapäeval on andmete turvaline töötlemine peaaegu kõigi ettevõtete ja asutuste jaoks eksistentsiaalse tähtsusega. Seejuures võivad andmed olla salvestatud nii paberile, arvutitesse kui ka töötajate mälusse. Andmete kaitseks ei piisa ainult tehniliste turvameetmete rakendamisest. Nõuetele vastavat infoturbe taset on võimalik saavutada ja säilitada vaid kõigi asjaosaliste plaanipärase ja organiseeritud tegevusega. Turvameetmete otstarbekohase rakendamise ning efektiivsuse kontrollimise eelduseks on süstemaatiline tegutsemisviis. Seda planeerimis-, suunamis- ja kontrollifunktsiooni nimetatakse infoturbe halduseks või ka IT-turbe halduseks.

Mõiste infoturve on laialdasem kui IT-turve ning leiab seetõttu üha ulatuslikumat kasutamist. Kuna aga mõiste IT-turve on kasutusel nii käesolevas kui ka teistes väljaannetes, kasutatakse seda ka alljärgnevalt.

Hästi funktsioneeriv IT-turbe haldus tuleb iga asutuse olemasolevatesse halldusstruktuuridesse sisse viia. Seetõttu ei ole igale asutusele vahetult rakendatava IT-turbe halduse organisatsioonilise struktuuri etteandmine praktiliselt võimalik. Pigem osutub tihti vajalikuks selle kohandamine vastavalt olemasolevatele spetsiifilistele tingimustele.

Käesoleva mooduli ülesandeks on näidata, kuidas korraldada hästi funktsioneerivat IT-turbe haldust ning kuidas seda jooksva töö käigus edasi arendada. Moodul kirjeldab süstemaatiliseks infoturbe protsessiks vajalikke samme ning annab juhiseid ulatusliku infoturbe kontseptsiooni väljatöötamiseks. Moodul põhineb BSI-standardil 100-1 Infoturbe haldussüsteemid ja BSI-standardil 100-2 Infosüsteemide etalonturbe rakendusjuhend ning teeb nende põhjal kokkuvõtte tähtsamatest infoturbe haldust puudutavatest aspektidest.

Ohud

Ohud infoturbe halduse valdkonnas võivad olla mitmesugust laadi. Paljude ohtude asemel käsitletakse käesolevas moodulis alljärgnevaid tüüpilisi ohtusid:

Organisatsioonilised puudused:

- G 2.66 Puudulik infoturbehaldus
- G 2.105 Õigusaktide ja lepingute sätete rikkumine
- G 2.106 Turbeintsidentidest tingitud häiringud tööprotsessides
- G 2.107 Puudulikust infoturbehaldusest tingitud ressursside ebaökonoomne kasutamine

Soovitatavad meetmed

Vaadeldava IT-süsteemi turvalisuse tagamiseks tuleb lisaks käesolevale moodulile rakendada veel teisigi mooduleid vastavalt infosüsteemide etalonturbe rakendusjuhendi modelleerimise tulemustele.

Infoturbe halduse käigus on vaja rakendada terve rida meetmeid, alustades sobivate organisatsiooniliste struktuuride ülesehitusega ning lõpetades regulaarse auditiga. Alljärgnevalt tutvustatakse etappe, mis selleks on vajalik läbida, ning meetmeid, millele vastavate etappide läbimisel tuleks tähelepanu pöörata.

Üheks tähtsaks eelduseks vajaliku turvataseme saavutamiseks on asjaolu, et juhtkond toetaks turvaeesmärkide saavutamist ning oleks teadlik oma vastutusest infoturbe tagamisel. Juhtkonna ülesandeks on infoturbe protsessi käivitada, juhtida ja kontrollida, et see realiseeruks asutuse kõikides valdkondades. (vt M 2.336 Koguvastutus infoturbe eest juhtkonna tasemel).

Järgmisena tuleb kehtestada pidev infoturbe protsess ning määrata kindlaks konkreetsele asutusele sobiv infoturbe strateegia (vt M 2.335 Infoturbe eesmärkide ja strateegia kehtestamine). Juhtkonna ülesandeks on seejuures, nagu ka kõikide teiste turvaprobleemide lahendamisel, peavastutaja määramine. Peavastutaja ülesandeks on infoturbeks sobiva organisatsioonilise struktuuri ülesehitamine ja säilitamine. (vt M 2.193 Infoturbeks sobiva organisatsioonilise struktuuri rajamine). Üheks esimeseks ettevõtmiseks peaks olema infoturbepoliitika väljatöötamine (vt M 2.192 Infoturbepoliitika koostamine).

Infoturve peab olema sisse viidud asutuse kõikidesse valdkondadesse (vt M 2.337 Infoturbe integreerimine üleorganisatsioonilistesse tegevustesse ja protsessidesse). Selle hulka kuulub lisaks infoturbe kontseptsiooni koostamisele (vt M 2.195 Infoturbe kontseptsiooni loomine ja M 2.197 Töötajate kaasamine turbeprotsessi) ning sihtrühmakohase infoturbepoliitika väljatöötamine (vt M 2.338 Sihtrühmakohase infoturbepoliitika koostamine).

Alljärgnevalt tutvustatakse meetmete kogumit rakendamiseks valdkonnas "Infoturbe haldus".

Planeerimine ja kontseptsioon

- (L) M 2.192 Infoturbepoliitika koostamine
- (L) M 2.335 Infoturbe eesmärkide ja strateegia kehtestamine
- (M) M 2.336 Koguvastutus infoturbe eest juhtkonna tasemel

Rakendamine

- (L) M 2.193 Infoturbeks sobiva organisatsioonilise struktuuri rajamine

- (L) M 2.195 Infoturbe kontseptsiooni loomine
- (L) M 2.197 Töötajate kaasamine turbeprotsessi
- (M) M 2.337 Infoturbe integreerimine üleorganisatsioonilistesse tegevustesse ja protsessidesse
- (M) M 2.338z Sihtrühmakohase infoturbepoliitika koostamine
- (M) M 2.339z Ressursside ökonoomne kasutamine infoturbeks
- (L) M 2.475 Lepingu koostamine väljast tellitava infoturbespetsialistiga

Kasutamine

- (M) M 2.217 Teabe, rakenduste ja süsteemide hoolikas liigitamine ja käitlus
- (L) M 2.200 Infoturbearuanded juhtkonnale ja hinnangud infoturbele
- (L) M 2.201 Infoturbe protsessi dokumenteerimine

Valmisolek hädaolukorraks

- (M) M 6.16z Kindlustus

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele kohustuslikud üldmeetmed Kohustuslikud üldmeetmed

- HG.54 Regulaarse turvaauditi kohustus

Teabe käideldavus (K)

-

Teabe terviklus (T)

- HT.11 Infoturbe regulaararuanded juhtkonnale
- HT.23 Muudatuste eelnev turvajuhi poolne kinnitamine
- HT.29 Kombineeritud autentimise nõue

Teabe konfidentsiaalsus (S)

-

B 1.1 Organisatsioon

Käesolevas moodulis tutvustatakse üldiseid ja tähtsamaid organisatsiooni valdkonnas rakendatavaid meetmeid, mis on organisatsiooniliste standardmeetmetena vajalikud minimaalse turvataseme saavutamiseks. Spetsiaalseid organisatsioonilisi meetmeid, mis on otseses seoses teiste meetmetega (nt. LAN süsteemi haldamine), käsitletakse vastavates moodulites. Infotehniliste komponentide haldamisele (riistvara või tarkvara) suunatud standardturvameetmetest annab ülevaate moodul B 1.9 Riist- ja tarkvara haldus.

Ohud

Käesolev moodul annab ülevaate alljärgnevatest infoturbega seotud tüüpilistest ohtudest.
Organisatsioonilised puudused:

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.2 Reeglite puudulik tundmine
- G 2.3 Puuduvad, puudulikud või ühildumatud ressursid
- G 2.5 Hoolduse puudumine või puudulikkus
- G 2.6 Volitamata pääs ruumidesse
- G 2.7 Õiguste volitamata kasutamine
- G 2.8 Ressursside kontrollimatu kasutamine

Inimvead:

- G 3.1 Andmete konfidentsiaalsuse või tervikluse kadu kasutaja vea tõttu
- G 3.6 Koristajad jm väljastpoolt tellitud töötajad

Ründed:

- G 5.1 IT-seadmete või -tarvikute manipuleerimine ja hävitamine
- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.3 Volitamatu sisenemine hoonesse
- G 5.4 Vargus
- G 5.5 Vandalism
- G 5.6 Füüsiline rünne
- G 5.16 Ohud hoolde- ja haldustööde ajal
- G 5.68 Volitamata juurdepääs aktiivsetele võrgukomponentidele
- G 5.102 Sabotaaž

Soovitatavad meetmed

Vaadeldava IT-süsteemi turvalisuse tagamiseks tuleb lisaks käesolevale moodulile rakendada veel teisigi mooduleid vastavalt infosüsteemide etalonturbe rakendusjuhendi modelleerimise tulemustele.
Minimaalse turvataseme saavutamine asutuses on võimalik vaid juhul, kui

infoturbe tähtsamate reeglite täitmine tehakse kohustuslikuks. Seejuures on vajalik rakendada terve rida meetmeid, alustades üksikute objektide eest vastutavate isikute kindlaksmääramisest (nt andmed, tööprotsessid, rakendused, IT-komponendid), millele järgneb vastavate organisatsiooniliste tegutsemisjuhiste väljatöötamine, ning lõpetades kaitsmist vajavate ressurssidega käitlemisega. Alljärgnevalt tutvustatakse etappe, mis tuleb läbida katkematu infoturbeprotsessi tagamiseks, ning meetmeid, millele vastavate etappide läbimisel tuleks tähelepanu pöörata.

Planeerimine ja kontseptsioon

Turvaeesmärkidest ja -suunistest tulenevate protsesside algatamiseks ja realiseerimiseks on vajalik kindlaks määrata organisatsioonilised ja personaalsed kohustused (vt M 2.40 Töötajate esinduse õigeaegne kaasamine). Erinevad organisatsioonilised tasandid ning nendel tasanditel tegevad töötajad vajavad konkreetseid tegevusjuhiseid ja vastutuspiiride kindlaksmääramist neid puudutavate protsesside korraldamiseks (vt M 2.225 Teabe, rakenduste ja IT-komponentide alaste vastutuste kinnistamine).

Strateegiliste kaalutluste rakendamine ettevõttes või asutuses tuleb tegevuskavas üksikasjalikult määratleda.

Vajalike ressursside kasutamine tuleb viia vastavusse ülesannete täitmise ja turvanõuetega ning ressursside halduse kaudu (vt M 2.2 Ressursside haldamine) dokumenteerida. Dokumentatsioon peab olema täielik ning seda tuleb vastavate protsesside abil alati kaasaegsena hoida.

Hästi funktsioneeriva, häiretele adekvaatselt reageeriva IT-infrastruktuuri eelduseks on eeskirjade olemasolu tagavaraosade saamiseks ning remondi- ja hooldustööde korraldamiseks (vt M 2.4 Hooldus- ja remonditööde reeglid). Hoolduslepingutes on kohustuslik reguleerida tähtajaliselt ja sisuliselt üksikute IT-süsteemide (või gruppide) hooldus, samuti nõutavad juurdepääsud (remote, on-site) ning hoolduse eest vastutava personali turvanõuetele vastavad reageerimisajad.

Kohustuste jagamine ja selleks vajalikud funktsioonid (vt M 2.5 Vastutuse ja ülesannete jaotamine) tuleb struktureerida nii, et operatiivsed kohustused ja kontrollifunktsioon oleks jagatud erinevate inimest vahel, selleks et minimeerida või täielikult kõrvaldada asjaosaliste huvikonfliktid.

Kasutamine

Väljatöötatud kontseptsioonide põhjal formuleeritakse konkreetsed tegevusjuhised ning võetakse need kohustuslikena tegevuse aluseks. Töötajaid puudutavate reeglite koostamisel peab vaatluse alla võtma töötaja kogu teenistuskäigu ettevõttes, alustades tema tööleasumisest ja lõpetades töölt lahkumisega. “ Need-to-know ” printsiibi ja neljasilma printsiibi kasutamisega tuleb tagada, et volituste andmine erinevatel tasanditel (nt sissepääs ruumidesse, juurdepääs IT-süsteemidele) toimuks eesmärgikindlalt ja otstarbekohaselt (vt M 2.6 Sissepääsuõiguste andmine ja M 2.7 Süsteemi ja võrgu pääsuõiguste andmine).

Antud volitused tuleb dokumenteerida ning nende toetamiseks tuleb kasutada erinevaid meetodeid, nt kontrollitud ja tõestatav võtmete väljaandmine volitatutele (vt M 2.14 Võtmete (ja kaartide) haldus), juurdepääsu autentimine, juurdepääsukontroll spetsiaalselt kaitstud valdkondadele ning kontroll välispersonali tegevuse üle (vt M 2.16 Välispersonali ja külastajate valve ja saatmine). Töötajate ja töötajate gruppidele kindlate rollide kehtestamine kergendab volituste haldamist (vt

M 2.8 IT-rakendustele ja andmetele pääsuõiguste andmine). Kui turvapoliitikat rikutakse teadlikult või mitteteadlikult, peavad sellele järgnevad teavitus- ja eskalatsiooniprotsessid töötajatele teada olema, et rikkumisele saaks järgneda sihikindel reaktsioon (vt M 2.39 Vastutus turvapoliitika rikkumise eest).

Väljavahetamine

Andmekandjad, ressursid ja tooted, mis vajavad spetsiaalset kaitset, tuleb hävitada nii, et nende kasutamisest või sisust ei jääks mingeid jälgi (vt M 2.13 Tundlike ressursside jäljetu hävitamine). Selleks on vaja kehtestada vastavad reeglid, mida tuleb vajadusel laiendada ka välisfirmadele. Järgida tuleb vastavaid andmekaitse eeskirju.

Alljärgnevalt tutvustatakse meetmete kogumit, mida tuleb rakendada valdkonnas "Organisatsioon".

Planeerimine ja kontseptsioon

- (L) M 2.1 IT kasutajate vastutuse ja reeglite kehtestamine
- (L) M 2.2 Ressursside haldamine
- (L) M 2.4 Hooldus- ja remonditööde reeglid
- (L) M 2.5 Vastutuse ja ülesannete jaotamine
- (M) M 2.40z Töötajate esinduse õigeaegne kaasamine
- (L) M 2.225 Teabe, rakenduste ja IT-komponentide alaste vastutuste kinnistamine
- (L) M 2.393 Infovahetuse reguleerimine

Kasutamine

- (L) M 2.6 Sissepääsuõiguste andmine
- (L) M 2.7 Süsteemi ja võrgu pääsuõiguste andmine
- (L) M 2.8 IT-rakendustele ja andmetele pääsuõiguste andmine
- (L) M 2.16 Välispersonali ja külastajate valve ja saatmine
- (L) M 2.18z Kontrollringkäigud
- (L) M 2.37 Korrastatud töölaud
- (L) M 2.39 Vastutus turvapoliitika rikkumise eest
- (M) M 2.177z Kolimise turve
- (M) M 5.33 Kaughoolduse turve

Väljavahetamine

- (M) M 2.13 Tundlike ressursside jäljetu hävitamine

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.3 Tõrgete kaugindikatsiooni vastuvõtmiskohustus
- HG.20 Taustauuring personali palkamisel
- HG.21 Personali perioodiline turva-alane atasteerimine
- HG.38 Turvapaikade paigaldatuse regulaarseire
- HG.59 Sagedasem turvameetmete läbivaatus

Teabe käideldavus (K)

-

Teabe terviklus (T)

- HT.2 Süsteemi ja võrgu pääsuõiguste perioodiline seire
- HT.3 Rakenduste ja andmete pääsuõiguste perioodiline seire
- HT.4 Sagedasem tarkvara inventuur
- HT.6 Esemeliste pääsuvahendite halduse seire
- HT.7 Kasutajate ja nende profiilide perioodiline seire
- HT.26 Serveriruumi ja andmearhiivi külastajate logiraamatu pidamine
- HT.47 Lisanõuded hooldustöödele ja remondile

Teabe konfidentsiaalsus (S)

- HS.17 Lisanõuded külastajate saatmisele
- HS.34 Lisanõuded kolimise turbele
- HS.51 Lisanõuded tundlike ressursside hävitamisele
- HS.60 Juuresolekunõue kõrgkonfidentsiaalsete dokumentide paljundamisel
- HS.75 Lisanõuded infovahetuse reguleerimisele

B 1.2 Personal

Käesolevas moodulis selgitatakse tähtsamaid infosüsteemide turvameetmeid, mis vastavalt standardile on ette nähtud rakendamiseks personali puudutavas valdkonnas. Alates töötajate töölevõtmisest kuni nende lahkumiseni asutusest on vaja rakendada hulgaliselt meetmeid. Personaalseid soovitusi, mis on seotud ühe kindla funktsiooniga, nagu nt LAN süsteemi administraatori määramine, käsitletakse IT-spetsiifilistes moodulites.

Ohud

Käesolev moodul annab ülevaate alljärgnevatest infoturbega seotud tüüpilistest ohtudest.

Vääramatu jõud:

- G 1.1 Personali väljalangemine
- G 1.2 IT-süsteemi avarii

Organisatsioonilised puudused:

- G 2.2 Reeglite puudulik tundmine
- G 2.7 Õiguste volitamata kasutamine

Inimvead:

- G 3. 1 Andmete konfidentsiaalsuse või tervikluse kadu kasutaja vea tõttu
- G 3.2 Seadme või andmete hävitamine hooletuse tõttu
- G 3.3 Hooletus turvameetmete suhtes
- G 3.8 IT-süsteemi väär kasutamine
- G 3.9 IT-süsteemi väär haldus
- G 3.36 Sündmuste väär tõlgendamine
- G 3.37 Tulemusteta otsingud
- G 3.43 Puudulik paroolihooldus
- G 3.44 Teabe hooletu kasutamine
- G 3.77 Infoturbe vähene aktsepteerimine

Ründed:

- G 5.1 IT-seadmete või -tarvikute manipuleerimine ja hävitamine
- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.20 Administraatori õiguste väärkasutus
- G 5.23 Viirused
- G 5.42 Inimestega manipuleerimine (Social Engineering)
- G 5.80 Pettemeilid
- G 5.104 Infoluure

Soovitatavad meetmed

Vaadeldava IT-süsteemi turvalisuse tagamiseks tuleb lisaks käesolevale moodulile rakendada veel teisigi mooduleid vastavalt infosüsteemide etalonturbe rakendusjuhendi modelleerimise tulemustele.

Ettevõtte või asutuse personaliga töötamiseks on vaja rakendada terve rida abinõusid, mille hulka kuuluvad muu hulgas eeskirjad uute töötajate tutvustamiseks tööga, IT alase väljaõppe korraldamiseks ning töötajate töölt lahkumiseks. Alljärgnevalt tutvustatakse etappe, mis on seejuures vaja läbida, ning meetmeid, millele teatud etappidel tuleb tähelepanu pöörata.

Rakendamine

Ettevõte või asutus peab tutvustama uutele töötajatele kehtivaid eeskirju ja tegevusjuhiseid (vt M 3.1 Uute töötajate esmane juhendamine ja väljaõpe), et neid kiiresti käimasolevatesse protsessidesse integreerida. Samuti on hädavajalik kõikide töötajate informeerimine eeskirjades tehtavate muudatuste ning nende spetsiifiliste mõjude kohta protsessile või üksikule töötajale. Eriti turvakriitilises töökeskkonnas on soovitatav teha eeskirjade täitmine töötajatele kohustuslikuks ning lasta kontrollida töötajate usaldusväärsust (vt M 3.33 Personali taustakontroll). Erilist tähtsust tuleb seejuures omistada erifunktsioone ja -volitusi omavate isikute usaldusväärsusele (vt M 3.10 Usaldusväärse administraatori ja tema asetäitja valimine).

Kasutamine

Kõikide töötajate motiveeritust, valmidust aktsepteerida infoturvet tegevusprotsessides ning seda ainuvastutavalt ellu viia tuleb motiveerida ja arendada vastavate koolituste korraldamise (vt M 3.5 Turvameetmete koolitus) ja detailsete rakendusalaste teadmiste andmise kaudu (vt M 3.4 Väljaõpe enne programmi tegelikku kasutamist) erialasel tasemel. Seejuures on erilise tähtsusega hooldus- ja halduspersonali väljaõpe (vt M 3.11 Hooldus- ja halduspersonali väljaõpe), kuna nimetatud isikutel on tulenevalt nende laialdastest õigustest infotehnoloogiaga ümberkäimisel väga suur vastutus.

Tähtsate protsesside pideva käideldavuse tagamiseks tuleb hoolitseda, et võtmepositsioonid oleksid alati täidetud (vt M 3.3 Asendamise korraldamine).

Suhtlusprobleemid, isiklikud probleemid, asutuse halb tööõhkkond, laiaulatuslikud organisatoorsed muudatused ja muud taolised faktorid võivad viia võimalike turvariskideni (vt M 3.7 Kontaktisik isiklikes küsimustes).

Funktsioonide muutumine

Töötajate suhtes, kes asutusest lahkuvad või kelle töökohustused muutuvad, tuleb kehtivaid reegleid rakendada kõrgendatud tähelepanuga (vt M 3.6 Reguleeritud protseduur töösuhete lõpetamiseks). Töötajate etteteatamisajata töölt lahkumine võib olla seotud riskiga, et võetakse volitamata kaasa konfidentsiaalseid andmeid või märgatakse alles tagantjärele, et on toimunud sihilik manipuleerimine IT-objektide ja andmetega.

Alljärgnevalt tutvustatakse meetmete kogumit, mida tuleb rakendada valdkonnas “Personal”.

Planeerimine ja kontseptsioon

- (M) M 2.226 Asutusevälise personali kasutamise protseduurid
- (L) M 3.51z Personali rakendamise ja kvalifitseerimise kontseptsioon
- (L) M 3.83z Personaliga seotud turbefaktorite analüüs

Soetamine

- (L) M 3.50z Personali valimine

Rakendamine

- (L) M 3.1 Uute töötajate esmane juhendamine ja väljaõpe
- (L) M 3.10 Usaldusväärse administraatori ja tema asetäitja valimine
- (M) M 3.33z Personali taustakontroll
- (M) M 3.55 Konfidentsiaalsuslepingud

Kasutamine

- (L) M 3.3 Asendamise korraldamine
- (L) M 3.4 Väljaõpe enne programmi tegelikku kasutamist
- (M) M 3.5 Turvameetmete koolitus
- (M) M 3.7z Kontaktisik isiklikes küsimustes
- (L) M 3.8z Tööõhkkonda kahjustavate tegurite vältimine
- (M) M 3.11 Hooldus- ja halduspersonali väljaõpe

Väljavahetamine

- (L) M 3.6 Reguleeritud protseduur töösuhete lõpetamiseks

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.3 Tõrgete kaugindikatsiooni vastuvõtmiskohustus
- HG.20 Taustauuring personali palkamisel

- HG.21 Personali perioodiline turva-alane atasteerimine

Teabe käideldavus (K)

- HK.10 Lisanõuded personali asendamisele

Teabe terviklus (T)
-
Teabe konfidentsiaalsus (S)

- S.60 Juuresolekunõue kõrgkonfidentsiaalsete dokumentide paljundamisel

B 1.3 Hädaolukorraks valmisoleku kontseptsioon

NB! Käesolevas peatükis ei peeta hädaolukorra all silmas hädaolukorda Eesti Vabariigi hädaolukorra seaduse mõttes.

Hädaolukord on kahju tekitav olukord, kus institutsiooni protsessid või ressursid ei toimi nii, nagu nad peaksid toimima. Vajalike protsesside ja ressursside käideldavust ei õnnestu selleks ette nähtud aja jooksul taastada. Igapäevased tööprotsessid on tugevalt pärsitud. Võimalikke teenindusleppeid (Service Level Agreements(SLA)) ei suudeta täita. Tekivad suured kuni väga suured kahjud, mis mõjutavad märkimisväärselt ja vastuvõetamatult suurel määral ettevõtte aasta tulemit või ametiasutuste ülesannete täitmist. Hädaolukordade kõrvaldamiseks igapäevastest tööprotsessidest enam ei piisa. Nende kõrvaldamiseks läheb eraldi tarvis hädaolukordade likvideerimiseks mõeldud töökorraldust.

Hädaolukordade kohta saab lisa lugeda BSI standardist 100.-4 „hädaolukordade haldus“, mis on kättesaadav Riigi Infosüsteemi Ameti veebilehelt.

Hädaolukorraks valmisolek hõlmab meetmeid, mis on suunatud infosüsteemi talitlusvõime taastamisele pärast (tehnilistel põhjustel, lohaka või tahtliku tegevuse tõttu) toimunud avariid.

Et hoida tegevuses majanduslikult otstarbekat hädaolukorraks valmisoleku kontseptsiooni, tuleb sellega kaasnevaid kulusid võrrelda potentsiaalsete kahjudega (kulud hädaolukorra tõttu tekkiva puuduliku talitlusvõime korral) ning anda kokkuvõtlik hinnang. Kulude hulka tuleb arvestada:

- hädaolukorraks valmisoleku kontseptsiooni koostamise kulud,
- IT-tegevusega kaasnevate hädaolukorraks valmisoleku meetmete realiseerimise ja käigushoidmise kulud,
- hädaolukorras tegutsemise harjutamiseks korraldatavate õppuste kulud
- süsteemi talitlusvõime taastamise kulud.

Nimetatud mooduli ülesandeks on näidata süstemaatilisel viisil, kuidas koostada hädaolukorraprotseduuride juhend ning harjutada selle rakendamist. Kulutused hädaolukorraprotseduuride juhendi koostamiseks koos selle juurde kuuluvate vajalike meetmetega on küllaltki suured. Seepärast on seda moodulit eriti mõttekas kasutada:

- väga head talitlusvõimet vajavate IT-süsteemide,
- suuremate IT-süsteemide (suurarvutid, serverid, laiaulatuslikud võrgud) või
- ühte kohta kontsentreeritud suhteliselt suurema arvu IT-süsteemide korral.

Ohud

Kõikide infoturbe ohtude asemel käsitletakse käesolevas moodulis alljärgnevat ohtu, mis võib esile kutsuda süsteemi avarii.

Vääramatu jõud

- G 1.1 Personali väljalangemine
- G 1.2 IT-süsteemi avarii
- G 1.10 Laivõrgu tõrge
- G 1.18 Hoone väljalangemine
- G 1.19 Teenuspakkuja või tarnija väljalangemine

Soovitatavad meetmed

Vaadeldava IT-süsteemi turvalisuse tagamiseks tuleb lisaks käesolevale moodulile rakendada veel teisigi mooduleid vastavalt infosüsteemide etalonturbe rakendusjuhendi modelleerimise tulemustele.

Hädaolukorraks valmisoleku kontseptsiooni koostamiseks tuleb rakendada terve rida meetmeid, alustades strateegilise planeerimisega, millele järgneb tähtsate tegevusprotsesside kaasamine ning lõpetades konkreetsete meetmetega, mida rakendatakse kõnealuste protsesside juurde kuuluvatele IT-süsteemidele. Alljärgnevalt kirjeldatakse etappe, mis tuleb seejuures läbida, ning meetmeid, millele teatud etappidel tuleb tähelepanu pöörata.

Planeerimine ja kontseptsioon

Erinevate tegevusprotsesside või organisatsiooniüksuste jaoks tuleb koostada individuaalsed hädaolukorraks valmisoleku kontseptsioonid, milles arvestatakse konkreetseid asjaolusid. Valitakse välja IT-valdkonnale sobivad ning majanduslikult tasuvad meetmed. Kaitsevajaduste kindlaksmääramise käigus selgunud andmete käideldavusnõuete baasil määratakse kindlaks vajalikud ennetavad meetmed IT-süsteemi talitluse ajaks (nt suitsetamiskeeld, katkematu elektrivooluga varustamine, hooldus, andmekaitse) (vt M 6.1 Käideldavusnõuete inventuur), et vältida hädaolukordi või vähendada hädaolukordade tagajärjel tekkivaid kahjusid.

Kui käideldavusnõuete kindlaksmääramise tulemusena selgub, et infosüsteemi talitluseks on vajalik alternatiivsüsteem, tuleb hädaolukorraprotseduuride juhendis kirjeldada ajutise või püsiva alternatiivsüsteemi tingimused ja protseduurid.

Hädaolukorraprotseduuride juhend peab olema koostatud nii, et kriitilised tegevusprotsessid ja IT-objektid oleks nõutud ajavahemiku jooksul jälle käideldavad. Eeskätt tuleb dokumenteerida personali võtmepositsioonid ning nende ülesanded ja volitused. Seejuures fikseeritakse hädaolukorraprotseduuride plaanis, mis on hädaolukorraprotseduuride juhendi koostisosa, milliseid meetmeid mingi hädaolukorra esinemisel tuleb rakendada. Hädaolukorraprotseduuride juhend tuleb tehnilisi, organisatsioonilisi ja personaliga seotud muudatusi silmas pidades alati kaasaegsena hoida. Erinevatele valdkondadele suunatud hädaolukorraks valmisoleku meetmed peavad hädaolukorraprotseduuride juhendis olema kirjeldatud nii, et nende rakendamisega saaks hakkama asjatundlik kolmas isik.

Rakendamine

Hädaolukorraprotseduuride juhend peab olema kohandatud ettevõtte või asutuse spetsiifilisele IT-situatsioonile. Selles tuleb detailselt fikseerida vastutavad ja kaasatud isikud, vastuvõtmist vajavad otsused, hädaolukorra kindlakstegemisel koheselt rakendatavad meetmed ning tegevusjuhised erisündmuste korral. Kirjeldatakse nii ennetavaid meetmeid kui ka meetmeid, mida rakendatakse kahju korvamiseks, IT-süsteemide hädaolukorrajärgseks taastamiseks ning asendushangeteks.

Hädaolukorraprotseduuride juhend peab olema hädaolukorral kiiresti kättesaadav ja transporditav. Kui dokument on olemas vaid elektroonilisel kujul või tööriistadele tugineval kujul, on vajalik ühe või mitme hädaolukorra-sülearvuti valmisolek.

Kasutamine

Erilist tähtsust tuleb omistada valmisoleku harjutamiseks läbiviidavatele õppustele. Lisaks sellele tuleks pidevalt tegelda hädaolukorra jaoks vajaliku võtme-

personali (avariiülema) koolitamise ja teadlikkuse tõstmisega. Kui kasutatakse hädaolukorra-sülearvuteid, tuleb seda teha lühiajaliselt.

Planeerimine ja kontseptsioon

- (L) M 6.110 Kehtivusala ja hädaolukorrahalduse strateegia määratlemine
- (M) M 6.111 Hädaolukorrahalduse ja juhtkonnapoolse koguvastutuse võtmise poliitika

Rakendamine

- (M) M 6.113 Hädaolukorrahalduse jaoks sobivate ressursside eraldamine
- (L) M 6.112 Sobiva hädaolukorrahalduse organisatsioonilise struktuuri rajamine
- (L) M 6.114 Hädaolukorraks valmisoleku kontseptsiooni koostamine
- (L) M 6.115 Kaastöötajate integreerimine hädaolukorra haldusprotsessi
- (M) M 6.116 Hädaolukorra halduse integreerimine üleorganisatsioonilistesse protseduuridesse ja protsessidesse

Kasutamine

- (M) M 6.118 Hädaolukorra meetmete kontroll ja käigushoidmine
- (L) M 6.117 Testid ja valmisoleku harjutused
- (M) M 6.119 Hädaolukorra haldusprotsessi dokumentatsioon
- (M) M 6.120 Hädaolukorraks valmisoleku süsteemi kontroll ja juhtimine

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.2 Tuletõrje-eeskirjade täitmise seire
- HG.4 Võrguhaldussüsteemi turbe regulaarseire
- HG.13 Lisanõuded andmete kaugedastuse hädaolukorraplaanile
- HG.14 Lisanõuded hädaolukorrajärgsele taasteplaanile
- HG.15 Tihendatud perioodiga hädaolukorraõppused
- HG.16 Andmevarundusplaani perioodiline läbivaatus
- HG.17 Asendushankeplaani perioodiline läbivaatus
- HG.18 Leppetrahvid tarnijatega tehtavatesse lepingutesse
- HG.19 Lisanõuded andmetaaste harjutamisele
- HG.22 Ööpäevaringne intsidentidest teatamise võimalus

- HG.27 Tulemüüri ründekatsete kaugindikatsioon
- HG.28 Kõrge turbetaseme serveri kettatäitumise kaugindikatsioon
- HG.31 Traadita kohtvõrgu väline turvaaudit
- HG.33 Meiliaadresside asenduskorra regulaarseire
- HG.36 Väljasttellimise avariiplaani regulaarne läbivaatus

Teabe käideldavus (K)

- HK.6 Edastmiseks genereeritud andmete kahes eksemplaris varukopeerimine
- HK.7 Kahes eksemplaris varukopeerimine kodutööl
- HK.9 Varusidekanali nõue
- HK.10 Lisanõuded personali asendamisele
- HK.15 Lisanõuded arhiveerimisprotsessi auditeerimisele
- HK.36 Käideldavusnõuete täidetuse regulaarseire

Teabe terviklus (T)

-

Teabe konfidentsiaalsus (S)

-

B 1.4 Andmevarunduspoliitika

Tehniliste rikete, tahtliku kustutamise või manipuleerimise tõttu võivad salvestatud andmed muutuda käideldamatuks või kaduma minna. Andmekaitse peab tagama, et täiendava andmevaru abil oleks võimalik IT-talitlus lühikese aja jooksul taastada, kui operatiivse andmevaru osad kaduma lähevad.

Sobiva ja hästi funktsioneeriva andmevarunduspoliitika kontseptsioon vajab selle mitmetahulisuse tõttu igal juhul süsteemset toimimisviisi. Käesolevas moodulis kirjeldatakse viisi, kuidas koostada IT-süsteemi andmevarunduspoliitika kontseptsiooni.

Ohud

Andmete kaitsmisel andmevarunduspoliitika kaudu peetakse infosüsteemide turvalisust mõjutavaks järgmist tüüpilist ohtu:

Tehnilised rikked ja defektid:

- G 4.13 Salvestatud andmete hävimine

Soovitatavad meetmed

Vaadeldava IT-süsteemi turvalisuse tagamiseks tuleb lisaks käesolevale moodulile rakendada veel teisigi mooduleid vastavalt infosüsteemide etalonturbe rakendusjuhendi modelleerimise tulemustele.

Efektiivse andmevarunduse sisseseadmiseks on vajalik läbida terve rida etappe. Need on kirjeldatud meetmes M 6.33 Andmevarunduskontseptsiooni loomine ning neid selgitatakse selles esitatud näidete põhjal. Sellepärast tuleks alustada meetme M 6.33 Andmevarunduskontseptsiooni loomine rakendamisega.

Alljärgnevalt tutvustatakse andmevarunduspoliitika elluviimiseks vajalike meetmete kogumit, mida on eelkõige mõttekas rakendada suurte IT-süsteemide või suure andmete hulgaga IT-süsteemide korral. Meetmete analüüsimine peaks toimuma antud järjekorras, et andmevarunduspoliitika koostamine toimuks süstemaatiliselt.

Planeerimine ja kontseptsioon

- (L) M 6.33 Andmevarunduskontseptsiooni loomine
- (M) M 6.34 Andmevarunduse mõjutegurite määratlemine
- (M) M 6.35 Andmevarunduseks vajalike protseduuride määratlemine
- (L) M 6.36 Minimaalse andmevarunduse kontseptsiooni määratlemine

Soetamine

- (L) M 2.137 Sobiva andmevarundussüsteemi hankimine

Rakendamine

- (L) M 2.41 Töötajate kaasamine andmevarundusse
- (L) M 6.21 Kasutatava tarkvara varukoopia
- (L) M 6.37 Andmevarunduse dokumenteerimine

Kasutamine

- (L) M 6.20 Varukoopia andmekandjate õige ladustus

Valmisolek hädaolukorraks

- (L) M 6.32 Regulaarne andmevarundus
- (L) M 6.41 Andmete taastamise harjutamine

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.16 Andmevarundusplaani perioodiline läbivaatus
- HG.19 Lisanõuded andmetaaste harjutamisele

Teabe käideldavus (K)

- HK.7 Kahes eksemplaris varukopeerimine kodutööl
- HK.8 Andmebaasi tervikliku varundamise nõue

Teabe terviklus (T)

-
Teabe konfidentsiaalsus (S)

- HS.51 Lisanõuded tundlike ressursside hävitamisele
- HS.76 Mobiilsete andmekandjate võimalik vältimine

B 1.5 Andmekaitse

Andmekaitse tagamine käesoleva mooduli mõistes tähendab isikuandmete kaitse seaduse järgimist. Andmekaitse Inspektsiooni juhendmaterjalid leiab veebilehelt www.aki.ee, isikuandmete kaitse seadus on leitav Riigi Teatajast.

B 1.6 Viirusetõrje kontseptsioon

Viirusetõrje kontseptsiooni ülesandeks on sobivate meetmete leidmine, mis kaitseks kahjustavate programmide eest. Tagatud peab olema, et arvutiviiruste esinemine oleks takistatud või võimalikult kiiresti avastatav. Lisaks sellele peavad olema nimetatud meetmed, mis aitavad kahjustusi minimeerida, kui kahjustavat programmi õigeaegselt ei avastata. Oluline on meetmete järjekindel rakendamine ning kasutatavate tehniliste meetmete pidev uuendamine. See nõue on tingitud iga päev uuenevatest viirustest või juba tuntud viiruste variatsioonidest. Kasutamissüsteemide, programmeerimiskeelte ja rakendatava tarkvara edasiarendamise tõttu täiustub ka viiruste ründepotentsiaal, seepärast tuleb õigeaegselt rakendada vastumeetmeid.

Kui asutused või ettevõtted on liitunud avalike kommunikatsioonivõrkudega, on viiruste poolt tekitatav oht eriti suur. Kasutuses olevaid arvuteid tuleb seetõttu pidevalt viiruste suhtes kontrollida.

Et tagada kogu organisatsioonile efektiivne viirusetõrje, kirjeldatakse käesolevas moodulis üksikute sammudena tegutsemisviisi viirusetõrje kontseptsiooni väljatöötamisel ja realiseerimisel. Üksikute IT-süsteemide viirusetõrjeks soovitatavad meetmed on ära toodud süsteemispetsiifilistes moodulites.

Ohud

Infosüsteemide etalonturvet mõjutavad viiruste osas alljärgnevad tüüpilised ohud:

Organisatsioonilised puudused:

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.2 Reeglite puudulik tundmine
- G 2.3 Puuduvad, puudulikud või ühildumatud ressursid
- G 2.4 Turvameetmete ebapiisav järelevalve
- G 2.8 Ressursside kontrollimatu kasutamine
- G 2.9 Halb kohanemine IT muutustega
- G 2.136 Puudulik ülevaade IT-kooslusest

Tehnilised rikked:

- G 4.13 Salvestatud andmete hävimine
- G 4.22 Tüüptarkvara turvaaugud või vead

Ründed:

- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.23 Viirused
- G 5.28 Teenuse halvamine

- G 5.42 Inimestega manipuleerimine (Social Engineering)
- G 5.71 Tundliku informatsiooni konfidentsiaalsuse kadu
- G 5.85 Tundliku informatsiooni tervikluse kadu
- G 5.142 Pahavara levimine kaasaskantavate andmekandjate kaudu

Soovitatavad meetmed

Viirusetõrje kontseptsiooni koostamisel (vt M 2.154 Viirusetõrje kontseptsiooni loomine) tuleb kõigepealt kindlaks teha, millised olemasolevad või planeeritud IT-süsteemid tuleks viirusetõrje kontseptsiooni kaasata (vt M 2.155 Potentsiaalselt viiruste poolt ohustatud IT-süsteemide tuvastamine). Nende süsteemidega seoses on vajalik vaadelda turvameetmete rakendamiseks tähtsaid mõjufaktoreid. Nendele toetudes on võimalik välja valida tehnilised ja organisatsioonilised meetmed. Siinjuures tuleb erilist tähelepanu pöörata sobivate tehniliste vastumeetmete valikule, nagu seda on viiruseskännerid (vt M 2.156 Sobiva viirusetõrjestrateegia valimine ja M 2.157 Sobiva viiruseskanneri valimine). Lisaks viirusnakkustest teatamise korrale (vt M 2.158 Viirusnakkustest teatamine) ja rakendatavate viiruseskännerite värskendamise koordineerimisele (vt M 2.159 Viiruseskanneri värskendamine) tuleb kontseptsiooni rakendamiseks kooskõlastada veel terve hulk reegleid (vt M 2.11 Paroolide kasutamise reeglid), millega määratakse kindlaks täiendavad vajaminevad viirusetõrjemeetmed.

Üks tähtsamatest viiruste ennetusmeetmetest on regulaarne andmevarundus (vt M 6.32 Regulaarne andmevarundus).

Vaadeldava IT-süsteemi turvalisuse tagamiseks tuleb lisaks käesolevale moodulile rakendada veel teisigi mooduleid vastavalt infosüsteemide etalonturbe rakendusjuhendi modelleerimise tulemustele.

Planeerimine ja kontseptsioon

- (L) M 2.154 Viirusetõrje kontseptsiooni loomine
- (L) M 2.155 Potentsiaalselt viiruste poolt ohustatud IT-süsteemide tuvastamine
- (L) M 2.156 Sobiva viirusetõrjestrateegia valimine
- (L) M 2.160 Viirusetõrje eeskirjad
- (L) M 3.69w Sissejuhatus viirustest tulenevatesse ohtudesse

Soetamine

- (L) M 2.157 Sobiva viiruseskanneri valimine

Rakendamine

- (L) M 4.84 BIOSi turvamehhanismide kasutamine

Kasutamine

- (L) M 2.34 IT-süsteemi muutuste dokumenteerimine
- (L) M 2.158 Viirusnakkustest teatamine
- (L) M 2.159 Viiruseskanneri värskendamine
- (L) M 2.224 Trooja hobuste tõrje
- (L) M 4.3 Viirustõrjeprogrammi regulaarne kasutamine
- (L) M 4.33 Viirustõrjeprogrammi kasutamine andmekandjate vahetamisel ja andmete edastamisel
- (L) M 4.253 Nuhkvara tõrje

Valmisolek hädaolukorraks

- (L) M 6.23 Käitumisreeglid arvutiviiruste esinemisel
- (L) M 2.24 IT-passi juurutamine
- (L) M 6.32 Regulaarne andmevarundus

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.5 Lisanõuded viiruseskänneri värskendamisele
- HG.23 Kahe erineva tootja pahavara- ja ründetuvastusprogrammi kasutamine

Teabe käideldavus (K)

-

Teabe terviklus (T)

-

Teabe konfidentsiaalsus (S)

-

B 1.7 Krüptokontseptsioon

Käesolev moodul kirjeldab tegutsemisviisi, kuidas on heterogeenses keskkonnas võimalik nii lokaalselt salvestatud kui ka ülekantavaid andmeid efektiivselt krüptoprotseduuride ja -võtetega kaitsta. Selleks kirjeldatakse, kuidas ja kus on heterogeenses keskkonnas võimalik kasutada krüptoprotseduure ja vastavaid komponente. Kuna krüptoprotseduuride rakendamisel tuleb tähelepanu pöörata väga paljudele komplekssetele mõjufaktoritele, on selleks vajalik koostada

krüptokontseptsioon.
Käesolevas moodulis kirjeldatakse krüptokontseptsiooni koostamist. Alustada tuleb vajaduse väljaselgitamisest ja mõjufaktorite kõrvaldamisest, millele järgneb sobivate krüptograafiliste lahenduste ja toodete valik, ning lõpuks tuleb hoolitseda selle kasutajate teadlikkuse tõstmise ja koolituste ning krüpto hädaolukorraks valmisoleku eest.
Käesolevat moodulit võib kasutada ka juhul, kui ühele võimalikest rakendusaladest tuleb valida vaid üks krüptotoode. Sel juhul võib mõned alljärgnevalt kirjeldatud etappidest välja jätta ning piirduda vaid konkreetse rakendusala oluliste osade analüüsimisega.
Käesoleva mooduli rakendamiseks peaks omama elementaarseid teadmisi tähtsamatest krüptograafilistest mehhanismidest. Ülevaate krüptograafia põhiterminitest annab M 3.23 Sissejuhatus krüptograafia põhimõistetesse .

Ohud

Krüptoprotseduure rakendatakse andmete

- konfidentsiaalsuse,
- tervikluse,
- autentsuse ja
- mittevaidlustatavuse tagamiseks.

Kui rakendatakse krüptoprotseduure, tuleks infosüsteemide etalonturbes tähelepanu pöörata veel alljärgnevatele ohtudele:
Organisatsioonilised puudused

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.2 Reeglite puudulik tundmine
- G 2.4 Turvameetmete ebapiisav järelevalve
- G 2.19 Krüpteerimise halb korraldus

Inimvead

- G 3.1 Andmete konfidentsiaalsuse või tervikluse kadu kasutaja vea tõttu
- G 3.32 Seaduste rikkumine krüptoprotseduuride kasutamisel
- G 3.33 Krüptomoodulite väär kasutamine

Tehnilised rikked

- G 4.22 Tüüptarkvara turvaaugud või vead

- G 4.33 Autentimise puudumine või puudulikkus
- G 4.34 Krüptomooduli rike
- G 4.35 Ebaturvaline krüptoalgoritm
- G 4.36 Vead krüpteeritud andmetes

Ründed

- G 5.27 Sõnumi salgamine
- G 5.71 Tundliku informatsiooni konfidentsiaalsuse kadu
- G 5.81 Krüptomooduli volitamata kasutamine
- G 5.82 Krüptomooduli manipulatsioon
- G 5.83 Krüptograafiliste võtmete paljastamine
- G 5.84 Võltsitud sertifikaadid
- G 5.85 Tundliku informatsiooni tervikluse kadu

Soovitatavad meetmed

Vaadeldava IT-süsteemi turvalisuse tagamiseks tuleb lisaks käesolevale moodulile rakendada veel teisigi mooduleid vastavalt infosüsteemide etalonturbe rakendusjuhendi modelleerimise tulemustele.

Lisaks sellele tuleb krüptoprotseduuride valdkonnas läbida alljärgnevad põhietapid:

1. Krüptokontseptsiooni väljatöötamine (vt M 2.161 Krüptokontseptsiooni väljatöötamine)
   Krüptoprotseduuride kasutamine sõltub paljudest teguritest. Nimetatud tegurite hulka kuuluvad muu hulgas IT-süsteem, vajalik turvalisuse tase ning nõuded andmete käideldavusele. Seepärast tuleb kõigepealt välja töötada kontseptsioon, milles võetakse arvesse kõikide mõjutavate tegurite suurust ja otsustuskriteeriume konkreetse krüptoprotseduuri ning vastavate toodete valikuks, mis oleks ka majanduslikult õigustatud.
2. Krüptoprotseduuridele esitatavate nõuete väljaselgitamine
   Vajalik on koostada nõuete kataloog, milles kirjeldatakse krüptoprotseduuride rakendamist mõjutavate tegurite suurust ja otsustuskriteeriume. (vt M 2.162 Krüptoprotseduuride ja -toodete vajaduse määramine ja M 2.163 Krüptoprotseduure ja -tooteid mõjutavate tegurite määramine). Krüptoprotseduure võib rakendada ISO/OSI-etalonmudeli eri kihtides. Vastavalt kindlaksmääratud nõudmistele või ohtudele on nende kasutamine teatud kihtides soovitatav (vt ka M 4.90 Krüptoprotseduuride kasutamine ISO/OSI etalonmudeli eri kihtides).
3. Sobivate krüptoprotseduuride valimine (vt M 2.164 Sobiva krüptoprotseduuri valimine)
   Krüptoprotseduuride valimisel on kõigepealt tähtsaimaks küsimuseks, kas sobivad sümmeetrilised, asümmeetrilised või hübriidsed algoritmid ning seejärel mehhanismide tugevus. Lõpuks tuleb välja valida sobivad tooted.
4. Sobiva krüptotoote valimine (vt M 2.165 Sobiva krüptotoote valimine)
   Pärast raamtingimuste kindlaksmääramist tuleb välja valida toode, mis vastab krüptokontseptsioonis esile toodud turvalisuse tagamise tingimustele.

Niisugune toode, mida alljärgnevalt nimetatakse lühidalt krüptomooduliks, võib koosneda riistvarast, tarkvarast, püsivarast või nende kombinatsioonist ning krüptoprotseduuride läbiviimiseks vajalikest komponentidest nagu salvesti, protsessorid, siinid, elektrivooluga varustamine jne. Krüptomoodulit võib rakendada konfidentsiaalsete andmete või informatsiooni kaitsks erinevates arvuti- ja telekommunikatsioonisüsteemides.

5. Krüptomoodulite sobiv kasutamine (vt M 2.166 Krüptomoodulite kasutamist reguleerivad sätted)
   Ka töö käigus tuleb krüptomoodulile esitada terve rida turvanõudeid. Lisaks krüptomooduli rakendamisel saavutatud kaitsmisele kuuluvate andmete turvalisusele tuleb esmajärgulist tähelepanu pöörata ka krüptomooduli enda kaitsele vahetute rünnete ja välismõjude eest.
6. Turvatehnilised nõuded IT-süsteemidele, milles kasutatakse krüptoprotseduure, on välja toodud vastavates süsteemispetsiifilistes moodulites.
7. Valmisolek hädaolukorraks. Siia kuuluvad

   - andmevarundus krüptoprotseduuride kasutamisel (vt M 6.56 Andmevarundus krüptoprotseduuride kasutamisel kasutamisel), niisiis võtmete, kasutatud toodete konfiguratsiooniandmete, krüpteeritud andmete varundamine,
   - informatsiooni hankimine turvaaukude kohta ning reageerimine turvaaukudele.

Alljärgnevalt tutvustatakse turvameetmete kogumit rakendamiseks valdkonnas "Krüptokontseptsioon". Teistes moodulites toodud turvameetmete kordamisest on loobutud.
Planeerimine ja kontseptsioon

- (L) M 2.161 Krüptokontseptsiooni väljatöötamine
- (L) M 2.162 Krüptoprotseduuride ja -toodete vajaduse määramine
- (L) M 2.163 Krüptoprotseduure ja -tooteid mõjutavate tegurite määramine
- (L) M 2.164 Sobiva krüptoprotseduuri valimine
- (L) M 2.165 Sobiva krüptotoote valimine
- (M) M 2.166 Krüptomoodulite kasutamist reguleerivad sätted
- (M) M 3.23w Sissejuhatus krüptograafia põhimõistetesse
- (M) M 4.41 Sobivate IT-süsteemide turvatoodete valimine
- (M) M 4.90w Krüptoprotseduuride kasutamine ISO/OSI etalonmudeli eri kihtides
- (M) M 4.433z Serveriteenuste turvaline konfiguratsioon
- (M) M 4.435z Isekrüpteerivad kõvakettad
- (M) M 5.63z GnuPG või PGP kasutamine
- (M) M 5.67z Ajatempliteenuse kasutamine
- (M) M 5.110z Meili kaitse SPHINXi (S/MIME) abil

Soetamine

- (L) M 2.165 Sobiva krüptotoote valimine
- (M) M 4.85z Sobiv krüptomoodulite liideste disain

- (L) M 4.88 Nõuded operatsioonisüsteemide turvalisusele krüptomoodulite kasutamise korral

Rakendamine

- (L) M 2.46 Krüpteerimise õige korraldus
- (L) M 4.86 Krüptomoodulite kindel rollijaotus ja konfigureerimine
- (M) M 4.87z Krüptomoodulite füüsiline turve

Valmisolek hädaolukorraks

- (L) M 6.56 Andmevarundus krüptoprotseduuride kasutamisel
- (L) M 6.162z Reageerimine krüpteerimismeetodi praktilise nõrgenemise korral

Paljud teised moodulid sisaldavad meetmeid, mis puudutavad krüptoprotseduure ning mida saab vaadelda rakendamisnäidistena. Nende hulka kuuluvad näiteks:

- (M) M 4.29 Kaasaskantavatele IT-süsteemidele mõeldud krüpteerimistoote kasutamine
- (L) M 4.30 Rakendusprogrammide turvavahendite kasutamine
- (M) M 4.34 Krüpteerimise, kontrollsummade ja digitaalallkirjade rakendamine
- (L) M 4.72z Andmebaasi krüpteerimine
- (M) M 5.33 Kaughoolduse turve
- (M) M 5.34 Ühekordsed paroolid
- (L) M 5.52 Sidearvutite turvanõuded
- (M) M 5.64 Secure Shell (SSH)
- (M) M 5.66z SSL-i/TLS-i kasutamine kliendis

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed
-
Teabe käideldavus (K)
-
Teabe terviklus (T)

- HT.10 Andmebaasi kannete krüptoaheldamine
- HT.14 Süsteemi tegevuslogide krüptoaheldamine
- HT.13 Tulemüüri konfiguratsioonimuudatuste krüptoaheldamine
- HT.34 Digiallkirja kasutamine
- HT.48 Lisanõuded krüptolahenduste võtmehaldusele =HS.35
- HT.52 Lisanõuded krüptovahenditele =HS.38
- HT.63 Sülearvutite krüpteerimine =HS.52
- HT.67 Pihuarvutite krüpteerimine =HS.53

Teabe konfidentsiaalsus (S)

- HS.39 Lisanõuded andmebaaside krüpteerimisele
- HS.77 Kiirgusturve

B 1.8 Turvaintsidentide käsitlus

Turvaintsidendiks nimetatakse sündmust, mille tagajärjel võib tekkida suur kahju. Nende kahjude ärahoidmiseks või vähendamiseks peaks turvaintsidentide käsitlemine toimuma pidevalt ja efektiivselt. Kui seejuures on võimalik toetuda etteantud meetodile, saab viia reageerimisajad miinimumini. Turvaintsidentidega kaasnevad võimalikud kahjud võivad mõjutada nii andmete konfidentsiaalsust või terviklust kui ka nende käideldavust.

Turvaintsidentide käsitlemise eraldi valdkonna moodustab valmisolek hädaolukorraks (vaata moodulit B 1.3 Hädaplaanimine). Hädaolukorraks valmisoleku kontseptsioonis viiakse eelnevalt läbi konkreetne vastavate IT-süsteemide kriitiliste komponentide väljalangemise analüüs ning määratakse kindlaks tegutsemisviis andmete käideldavuse alalhoidmiseks või taastamiseks.

Turvaintsidendid võivad esineda alljärgnevatel juhtudel:

- kasutaja vale käitumine, mille tagajärjeks on andmete kadu või turvakriitiline süsteemiparameetrite muutumine
- turvaaukude esinemine riist- või tarkvarakomponentides
- massiline viiruste esinemine
- internetiserverite ründamine,
- konfidentsiaalsete andmete avalikustamine,
- personali puudumine või
- kriminaalne tegevus (nagu sissemurdmine, vargus või väljapressimine seoses IT-ga).

Käesolevas moodulis tuleb süstemaatiliselt välja tuua, kuidas peab toimuma turvaintsidentide käsitluse kontseptsiooni koostamine ja selle realiseerimise ja sisseseadmise kindlustamine ettevõttes või asutuses. Sellise kontspetsiooni koostamise ja realiseerimise kulud ei ole väikesed. Sellepärast peaks käesolevat moodulit järgima eelkõige suuremate ja/või asutusele või ettevõttele suure tähtsusega IT-süsteemide korral.

Mõistlik on turvantsidendid süstematiseerida tagajärje või mõne muu asutusele olulise parameetri järgi. Abimaterjaline saab kasutada ITILi intsidentide kategoriseemisit või võtta aluseks veebilehel http://www.us-cert.gov/federal/reportingRequirements.html olev tabel.

Ohud

Ohtude kataloogis on ära toodud suur hulk ohtusid, mis võivad esile kutsuda väiksemaid või suuremaid turvaintsidente.

Suurt kahju võivad tekitada nimetatud ohud sel juhul, kui nende kaitsmiseks pole ette nähtud sobivat lähenemisviisi. Käesolevas moodulis käsitletakse seetõttu kõigi ohtude asemel, mis turvaintsidentidega seoses võivad esineda, alljärgnevat ohtu:

- G 2.62 Turvaintsidentide puudulik käsitlus
- G 2.141 Märkamata jäänud turvaintsidendid
- G 2.142 Tõendite hävitamine turvaintsidentide käsitlemisel

Soovitatavad meetmed

Vaadeldava IT-süsteemi turvalisuse tagamiseks tuleb lisaks käesolevale moodulile rakendada veel teisigi mooduleid vastavalt infosüsteemide etalonturbe rakendusjuhendi modelleerimise tulemustele.

Turvaintsidentide käsitlemiseks efektiivse süsteemi sisseseadmiseks on vajalik läbida terve rida etappe. Need on kirjeldatud meetmes M 6.58 Turvaintsidentide käsitluse haldussüsteemi rajamine ning põhjalikuma selgituse nende kohta annavad nimetatud meetmega seonduvad meetmed. Sellepärast tuleks alustada meetme M 6.58 Turvaintsidentide käsitluse haldussüsteemi rajamine .

Alljärgnevalt tutvustatakse meetmete kogumit, mida tuleb rakendada valdkonnas "Turvaintsidentide käsitlemine".

Planeerimine ja kontseptsioon

- (M) M 6.58 Turvaintsidentide käsitluse haldussüsteemi rajamine
- (L) M 6.59 Turvaintsidentide käsitlemise eest vastutavate isikute määramine
- (L) M 6.60 Turvaintsidentide käsitlusprotseduurid ja teavitamiskanalid
- (M) M 6.61 Turvaintsidentide käsitluse eskalatsioonistrateegia
- (M) M 6.62z Prioriteetide kindlaksmääramine turvaintsidentide käsitlemiseks
- (L) M 6.121 Suuniste väljatöötamine turvaintsidentide käsitlemiseks
- (L) M 6.122 Turvaintsidendi defineerimine

Rakendamine

- (M) M 6.67z Turvaintsidentide avastamismeetmete rakendamine
- (M) M 6.123z Ekspertmeeskonna moodustamine turvaintsidentide käsitlemiseks
- (M) M 6.124z Turvaintsidentide käitlemise liideste kindlaksmääramine tõrgete ja vigade kõrvaldamiseks
- (L) M 6.125 Tsentraalse kontaktkoha sisseseadmine turvaintsidentide registreerimiseks
- (L) M 6.126w Sissejuhatus arvutipõhisesse kohtulikku juurdlusesse
- (M) M 6.127z Tõendite varundusmeetmete kindlaksmääramine seoses turvaintsidendiga
- (M) M 6.128z Koolitus tõendusmaterjalide varundamise alal

- (M) M 6.129 Teenustoe töötajate koolitamine turvaintsidentide käsitlemise alal

Kasutamine

- (L) M 6.64 Turvaintsidentide likvideerimine
- (L) M 6.65 Asjassepuutuvate isikute teavitamine turvaintsidentidest
- (M) M 6.66 Turvaintsidentide järelhindamine
- (M) M 6.68 Turvaintsidentide käsitluse süsteemi tõhususe testimine
- (L) M 6.130 Turvaintsidentide äratundmine ja mõistmine
- (L) M 6.131 Turvaintsidentide kvalifitseerimine ja hindamine
- (L) M 6.132 Turvaintsidentide mõju tõkestamine
- (M) M 6.133 Töökeskkonna taastamine pärast turvaintsidente
- (L) M 6.134 Turvaintsidentide dokumenteerimine

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele Kohustuslikud üldmeetmed

- HG.3 Tõrgete kaugindikatsiooni vastuvõtmiskohustus
- HG.22 Ööpäevaringne intsidentidest teatamise võimalus
- HG.40 CERT-EE teavitamine välismõjuga turvaintsidendist
- HG.65 Mitmekordse nurjunud logimise automaatteavitus

Teabe käideldavus (K)

-

Teabe terviklus (T)

-

Teabe konfidentsiaalsus (S)

-

B 1.9 Riist- ja tarkvara haldus

Et saavutada kogu organisatsiooni hõlmav vajalik ja soovitud turvatase, ei piisa vaid üksikute IT-komponentide kindlustamisest. Pigem on vajalik kujundada ka kõik konkreetset IT-süsteemi puudutavad protsessid ja protseduurid nii, et oleks võimalik saavutada ja säilitada vajalik infoturbe tase. Sellepärast tuleb kõigi protseduuride läbiviimiseks kehtestada reeglid ja neid järgida, mis tagab turvameetmete efektiivsuse.

Käesoleva mooduli keskmeks on reeglid, mis puudutavad spetsiifiliselt just arvutisüsteemide riistvara ja tarkvara komponente, mille eesmärgiks on nõuetele vastava IT-töö halduse või organiseerimise tagamine. Turvalisus peaks olema IT-süsteemi või toote kogu elutsükli integreeritud koostisosa

Ohud

Käesolevas moodulis vaadeldaks alljärgnevaid infoturbele mõjuvaid tüüpilisi ohtusid:

Vääramatu jõud:

- G 1.1 Personali väljalangemine
- G 1.2 IT-süsteemi avarii
- G 1.4 Kahjutuli
- G 1.5 Vesi
- G 1.8 Tolm, saastumine
- G 1.19 Teenuspakkuja või tarnija väljalangemine

Organisatsioonilised puudused

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.2 Reeglite puudulik tundmine
- G 2.4 Turvameetmete ebapiisav järelevalve
- G 2.6 Volitamata pääs ruumidesse
- G 2.7 Õiguste volitamata kasutamine
- G 2.9 Halb kohanemine IT muutustega
- G 2.10 Probleemid andmekandjate kättesaadavusega
- G 2.15 Konfidentsiaalsusaugud Unix-süsteemis
- G 2.21 Korraldamata kasutajavahetus
- G 2.22 Logiandmete analüüsimata jätmine
- G 2.24 Kaitsetus välisvõrgu vastu
- G 2.67 Pääsuõiguste puudulik haldus

Inimvead:

- G 3.1 Andmete konfidentsiaalsuse või tervikluse kadu kasutaja vea tõttu
- G 3.2 Seadme või andmete hävitamine hooletuse tõttu
- G 3.3 Hooletus turvameetmete suhtes
- G 3.5 Liinide juhuslik kahjustamine

- G 3.6 Koristajad jm väljastpoolt tellitud töötajad
- G 3.8 IT-süsteemi väär kasutamine
- G 3.9 IT-süsteemi väär haldus
- G 3.11 Sendmaili väär konfiguratsioon
- G 3.17 Arvutikasutajate väär vahetumine
- G 3.35 Töötava serveri elektritoite väljalülitamine
- G 3.44 Teabe hooletu kasutamine

Tehnilised rikked:

- G 4.10 Keerukad ligipääsuvõimalused võrgustatud IT-süsteemides
- G 4.13 Salvestatud andmete hävimine
- G 4.22 Tüüptarkvara turvaaugud või vead
- G 4.31 Võrgukomponentide rike või tõrge
- G 4.35 Ebaturvaline krüptoalgoritm
- G 4.38 Võrgu- või süsteemihaldussüsteemi komponendi rike
- G 4.39 Tarkvarakontseptsiooni viga
- G 4.43 Dokumenteerimata funktsioonid

Ründed:

- G 5.1 IT-seadmete või -tarvikute manipuleerimine ja hävitamine
- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.4 Vargus
- G 5.9 IT-süsteemide volitamata kasutamine
- G 5.21 Trooja hobused
- G 5.23 Viirused
- G 5.26 Sõnumivoo analüüsimine
- G 5.68 Volitamata juurdepääs aktiivsetele võrgukomponentidele
- G 5.71 Tundliku informatsiooni konfidentsiaalsuse kadu
- G 5.82 Krüptomooduli manipulatsioon
- G 5.83 Krüptograafiliste võtmete paljastamine
- G 5.84 Võltsitud sertifikaadid
- G 5.87 Veebilehe võltsimine

Soovitatavad meetmed

Vaadeldava IT-süsteemi turvalisuse tagamiseks tuleb lisaks käesolevale moodulile rakendada veel teisigi mooduleid vastavalt infosüsteemide etalonturbe rakendusjuhendi modelleerimise tulemustele.

IT-süsteem koosneb paljudest IT-komponentidest, mis tuleks kõigepealt kindlustada üksikkomponentidena vastavates moodulites soovitatud meetmeid rakendades. Et saavutada kõikide kasutuses olevate IT-komponentide suhtes ühesugune turvatase, tuleks riist- ja tarkvara halduse kaudu kehtestada ühtsed reeglid.

Riist- ja tarkvara halduse käigus tuleb sõltumata rakendatud IT-komponentide liigist rakendada terve hulk meetmeid, alustades soetamise kontseptsioonist ning lõpetades tööga. Alljärgnevalt tutvustatakse etappe, mis tuleb seejuures läbida, ning meetmeid, millele teatud etappidel tuleb tähelepanu pöörata.

Planeerimine ja kontseptsioon

IT alase turvalisuse aspektid peavad varakult sulanduma strateegilisse juhtimisse ja IT-süsteemide soetamisse, kuna neil on täiesti konkreetne mõju ülesannete täitmisele ja tööprotsesside kulgemisele. Seejuures tuleb kindlustada juba olemasolevate IT-süsteemide kaitseks kehtestatud turvanõuded ning planeeritud rakendusstsenaariumidest tulenevad nõuded (vt M 2.214 IT-kasutuse kontseptsioon). Riistvara ja tarkvara soetamiseks ja töösserakendamiseks on vaja kehtestada erinevatele kasutajatele spetsiifilised reeglid.

Seejuures tuleb tööprotsessi kindlaks kulgemiseks vajalikud IT-süsteemide turvaparameetrid kasutajatele arusaadavaks teha (vt M 2.223 Tüüptarkvara kasutamise turvaeesmärgid). Vaatamata intensiivsele koolitusele tuleb kasutajaid jooksva töö käigus programmide funktsionaalsust, kindlust ja tekkivaid probleeme silmas pidades eesmärgistatult ja järjekindlalt toetada (vt M 2.12 IT-kasutajate nõustamine). Selleks on vaja sisse seada kasutajate nõuande- ja infopunktid.

Kõikide IT-komponentide kindla kasutamise tagamiseks vajalikud meetmed peavad olema kindlaks määratud ühes turvasuunises. Selles määratletud turvatasemest kinnipidamine nõuab lisaks tehnilistele meetmetele ka ulatuslikku reeglite kogumit, mis pakub kasutajatele toetust ning on siduvaks ja täpseks juhiseks. Potentsiaalsed riskifaktorid ja turvaaugud, nagu paroolide ja asutusevälise personali kasutamine, aktsepteerimata IT-komponendid ja juurdepääs IT-süsteemidele tuleb organisatsiooniliste reeglite (vt M 2.226 Asutusevälise personali kasutamise protseduurid) või organisatsiooniliste ja tehniliste meetmete kombineerimise kaudu minimeerida. Kasutajate teadlikkust hoolika ümberkäimise osas turvakriitiliste andmete ja IT-komponentidega tuleb pidevalt tõsta (vt M 2.217 Teabe, rakenduste ja süsteemide hoolikas liigitamine ja käitlus).

Heterogeensete võrkude efektiivne ja turvaline kasutamine nõuab riist- ja tarkvara testimise, installeerimise ja dokumenteerimise suhtes kehtestatud rangeid suuniseid (vt M 2.216 IT-komponentide kinnitamise protseduur), samuti ka efektiivset kasutajate haldamist (vt M 2.30 Kasutajate ja kasutajarühmade määramise protseduurid). Füüsiline juurdepääs IT-süsteemidele ning kasutajate autentimine rakenduste ja süsteemide suhtes (vt M 2.220 Pääsu reguleerimise suunised) peaks põhimõtteliselt toimuma „ *need-to-know* “ printsiibil.

Väliste andmekandjate kasutamine võib olla seotud kõrge turvariskiga, kuna oletatavad turvabarjäärid on tihti lihtsalt kõrvaldatavad. Kasutamise, tähistamise ja kontrollimise reeglid – nt viiruste suhtes - diskettidele, CD-ROMidele, mälupulkadele ja teistele USB kaudu ühendatava andmete vahetamise seadmetele, on samuti kindla IT-töö säilitamise teenistuses (vt M 2.3 Andmekandjate haldus).

Muudatuste halduse ülesandeks on aktuaalsete konfiguratsioonide juures läbiviidud muudatuste formaalne dokumenteerimine ja evitamine (vt M 2.221 Muudatuste haldus). Seejuures tuleb tähelepanu pöörata ka turvakriitilistele aspektidele nagu tegevuste läbiviimine nelja-silma-printsiibil ja aktuaalsete muudatuste dokumenteerimine. Arvestada tuleb ka asjaoluga, et kasutada tohib vaid lubatud komponente, sest muidu pole kontrollitav tööprotsess võimalik (vt M 2.9 Aktsepteerimata riist- ja tarkvara kasutuse keeld).

Soetamine

IT-süsteemide hankimiseks tuleb formuleerida kontseptsioonist tulenevad nõuded vastavatele toodetele ja selle alusel sobivad tooted välja valida. Uue toote formaalsele aktsepteerimisele (vt M 2.62 Tarkvara vastuvõtuprotseduurid) peaks

eelnema nõutavate turvaomaduste funktsionaalsuse ja tervikluse kontroll (vt M 4.65 Uue riist- ja tarkvara testimine).

Rakendamine

Turvasuuniste rakendamine tööprotsessis nõuab turvanõuete kindlaksmääramist installeerimise ja esimese konfigureerimise käigus (vt M 4.135 Süsteemifailide pääsuõiguste andmise kitsendused) samuti ka IT-süsteemide jooksvaks tööks. Järjekindla programmi- ja töötailide eraldamise abil struktureeritud andmetalletus (vt M M 2.138 Struktureeritud andmetalletus) peaks baseeruma igakülgselt ühtsel süsteemide konfiguratsioonil. Seda omakorda toetab keskselt läbiviidav süsteemihaldus (vt M 2.69 Tüüpsete tööjaamade rajamine).

Täielik süsteemihalduse kindlustamine – ka haigustest ja puhkusel viibimisest tingitud väljalangemiste korral – on võimalik saavutada vastavate asendusreeglite rakendamise abil (vt M 2.26 Süsteemiülema ja ta asetäitja määramine). Asendaja pädevused tuleb teha läbipaistvaks.

Süsteemi konfiguratsiooni dokumentatsioon peab olema aktuaalne ja arusaadav ning selle dokumenteerimine peaks toimuma tööriistade toetusel (vt M 2.25 Süsteemi konfiguratsiooni dokumenteerimine). Lisaks füüsilistele IT-komponentidele tuleb dokumenteerida ka loogilised võrgustruktuurid, rollid ja pääsuõigused.

Kasutamine

Süsteemi administreerimise kaudu tuleb kindlustada erinevate raskuspunktidega kulgev tööprotsess. Töötajate migratsiooni, väljalangemise ja uute töötajate töölevõtmise tõttu vajalikud IT-inventuuri muudatused (vt M 4.78 Konfiguratsioonimuudatuste hoolikas teostamine) tuleb pärast nende aktsepteerimist kanda tagantjärele IT-inventuuri nimekirja (vt M 2.34 IT-süsteemi muutuste dokumenteerimine ja M 2.219 Infotöötluse pidev dokumenteerimine).

Tööprotsessi jooksev jälgimine ja hindamine (vt M 2.10 Riistvara ja tarkvara inventuur ja M 2.64 Logifailide kontroll) ühtivuse ja vastavate turvameetmete läbiviimise suhtes (vt M 2.215 Tõrkekäsitlus) nõuab pidevat teabe hankimist erinevate tootjate vastavate andmete uuendamise kohta (vt M 2.35 Teabe hankimine turvaaukude kohta). Nõutava turvapaiga installeerimise abil peaks vajalik turvatase olema juba eelnevalt saavutatav (vt M 2.273 Turvalisust mõjutavate paikade ja värskenduste kiire paigaldamine).

Organisatsiooni ja personali suhtes kindlaksmääratud turvameetmete kasutuskõlblikkust, aktsepteeritavust ja efektiivsust tuleb kontrollida.

Väljavahetamine

IT-süsteemide väljavahetamise korral tuleb hoolitseda selle eest, et tähtsad andmed ei läheks kaotsi, vaid enne IT-süsteemide loovutamist või lammutamist tuleb tagada nende turvalisus (vt meedet M 4.234 IT-süsteemide ja andmekandjate väljavahetamise kord). Veelgi tähtsam on aga, et väljavahetatavate süsteemide andmekandjad nii põhjalikult kustutatakse (vt meedet B 1.15 Andmete kustutamine ja hävitamine), et tagantjärele ei oleks võimalik volitamatu juurdepääs konfidentsiaalsetele andmetele, sest reeglina puudub pärast süsteemide väljavahetamist kontroll selle üle, mis nendega edasi juhtub.

Alljärgnevalt tutvustatakse valdkonnas “Riist- ja tarkvara haldus” rakendatavat meetmete kogumit:

Planeerimine ja kontseptsioon

- (L) M 2.3 Andmekandjate haldus
- (L) M 2.9 Aktsepteerimata riist- ja tarkvara kasutuse keeld
- (M) M 2.12 IT-kasutajate nõustamine
- (M) M 2.24z IT-passi juurutamine
- (L) M 2.30 Kasutajate ja kasutajarühmade määramise protseduurid
- (L) M 2.214 IT-kasutuse kontseptsioon
- (L) M 2.216 IT-komponentide kinnitamise protseduur
- (L) M 2.218 Andmekandjate ja IT-komponentide kaasavõtmise protseduurid
- (L) M 2.221 Muudatuste haldus
- (M) M 2.223 Tüüptarkvara kasutamise turvaeesmärgid
- (L) M 4.134z Sobivate andmevormingute valimine
- (L) M 4.434 Eraldiseisvate seadmete kasutamine
- (M) M 5.68z Krüpteerimisprotseduuride kasutamine võrgusuhtluses
- (M) M 5.77z Alamvõrkude rajamine
- (M) M 2.E22 Krüptograafiliste algoritmide vahetatavuse noõue

Soetamine

- (L) M 2.62 Tarkvara vastuvõtuprotseduurid

Rakendamine

- (L) M 1.29z IT-süsteemi õige paigutus
- (M) M 1.32 Printerite ja koopiamasinate turvaline paigutus
- (L) M 2.25 Süsteemi konfiguratsiooni dokumenteerimine
- (L) M 2.26 Süsteemiülema ja ta asetäitja määramine
- (M) M 2.38 Administraatorirollide jagamine
- (M) M 2.69 Tüüpsete tööjaamade rajamine
- (L) M 2.111 Juhendite käepärast hoidmine
- (L) M 2.138 Struktureeritud andmetalletus
- (L) M 2.204 Ebaturvalise võrkupääsu tõkestamine
- (L) M 4.1 IT-süsteemide paroolkaitse
- (L) M 4.7 Algparoolide muutmine
- (L) M 4.65 Uue riist- ja tarkvara testimine
- (L) M 4.84 BIOSi turvamehhanismide kasutamine
- (L) M 4.135 Süsteemifailide pääsuõiguste andmise kitsendused
- (M) M 5.87 Leping kolmandate poolte võrkudega ühendamise kohta
- (M) M 5.88 Lepingud andmevahetuse kohta kolmandate pooltega

Kasutamine

- (M) M 1.46z Vargusetõrjevahendid
- (L) M 2.10 Riistvara ja tarkvara inventuur
- (L) M 2.34 IT-süsteemi muutuste dokumenteerimine
- (L) M 2.35 Teabe hankimine turvaaukude kohta
- (L) M 2.64 Logifailide kontroll
- (L) M 2.65 IT-süsteemi kasutajate eraldatuse kontroll

- (L) M 2.110 Andmeprivaatsuse suunised logimisprotseduurides
- (L) M 2.215 Tõrkekäsitlus
- (L) M 2.219 Infotöötluse pidev dokumenteerimine
- (L) M 2.273 Turvalisust mõjutavate paikade ja värskenduste kiire paigaldamine
- (L) M 4.78 Konfiguratsioonimuudatuste hoolikas teostamine
- (L) M 4.107 Tootja ressursside kasutamine
- (L) M 4.109z Tööjaamade tarkvara reinstalleerimine
- (M) M 4.254z Juhtmeta klaviatuuri ja hiire turvaline kasutuselevõtt
- (M) M 4.306z Paroolisalvestusvahenditega ümberkäimine
- (M) M 4.345z Kaitse soovimatu infoäravoolu eest
- (M) M 5.150 Penetratsioonitestide läbiviimine

Väljavahetamine

- (M) M 2.167 Andmete kustutamine või hävitamine
- (L) M 4.234 IT-süsteemide ja andmekandjate väljavahetamise kord

Valmisolek hädaolukorraks

- (L) M 6.27 BIOS-süsteemi turvaline värskendamine

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele Kohustuslikud üldmeetmed

- HG.37 Tarkvara tervikluskontroll igal installeerimisel
- HG.38 Turvapaikade paigaldatuse regulaarseire
- HG.39 Lisanõuded tarkvara vastuvõtuprotseduuridele
- HG.54 Regulaarse turvaauditi kohustus
- HG.59 Sagedasem turvameetmete läbivaatus
- HG.81 Krüptograafilisi detaile peitva vaheteegi kasutamine
- M 2.E22 Krüptograafiliste algoritmide vahetatavuse noõue

Teabe käideldavus (K)

- HK.37 Usaldusele toetuv deponeerimine (Escrow)

Teabe terviklus (T)

- HT.3 Rakenduste ja andmete pääsuõiguste perioodiline seire
- HT.4 Sagedasem tarkvara inventuur
- HT.23 Muudatuste eelnev turvajuhi poolne kinnitamine
- HT.53 Lisanõuded paroolisalvestusvahenditele
- HT.65 Lisanõuded teisaldatavate andmekandjate kasutusele

Teabe konfidentsiaalsus (S)

- HS.11 Lisanõuded andmekandjate turvalisele kasutamisele
- HS.40 Juhtmeta klaviatuuri kasutuskeeld

- HS.51 Lisanõuded tundlike ressursside hävitamisele
- HS.56 Paroolide taastamise/uuendamise lisanõuded
- HS.74 Piirangud IT süsteemide virtualiseerimisele

B 1.10 Tüüptarkvara

Tüüptarkvara all mõistetakse tarkvara, mida turul pakutakse ning mis on üldiselt kättesaadav edasimüüjate, nt kataloogide kaudu. Iseloomulikuks asjaoluks on, et see on kasutaja poolt ise installeeritav ning et kasutajaspetsiifiliseks kohandamiseks on vajalikud vaid väikesed kulutused.

Käesolevas moodulis kujutatakse tüüptarkvara kasutamist turvalisuse seisukohast lähtudes. Seejuures võetakse vaatluse alla tüüptarkvara kogu elutsükkel: nõuete kataloogi koostamine, sobiva toote eelnev väljavalimine, testimine, evitamine, installeerimine, litsentsi haldus ja deinstalleerimine.

Tüüptarkvara arendaja kvaliteedihaldussüsteem ei kuulu käesoleva mooduli rakendusvaldkonda. Eeldatakse, et tarkvara arendamine toimus üldtuntud kvaliteedistandardite järgi.

Kirjeldatud tegutsemisviis on aluseks tüüptarkvara turvaprotsessi realiseerimiseks. Vajadusel võib käesolevas moodulis näidatud tegutsemisviisi kasutada ka võrdluseks juba juurutatud protseduuriga.

Ohud

Tüüptarkvara valdkonnas võetakse vaatluse alla alljärgnevad infoturbele mõjuvad tüüpilised ohud:

Vääramatu jõud:

- G 1.2 IT-süsteemi avarii

Organisatsioonilised puudused:

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.2 Reeglite puudulik tundmine
- G 2.3 Puuduvad, puudulikud või ühildumatud ressursid
- G 2.7 Õiguste volitamata kasutamine
- G 2.26 Ebapiisavad või puuduvad tarkvara katsetamis- ja evitusprotseduurid
- G 2.27 Ebapiisav või puuduv dokumentatsioon
- G 2.28 Autoriõiguste rikkumine
- G 2.29 Tarkvara testimine tootmisandmetega
- G 2.67 Pääsuõiguste puudulik haldus

Inimvead:

- G 3.2 Seadme või andmete hävitamine hooletuse tõttu
- G 3.3 Hooletus turvameetmete suhtes
- G 3.8 IT-süsteemi väär kasutamine
- G 3.16 Väär pääsuõiguste haldus
- G 3.17 Arvutikasutajate väär vahetumine

Tehnilised rikked:

- G 4.7 Defektsed andmekandjad

- G 4.22 Tüüptarkvara turvaaugud või vead

Ründed:

- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.9 IT-süsteemide volitamata kasutamine
- G 5.21 Trooja hobused
- G 5.23 Viirused
- G 5.43 Makroviirused

Soovitatavad meetmed

Vaadeldava IT-süsteemi turvalisuse tagamiseks tuleb lisaks käesolevale moodulile rakendada veel teisigi mooduleid vastavalt infosüsteemide etalonturbe rakendusjuhendi modelleerimise tulemustele.

Tüüptarkvaraga seonduvalt on vajalik rakendada terve rida meetmeid, alustades selle rakendamise planeerimisest, millele järgneb hankimine, ning lõpetades deinstalleerimisega. Alljärgnevalt tutvustatakse etappe, mis tuleb seejuures läbida ning meetmeid, millele teatud etappidel tuleb tähelepanu pöörata.

Planeerimine ja kontseptsioon

Enne kindla tüüptarkvara väljavalimist tuleks koostada nõuete kataloog, mille alusel saab toote objektiivsete ja selgete kriteeriumide alusel välja valida, et oleks olemas teatud usaldusväärsus, et kasutusse võetaks enam-vähem optimaalne toode. Nimetatud faasis tuleks komplekssemate toodete korral kindlaks määrata ka vastutajad nende hankimise ja töölerakendamise eest.

Soetamine

Hankimisel saab kataloogist konkreetsete spetsifikatsioonide abil kontrollida, milline müügis olevatest toodetest sobib oma funktsionaalsuselt kõige paremini.

Rakendamine

Vajalikul tasemel läbiviidud testimise abil tuleb kindlaks määrata, kas väljavalitud tootel on tõepoolest olemas dokumentatsioonis näidatud funktsionaalsus. Niivõrd kuivõrd toode on laialdaselt kasutatav, tuleb see kohandada olemasolevate installeerimismeetoditega, ning installatsioon ise tuleb dokumenteerida. Üleüldine kasutamine tohib toimuda alles seejärel, kui toode on pärast testide edukat läbimist ja ettevalmistustööde lõpetamist selleks teavitatud.

Kasutamine

Installeeritud versioonide kontroll ja olemasolevate litsentside järelkontroll ja nende võrdlus installeeritud toodete arvuga peab tüüptarkvara kasutamise ajal toimuma pidevalt.

Väljavahetamine

Tüüptarkvara puhas deinstalleerimine on tihti seotud ulatuslike ja komplekssete töödega, ulatudes üksikutel juhtudel kuni arvutite uuesti installeerimiseni.

Alljärgnevalt tutvustatakse meetmete kogumit, mida tuleb rakendada valdkonnas "Tüüptarkvara“. Olenevalt vastava tüüptarkvara liigist ja mahust, tuleb kaaluda, üksikute meetmete rakendamist vähendatud mahus. Meetmed M 2.79 Vastutuste määramine tüüptarkvara alal kuni M 2.89 Tüüptarkvara deinstalleerimine

kujutavad endast antud järjekorras ulatuslikku kirjeldust, kuidas on võimalik kujundada tüüptarkvara elutsüklit. Neid täiendavad teised nimetatud meetmed.

Planeerimine ja kontseptsioon

- (L) M 2.79 Vastutuste määramine tüüptarkvara alal
- (L) M 2.80 Tüüptarkvara nõuete kataloogi koostamine
- (L) M 2.82 Tüüptarkvara testimisplaani väljatöötamine
- (L) M 2.378z Süsteemiarendus
- (M) M 2.379z Tarkvaraarendus lõppkasutaja poolt
- (M) M 4.34z Krüpteerimise, kontrollsummade ja digitaalallkirjade rakendamine

Soetamine

- (M) M 2.66z Sertifikaatidega arvestamine IT soetamisel
- (L) M 2.81 Sobiva tüüptarkvaratoote eelvalimine

Rakendamine

- (L) M 2.83 Tüüptarkvara testimine
- (L) M 2.84 Tüüptarkvara installeerimisjuhendite otsustamine ja koostamine
- (L) M 2.85 Tüüptarkvara kinnitamine
- (L) M 2.86 Tarkvara tervikluse tagamine
- (L) M 2.87 Tüüptarkvara installeerimine ja konfigureerimine
- (M) M 2.90 Kohaletoimetuse kontroll
- (L) M 4.42z Turvafunktsioonide rakendamine IT-rakenduses

Kasutamine

- (M) M 2.88 Tüüptarkvara litsentsi- ja versioonihaldus

Väljavahetamine

- (L) M 2.89 Tüüptarkvara deinstalleerimine

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele Kohustuslikud üldmeetmed

- HG.37 Tarkvara tervikluskontroll igal installeerimisel
- HG.39 Lisanõuded tarkvara vastuvõtuprotseduuridele
- HG.59 Sagedasem turvameetmete läbivaatus

Teabe käideldavus (K)

-

Teabe terviklus (T)

- HT.54 Lisanõuded turvafunktsioonide rakendamisel
- HT.55 Värske tarkvara kasutuskeeld

Teabe konfidentsiaalsus (S)

-

B 1.11 Väljasttellimine (Outsourcing)

Väljasttellimise korral tellitakse organisatsiooni tootmis- või äriprotsesside täitmine täielikult või osaliselt välistelt teenuste pakkujatelt. Väljasttellimine võib puudutada nii riist- ja tarkvara kasutamist kui ka teenuseid. Seejuures ei ole oluline, kas teenuse osutamine toimub tellija ruumides või teenust pakkuva teenindaja töökohas. Tüüpilisteks näideteks on arvutuskeskuse, rakendusprogrammide, veebilehe või valveteenistuse töö. Väljasttellimine ehk *Outsourcing* on üldmõiste, mida tihtipeale täiendavad veel teised mõisted: *Tasksourcing* tähistab osade valdkondade väljastpoolt teenindamist. Kui osutatakse infoturbealaseid teenuseid, räägitakse mõistetest *Security Outsourcing* või *Managed Security Services* (hallatavad turvateenused). Näideteks on tulemüüri, võrgu monitooringu, viirusetõrje või virtuaalse privaatvõrgu (VPN) töö. *Application Service Provider* (ASP) (rakendusteenuste pakkuja) all mõistetakse teenusepakkujat, kes tegeleb omaenese süsteemidel üksikute rakendusteenuste või tarkvara tarnimisega oma klientidele (e-post, SAP rakendused, arhiveerimine, veebikaubandus, soetamine). Tellijad ja teenustepakkujad on seejuures teineteisega interneti või VPN võrgu kaudu ühenduses. *Application Hosting* (rakendusmajutus) korral toimub rakendusteenuste tellimine teenusepakkujalt, siiski kuuluvad vastupidiselt ASP mudelile rakendused vastavatele klientidele. Kuna klassikalise väljasttellimise ja puhta rakendusteenuste pakkuja (ASP) piirid sulavad praktikas üha enam kokku, kasutatakse alljärgnevalt veel vaid põhimõistet “Väljasttellimine” (*Outsourcing*).

Äri- ja tootmisprotsesside väljasttellimine on tänapäeva organisatsiooniliste strateegiate kindlaksmääratud koostisosa. Viimastel aastakümnetel on väljasttellimise trend tohutult tõusnud ning see näib jätkuvat ka tulevikus. Aga on ka olemas juba avalikustatud näiteid nurjunud väljasttellimise projektidest, kus tellija ütles väljasttellimise lepingu üles ning teostab tellitud toimingud taas oma ettevõttes (*Insourcing*).

Väljasttellimise põhjuseid on mitmeid: organisatsiooni keskendumine oma põhikompetentsidele, võimalus kulude kokkuhoiuks (nt kokkuhoid IT-süsteemide hanke- ja käitamiskuludelt), juurdepääs spetsiaalsetele teadmistele ja ressurssidele, sisemiste ressursside vabanemine teiste ülesannete täitmiseks, sisehalduse rangemaks muutmine, äri- ja tootmisprotsesside parem skaleeritavus, paindlikkuse tõus ning organisatsiooni konkurentsivõimelisus on vaid mõned näited.

IT-le tuginevate organisatsiooniliste protsesside väljasttellimisel on teenuseid tellivate organisatsioonide ja nende välise teenuste pakkuja IT-süsteemid ja võrgud reeglina üksteisega tihedalt seotud, nii et sisemised toimingud kulgevad osaliselt välise teenustepakkuja juhtimise ja kontrolli all. Ka personali tasemel toimub intensiivne suhtlus.

Tihe seotus teenustepakkujaga ja tekkiv sõltuvus teenuste kvaliteedist kujutavad endast ohuallikaid teenuste tellijale, mille tõttu halvimal juhul võivad oluliselt kahjustatud saada isegi ettevõtte või asutuse äritegevuse alused. (Näiteks võib organisatsiooni konfidentsiaalne info tahtlikult või tahtmatult välja imbuda.) Väljasttellimise korral tuleb suurt tähtsust omistada turvaaspektide ja lepinguliste kokkulepete kujundamisele teenuste tellija ja teenuste pakkuja vahel.

Käesoleva mooduli keskmes on meetmed, mille sisuks on väljasttellimise IT alased turvaaspektid. Siia kuuluvad ka sobivad meetmed lepinguliste eesmärkide ja teenuste kontrollimiseks ning IT alased turvameetmed.

Ohud

Väljasttellimise projektist lähtuvad ohud on silmnähtavalt mitmetahulised. Otsus mingi spetsiaalse tegevuse väljasttellimise kohta mõjutab kestvalt organisatsiooni strateegilist orientatsiooni, selle põhikompetentside määratlemist, väärtusloome keti kujundamist ning puudutab paljusid teisi olulisi organisatsiooni haldamise vajadusi. Vajalik on teha suuri jõupingutusi, et õigeaegselt ära tunda ja takistada ettevõtte või asutuse väärarenguid.

Ohud võivad eksisteerida paralleelselt nii füüsilisel, tehnilisel kui ka inimlikul tasandil ning on alljärgnevalt jagatud vastavate ohtude kataloogidesse. Et eksisteerivaid ohtusid kvantitatiivselt hinnata, tuleb kõigepealt hinnata ja klassifitseerida organisatsioonile omased väärtused ja info vastavalt nende strateegilisele tähendusele organisatsiooni jaoks.

Vääramatu jõud:

- G 1.10 Laivõrgu tõrge

Organisatsioonilised puudused:

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.7 Õiguste volitamata kasutamine
- G 2.26 Ebapiisavad või puuduvad tarkvara katsetamis- ja teavitusprotseduurid
- G 2.47 Failide ja andmekandjate ebaturvaline transport
- G 2.66 Puudulik infoturbehaldus
- G 2.67 Pääsuõiguste puudulik haldus
- G 2.83 Halb väljasttellimise strateegia
- G 2.84 Puudused välisteenusepakkujaga sõlmitud lepingu tingimustes
- G 2.85 Halvad väljast tellitud projekti lõpetamise sätted
- G 2.86 Sõltuvus välisteenusepakkujast

- G 2.88 Väljast tellitava projekti negatiivne mõju organisatsiooni sisekliimale
- G 2.89 Puudulik infoturve väljasttellimise sissejuhatavas etapis
- G 2.93 Puudulik jätkusuutlikkuse planeerimine väljasttellimise korral

Inimvead:

- G 3.1 Andmete konfidentsiaalsuse või tervikluse kadu kasutaja vea tõttu
- G 3.105 Väliste teenuste volitamata kasutamine

Tehnilised rikked:

- G 4.33 Autentimise puudumine või puudulikkus
- G 4.34 Krüptomooduli rike
- G 4.48 Välisteenusepakkuja süsteemide rike
- G 4.97 Välisteenuse osutajaga seotud kitsaskohad

Ründed:

- G 5.10 Kaughooldeportide väärkasutus
- G 5.20 Administraatori õiguste väärkasutus
- G 5.42 Inimestega manipuleerimine (Social Engineering)
- G 5.71 Tundliku informatsiooni konfidentsiaalsuse kadu
- G 5.85 Tundliku informatsiooni tervikluse kadu
- G 5.107 Välisteenusepakkuja poolne andmete paljastamine kolmandatele isikutele

Soovitatavad meetmed

Vaadeldava IT-süsteemi turvalisuse tagamiseks tuleb lisaks käesolevale moodulile rakendada veel teisigi mooduleid vastavalt infosüsteemide etalonturbe rakendusjuhendi modelleerimise tulemustele.

Väljastpoolt teenuseid tarniv IT-süsteem võib koosneda nii komponentidest, mis paiknevad eranditult välise teenusetarnija valduses, kui ka teenuse tellija valduses asuvatest komponentidest. Reeglina on seejuures olemas liidesed süsteemide ühendamiseks. Iga osasüsteemi ja iga liidesefunktsiooni jaoks peab olema garanteeritud infoturve.

Väljasttellimise projekt koosneb paljudest faasidest.

Faas 1: Väljasttellimise strateegiline planeerimine

Juba strateegilise otsustamise käigus, kas ja millises vormis väljasttellimise projekt realiseeritakse, on vajalik välja töötada turvalisuse seisukohalt tähtsad seisukohad. Meetmes M 2.250 Väljasttellimise strateegia määramine tutvustatakse tähtsamaid aspekte, millele tuleb tähelepanu pöörata.

Faas 2: Oluliste turvanõuete spetsifitseerimine

Kui otsus väljasttellimise kasuks on langetatud, tuleb kindlaks määrata väljasttellimisprojektide turvalisuse seisukohalt olulised nõuded. Kõne all olevad turvanõuded on hanke väljakuulutamise aluseks. (vt M 2.251 Väljasttellimisprojektide turvanõuete spetsifitseerimine).

Faas 3: Väljasttellitava teenuse tarnija valimine

Väljasttellitava teenuse tarnija valimine on suure tähtsusega (vt M 2.252 Väljasttellitava teenuse sobiva tarnija valimine).

Faas 4: Lepingu koostamine

Funktsionaalsete spetsifikatsioonide baasil tuleb partneriga sõlmida leping, millega määratakse kindlaks soovitud teenused koos kvaliteedistandardiga ja tähtaegadega, mis on kooskõlas kehtiva seadusandlusega. Neid lepinguid nimetatakse tihti *Service Level Agreements* (SLA) ehk teenustaseme lepinguteks. Kõnealuses lepingus peavad olema välja toodud ka täpsed koostööd puudutavad üksikasjad: kontaktisikud, reageerimisajad, IT-süsteemide ühendamine, teenuste kontroll, IT turvameetmete kujundamine, konfidentsiaalsete andmetega ümberkäimine, kasutusõigused ja andmete edasiandmine kolmandatele osapooltele (vt ka M 2.253 Välise teenusepakkujaga sõlmitava lepingu koostamine).

Faas 5: IT turvakontseptsiooni koostamine väljastpoolt teenindatavale IT-süsteemile

Tellija ja väliste teenuste tarnija peavad tihedas koostöös koostama detailse turvakontseptsiooni (M 2.254 Väljast tellitud projektile infoturbekontseptsiooni loomine), mis sisaldab ka valmisolekut hädaolukorraks(M 6.83 Väljasttellimise avariiplaan).

Faasis 5 saab reeglina kokku leppida alles pärast migratsioonifaasi lõpetamist, kuna IT-süsteemide ja rakenduste migratsiooni ajal avastatakse üha uusi aspekte, mida tuleks IT turvakontseptsiooni sisse viia.

Faas 6: Migratsioonifaas

Eriti turvakriitiline on migratsiooni- või üleviimisfaas, mille planeerimine peab olema väga hoolikas (vt M 2.255 Turvaline üleviimine väljast tellitud projektides).

Faas 7: Jooksva töö planeerimine ja tagamine

Kui väliste teenuste tarnija on üle võtnud süsteemid või tegevusprotsessid, on infoturbe käigushoidmiseks väljasttellimistegevuste ajal vajalikud erinevad meetmed nagu süsteemihoolduse regulaarne kontroll ja läbiviimine (vt M 2.256 Infoturbe planeerimine ja käigushoidmine väljasttellimise tegevuste ajal). Need tuleb eelnevalt planeerida. Planeerimisse tuleb kindlasti kaasata ka hädaolukorra- ja eskalatsioonistsenaariumid.

Alljärgnevalt tutvustatakse valdkonnas “Väljasttellimine” (Outsourcing) rakendatavat meetmete kogumit.

Planeerimine ja kontseptsioon

- (M) M 2.40z Töötajate esinduse õigeaegne kaasamine
- (M) M 2.42 Võimalike suhtluspartnerite määramine

- (L) M 2.221 Muudatuste haldus
- (M) M 2.226 Asutusevälise personali kasutamise protseduurid
- (L) M 2.250 Väljasttellimise strateegia määramine
- (L) M 2.251 Väljasttellimisprojektide turvanõuete spetsifitseerimine
- (L) M 2.254 Väljast tellitud projektile infoturbekontseptsiooni loomine

Soetamine

- (L) M 2.252 Väljasttellitava teenuse sobiva tarnija valimine

Rakendamine

- (L) M 2.253 Välise teenusepakkujaga sõlmitava lepingu koostamine
- (L) M 2.255 Turvaline üleviimine väljast tellitud projektides
- (M) M 2.460 Väliste teenuste reguleeritud kasutamine
- (M) M 3.33z Personali taustakontroll
- (L) M 5.87 Leping kolmandate poolte võrkudega ühendamise kohta
- (L) M 5.88 Lepingud andmevahetuse kohta kolmandate pooltega

Kasutamine

- (L) M 2.256 Infoturbe planeerimine ja käigushoidmine väljasttellimise tegevuste ajal

Ressursside väljavahetamine

- (L) M 2.307 Väljasttellimissuhte nõuetekohane lõpetamine

Valmisolek hädaolukorraks

- (M) M 6.109 Virtuaalse privaatvõrgu (VPN) hädaolukorraks valmisoleku plaan
- (L) M 6.83 Väljasttellimise avariiplaan

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele Kohustuslikud üldmeetmed

- HG.18 Leppetrahvid tarnijatega tehtavatesse lepingutesse
- HG.20 Taustauuring personali palkamisel
- HG.36 Väljasttellimise avariiplaani regulaarne läbivaatus

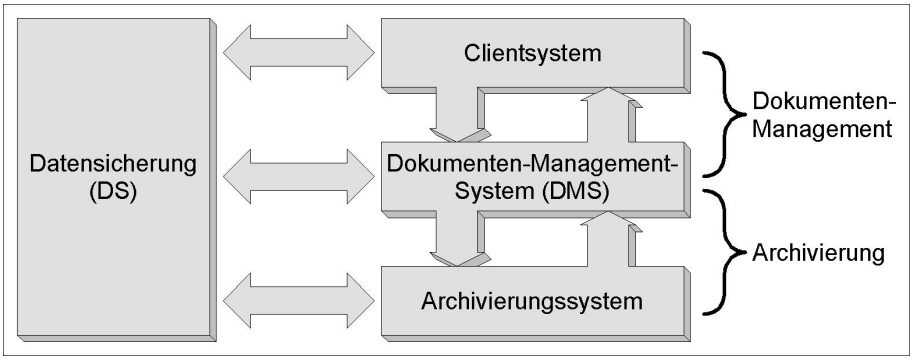
Teabe käideldavus (K)
-
Teabe terviklus (T)
-
Teabe konfidentsiaalsus (S)
-

B 1.12 Arhiveerimine

Tegevusprotsesside ja –aluste dokumenteerimine elektroonilisel kujul eeldab sobiva arhiivi olemasolu, tagamaks salvestatud andmete hilisemat kasutamist, ülesleidmist ja kättesaadavaks tegemist. See puudutab nii andekogumeid kui ka paberkandjal dokumentide ja tõendite elektroonilisi kujutusi. Elektrooniliste dokumentide ja teiste andmete pikaajalist ja muutumatul kujul salvestamist nimetatakse arhiveerimiseks.

Arhiveerimine on üks osa dokumentide haldusprotsessist. Lisaks elektrooniliste dokumentide koostamisele, töötlemisele ja haldamisele omab suurt tähtsust ka pikaajaline salvestamine (arhiveerimine), sest tavaliselt oodatakse, et dokumendid oleksid mingi kindla säilitamistähtaja lõpuni kättesaadavad ning et nende konfidentsiaalsus ja terviklus säiliksid. Teatud juhtudel peavad elektroonilised dokumendid olema piiramatu ajani kättesaadavad.

Nimetatud protsessi tehniline väljaarendamine toimub dokumendihaldus- ja arhiveerimissüsteemide abil (vt joonist). Käesolevas moodulis vaadeldakse eranditult vaid elektroonilisi arhiveerimissüsteeme.



Joonis: Arhiveerimise tehniline väljaarendamine dokumendihaldus- ja arhiivisüsteemide abil.

Joonis: Datensicherung (DS) – andmevarundus, Clientsystem – kliendisüsteem, Dokumenten-Managment-System (DMS) – dokumendihaldussüsteem, Archivierungssystem – arhiveerimissüsteem, Dokumenten-Management – dokumendihaldus, Archivierung – arhiveerimine.

Ühe sellise arhiivisüsteemi realiseerimisvõimalused hõlmavad:

- väikeseid arhiivisüsteeme, nt mis koosnevad ühest arhiiviserverist, mis on ühendatud mäluseadmete massiivsüsteemiga (nagu kõvaketas või jukebox ehk plaadiautomaat),

- kuni komplekssete, teatud juhtudel ülemaailmselt jaotatud arhiivisüsteemideni tähtsate äriandmete üleorganisatsiooniliseks arhiveerimiseks, mis koosnevad:
- tsentraalsetest RAID-süsteemidega arhiiviserveri komponentidest, jukeboxidest või ühendamisest Storage Area Networks (SAN) süsteemiga andmepankade keskseks salvestamiseks,
- WORM-andmekandjatest andmete vaatamiskindlaks ja muutmatuks salvestamiseks,
- komponentidest, mis on ette nähtud andmete indeksseerimiseks, kogumiseks ja salvestusvormingute muutmiseks (Rendition),
- detsentraalsetest puhverserveritest kiireks ligipääsuks tihti vajaminevatele andmetele,
- klienditarkvarast, mis võimaldab otsest juurdepääsu arhiivi andmetele (nt ka Office 'i rakenduste kaudu).

Otstarbekas on eraldada elektroonilised arhiivid andmevarundussüsteemidest. Andmete varundamisel seatakse sisse süsteemi- ja haldusandmete koopiad. Varundatud andmed eraldatakse seejuures füüsiliselt IT-süsteemist ning säilitatakse turvaliselt. Elektroonilised arhiivid seevastu on reeglina ühenduses töötava süsteemiga. Seejuures jäetakse tavaliselt kõrvale terve hulk haldusandmeid (elektroonilised dokumendid), mida on elektroonilisest arhiivisüsteemist alati võimalik kätte saada. Spetsiaalse ülesehituse korral (nt salvestuskomponentide üleliigne tõlgendamine ning vastav ruumiline korraldus) võivad suuremad arhiivisüsteemid osaliselt üle võtta andmevarunduse funktsiooni (haldusandmed).

Käesolevas moodulis tuleb süstemaatiliselt välja tuua, kuidas peab toimuma elektroonilise arhiveerimise kontseptsiooni koostamine ning kuidas peab toimuma selle ülesehitamise ja sisseseadmise kindlustamine ettevõttes või asutuses. Nimetatud kontspetsiooni koostamise ja realiseerimise kulud ei ole väikesed. Käesolevat moodulit peaks rakendama alati, kui arhiveeritavad andmed on asutusele või ettevõttele pikaajaliselt suure tähtsusega.

Ohud

Elektrooniliseks arhiveerimiseks kasutatavad arhiivisüsteemid ning nendega kaasnevad organisatsioonilised protsessid on mõjutatavad alljärgnevatest infoturbealastest tüüpilistest ohtudest:

Vääramatu jõud:

- G 1.2 IT-süsteemi avarii
- G 1.7 Lubamatu temperatuur ja niiskus
- G 1.9 Tugevast magnetväljast tingitud andmekadu
- G 1.14 Tugevast valgusest tingitud andmekadu

Organisatsioonilised puudused:

- G 2.7 Õiguste volitamata kasutamine
- G 2.72 Arhiivisüsteemide üleviimise puudused

- G 2.73 Arhiivisüsteemide puudulikud kontrolljäljed
- G 2.74 Arhiivide indekseerimisvõtmete puudused
- G 2.75 Arhiivi salvestuskandjate ebapiisav maht
- G 2.76 Arhiivipöörduste puudulik dokumenteerimine
- G 2.77 Paberdokumentide elektroonilise arhiveerimise puudused
- G 2.78 Arhiveeritud andmestike regenereerimise puudused
- G 2.79 Arhiivisäilikute digitaalsignatuuride regenereerimise puudused
- G 2.80 Arhiveerimisprotseduuride puudulik auditeerimine
- G 2.81 Arhiivi andmekandjate puudulik hävitamine
- G 2.82 Arhiivisüsteemi asukoha halb planeerimine

Inimvead:

- G 3.1 Andmete konfidentsiaalsuse või tervikluse kadu kasutaja vea tõttu
- G 3.16 Väär pääsuõiguste haldus
- G 3.35 Töötava serveri elektritoite väljalülitamine
- G 3.54 Ebasobiva andmekandja kasutamine arhiveerimiseks
- G 3.55 Õiguslike raamtingimuste rikkumised arhiivsüsteemide kasutamisel

Tehnilised rikked:

- G 4.7 Defektsed andmekandjad
- G 4.13 Salvestatud andmete hävimine
- G 4.20 Andmekadu andmekandja täitumise tõttu
- G 4.26 Andmebaasi rike
- G 4.30 Andmebaasi tervikluse ja vastavuse kadu
- G 4.31 Võrgukomponentide rike või tõrge
- G 4.45 Arhiivipäringute hilinemine
- G 4.46 Indeksiandmete väär sünkroniseerimine arhiveerimisel
- G 4.47 Vananenud krüptomeetodid

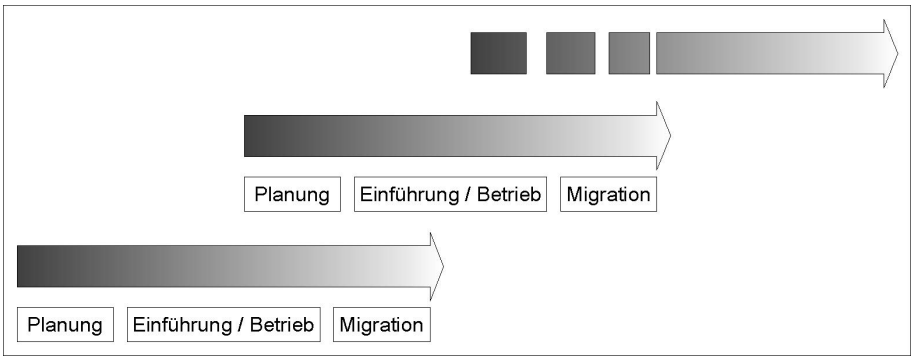
Ründed:

- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.6 Füüsiline rünne
- G 5.29 Andmekandjate volitamata kopeerimine
- G 5.82 Krüptomooduli manipulatsioon
- G 5.83 Krüptograafiliste võtmete paljastamine
- G 5.85 Tundliku informatsiooni tervikluse kadu
- G 5.102 Sabotaaž
- G 5.105 Arhiivisüsteemi teenuste halvamine
- G 5.106 Arhiivi andmekandjate volitamata ülekirjutamine ja kustutamine

Soovitatavad meetmed

Vaadeldava IT-süsteemi turvalisuse tagamiseks tuleb lisaks käesolevale moodulile rakendada veel teisigi mooduleid, vastavalt infosüsteemide etalonturbe rakendusjuhendi modelleerimise tulemustele.

Lisaks soovitatakse elektrooniliste arhiivisüsteemide sisseseadmiseks ja käigushoidmiseks alljärgnevalt kirjeldatud tegutsemisviisi. Juba planeerimisel tuleb pöörata tähelepanu asjaolule, et kasutatavad arhiivisüsteemid ja andmekandjad vananevad aja jooksul tehnoloogiliselt ja füüsiliselt. Seepärast järgneb planeerimis- ja rakendamis/käigushoidmisfaasile migratsioonifaas, milles olemasolev arhiivisüsteem või selle osad asendatakse uue tehnoloogia ja uute komponentidega. Migratsioonifaas hõlmab ka arhiveeritud andmete ja dokumentide ülekandmist tulevikus kasutatavatesse andmevormingutesse.



Joonis: Migratsioonifaaside planeerimine arhiveerimissüsteemi planeerimise käigus.

Joonis: Planung – planeerimine, Einführung / Betrieb – Realiseerimine / käigushoidmine, Migration - migratsioon

Alljärgnevalt selgitatakse lühidalt üksikuid faase ning nende käigus rakendatavaid abinõusid.

1. Planeerimisfaas

Planeerimisfaasis tuleb määratleda eesmärgid, mis on seotud arhiivisüsteemi töösserakendamisega (vt M 2.242 Elektroonilise arhiveerimise eesmärkide määratlemine). Seejuures on vaja kindlaks teha tähtsad organisatsioonilised, õiguslikud ja tehnilised nõuded, kusjuures tuleb ka ette näha, kuidas nõuded töösserakendatava arhiivisüsteemi oodatava käigusoleku aja jooksul arenevad (vt M 2.244 Elektroonilise arhiveerimise tehniliste tegurite väljaselgitamine , M 2.245 Elektroonilise arhiveerimise õiguslike tegurite väljaselgitamine ja M 2.246 Elektroonilise arhiveerimise organisatsiooniliste tegurite väljaselgitamine). Tulemused tuleb kirja panna arhiveerimiskontseptsioonis (vt M 2.243 Arhiveerimiskontseptsiooni väljatöötamine).

2. Rakendamine ja käigushoidmine

Arhiivisüsteemi töösserakendamisel tuleb kõigepealt valida süsteem, mis vastab kindlaksmääratud tingimustele. Lisaks sellele tuleb kindlasti määrata süsteemi asukoht ning arhiivi andmekandjate säilituskoht (vt M 4.168 Sobiva arhiivisüsteemi valimine , M 4.169 Sobiva arhiveerimis-andmekandja valimine , M 4.170 Dokumentide arhiveerimiseks sobivate andmevormingute valimine , M 1.59 Arhiivisüsteemide asjakohane rajamine ja M 1.60 Arhiivi-andmekandjate asjakohane säilitus).

Lisaks arhiivisüsteemile tuleb arhiivi sisu haldamiseks sisse viia sobiv üldine dokumentide haldussüsteem (vt M 2.258 Dokumentide järjekindel indekseerimine arhiveerimisel ja M 2.259 Üldise dokumendihaldussüsteemi kasutuselevõtt).

Kindlaks tuleb määrata reeglid nii arhiivisüsteemi kui ka digitaalsete allkirjade kasutamiseks ning koolitada välja süsteemiülemad ja kasutajad (vt M M 2.262 Arhiivisüsteemide kasutamise reguleerimine , M 2.265 Digitaalallkirjade õige kasutamine arhiveerimisel , M 3.34 Arhiivisüsteemi haldamise koolitus ja M 3.35 Arhiivisüsteemi kasutamise koolitus kasutajatele).

Reeglitele vastavuse pikaajaliseks säilitamiseks tuleb arhiveerimisprotsessi hoida pideva järelevalve all ning kontrollida selle korrektsust (vt M 2.257 Arhiveerimisandmekandja salvestusressursside seire , M 2.260 Arhiveerimisprotseduuri regulaarne auditeerimine , M 2.263 Arhiveeritud andmeressursside regulaarne regenereerimine , M 4.171 Arhiivisüsteemi indeksiandmebaasi tervikluse kaitse , M 4.172 Arhiivipöörduste logimine ja M 4.173 Arhiveerimise regulaarsed talitlus- ja taastetestid).

Sõltuvalt konkreetsest rakendatud arhiivitarkvarast tuleb rakendada ka moodulis B 5.7 Andmebaasid kirjeldatud meetmeid.

3. Migratsioonifaas

Migratsioonifaasi põhjustavad tihti alljärgnevad sündmused:

- On toimunud süsteemikomponentide või andmevormingute tehnoloogia vahetus, seepärast tuleks selles valdkonnas toimuvatele arengutele tähelepanu pöörata (vt M 2.261 Regulaarsed arhiivisüsteemide turu-uuringud).
- Süsteemi komponendid, eriti andmekandjad, on vananenud ning tuleb uute vastu välja vahetada (vt M 2.266 Arhiivisüsteemi tehniliste komponentide regulaarne asendamine)
- Arhiivisüsteemi kasutustingimused on muutunud.
- Krüptoprotseduurid, -tooted või -võtmed (vt M 2.264 Krüpteeritud andmete regulaarne regenereerimine arhiveerimisel).

Alljärgnevalt tutvustatakse meetmete kogumit elektroonilise arhiivisüsteemi töösserakendamiseks:

Planeerimine ja kontseptsioon

- (L) M 2.242 Elektroonilise arhiveerimise eesmärkide määratlemine
- (L) M 2.243 Arhiveerimiskontseptsiooni väljatöötamine
- (L) M 2.244 Elektroonilise arhiveerimise tehniliste tegurite väljaselgitamine
- (L) M 2.245 Elektroonilise arhiveerimise õiguslike tegurite väljaselgitamine
- (L) M 2.246 Elektroonilise arhiveerimise organisatsiooniliste tegurite väljaselgitamine
- (M) M 2.259z Üldise dokumendihaldussüsteemi kasutuselevõtt
- (L) M 2.262 Arhiivisüsteemide kasutamise reguleerimine
- (M) M 2.265z Digitaalallkirjade õige kasutamine arhiveerimisel

Soetamine

- (M) M 4.168 Sobiva arhiivisüsteemi valimine
- (M) M 2.169 Süsteemihalduse strateegia väljatöötamine

- (M) M 4.170 Dokumentide arhiveerimiseks sobivate andmevormingute valimine

Rakendamine

- (L) M 1.59 Arhiivisüsteemide asjakohane rajamine
- (L) M 2.266 Arhiivisüsteemi tehniliste komponentide regulaarne asendamine
- (L) M 3.34 Arhiivisüsteemi haldamise koolitus
- (L) M 3.35 Arhiivisüsteemi kasutamise koolitus kasutajatele

Kasutamine

- (L) M 1.60 Arhiivi-andmekandjate asjakohane säilitus
- (L) M 2.257 Arhiveerimis-andmekandja salvestusressursside seire
- (L) M 2.258 Dokumentide järjekindel indekseerimine arhiveerimisel
- (M) M 2.260 Arhiveerimisprotseduuri regulaarne auditeerimine
- (M) M 2.261 Regulaarsed arhiivisüsteemide turu-uuringud
- (L) M 2.263 Arhiveeritud andmeressursside regulaarne regenereerimine
- (M) M 2.264 Krüpteeritud andmete regulaarne regenereerimine arhiveerimisel
- (L) M 4.171 Arhiivisüsteemi indeksiandmebaasi tervikluse kaitse
- (L) M 4.172 Arhiivipöörduste logimine
- (M) M 4.173 Arhiveerimise regulaarsed talitlus- ja taastetestid

Valmisolek hädaolukorraks

- (L) M 6.84 Süsteemi- ja arhiiviandmete regulaarne varundamine

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

-

Teabe käideldavus (K)

- HK.12 Arhiveerimisel kasutatavate andmekandjate taustauuring
- HK.13 Arhiveerimisel kasutatavate andmekandjate regulaarkontroll
- HK.14 Arhiivketta salvestusressursside kaugindikatsioon
- HK.15 Lisanõuded arhiveerimisprotsessi auditeerimisele
- HK.38 Krüptograafiliste algoritmide kasutuskataloog

Teabe terviklus (T)

- HT.31 Arhiveerimisel kasutatavate andmekandjate regulaarkontroll
- HT.34 Digiallkirja kasutamine
- HT.49 Lisanõuded arhiveeritud andmete krüptoatribuutide regenereerimisele
- HT.65 Lisanõuded teisaldatavate andmekandjate kasutusele

Teabe konfidentsiaalsus (S)

- HS.51 Lisanõuded tundlike ressursside hävitamisele
- HS.76 Mobiilsete andmekandjate võimalik vältimine

B 1.13 Infoturbe teadlikkus ja -koolitus

Kirjeldus

Selles meetmes kirjeldatakse, kuidas tuleb ettevõttes või asutuses luua infoturbe ohtusid käsitlev teavitus- ja koolitusprogramm ning kuidas seda programmi töös hoida.

Et infoturbe meetmeid efektiivselt rakendada, tuleb ettevõttes või asutuses luua infoturbekultuur ning tõsta infoturbeteadlikkust. Kõik töötajad peavad olema veendunud, et infoturve on iga organisatsiooni edu üheks oluliseks teguriks. Selle juurde kuulub ka selgitustöö, miks teatud kindlate infoturbemeetmete rakendamine on tähtis ja otstarbekohane. Samuti peavad kõik töötajad olema teadlikud, mida nendelt infoturbe vallas oodatakse ning kuidas nad turvakriitilises situatsioonis reageerima peavad. See eeldab paljudes valdkondades töötajate ajapikku hoiakute muutumist ning seda on võimalik saavutada vaid pikaajalise ja katkematu protsessi tulemusena. Ühekordsest koolitusest ja teadvustamisest siin ei piisa.

Vajaliku teabe ja oskuste edasiandmiseks tuleb võrdsel määral tegelda nii teavituse kui ka koolitamisega. Turbealase teavitustöö eesmärk on suurendada töötajate teadlikkust selle kohta, millised olukorrad võivad olla turbe jaoks kriitilised ning millised on nende võimalikud tagajärjed. Infoturbealastel koolitustel peaksid kõik töötajad omandama vajalikud teadmised ja oskused, kuidas vastavates olukordades õigesti toimida.

Informeeritud ja koolitatud töötajad on eelduseks, et asutus või ettevõtte saavutaks püstitatud eesmärgid. Peale selle tagatakse informeerimise ja koolituse kaudu, et kõik töötajad oskaksid hinnata oma tegevuse tagajärgi ning mõju tööalases ja isiklikus sfääris. Infoturbealase teadvustamise eesmärgiks on töötajate teadlikkuse tõstmine infoturbealaste probleemide vallas. Infoturbekoolituste kaudu antakse töötajatele vajalikud infoturbealased oskused, mida nad vajavad oma tööülesannete täitmisel. Garanteerida tuleb, et kõik töötajad tunneksid protseduure, ning teaksid, kelle poole nad peavad pöörduma, kui tekivad turvaprobleemid või kui tuleb lahendada turvaprobleeme.

Et koolitus- ja teadvustusmeetmete rakendamine leiaks pidevat toetust, on tähtis, et pööratakse juhtkonna tähelepanu infoturbe tähtsusele. Käesolev moodul on mõeldud põhimõtteliselt kõigile, kes on vastutavad asutuse (ükskõik kui suure) infoturbe eest.

Käesolevas moodulis kirjeldatakse, kuidas peaks toimuma efektiivse infoturbe-

alase koolitus- ja teadvustusprogrammi loomine ja alalhoidmine.

Ohud

Käesolevas moodulis käsitletakse alljärgnevaid infoturvet mõjutavaid tüüpilisi ohtusid:

Organisatsioonilised puudused:

- G 2.2 Reeglite puudulik tundmine
- G 2.7 Õiguste volitamata kasutamine
- G 2.102 Inimeste infoturbeteadlikkuse ebapiisav suurendamine
- G 2.103 Töötajate ebapiisav koolitamine
- G 2.105 Õigusaktide ja lepinguliste kokkulepete rikkumine
- G 2.141 Märkamata jäänud turvaintsidendid
- G 2.201 Ebapiisav arvestamine töökeskkonnas aset leidnud muudatustega

Inimvead:

- G 3. 1 Andmete konfidentsiaalsuse või tervikluse kadu kasutaja vea tõttu
- G 3.3 Hooletus turvameetmete suhtes
- G 3.8 IT-süsteemi väär kasutamine
- G 3.9 IT-süsteemi väär haldus
- G 3.44 Teabe hooletu kasutamine
- G 3.77 Infoturbe vähene aktsepteerimine

Ründed:

- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.9 IT-süsteemide volitamata kasutamine
- G 5.19 Kasutajaõiguste väärkasutus
- G 5.20 Administraatori õiguste väärkasutus
- G 5.42 Inimestega manipuleerimine (Social Engineering)
- G 5.102 Sabotaaž
- G 5.104 Infoluure

Soovitatavad meetmed

Vaadeldava IT-koosluse turvalisuse tagamiseks tuleb lisaks käesolevale moodulile rakendada veel teisigi mooduleid vastavalt infosüsteemide etalonturbe rakendusjuhendi modelleerimise tulemustele.

Teavitus- ja koolitusprogramm peab arvestama organisatsiooni eripärade, valitseva töökultuuri (vt M 3.83z Personaliga seotud turbefaktorite analüüs) ja vajaliku turbeastmega. Eesmärgi saavutamiseks tuleks kasutada võimalikult erinevaid, kuid üksteisega hästi kokkusobitatud meetodeid ja infoedastuslahendusi.

Planeerimine ja kontseptsioon

Turbeprotsessi jaoks on väga oluline, et sellel oleks pidev ja aktiivne juhatuse toetus. Selleks peab juhatus mõistma infoturbe tähendust seoses organisatsiooni eesmärkide saavutamisega (vt M 3.44 Juhtkonna teadlikkuse tõstmine infoturbe

alal). Juhatusepoolseid abistavaid tegevusi teavitus- ja koolitusprogrammi järjepidevuse tagamise osas kirjeldatakse meetmes M 3.96 Juhatuse tugi teavitusele ja koolitusele .

Toetav tegevus võib alata nt sellega, et antakse käsk asjakohaste kontseptsioonide väljatöötamiseks. Vajalikke samme kirjeldatakse meetmetes M 2.312 Infoturbealase koolitus- ja teavitusprogrammi kavandamine ja M 2.557 Infoturbealase koolitusprogrammi kontseptsioon . Eriti oluline on siinkohal määratleda vastavad sihtrühmad (vt M 3.93 Teavitus- ja koolitusprogrammide sihtrühmade analüüs).

Soetamine

Teavitus- ja koolitusmeetmete ettevalmistamiseks ja läbiviimiseks on tarvis koolituspersonali kas organisatsiooni seest või väljastpoolt organisatsiooni (vt M 3.48z Koolitajate või koolitusfirmade valimine).

Rakendamine

Rakendamise etapis jagatakse koolitajate vahel ära eelnevalt määratletud sihtrühmad ning valitakse välja teavitus- ja koolitusprogrammides kasutatavad materjalid (vt M 3.45 IT-turbealaste koolituste sisu kavandamine). Lisaks tuleb võtta meetmeid, mis aitavad töötajatele meelde tuletada kontaktisikuid, kelle poole turbeküsimustes pöörduda (vt M 3.46 Kontaktisik turvalisuse alal).

Koolitus- ja teadvustusmeetmete realiseerimiseks vajatakse mitmesuguseid ressursse, nt personali, sobivaid ruume ja spetsiaalset varustust. Koolitusruumide spetsiaalseid turvaaspekte käsitletakse lähemalt moodulis B 2.11 Nõupidamis-, üritus- ja koolitusruumid .

Protsessi tööshoidmine ning pidev uuendamine ja edasiarendamine

Koolituste sisu edukaks edasiandmiseks tuleb kasutada sobivaid metoodikaid ja andmeedastuskanaleid (vt M 2.198 Personali evitamine infoturbe küsimustest ja M 3.47z IT-turbealased tegevus- ja rollimängud).

Infoturvet käsitelevatel koolitustel on olulisel kohal ka infotehnoloogia kasutamine (vt M 3.26 Personali juhendamine IT-vahendite turvalise kasutamise kohta). Eriti oluline on teavitada ja koolitada töötajaid tehnoloogia kasutamise ning selle võimalike ohtude ja turbemeetmete osas enne seda, kui organisatsioon võtab kasutusele mõne uue tehnoloogia.

Koolituste käigus käsitletavate teemade paremaks meeldejäämiseks saab rakendada õppematerjali kinnistamise meetodeid (vt M 3.95z Õppematerjali kinnistamine). Samuti tuleks regulaarselt kontrollida, kas teavitus- ja koolitusmeetodid on piisavalt tõhusad (vt M 3.94 Õpitulemuste edukuse mõõtmine ja hindamine). Vajaduse korral tuleb teha asjakohased kohandused.

Planeerimine ja kontseptsioon

- (L) M 2.312 Infoturbe alase koolitus- ja teavitusprogrammi kavandamine
- (L) M 2.557 Infoturbealase koolitusprogrammi kontseptsioon
- (L) M 3.44 Juhtkonna teadlikkuse tõstmine infoturbe alal
- (L) M 3.51z Personali rakendamise ja kvalifitseerimise kontseptsioon
- (L) M 3.53w Sissejuhatus SAP süsteemidesse
- (L) M 3.93 Teavitus- ja koolitusprogrammide sihtrühmade analüüs
- (L) M 3.96 Juhatuse tugi teavitusele ja koolitusele

Soetamine

- (M) M 3.48z Koolitajate või koolitusfirmade valimine

Rakendamine

- (L) M 3.45 IT-turbealaste koolituste sisu kavandamine
- (L) M 3.46 Kontaktisik turvalisuse alal
- (M) M 3.49 Koolitus etalonturbe protseduuride alal

Kasutamine

- (L) M 2.198 Personali teadvustamine infoturbe küsimustes
- (M) M 3.47z IT-turbealased tegevus- ja rollimängud
- (L) M 3.94 Õpitulemuste edukuse mõõtmine ja hindamine
- (L) M 3.95z Õppematerjali kinnistamine

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele Kohustuslikud üldmeetmed

- HG.21 Personali perioodiline turva-alane atasteerimine
- HG.58 Lisanõuded turvakoolitusele

Teabe käideldavus (K)

-

Teabe terviklus (T)

-

Teabe konfidentsiaalsus (S)

-

B 1.14 Turvapaikade ja muudatuste haldus

Muudatuste haldamise ülesandeks on rakendustes, infrastruktuuris, dokumentatsioonis, protsessides ja meetodites tehtavate muudatuste juhtimis- ja kontrollimisekindel kujundamine. Eriti infotehnoloogia valdkonnas peavad paljud asutused ja ettevõtted üha kiireneva arengu ja kasutajate kasvavate nõudmiste tõttu viima korrektselt ja kiiresti sisse süsteemi komponentide uuendused.

Asutuste ja ettevõtete kogemused näitavad, et turvaaukude või rikete tekkimine süsteemi käitamisel on tihti tingitud vigastest või läbiviimata muudatustest. Puuduva või unarusse jäetud turvapaikade ja muudatuste halduse tagajärjel tekivad tihti üksikutes komponentides turvaaugud ning nendega kaasnevate võimalikud ründepunktid.

Käesolevas moodulis kirjeldatakse, kuidas on asutuses võimalik üles ehitada hästi toimiv turvapaikade ja muudatuste haldus, kuidas on võimalik kontrollida ja optimeerida turvapaikade ja muudatuste halduse protsessi, et vältida tõrkeid süsteemi töös, minimeerida turvaaukude teket ja vajadusel need kiiresti kõrvaldada. Kirjeldused on suunatud eeskätt ITle, kuid neid võib rakendada ka teistes tööprotsessides, kui see osutub mõttekaks. Turvapaikade ja muudatuste halduse all mõeldakse käesolevas moodulis muudatuste planeerimise ja juhtimise ülesannet, kuigi seda mõistet kasutatakse teises kontekstis osaliselt isikute tähistamiseks, kes sellega tegelevad.

Kulutused, mis on vajalikud sellise protsessi loomiseks ja realiseerimiseks ei ole väikesed. Seetõttu peaksid käesolevat mooduli rakendama eelkõige suuremad IT-kooslused. Väiksemate ja vähem keeruka struktuuriga IT-koosluste korral piisab teatud juhtudel ka meetme M 2.221 Muudatuste haldus .

Ohud

Käesolevas moodulis vaadeldakse IT-etalonturbega seotud alljärgnevaid tüüpilisi ohte.

Organisatsioonilised puudused:

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.9 Halb kohanemine IT muutustega
- G 2.17 Andmekandjate puudulik märgistus
- G 2.26 Ebapiisavad või puuduvad tarkvara katsetamis- ja evitusprotseduurid
- G 2.27 Ebapiisav või puuduv dokumentatsioon
- G 2.28 Autoriõiguste rikkumine
- G 2.132 Tööprotsesside puudulik arvestamine turvapaikade ja muudatuste haldamisel
- G 2.133 Kohustuste puudulik jaotus turvapaikade ja muudatuste haldamisel

- G 2.134 Ebapiisavad ressursid turvapaikade ja muudatuste haldamisel
- G 2.135 Puudulik side turvapaikade ja muudatuste haldamisel
- G 2.136 Puudulik ülevaade IT-kooslusest
- G 2.137 Ebapiisav või puuduv planeerimine turvapaikade ja muudatuste evitamisel
- G 2.138 Puudulikud taastamisvõimalused turvapaikade ja muudatuste haldamisel
- G 2.139 Mobiilsete terminalidega puudulik arvestamine turvapaikade ja muudatuste haldamisel
- G 2.140 Ebapiisav hädaolukorraks valmisoleku konspetsioon turvapaikade ja muudatuste haldamisel

Inimvead:

- G 3.38 Vead konfigureerimisel ja kasutamisel
- G 3.92 Turvapaikade ja muudatuste prioriteetide väär hindamine

Tehnilised rikked:

- G 4.22 Tüüptarkvara turvaaugud või vead
- G 4.33 Autentimise puudumine või puudulikkus
- G 4.71 Probleemid paikade ja muudatuste automaatsel evitamisel

Ründed:

- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.145 Andmete ja utiliitide manipuleerimine turvapaikade ja muudatuste haldamisel

Soovitatavad meetmed

Vaadeldava IT-koosluse turvalisuse tagamiseks tuleb lisaks käesolevale moodulile rakendada veel teisigi mooduleid vastavalt infosüsteemide etalonturbe rakendusjuhendi modelleerimise tulemustele.

Turvapaikade ja muudatuste käsitluse efektiivse süsteemi sisseseadmiseks on vaja läbida terve rida etappe.

Planeerimine ja kontseptsioon

Turvapaikade ja muudatuste halduse kaudu peaks olema võimalik juhtida ja kontrollida kõiki riist- ja tarkvaraga seoses tehtavaid muudatusi ning nende konfiguratsioone. Kõikide muudatuste registreerimiseks ja hindamiseks peaksid kõik turvapaikade ja muudatuste haldusega tegelevad IT-süsteemid olema sellele allutatud (vt M 2.423 Vastutusalade kindlaksmääramine turvapaikade ja muudatuste halduseks). Konfiguratsiooni ja süsteemide seisundit on seega võimalik muuta vaid turvapaikade ja muudatuste halduse kaudu. Selleks on vajalik vastav vastutuste delegeerimine asutuse või ettevõtte juhatuse kaudu. Turvapaikade ja muudatuste organisatoorne rakendamine kujutab endast funktsiooni, mis hõlmab asutuse erinevates osakondades paralleelselt kulgevaid protsesse. Eriti tuleks sellesse kaasata IT-töö, infoturbe haldus ning erialaosakonnad.

Üksik turvapaikade või muudatuste protseduur saab alguse muudatusnõuetest. Kõigepealt tuleb need registreerida ning muudatuste haldaja poolt kontrollida. Sellesse muudatusse tuleks kokku võtta ja kirja panna tähtsus, hädavajalikkus, planeeritud läbiviimine (tähtaeg, kulg) ning võimalikud riskid ja probleemid (vt M 2.421 Turvapaikade ja muudatuste halduse planeerimine ja M 2.422 Muudatustaotluste käsitlemine).

Turvapaikade ja muudatuste haldust on võimalik efektiivselt toetada tehniliste abivahenditega, näiteks tarkvara automaatsel jaotamisel. Kui turvapaikade ja muudatuste haldamiseks kasutatakse spetsiaalseid instrumente, tuleb kindlaks teha, et nende kasutamiseks koostataks kontseptsioon (vt M 2.424 Paikade ja muudatuste haldamise tööriistade turvapoliitika).

Soetamine

Turvapaikade ja muudatuste haldusprotsessi toetamiseks on erinevaid tooteid. Et nende toodete hulgast sobivad välja valida, tuleb enne soetamist kindlaks määrata instrumentidele esitatavad nõuded, näiteks milliseid platvorme need peavad toetama (vt M 2.425 Asjakohane turvapaikade ja muudatuste haldusinstrumentide valik).

Rakendamine

Rakendamisel tuleks kõik turvapaikade ja muudatuste halduse abil hooldatavad IT-süsteemid sellele üksikuna või grupikaupa allutada. Lisaks sellele tuleb muudatused süsteemides tsentraalses kohas dokumenteerida (vt M 2.34 IT-süsteemi muutuste dokumenteerimine).

Kasutamine

Vastavalt turvapaiga või sisseviidud muudatuse suurusele või keerukusele on soovitatav rakendusplaanis defineerida testid, kontrolli- ja katkestuspunktid, samuti jaotamise prioriteedid. Seejuures tuleb tagada, et soovitud turvatase muudatuse sisseviimise ajal ja pärast seda alles jääks. Muudatuste evitamine ja läbiviimine tuleks kooskõlastada arvestades seejuures erialavaldkondade ja IT-töö ressursse ja huvisid (vt M 2.426 Turvapaikade ja muudatuste halduse integreerimine äriprotsessidesse ja M 2.427 Muudatustaotluste kooskõlastamine).

Kvaliteedi tagamiseks ja vigade avastamiseks või tulevikus tekkida võivate vigade vältimiseks tuleks igale turvapaigale ja muudatusele enne installeerimist anda hinnang (vt M 2.429 Muudatustaotluste tulemuste hindamine).

Muudatusi, eriti tarkvara uuendamist, on võimalik läbi viia käsitsi, kuid ka vastavate instrumentide abil. Nimetatud instrumentide kasutamisel tuleb tähelepanu pöörata asjaolule, et need oleks kaitstud kuritarvitamise vastu ega ohustaks üldist turvalisust kuna need töötavad tihti süsteemiadministraatori volitustega. Instrumentide abil on võimalik muudatusi mitmetes süsteemides korraga läbi viia. Seetõttu mitmekordistuvad aga ka vigade tagajärjed, seepärast tuleks enne muudatuste sisseviimist läbi viia hoolikas testimine (vt M 2.248 Exchange/Outlook 2000 turvapoliitika määratlemine). Arvestada tuleb ka asjaoluga, et muudetavad süsteemid võiks ajutiselt või kestvalt olla välja lülitatud või mitte kättesaadavad. See puudutab eelkõige mobiilseid seadmeid, näiteks sülearvuteid, nutitelefone ja pihuarvuteid (vt M 4.323 Sünkroniseerimine turvapaikade ja muudatuste halduse raames). Lisaks sellele tuleb kogu turvapaikade ja muudatuste halduse protsessi käigus tehniliselt tagada kasutatud tarkvara terviklus ja autentsus (vt M 4.177 Tarkvarapakettide tervikluse ja autentsuse tagamine).

Kasutatud tarkvara automaatsete uuendusmehhanismidega peab turvapaikade ja muudatuste halduse protsessis arvestama sõltumata nende kasutusmäärast (vt M 4.324 Automaatsete uuendusmehhanismide konfiguratsioon turvapaikade ja muudatuste haldamisel).

Likvideerimine

Kui süsteemid likvideeritakse turvapaikade ja muudatuste halduseks, tuleb need vastavalt reeglitele hävitada. Põhjalikumat informatsiooni annab meede M 2.13 Tundlike ressursside jäljetu hävitamine .

Valmisolek hädaolukorraks

Hädaolukorraks valmisoleku plaani koostamisse tuleb kaasata rakenduste ja IT-süsteemide üksikud avariiplaanid, mille haldamine toimub turvapaikade ja muudatuste halduse raames (vt B 1.3 Hädaplaanimine). Kuna turvapaikade ja muudatuste haldus aitab kaasa turvalisuse tehniliseks rakendamiseks asutuses, tuleb valmis panna sobivad tehnilised varu- ja asendussüsteemid, et hoida ära seadmete mitte kompenseeritavat väljalangemist. Lisaks sellele on väga oluline asenduse korraldamine, et hoida käigus otsustus- ja teavitusprotsess.

Planeerimine ja kontseptsioon

- (L) M 2.221 Muudatuste haldus
- (M) M 2.421 Turvapaikade ja muudatuste halduse planeerimine
- (M) M 2.422 Muudatustaotluste käsitlemine
- (L) M 2.423 Vastutusalade kindlaksmääramine turvapaikade ja muudatuste halduseks
- (L) M 2.424 Paikade ja muudatuste haldamise tööriistade turvapoliitika
- (L) M 3.66w Turvapaikade ja muudatuste halduse põhimõisted

Soetamine

- (L) M 2.62 Tarkvara vastuvõtuprotseduurid
- (M) M 2.425 Asjakohane turvapaikade ja muudatuste haldusinstrumentide valik

Rakendamine

- (L) M 4.65 Uue riist- ja tarkvara testimine

Kasutamine

- (L) M 2.219 Infotöötluse pidev dokumenteerimine
- (M) M 2.426 Turvapaikade ja muudatuste halduse integreerimine äriprotsessidesse
- (M) M 2.427 Muudatustaotluste kooskõlastamine
- (M) M 2.428z Skaleeritavus paikade ja muudatuste halduses
- (M) M 2.429z Muudatustaotluste tulemuste hindamine
- (L) M 4.78 Konfiguratsioonimuudatuste hoolikas teostamine
- (L) M 4.177 Tarkvarapakettide tervikluse ja autentsuse tagamine
- (M) M 4.323z Sünkroniseerimine turvapaikade ja muudatuste halduse raames
- (M) M 4.324 Automaatsete uuendusmehhanismide konfiguratsioon turvapaikade ja muudatuste haldamisel

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele Kohustuslikud üldmeetmed

- HG.37 Tarkvara tervikluskontroll igal installeerimisel
- HG.38 Turvapaikade paigaldatuse regulaarseire
- HG.39 Lisanõuded tarkvara vastuvõtuprotseduuridele
- HG.56 Lisanõuded muudatuste haldusele
- HG.57 Muudatuste haldusinstrumentide pääsuõiguste määramine
- HG.60 Lisanõuded automaatsete uuendusmehhanismide konfigureerimisele

Teabe käideldavus (K)

- HK.38 Krüptograafiliste algoritmide kasutuskataloog

Teabe terviklus (T)

-

Teabe konfidentsiaalsus (S)

-

B 1.15 Andmete kustutamine ja hävitamine

Vältimaks informatsiooni sattumist valedesse kätesse, on vajalik järgida teatud kindlaid protseduure andmete ja andmekandjate täielikuks ja usaldusväärseks kustutamiseks või hävitamiseks. See puudutab kaitset vajavat informatsiooni, mis on salvestatud paberkandjale või teistele analoogsetele andmekandjatele nagu mikrofilm (video, kitsasfilm, fotod, heliplaadid, dokumendid, audiokassetid), samuti ka digitaalsetele andmekandjatele (elektrooniline, magnetiline, optiline), näiteks DVD-le ja CD-le.

Kui kustutamata või mittetäielikult kustutatud andmekandjaid edastatakse, müüakse või likvideeritakse, võib ettekavatsematu informatsiooni edastamine põhjustada suurt kahju. Potentsiaalseteks riskiallikateks on eelkõige krüptovõtmed, paroolid, konfidentsiaalne informatsioon ja muu ülitundlik informatsioon töösalvestis või saalimisfailides (swap files).

Seepärast peab igal asutusel ja ettevõttel olema välja töötatud kindlad protseduurid informatsiooni turvaliseks kustutamiseks. Käesolevas moodulis kirjeldatakse, kuidas asutusel on võimalik luua kontseptsioon andmete turvaliseks kustutamiseks ja hävitamiseks.

Ohud

Infosüsteemide etalonturbes peetakse kaitset vajavate andmete ja seega nende andmete turvalist kustutamist mõjutavateks ohtudeks järgmisi tüüpilisi ohtusid:

Organisatsioonilised puudused:

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.2 Reeglite puudulik tundmine
- G 2.3 Puuduvad, puudulikud või ühildumatud ressursid
- G 2.27 Ebapiisav või puuduv dokumentatsioon
- G 2.48 Andmekandjate ja dokumentide puudulik hävitamine
- G 2.54 Konfidentsiaalsuse kadu jääkinfo kaudu
- G 2.102 Inimeste infoturbeteadlikkuse ebapiisav suurendamine

Inimvead:

- G 3. 1 Andmete konfidentsiaalsuse või tervikluse kadu kasutaja vea tõttu
- G 3.13 Väära või soovimatu andmekogumi saatmine
- G 3.31 Struktureerimata andmekorraldus
- G 3.44 Teabe hooletu kasutamine
- G 3.93 Väär ümberkäimine defektsete andmekandjatega

Ründed:

- G 5.71 Tundliku informatsiooni konfidentsiaalsuse kadu
- G 5.146 Saalimisfailidest tingitud konfidentsiaalsuse kadu

Soovitatavad meetmed

Vaadeldava IT-koosluse turvalisuse tagamiseks tuleb lisaks käesolevale moodulile rakendada veel teisigi mooduleid vastavalt infosüsteemide etalonturbe rakendusjuhendi modelleerimise tulemustele.

Andmete turvaliseks kustutamiseks ja hävitamiseks tuleb rakendada terve rida meetmeid. Järgnevalt on ära toodud etapid, mis seejuures tuleb läbida, ning meetmed, mida teatud etappidel on vaja rakendada. Toimingute raskuskese paikneb loomulikult likvideerimise faasis. Paljusid andmekandjaid edastatakse aga ka teistes faasides, mistõttu tuleb nendel paiknev edastamisele mittekuuluv informatsioon turvaliselt kustutada.

Planeerimine ja kontseptsioon

Plaanipäraste protseduuride kindlaksmääramine andmekandjate kustutamiseks ja hävitamiseks takistab salvestatud informatsiooni kuritarvitamist (vaata M 2.431 Korrakohased protseduurid informatsiooni kustutamiseks või hävitamiseks). Nimetatud protseduurid peavad konkreetse suunisena olema kättesaadavad kõikidele töötajatele (vt M 2.432 Eeskirjad informatsiooni kustutamiseks ja hävitamiseks).

Soetamine

Andmete kustutamiseks ja hävitamiseks vajalike seadmete soetamiseks tuleb formuleerida kontseptsioonist tulenevad toodetele esitatavad nõuded ning seejärel nendest lähtuvalt sobivad tooted ja teenused välja valida (vaata M 2.434 Andmete kustutamiseks või hävitamiseks vajalike seadmete soetamine ja M 2.436 Andmekandjate hävitamine välise teenusetarnija poolt).

Rakendamine

Kõik töötajad peaksid tundma informatsiooni kustutamiseks või hävitamiseks kindlaks määratud protseduure (vaata M 3.67 Töötajate koolitamine andmete kustutamise või hävitamise alal).

Kasutamine

Igat liiki informatsiooni haldamine peab põhimõtteliselt toimuma selgete struktuuride alusel. Lisaks sellele tuleks need jagada tundlikkuse alusel kategooriatesse. See võimaldab kogu kustutamisele või hävitamisele kuuluvat informatsiooni identifitseerida ning leida kohad, kus neid töödeldi ja salvestati (vaata M 2.217 Teabe, rakenduste ja süsteemide hoolikas liigitamine ja käitlus).

Likvideerimine

Andmekandjate ja IT-süsteemide likvideerimisel tuleb rakendada erinevaid meetmeid tagamaks, et tähtsad andmed kaotsi ei läheks ega tundlikud andmed alles ei jääks. Vastavatest turvasoovitustest annab ülevaate meede M 4.234 IT-süsteemide ja andmekandjate väljavahetamise kord . Soovitused rakendamiseks erinevate IT-süsteemide puhul asuvad infosüsteemide etalonturbe kataloogide vastavates moodulites, näiteks M 2.320 Serveri nõuetekohane kasutuselt kõrvaldamine ja M 2.323 Kliendi korrakohane kasutuselt kõrvaldamine)

Järgnevalt tutvustatakse turvameetmete kogumit rakendamiseks valdkonnas „Andmete kustutamine ja hävitamine".

Planeerimine ja kontseptsioon

- (L) M 2.3 Andmekandjate haldus
- (L) M 2.431 Korrakohased protseduurid informatsiooni kustutamiseks või hävitamiseks
- (L) M 2.432z Eeskirjad informatsiooni kustutamiseks ja hävitamiseks

- (M) M 2.433w Ülevaade meetoditest andmete kustutamiseks ja hävitamiseks

Soetamine

- (M) M 2.434z Andmete kustutamiseks või hävitamiseks vajalike seadmete soetamine
- (M) M 2.435z Sobiva dokumendipurusti valik
- (L) M 2.463z Bluetooth-lisaseadmete seadmekogu kasutamine

Rakendamine

- (M) M 2.217 Teabe, rakenduste ja süsteemide hoolikas liigitamine ja käitlus
- (L) M 3.67 Töötajate koolitamine andmete kustutamise või hävitamise alal
- (L) M 4.32 Andmekandjate füüsiline kustutamine enne ja pärast nende kasutamist
- (L) M 4.64 Ülekantavate andmete kontrollimine enne edastamist/peidetud info kõrvaldamine
- (L) M 4.325 Likvideerimisele kuuluvate failide kustutamine

Likvideerimine

- (M) M 2.13 Tundlike ressursside jäljetu hävitamine
- (M) M 2.167 Andmete kustutamine või hävitamine
- (L) M 4.234 IT-süsteemide ja andmekandjate väljavahetamise kord

B 1.16 Nõuete haldus

Igas asutuses on erinevat liiki seadusi, lepinguid, struktuurseid ja asutusesiseseid direktiive ja eeskirju, mida tuleb järgida. Mõnedel nendest on otsene või kaudne mõju infoturbe haldusele. Nõuded on erinevad, sõltudes tegevusalast, asukohariigist ja teistest raamtingimustest. Lisaks sellele allub näiteks ametiasutus teistsugustele välistele eeskirjadele kui aktsiaselts. Asutuse juhtkond peab sobivaid järelevalvemeetmeid kasutades tagama nõuete täitmise (compliance).

Nõuete halduse eesmärgiks on omada igal ajal ülevaadet asutuse üksikutele valdkondadele esitatavatest erinevatest nõuetest ja identifitseerida ning rakendada sobivaid meetmeid, et vältida nõuete eiramist.

Nimetatud ülesanne antakse tavaliselt ühele töötajatest. Selle rolli täitjat nimetatakse edaspidi nõudehalduriks. Mõnedes ettevõtetes kasutatakse ka nimetust compliance manager. Niikaua kuni eeskirjad ette ei näe, ei ole selleks vaja luua uusi töökohti. Ülesande võib näiteks üle võtta infoturbe osakond, revisjoni ja kontrolli korraldaja või juriskonsult.

Olenevalt asutuse suurusest võivad sellel olla erinevad haldusprotsessid, mille sisuks on riskihalduse erinevad aspektid, näiteks turva- ja andmekaitsehaldus, nõuete haldus ja kontrollimine. Need peaksid üksteist usaldades koostööd tegema, kasutamaks ära sünergiaefekti ja seeläbi konfliktid õigeaegselt kõrvaldada.

Käesolevas moodulis vaadeldakse nõudeid, mis mõjutavad asutuse IT-alase turvalisuse kujundamist.

Ohud

Kõikide nõuete haldust mõjutavate ohtude asemel vaadeldakse käesolevas moodulis järgmist tüüpilist ohtu:

Organisatsioonilised puudused:

- G 2.105 Õigusaktide ja lepingute sätete rikkumine

Soovitatavad meetmed

Vaadeldava IT-koosluse turvalisuse tagamiseks tuleb lisaks käesolevale moodulile rakendada veel teisigi mooduleid vastavalt infosüsteemide etalonturbe rakendusjuhendi modelleerimise tulemustele.

Nõuete halduse raamides on vajalik rakendada terve rida meetmeid, alustades kontseptsiooni väljatöötamisest, millele järgneb sobivate organisatsioonistruktuuride ülesehitamine ja lõpetades regulaarse revisjoniga. Järgnevalt on ära toodud etapid, mis seejuures tuleb läbida, ning meetmed, mida vastavatel etappidel on vaja rakendada.

Planeerimine ja kontseptsioon

Vajalik on kindlaks määrata protsessid ja organisatsiooni struktuurid, et tagada ülevaade erinevatest nõuetest (vaata M 2.439 Nõuete halduse kontseptsioon ja organisatsioon.). Lisaks asutust puudutavatele välistele õigusaktidele peavad olema defineeritud ja läbipaistvalt kujundatult ka asutusesesisesed suunised ja nõuded. Üheks tähtsaks tingimuseks asutuse töö seisukohalt tähtsa teabe, olulise tähtsusega äriprotsesside ja süsteemide turvalisuse tagamisel on nende kaitsevajaduse kindlaksmääramine (vaata M 2.217 Teabe, rakenduste ja süsteemide hoolikas liigitamine ja käitlus). Sellest tulenevad kaitset vajavatele objektidele esitatavad konkreetsed turvanõuded.

Rakendamine

Identifitseeritud nõuete rakendamine toimub asutuse haldusprotsesside, eriti ka turvaprotsessi kaudu. Töötajate, aga ka külastajate ja väliste teenusetarnijate tähelepanu tuleb juhtida nende kohustusele olla informatsiooni ja IT-süsteemide kasutamisel hoolikas enne kui nad sellele juurdepääsu saavad (vaata M 3.2 Uute töötajate kohustamine eeskirju järgima).

Kasutamine

Turvaeeskirjadest, mille asutus on välja töötanud nõuete täitmiseks, tuleb kestvalt kinni pidada. Nõuete täitmist tuleb regulaarselt kontrollida (vaata M 2.217 Teabe, rakenduste ja süsteemide hoolikas liigitamine ja käitlus). Nii asutuse oma õigusaktid kui ka õiguslikud raamtingimused, millele asutus allub, võivad muutuda. Sellega tuleb nõuete halduse raames arvestada (vaata M 2.340 Õiguslike raamtingimuste järgimine).

Järgnevalt tutvustatakse turvameetmete kogumit rakendamiseks valdkonnas „Nõuete haldus".

Planeerimine ja kontseptsioon

- (M) M 2.163 Krüptoprotseduure ja -tooteid mõjutavate tegurite määramine
- (L) M 2.439 Nõuete halduse kontseptsioon ja organisatsioon.

Rakendamine

- (L) M 3.2 Uute töötajate kohustamine eeskirju järgima
- (M) M 4.99 Kaitse info muutmise eest pärast üleandmist

Kasutamine

- (M) M 2.217 Teabe, rakenduste ja süsteemide hoolikas liigitamine ja käitlus
- (L) M 2.340 Õiguslike raamtingimuste järgimine
- (M) M 2.380 Erandite kooskõlastamine

B 1.17 Pilvteenuse kasutamine

Kirjeldus

Pilvtöötlus on infotehnoloogia paradigma, mis võimaldab võrgu kaudu kiiret nõudmispõhist, asukohast sõltumatut, juurdepääsu elastselt konfigureeritavate füüsiliste või virtuaalsete ressursside ja võimete (võrkude, serverite, salvestite, rakenduste, teenuste) ühisfondile, kusjuures selline pääs vajab minimaalset haldustegevust või teenuseandja sekkumist. Andmete töötlemine avalikus pilves kujutab endast, sõltuvalt kasutatavast lahendusest, andmete töötlemist kolmanda osapoole taristus, platvormil ja/või infosüsteemis. Pilveteenus on pilve kaudu pakutav väärtus või hüve kliendi vajaduste rahuldamiseks.

Pilvtöötluse osapooled on järgmised:

- Pilveteenuse klient (kasutaja, Cloud Consumer) on ärisuhtes pilveteenuse osutajaga ning kasutab selle teenuseid;
- Pilveteenuse osutaja (Cloud Provider) vastutab kliendile pakutavate teenuste eest. Käesolevas moodulis pilveteenuse osutajale seatud nõuded kehtivad ka käsitletava teenuse allhanke tarnijate kohta;
- Pilvtöötluse maakler (Cloud Broker) haldab pilveteenuste kasutamist, jõudlust ja tarnet ning lepib kokku suhted pilveteenuse osutaja ja kliendi vahel. Käesolevas moodulis pilveteenuse maaklerile seatud nõuded kehtivad ka käsitletava teenuse allhanketarnijate kohta;
- Pilvtöötluse operaator (kandja, Cloud Carrier) vahendab ühendust ning teenuste transporti pilveteenuse osutaja ja kliendi vahel. Käesolevas moodulis pilveteenuse operaatorile seatud nõuded kehtivad ka käsitletava teenuse allhanketarnijate kohta;
- Pilvtöötluse audiitor (Cloud Auditor) on pilvtöötluse rakenduse sõltumatu hindaja.

Käesolevas moodulis kasutatakse järgmisi mõisteid:

- **Kõrgel usaldusväärsuse tasemel asukoht** - sellise asukoha puhul peavad pilvtöötluse osapooled asuma riigis või riikides, milles andmete turvalisus (sh käideldavus, terviklus ja konfidentsiaalsus) on kõrgel tasemel kaitstud riikidevaheliste lepingutega ning kontrollitav. Lisaks muudele tingimustele, peab kõrgel usaldusväärsuse tasemel pilve asukohariik kuuluma riikide hulka, millesse on lubatud isikuandmete edastamine vastavalt isikuandmete kaitse seaduse § 18 lõikele 2: “Isikuandmete edastamine on lubatud Euroopa Liidu liikmesriiki ja Euroopa Majanduspiirkonna lepinguga ühinenud riiki, samuti riiki, mille isikuandmete kaitse taset on Euroopa Komisjon hinnanud piisavaks. Isikuandmete edastamine ei ole lubatud riiki, mille andmekaitse taset on Euroopa Komisjon hinnanud ebapiisavaks”. Kõrgel usaldusväärsuse tasemel asukoht ning selle auditeerimine ja järelevalve peab olema sätestatud asjaosaliste riikide ja asutuste vaheliste lepingute tasemel;
- **Kõrgel usaldusväärsuse tasemel omandus** - sellise omanduse puhul peavad pilvtöötluse osapoolte omanikud olema kontrollitavalt ja kontrollitult

kõrgel usaldusväärsuse tasemel asukohariikide juriidilised isikud või selliste asukohariikide kodakondsusega füüsilised isikud. Kõrgel usaldusväärsuse tasemel omandus ning selle auditeerimine ja järelevalve peab olema sätestatud asjaosaliste riikide ja asutuste vaheliste lepingute tasemel;

- **Kõrgel usaldusväärsuse tasemel transport** - sellise transpordi puhul peab andmete transport pilves ning pilve ja selle osapoolte vahel toimuma kõrgel usaldusväärsuse tasemel riikide kaudu ning transpordi komponentide (nt võrgud, ruuterid, tarkvara) vahendite omanikud peavad olema kõrgel usaldusväärsuse tasemel; kasutatavad domeenid peavad olema kaitstud DNSSEC turvalaiendusega. Muuhulgas tähendab see, et kui kasutatakse avalikku internetti, peab andmete marsruutimine olema vastavalt kokku lepitud teenuseosutajaga. Kõrgel usaldusväärsuse tasemel transport ning selle pidev auditeerimine ja järelevalve peab olema sätestatud asjaosaliste riikide ja asutuste vaheliste lepingute tasemel.

Pilveteenuse põhiliigid on taristu teenusena (infrastructure as a service, IaaS), platvorm teenusena (platform as a service, PaaS) ja tarkvara teenusena (software as a service, SaaS). Talletust teenusena (storage as a service) võib vaadata kui eraldi teenust või IaaS komponenti.

Käesolev moodul sisaldab Eesti-spetsiifilist juhendmaterjali eelkõige pilvtöötluse kasutajale, kuid see võib olla kasulik ka muudele osapooltele. Koos teiste ISKE raamistiku materjalidega aitab käesolev moodul otsustada, kas ja milliseid andmeid ja andmekogusid võib erinevate pilveteenuste osutajate juures pilvtöödelda ja pilves käidelda ning milliseid nõudeid, turvameetmeid ja kontrollküsimusi tuleb pilveteenuse tellimisel ja kasutamisel arvestada.

Moodulit tuleks kasutada lähtekohana pilvtöötluse kavandamiseks Eesti riigi ja kohalike omavalitsuste andmekogude haldamisel. Tuleb arvestada ka muid vajalikke ISKE mooduleid, sealhulgas järgmisi.

- Moodul B 5.21 Veebirakendused
- esitab meetmed ja põhimõtted, mida tuleb järgida veebirakenduste, sealhulgas pilvtöötlusel põhinevate veebirakenduste kogu elutsükli jooksul, sealhulgas nende kavandamisel, väljatöötamisel ja käitamisel;
- Moodul B 5.24 Veebiteenused kirjeldab veebiteenuseid, nende elutsüklit, ohtusid ja turvameetmeid, tehes seda põhiliselt teenuseosutaja seisukohast;
- Moodul B 3.303 Salvestisüsteemid ja salvestivõrgud toob ära pilvsalvestuse võimalused ja meetodid. Pilveteenuse kasutaja saab seda rakendada täiendusena moodulitele B 1.17 ja B 5.24;
- Moodul B 3.304 Virtualiseerimine kirjeldab virtualiseerimise põhimõtteid, kavandamist, hankimist, rakendamist, käitamist, hädaolukorraks valmisolekut, ohtusid ning turvameetmeid;
- Mooduli B 1.7 Krüptokontseptsioon rakendamine on väga oluline pilvtöötluse konfidentsiaalsus- ning terviklusnõuete korral;
- Moodul B 1.11 Väljasttellimine (Outsourcing) toob ära ohud ja meetmed, mida tuleb arvestada ka pilvtöötluse kui ühe väljasttellimise erijuhu korral;
- Moodul B 1.14 Turvapaikade ja muudatuste haldus on eriti oluline pilvtöötluse korral, kuna pilvtöötlus on tundlik väliste osapoolte rünnete ja muude mõjude suhtes.

Pilvtöötlus on mitmes mõttes sarnane väljasttellimisega, samas on neil ka olulisi erinevusi. Näiteks jagavad kliendid pilveteenuse korral tihti ühist IT taristut, klient saab teenust läbi veebiliidese ise kiiresti mastabeerida, teenuse taristu võib paikneda väga erinevates asukohtades jne.

Pilvtöötluse eripärast tulenevad mitmed olulised probleemid. Näiteks, kui konfidentsiaalset teavet saadetakse krüpteeritult üle avaliku interneti, kontrollimata seejuures osapooli ning nende turvameetmeid, võib ründajal olla võimalik andmed vahepeal salvestada. Salvestatud andmed saab dekrüpteerida hiljem, kui kasutatud krüptomeetodid on vananenud ning dekrüpteerimise meetodid edasi arenenud, kusjuures see võimalus võib realiseeruda enne salastamistähtaja möödumist.

Hinnanguliselt on krüptoalgoritmide uuringute usaldusväärsuse ajahorisont viis aastat. Meetmes M 2.264 Krüpteeritud andmete regulaarne regenereerimine arhiveerimisel märgitakse, et kui andmeid on tarvis säilitada 10 aastat või kauem, tuleb krüpteeritud või allkirjaga varustatud andmete usaldusväärsuse ja tervikluse tagamiseks vastavad andmed korduvalt uute võtmetega ja vajadusel ka uute algoritmidega ümber krüpteerida. Lisaks tuleb pidevalt uurida usaldusväärseid infoallikaid ning kui kasutatud krüptograafilised protseduurid iganevad, tuleb andmed uuesti krüpteerida või allkirjastada. Arvestades esimest eeltoodud hinnangut ning vajadust pidevalt jälgida krüptograafilisi protseduure, on käesolevas moodulis jäädud viieaastase krüptoalgoritmide usaldusväärsuse ajahorisondi juurde. Konkreetse andmekogu puhul võib asutuse poolt läbi viidud täiendav riskianalüüs viia teistsuguse hinnanguni.

Samuti ei ole kõik pilvtöötluse aspektid üldjuhul kasutaja poolt kontrollitavad (auditeeritavad).

ISKE rakendusjuhend näeb ette täiendava turvaanalüüsi (ISKE rakendusjuhend, rakendamise samm 10). Selline turvaanalüüs võib viia täiendavate turvameetmete rakendamiseni või välistada mingit tüüpi tegevused (nt teatavate andmete hoidmise pilves või andmete saatmise üle avaliku interneti). Pilvtöötluse puhul tuleks täiendav turvaanalüüs läbi viia juba pilvtöötluse kavandamisel, sealhulgas meetmete planeerimise juures (samm 8). Kui turvaanalüüsi tulemusena otsustatakse tugevdada olemasolevaid ISKE meetmeid või lisada uusi meetmeid, siis võib see otsus kaasa tuua täiendavaid kulutusi, kuid vähendab turvariske ning on kooskõlas ISKE põhimõtetega.

Pilves, mille serverid paiknevad füüsiliselt Eesti territooriumil, mis vastab kindlustavate süsteemide, sh ISKE nõuetele (L, M, H) ja on ISKE vastu nõuetekohaselt auditeeritud, võib töödelda vastava taseme andmeid. Ka Eestis paikneva kolmanda osapoole poolt pakutava pilveteenuse kasutamisel tuleb eelnevalt teostada põhjalik riskianalüüs, sh hinnata andmete pilves töötlemisega ja väljasttellimisega kaasnevaid riske ning järgida muuhulgas teenuse väljasttellimise ja andmete pilves töötlemise ISKE nõudeid. Eesti territooriumil servereid majutava ja ISKE auditi läbinud pilveteenuse osutaja puhul viiakse läbi lihtsustatud riskianalüüs, mis ei pea käsitlema pilveteenuse osutaja valimisega kaasnevaid riske.

RIA on välja töötanud soovitusliku juhendi avalike pilveteenuste turvaliseks kasutamiseks riigisektoris, mis on leitav järgneval lingil: https://www.ria.ee/public/ISKE/Avalike-pilvede-kasutamise-juhend.pdf.

Ohud

Pilveteenusel on erinevaid omadusi, teenuse mudeleid ja rakendamise mudeleid. Pilvtöötluse ohud on enamasti üldisemad ning ei sõltu konkreetse pilveteenuse parameetritest.

IT-etalonturbe seisukohalt loetakse pilvteenuste kasutamise puhul tüüpilisteks järgmisi ohuallikaid:

Vääramatu jõud

- G 1.10 Laivõrgu tõrge
- G 1.19 Teenusepakkuja või tarnija väljalangemine

Organisatsioonilised puudused

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.2 Reeglite puudulik tundmine
- G 2.4 Turvameetmete ebapiisav järelevalve
- G 2.7 Õiguste volitamata kasutamine
- G 2.27 Ebapiisav või puuduv dokumentatsioon
- G 2.84 Puudused välisteenusepakkujaga sõlmitud lepingu tingimustes
- G 2.85 Ebapiisavad tingimused väljasttellimise kasutamise lõpetamiseks
- G 2.86 Sõltuvus välisteenusepakkujast
- G 2.87 Ebaturvalised protokollid avalikes võrkudes
- G 2.93 Puudulik jätkusuutlikkuse planeerimine väljasttellimise korral
- G 2.105 Õigusaktide ja lepinguliste kokkulepete rikkumine
- G 2. 151 Virtuaalsetel IT-süsteemidel kasutatavate rakenduste ebapiisav tootjatugi
- G 2.188 Pilvteenuse litsentsihalduse puudulik regulatsioon
- G 2.189 Pilvteenuse kasutamise puuduv või puudulik strateegia
- G 2.190 Pilvteenuse kasutamise ebapiisav administreerimismudel
- G 2.191 Ebapiisav rollide ja volituste kontseptsioon
- G 2.192 Piisava kvalifikatsiooniga personali puudus
- G 2.193 Institutsiooni ebapiisav kohandamine pilvteenuste kasutamisega
- G 2.194 Pilvteenuste kasutamise ebapiisav nõuete haldus
- G 2.195 Teenuste osutamise puudulik seire
- G 2.196 Pilvteenuste tervikliku kasutustsükli puuduv tulude ja kulude analüüs
- G 2.197 Pilvteenuste ebapiisav sidumine enda IT-lahendustega
- G 2.198 Pilvteenustele üleviimise puudulik planeerimine
- G 2.199 Pilvteenuste teenusepakkuja puudulik valimine

Inimvead

- G 3.43 Puudulik paroolihooldus
- G 3.122 Pilvteenuse väär kasutus

Tehnilised rikked

- G 4.10 Keerukad ligipääsuvõimalused võrgustatud IT-süsteemides
- G 4.22 Tüüptarkvara turvaaugud või vead
- G 4.35 Ebaturvaline krüptoalgoritm

- G 4.43 Dokumenteerimata funktsioonid
- G 4.47 Vananenud krüptomeetodid
- G 4.97 Välisteenuse osutajaga seotud kitsaskohad
- G 4.98 Pilvteenuste haldustööriistade tõrked pilvteenuste kasutamisel

Ründed

- G 5.20 Administraatori õiguste väärkasutus
- G 5.28 Teenuse halvamine
- G 5.190 Teenuste väärkasutus
- G 5.191 Teenusarvete andmete manipuleerimine
- G 5.107 Välisteenusepakkuja poolne andmete paljastamine kolmandatele isikutele
- G 5.E8 Välise teenuseosutaja poolne käideldavuse häirimine
- G 5.E9 Välise teenuseosutaja poolne tervikluse häirimine
- G 5.E10 Välise teenuseosutaja poolne konfidentsiaalsuse häirimine.

Rakendatavad turvameetmed

Pilvtöötluse puhul rakendatakse turvameetmeid käesolevast moodulist ning vastavalt vajadusele teistest pilvtöötlust käsitlevatest ISKE moodulitest: B 3.303 Salvestisüsteemid ja salvestivõrgud jt. Tuleb arvestada ka kõiki muid vajalikke ISKE mooduleid, sealhulgas eriti neid, mis on seotud krüpteerimisega (konfidentsiaalsus- ning terviklusnõuete korral, moodul B 1.7 Krüptokontseptsioon), väljast tellimisega (moodul B 1.11 Väljasttellimine (Outsourcing)) ning turvapaikade ja muudatuste haldusega (moodul B 1.14 Turvapaikade ja muudatuste haldus).

Juhul kui pilvteenuse haldamine usaldatakse pilvteenust tarbiva institutsiooni pilvadministraatorile, kes hakkab sel eesmärgil kasutama mõnda veebiteenuseid rakendavat haldustarkvara, tuleb täiendavalt arvestada ka mooduliga B 5.24 Veebiteenused .

Planeerimine ja kontseptsioon

- (L) M 2.40z Töötajate esinduse õigeaegne kaasamine
- (L) M 2.42 Võimalike suhtluspartnerite määramine
- (L) M 2.534 Pilvteenuse kasutamisstrateegia koostamine
- (L) M 2.535 Pilvteenuse kasutamise turvapoliitika koostamine
- (L) M 2.536 Tarbitavate pilvteenuste määratlemine teenuste tarbija poolt
- (L) M 2.537 Teenuste pilvteenusteks üleviimise turbe planeerimine
- (L) M 2.538 Pilvteenuste juurutamise turbe planeerimine
- (L) M 2.539 Pilvteenuste kasutamise turbekontseptsiooni koostamine
- (L) M 2.544 Pilvteenuste kasutamise auditeerimine
- (L) M 4.459 Krüpteeringu kasutamine pilvteenustes

Soetamine

- (L) M 2.540 Pilvteenuste osutaja hoolikas valimine

Rakendamine

- (L) M 2.541 Pilvteenuseosutajaga sõlmitava lepingu koostamine
- (L) M 2.542 Teenuste turvaline üleviimine pilvteenusteks

Kasutamine

- (L) M 2.264 Krüpteeritud andmete regulaarne regenereerimine arhiveerimisel
- (L) M 2.543 Pilvteenuste infoturbe tagamine igapäevatöös
- (L) M 2.544 Pilvteenuste kasutamise auditeerimine
- (L) M 4.462z Sissejuhatus pilveteenuse kasutamisse
- (L) M 6.56 Andmevarundus krüptoprotseduuride kasutamisel

Ressursside väljavahetamine

- (L) M 2.307 Väljasttellimissuhte nõuetekohane lõpetamine

Valmisolek hädaolukorraks

- (L) M 6.155 Pilvteenuse hädaolukorra kontseptsiooni koostamine
- (L) M 6.156 Organisatsioonisiseste andmevarunduste tegemine

B 1.18 Identiteedi- ja volituste haldus

Identiteedihalduse eesmärk on tuvastada kahtlusteta kõik subjektid, kellel on juurdepääs asutuse ressurssidele. Siinjuures on mõeldud eelkõige IT-ressursse. Juurdepääsuvõimalusega subjektid võivad olla isikud või ka IT-komponendid või lühidalt öeldes kasutajad. Identiteedihaldusega tähistatakse tuvastamiseks, aga ka autentimiseks vajalike andmete haldamist.
Volituste haldamise puhul on küsimus selles, kas ja kui üksikasjalikult need subjektid andmeid ja teenuseid kasutavad, võimaldades või keelates neile kasutajaprofiili alusel juurdepääsu. Volituste haldus hõlmab protsesse, mis on vajalikud õiguste andmiseks, äravõtmiseks ja kontrollimiseks.
Need kaks mõistet on suhteliselt sarnased ning seetõttu kasutatakse edaspidi mõistet „identiteedi- ja volituste haldus" (ingl IAM – Identity and Access Management). Identiteedi- ja volituste haldusega tagatakse, et kasutajatel oleks juurdepääs üksnes nendele IT-ressurssidele, mida nad vajavad oma töö jaoks ja milleks neid on volitatud.
Identiteedi- ja volituste haldus peab vastama järgmistele nõetele:

- protseduuride ülesehitus ja rakendamine, et juhtida ja kontrollida juurdepääsu teabele ning ligipääsu IT-ressurssidele, eelkõige identiteetide ja volituste käsitlemist ning nende haldamist,
- kasutajate registreerimine, õiguste andmine ja äravõtmine,
- kasutajatunnuste ja nende juurde kuuluvate volituste haldus,
- kasutajatunnuste kontrollimine.

Identiteedi- ja volituste haldus koosneb nii töökorralduslikest kui ka tehnilistest meetoditest. Sageli toimub identiteedi- ja volituste haldus enda vahenditega ja käsitsi. Selle meetodiga kaasnevad kõrged halduskulud ning ebastabiilsed ja vananenud kasutajaandmete kogud. IT-rakenduste kasutamine võib teostamist toetada, kuid see on ainult üks osa lahendusest. See moodul näitab, millised peaksid olema kindlad lahendused kasutajate ja volituste struktureeritud käsitlemiseks.

Volitusi tohib anda üksnes piiratult ja tööülesannete alusel vähimate volituste põhimõtte järgi. Asutuse ruumides ja praegusel ajal eriti IT-süsteemides asub suur osa selle asutuse intellektuaalsest omandist. IT-süsteemid toetavad peale selle ka paljusid ettevõtte või ametiasutuse eduks vajalikke äriprotsesse . Identiteedi- ja volituste haldusega tagatakse, et kasutajatele antakse üksnes vajalikud volitused. Volituste andmise, muutmise ja äravõtmise dokumenteeritud protseduur võimaldab juhtida pääsuandmeid ning vastavad taustsüsteemid võimaldavad salvestada ja hinnata toimuvaid tegevusi. Kahjujuhtumi või seadusest tulenevate nõuete korral on võimalik tegevusi hinnata ja kasutajatega siduda.

Ohud

Selles moodulis vaadeldakse järgmisi IT-etalonturbe tüüpilisi ohtusid:
Töökorralduslikud puudused

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.2 Reeglite puudulik tundmine
- G 2.4 Turvameetmete ebapiisav järelevalve
- G 2.6 Volitamata pääs ruumidesse

- G 2.7 Õiguste volitamata kasutamine
- G 2.67 Pääsuõiguste puudulik haldus
- G 2.214 Identiteedi- ja volituste halduse puuduv või mitteküllaldane kontseptsioon
- Inimvead
- G 3.16 Väär pääsuõiguste haldus
- G 3.43 Puudulik paroolihooldus

Tehnilised rikked

- G 4.10 Keerukad ligipääsuvõimalused võrgustatud IT-süsteemides
- G 4.33 Autentimise puudumine või puudulikkus

Ründed

- G 5.9 IT-süsteemide volitamata kasutamine
- G 5.18 Süstemaatiline paroolide mõistatamine
- G 5.19 Kasutajaõiguste väärkasutus
- G 5.20 Administraatori õiguste väärkasutus
- G 5.24 Sõnumite korduv sisestamine
- G 5.42 Inimestega manipuleerimine (Social Engineering)
- G 5.104 Infoluure

Soovitatavad meetmed

Vaadeldava IT-koosluse turvalisuse tagamiseks tuleb peale selle mooduli rakendada veel teisigi mooduleid, mis selguvad IT-etalonturbe rakendusjuhendi põhjal tehtava modelleerimise tulemusel.

Identiteedi- ja volituste halduse raames tuleb sõltumata kasutatavatest IT-komponentidest rakendada mitmeid meetmeid. Järgnevalt on esitatud ülevaade erinevatest kohustuslikest etappidest ja meetmetest, mida tuleks iga etapi puhul võtta.

Identiteedihalduse süsteemide jaoks on vajalikud mitmesugused komponendid, siia kuuluvad isiku- ja organisatsiooniandmete haldus (tavaliselt kataloogiteenused, vt B 5.15 Üldine kataloogiteenus) ja kasutajate identifitseerimise ja autentimise teenused, nt kataloogiteenustega, nagu nt Novell Directory Services, Microsoft Active Directory või IBMi suurarvutid.

Planeerimine ja kontseptsioon

Igas asutuses peab olemas olema asjakohane protseduur identiteetide ja volituste käsitlemiseks (vt M 2.585 Identiteedi ja volituste halduse kontseptsioon). Kõigepealt tuleb asutuses määratleda turbekontseptsioonist tulenevad põhilised raamtingimused, võttes arvesse identiteedi- ja volituste haldust. Kõik nõuded, nt nimeandmise põhimõtted ja asutusesised toimingud, peaksid olema kirjeldatud vastavas suunises (vt M 2.220 Pääsu reguleerimise suunised). Siia kuuluvad ka nõuded paroolide kasutamise reguleerimiseks (vt M 2.11 Paroolide kasutamise reeglid).

Kui töötajad võtavad uuesti üle tööülesanded, need ära annavad või asutusest lahkuvad, tuleb luua vastavad volitused või neid muuta või kustutada ning töötajate kasutajatunnused inaktiveerida (vt M 2.586 Volituste andmine, muutmine ja äravõtmine).

Täiendavate haldusnõuete kohta on meetmes M 2.587 Identiteedi ja volituste halduse protsesside protseduur ja kontseptsioon protseduuriliselt esitatud näide identiteedi- ja volituste halduse ülesehituse kohta.

Soetamine

Identiteedi- ja volituste halduse süsteemide ja autentimisvahendite soetamisel tuleks juba valikuprotsessis arvesse võtte töödeldava teabe kaitsevajadust. Seda on täpsemalt kirjeldatud meetmes M 4.499 Identiteedi- ja volituste halduse süsteemide asjakohane valik .

Teostus

Juurdepääs IT-süsteemidele peaks olema plaanitud ja teostatud nii, et töötajad pääseksid ligi ainult nendele andmetele, mida nad vajavad oma igapäevaseks tööks. Juurdepääsu kaitsmiseks tuleks rakendada asjakohaseid autentimisvahendeid (vt M 4.1 IT-süsteemide paroolkaitse). Seejuures tuleks kohe ära muuta ka algparoolid (vt M 4.7 Algparoolide muutmine).

Kõiki töötajaid tuleb regulaarselt koolitada turvaliste paroolide kasutamise ja teadvustamise suhtes (vt M 3.63 Kasutajate koolitus autentimiseks kataloogiteenuste abil).

Kasutamine

Identiteedi- ja volituste halduse raames reguleeritakse kõikide töötajate pääsuõigusi asutuse erinevatesse valdkondadesse ja kõikidesse ressurssidesse (vt M 2.6 Sissepääsuõiguste andmine , M 2.7 Süsteemi ja võrgu pääsuõiguste andmine ja M 2.8 IT-rakendustele ja andmetele pääsuõiguste andmine).

Kõik identiteedi- ja volituste halduse muudatused tuleb kirjalikult dokumenteerida (vt M 2.31 Volitatud kasutajate ja õiguste profiilide dokumenteerimine)

Valmisolek hädaolukorraks

Identiteedi- ja volituste halduse süsteemi tõrge võib põhjustada, et kasutajad ei saa enam sisse logida ning kasutajaprofiile ei saa enam muuta, luua ega kustutada. Tuleb uurida, millised on identiteedi- ja volituste halduse süsteemi tõrke turvalisusega seotud mõjud äriprotsessidele (vt M 6.166 Valmisolek hädaolukorraks identiteedi- ja volituste halduse süsteemi puhul).

Järgneb ülevaade „Identiteedi- ja volituste halduse" meetmete paketist.

Planeerimine ja kontseptsioon

- (L) M 2.5 Vastutuse ja ülesannete jaotamine
- (L) M 2.11 Paroolide kasutamise reeglid
- (L) M 2.30 Kasutajate ja kasutajarühmade määramise protseduurid
- (L) M 2.220 Pääsu reguleerimise suunised
- (L) M 4.250z Keskse võrgupõhise autentimisteenuse valimine
- (L) M 5.34z Ühekordsed paroolid

Teostus

- (L) M 2.555 Rakenduste autentimiskontseptsiooni koostamine
- (L) M 4.1 IT-süsteemide paroolkaitse
- (L) M 4.7 Algparoolide muutmine

Kasutamine

- (L) M 2.6 Sissepääsuõiguste andmine
- (L) M 2.7 Süsteemi ja võrgu pääsuõiguste andmine

- (L) M 2.8 IT-rakendustele ja andmetele pääsuõiguste andmine
- (L) M 2.31 Volitatud kasutajate ja õiguste profiilide dokumenteerimine
- (L) M 2.65 IT-süsteemi kasutajate eraldatuse kontroll
- (L) M 2.402z Paroolide uuendamine

B2 Infrastruktuur

Moodulite nimekiri

B 2.1 Hooned

Hooned kujutavad endast tööprotsesside välist raamistikku. Hoones paiknevad statsionaarsed töökohad, töödeldavad andmed ning tööks kasutatav infotehnoloogia, mille jaoks pakub hoone ka välist kaitset. Lisaks põhinevad tihti nii tööprotsessid kui ka IT-süsteemide käitamine hoones paiknevate taristute ärakasutamisel. Seetõttu on ühelt poolt oluline, et hoonel oleksid nõuetekohased ehituskonstruktsioonid (st seinad, laed, põrandad, uksed ja aknad) ning teiselt poolt kõik vajalikud kommunikatsioonid (nt elekter, vesi, küte, torupost).

Järgnevalt vaadeldakse hoonet, mida kasutab korraga ühe institutsiooni üks või ka mitu allüksust. Need võivad olla erinevate turbenõuetega. Kõige muu kõrval tuleb hoonete puhul arvestada ka sellega, et enamikul juhtudel peavad sinna sisenema ka institutsioonivälised isikud (kodanikud, kliendid, kullerid jt).

Kui hoonet kasutavad korraga erinevad osalised ja seda tehakse erineval otstarbel, tuleb hoone sisustus, varustus ja kasutuskontseptsioon omavahel kokku sobitada. Hoones töötavatele inimestele tuleb luua optimaalne töökeskkond. Välistada tuleb võimalus, et kõrvalised isikud võiksid volitamatult siseneda sellistesse hooneosadesse, kus tegeletakse turbe tagamisega, ning hoonesse üles seatud tehnoloogiat peab olema võimalik käitada turvaliselt ja efektiivselt.

Selles moodulis kirjeldatakse, milliseid meetmeid peaks institutsioon võtma, et kasutada hoonet infoturbe seisukohalt parimal võimalikul moel. Kuigi meetmete valik ja sisu olenevad paljuski ka institutsiooni liigist ja suurusest, on püütud siin moodulis esitatud soovitusi koostada nii, et neid saaks rakendada korraga nii suurtes, mitmest hoonest koosnevates kompleksides kui ka üksikutes hooneosades, kui sama hoonet kasutab korraga mitu institutsiooni.

Ohud

Hoone IT-turvameetmete puhul arvestatakse järgmiste tüüpiliste ohtudega:
Vääramatu jõud:

- G 1.3 Äike
- G 1.4 Kahjutuli
- G 1.5 Vesi
- G 1.12 Massiüritustest tingitud probleemid

Organisatsioonilised puudused:

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.6 Volitamata pääs ruumidesse
- G 2.105 Õigusaktide ja lepingute sätete rikkumine

Inimvead:

- G 3.85 Tuletõkete kahjustamine

Tehnilised rikked:

- G 4.1 Toitevõrgu katkestus
- G 4.2 Sisevõrkude katkestus
- G 4.3 Turvavahendi tõrge
- G 4.88 EMC nõuetele mittevastav elektrisüsteem

Ründed:

- G 5.3 Volitamatu sisenemine hoonesse
- G 5.4 Vargus
- G 5.5 Vandalism
- G 5.6 Füüsiline rünne

Soovitatavad meetmed

Vaadeldava IT-süsteemi turvalisuse tagamiseks tuleb lisaks käesolevale moodulile rakendada veel teisigi mooduleid vastavalt infosüsteemide etalonturbe rakendusjuhendi modelleerimise tulemustele.

Selles moodulis käsitletakse ettevõtete ja ametiasutuste tüüpiliste hoonete planeerimise ja kasutamisega seotud tehnilisi ja ka mittetehnilisi turbeaspekte. Samuti vaadeldakse kogu hoonete kasutustsüklit alates nõuetekataloogi koostamisest kuni ümberehitustööde või väljakolimiseni ning kõike muud, mis jääb nende vahele (kontseptsioon, sisseseade ja kasutus).

Hoone kaabeldust käsitletakse spetsiaalselt moodulites B 2.2 Elektrotehniline kaabeldus ja B 2.12 IT-kaabeldus , seevastu eriotstarbega ruumide, nt serveriruumide ja arhiivide käsitlused leiate moodulite teisest kihist.

Ettevõtete ja ametiasutuste käsutuses olevate hoonete puhul tuleb infoturbenõuete täitmiseks vajalike meetmete täitmiseks kasutada erinevaid strateegiaid. Uue hoone rajamisel on võimalik vajalike meetmetega suures osas arvestada juba hoone planeerimise etapis.

Seevastu olukorras, kus hoone kas üüritakse või kui asutakse kasutama juba varem valmis ehitatud hoonet, võib infoturbe tagamiseks vajalike meetmete võtmine olla tavapärasest palju keerulisem.

Planeerimine ja konseptsioon

Hoone kavandamisel ja turbeaspektidele vastaval sisustamisel tuleb lähtuda hoones aset leidvate tööprotsesside turbevajadusest. Hoone sobivuse analüüsimist tuleb alustada krundi asukoha ja selle paiknemise hindamisest, st tuleb hinnata, kas väljavalitud kinnistul paiknevat hoonet on võimalik kasutada ette nähtud otstarbel või kas seda saab kujundada nõuetele vastavaks.

Olemasoleva hoone hindamisel ja planeerimisel on soovitatav koostada ka tsoonimudel (vt M 1.79 Turvatsoonide rajamine), mille põhjal saab hoone kasutust planeerida turbevajaduse alusel (vt M 1.78 Hoone kasutuse turvakontseptsioon). Nende meetmete põhjal saab välja töötada nõuded, kuidas inimesed hoonesse sisse pääsevad ja selles liiguvad (neid kirjeldatakse lähemalt meetmes M 1.80

Juurdepääsukontrolli süsteem ja volituste haldus), samuti ustele ja akendele esitatavad nõuded ning muud turbe- ja seirelahendused.

Ruumide sisustuse planeerimisel tuleks arvestada meetmega M 1.8 Ruumide tuleohutus , juba olemasoleva hoone kasutamisel aga meetmega M 1.13 Kaitset vajavate ruumide paigutus . Ruumide planeeritavat kasutusotstarvet arvesse võttes tuleb alati hoolitseda ka selle eest, et töötajatel oleksid olemas piisavad elektriühendused (vt M 1.3 Juhtmestuse kohandamine).

Soetamine

Uue hoone rajamiseks vajaliku asukoha valimist kirjeldatakse meetmes M 1.16 Hoone sobiv asukoht ning juba olemasoleva hoone asukoha hindamist meetmes M 2.334 Sobiva hoone valimine .

Ehitusetapp ja ettevalmistus kasutamiseks

Ehitusetapis tuleb kõik planeerimisfaasis oluliseks määratud kaitsemeetmed rakendada. Ehitusetapis tuleb igal juhul järgida abinõusid M 1.1 Vastavus normidele ja eeskirjadele ning M 1.6 Tuletõrje-eeskirjade täitmine . M 1.2 Jaotusseadmete pääsueeskirjad samuti ka M 2.14 Võtmete (ja kaartide) haldus
tuleb hiljemalt hoonesse sisse kolides kindlalt määratleda. Samuti on vajalik sisenemise reguleerimine ning sisenemise kontrollimise kontseptsioon vastavalt M 2.17 Sisenemisreeglid ja reguleerimine).

Hoone kasutus

Hoone kasutuse faasi ajal on ette nähtud väga reeglipärane M 2.15 Tuleohutuse kontroll , millega kontrollitakse etteantud ettekirjutusi tuleohutuse kohta. Meetme M 1.15 Aknad ja uksed suletud reeglipärane kasutamine tagab, et hoones viibivad ainult volitatud isikud ning on olemas elementaarne kaitse sissemurdmise vastu.

Valmisolek hädaolukorraks

Et olla valmis hädaolukorraks, tuleb koostada alarmeerimisplaan. Reeglipäraselt tuleb läbi viia hädaolukorra õppused, vastasel korral varitseb oht, et hädaolukorra puhul võetakse vastu valed otsused või et vajalike toimingute juures valitseb ebakindlus. (vaata M 6.17 Avariiolukorrast teavitamise plaan ja tuleohutuse alased õppused).

Järgmisena tutvustatakse meetmete kogumit „Hoone“ kohta:

Planeerimine ja kontseptsioon

- (L) M 1.3 Juhtmestuse kohandamine
- (M) M 1.4 Piksekaitse
- (L) M 1.5 Välisliinide lahutuslülitid
- (L) M 1.7 Tulekustutid
- (L) M 1.8 Ruumide tuleohutus
- (M) M 1.10z Turvauksed ja -aknad
- (L) M 1.11 Trasside plaanid
- (L) M 1.12 Kaitstavate hooneosade märgistamata jätmine
- (L) M 1.13 Kaitset vajavate ruumide paigutus
- (M) M 1.14z Automaatne drenaaž

- (L) M 1.18 Valve- ja tuletõrjesignalisatsioon
- (M) M 1.19z Sissemurdmiskaitse
- (L) M 1.50 Kaitse suitsu eest
- (L) M 1.74z Virtuaalse taristu planeerimine
- (L) M 1.75 Hoonetesisene tuleohutusmärgistus
- (L) M 1.77z Inimeste kliimaseadmed
- (L) M 1.78 Hoone kasutuse turvakontseptsioon
- (L) M 1.79w Turvatsoonide rajamine
- (L) M 1.80w Juurdepääsukontrolli süsteem ja volituste haldus

Soetamine

- (L) M 1.16 Hoone sobiv asukoht
- (L) M 2.334z Sobiva hoone valimine

Rakendamine

- (L) M 1.1 Vastavus normidele ja eeskirjadele
- (L) M 1.2 Jaotusseadmete pääsueeskirjad
- (L) M 1.6 Tuletõrje-eeskirjade täitmine
- (L) M 1.17z Pääsla
- (M) M 1.51 Tulekoormuse vähendamine
- (L) M 2.17 Sisenemisreeglid ja reguleerimine
- (L) M 2.21 Suitsetamiskeeld
- (M) M 2.212 Organisatsioonilised eeskirjad puhastusteenindusele

Kasutamine

- (L) M 1.15 Aknad ja uksed suletud
- (L) M 1.23 Lukustatud uksed
- (L) M 2.14 Võtmete (ja kaartide) haldus
- (L) M 2.15 Tuleohutuse kontroll
- (L) M 2.391 Tuleohutuse eest vastutava isiku varajane informeerimine

Väljavahetamine

- (L) M 2.308z Väljakolimise kord

Valmisolek hädaolukorraks

- (M) M 6.17 Avariiolukorrast teavitamise plaan ja tuleohutuse alased õppused

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.1 Lisanõuded juhtmestuse kohandamisele
- HG.2 Tuletõrje-eeskirjade täitmise seire
- HG.4 Võrguhaldussüsteemi turbe regulaarseire
- HG.69 Ruumide turvatsoneerimise korraldamine

Teabe käideldavus (K)

-

Teabe terviklus (T)

- HT.6 Esemeliste pääsuvahendite halduse seire

Teabe konfidentsiaalsus (S)

- HS.31 Lisanõuded ruumide paigutusele

B 2.2 Elektrotehniline kaabeldus

Infosüsteemide ning teiste seadmete elektrotehniline kaabeldus hõlmab kõiki kaableid ja jagajaid hoones alates jagaja võrgu toitesüsteemist lõpetades tarbija elektriliste ühendustega. Nõuete- ja normikohase elektrotehnilise kaabelduse rakendamine loob aluse ohutuks IT-tegevuseks. IT-kaabeldust IT-süsteemide kommunikatsiooniks käsitletakse eraldiseisvas moodulis (vt. moodul B 2.12 IT-kaabeldus). Kuna mõlema kaabelduse liigi jaoks kasutatakse sageli ühiseid teid ja trasse, tuleb rakendada korraga mõlemaid mooduleid.

Ohud

Elektrotehnilise kaabelduse IT-turvameetmete puhul arvestatakse järgmiste tüüpiliste ohtudega:

Vääramatu jõud:

- G 1.6 Kaablite süttimine

Organisatsioonilised puudused:

- G 2.11 Liinide väike läbilaskevõime
- G 2.12 Kaablite puudulik dokumenteerimine
- G 2.13 Kaitsmata elektrikilbid

Inimvead:

- G 3.5 Liinide juhuslik kahjustamine
- G 3.85 Tuletõkete kahjustamine

Tehnilised rikked:

- G 4.6 Pinge kõikumine / ülepinge / vaegpinge
- G 4.62 Ebapiisav pistikupesade arv
- G 4.63 Tolmunud ventilaatorid

Ründed:

- G 5.8 Liinide manipuleerimine

Soovitatavad meetmed

Vaadeldava IT-süsteemi turvalisuse tagamiseks tuleb lisaks käesolevale moodulile rakendada veel teisigi mooduleid vastavalt infosüsteemide etalonturbe rakendusjuhendi modelleerimise tulemustele.

Elektrotehnilise kaabelduse jaoks tuleb rakendada terve rida meetmeid, alustades ümberpaigutuse planeerimisest kuni kasutamiseni. Sammud, mis sealjuures läbida tuleb, nagu ka meetmed, millega vastavate sammude juures arvestama peab, on järgnevalt kirja pandud. Nagu hoone juures, peab ka siin meeles pidama, et juba olemasolevasse hoonesse kolimisel on võimalused midagi muuta ka kaabelduse kindlustamisel oluliselt väiksemad kui uue hoone ehitamisel.

Planeerimine ja kontseptsioon

Planeerimisfaasis pannakse alus töövõimelisele, hästi turvatud kaabeldusele.

Kaabelduse mehaanilised ja elektrilised omadused määratakse kindlaks kasutatavate kaablitüüpide valiku alusel, samuti kaabli käsitsemise ja trasside ning ka ümbritseva keskkonna tingimuste alusel. Sobivate kaablitüüpide valikul ja sellele tüübile omase paigaldamise abil tuleb elektrotehniline installatsioon teha ümbritsevate ohtude suhtes vastupidavaks. Planeerimise juures tuleks võimaluse korral jälgida ka seda, et liinid ja hoone pea- ning alajaotused füüsiliselt turvatakse sobival viisil kuritarvitamise vastu.

Rakendamine

Üks põhiline tulekaitse element on õige kaablikanalite paigaldamine, mis puuduvate tuletõkete korral võivad põhjustada tõsiseid riske. Kaabelduse paigaldamise juures tuleb tagada ka põhjalik ja korrektne dokumentatsioon, sest hiljem on enamasti väga raske või isegi võimatu kindlaks teha, kus kaablid jooksevad ja mida nad ühendavad.

Kasutamine

Kindla ja häireteta töö tagamiseks tuleb installatsioone ja nende kasutamist reeglipäraselt kontrollida (vt. M 2.394 Elektriseadmete kontrollimine). Trassidega seotud töö juures tuleb tagada tuleohutuse eest vastutava isiku õigeaegne kaasamine planeerimisse ja kujundamisse (vt. M 2.391 Tuleohutuse eest vastutava isiku varajane informeerimine).

Väljavahetamine

Ka elektrikaablid, mida enam ei vajata, tuleb kõrvaldada või kompetentselt töövõimetuks teha (vt. M 5.1 Tarbetute liinide kõrvaldamine või lühistamine ja maandamine).

Hädaolukorra ennetamine

Kui käideldavusele esitatakse suuremaid nõudmisi, tuleb kaabeldus, vajadusel ka välised liinid, planeerida piisava varuga.

Järgmisena tutvustatakse meetmete kogumit „Elektrotehnilise kaabelduse“ kohta:

Planeerimine ja kontseptsioon

- (L) M 1.3 Juhtmestuse kohandamine
- (M) M 1.5w Välisliinide lahutuslülitid
- (L) M 1.20 Kaablite valimine füüsiliste/mehaaniliste omaduste järgi
- (L) M 1.21 Liinide õige dimensioneerimine
- (L) M 1.22z Liinide ja jaotuskilpide füüsiline kaitse
- (M) M 1.25 Liigpingekaitse

Rakendamine

- (L) M 1.9 Ruumide ja korruste tuleisolatsioon trassiavades
- (L) M 1.64 Elektriliste süttimisallikate vältimine
- (L) M 2.19 Neutraalne dokumentatsioon jaotuskilbis
- (L) M 5.4 Kaabelduse dokumenteerimine ja märgistus
- (L) M 5.5 Minimaalselt ohtlikud kaablitrassid

Kasutamine

- (L) M 2.391 Tuleohutuse eest vastutava isiku varajane informeerimine
- (L) M 2.394 Elektriseadmete kontrollimine

Väljavahetamine

- (L) M 5.1 Tarbetute liinide kõrvaldamine või lühistamine ja maandamine

Valmisolek hädaolukorraks

- (M) M 6.18z Varuliinid

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.64 Lisanõuded kaabelduse dokumenteerimisele ja märgistusele

Teabe käideldavus (K)

- HK.28 Nõuded toitevõrgu varukoormusele
- HK.31 Kõrgkäideldavuse lisanõuded kaabelduse paigaldusele
- HK.35 Lisanõuded elektriseadmete kontrollimisele

Teabe terviklus (T)

-

Teabe konfidentsiaalsus (S)

-

B 2.3 Bürooruum

Lokaalseks töökohaks peetakse institutsiooni sees paiknevat ala või alasid, milles viibib kas üks või mitu inimest, kes täidavad seal oma tööülesandeid. See võib olla näiteks bürooruum, tootmiskeskkond või müügisaal.

Tööülesanded võivad olla seotud eri valdkondadega ning neid toetavad kas osaliselt või täielikult IT-lahendused. Tööülesanded võivad hõlmata kirjatööde koostamist, kartoteekide ja loetelude läbitöötamist, nõupidamisi, telefonivestlusi, aktide jt dokumentide lugemist.

Kuna lokaalne töökoht asub institutsiooni sees, võib eeldada, et nende puhul saab võtta üldlevinud taristupõhiseid turvameetmeid, nt rakendada juurdepääsu kontrolli ja järgida tuleohutusnõudeid.

Selles moodulis kirjeldatakse erinevaid meetmeid, kuidas võidelda lokaalse töökoha tüüpiliste ohtudega.

Ohud

IT-etalonturbe seisukohalt loetakse lokaalse töökoha puhul tüüpilisteks järgmisi ohuallikaid.

Organisatsioonilised puudused:

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.6 Volitamata pääs ruumidesse
- G 2.14 IT halb tõhuses töötingimuste tõttu

Inimvead:

- G 3.6 Koristajad jm väljastpoolt tellitud töötajad

Ründed:

- G 5.1 IT-seadmete või -tarvikute manipuleerimine ja hävitamine
- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.4 Vargus
- G 5.5 Vandalism

Soovitatavad meetmed

Vaadeldava IT-koosluse turvalisuse tagamiseks tuleb peale selle mooduli rakendada veel teisigi mooduleid, mis selguvad IT-etalonturbe rakendusjuhendi kohase modelleerimise tulemusel. Lokaalsete töökohtade puhul tuleb võtta erinevaid meetmeid alates planeerimisest ja lõpetades kasutamisega. Järgnevalt on esitatud ülevaade erinevatest kohustuslikest etappidest ja meetmetest, mida iga etapi puhul tuleks võtta.

Planeerimine ja kontseptsioon

Lokaalse töökoha planeerimise võimalused, mida tuleks arvesse võtta, on koondatud meetmesse M 1.76 Lokaalse töökoha valimine ja kasutamine .

Soetamine

Lokaalsete töökohtade puhul, kus töötajatel endil ei ole võimalik võõraste inimeste juurdepääsu reguleerida (nt alades, kus liiguvad külalised, või suurtes avatud büroodes), tuleks sülearvutite kaitseks paigaldada vargalukud, sest muidu on väga suur tõenäosus, et ajal, mil neid seadmeid keegi otseselt ei jälgi, võivad need kaotsi minna. Jultunud kurjategijal kulub väga vähe aega, et sülearvuti või nutitelefon enda kätte haarata ja ruumist lahkuda.

Rakendamine

Ka lokaalsete töökohtade jaoks tuleks kindlaks määrata, kes ja mis tingimustel tohib nendele juurde pääseda. Eriti tähtis on otsustada, millistes alades tohivad liikuda külastajad ning millised alad on ette nähtud vaid ettevõtte või ametiasutuse enda töötajatele.

Kasutamine

Lokaalsetes töökohtades tuleb töödeldavate andmetega väga hoolikalt ümber käia. Seejuures tuleb järgida reegleid, mille tööandja on töökeskkonnale kehtestanud, ja tagada töövahendite turvaline hoidmine.

Ruumidesse sisenemise reeglite ja hoonesissepääsu turvareeglite põhjal tuleb kindlaks määrata ka see, kas büroo tuleb töötajate eemalviibimise ajaks alati lukustada või mitte. Olenevalt hoone eripäradest tuleb hoolitseda samuti selle eest, et volitamata sissepääs oleks välistatud ka siis, kui keegi üritab siseneda näiteks rõdu või akende kaudu.

Järgnevalt on esitatud ülevaade „Lokaalne töökoht" meetmete paketist.

Planeerimine ja kontseptsioon

- (M) M 3.9z Ergonoomiline töökoht
- (L) M 1.76 Lokaalse töökoha valimine ja kasutamine

Rakendamine

- (L) M 2.17 Sisenemisreeglid ja reguleerimine

Kasutamine

- (L) M 1.15 Aknad ja uksed suletud
- (L) M 1.23 Lukustatud uksed
- (L) M 1.45 Äridokumentide ja –andmekandjate sobiv talletus
- (M) M 1.46z Vargusetõrjevahendid
- (L) M 2.37 Korrastatud töölaud

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.2 Tuletõrje-eeskirjade täitmise seire
- HG.4 Võrguhaldussüsteemi turbe regulaarseire
- HG.69 Ruumide turvatsoneerimise korraldamine

Teabe käideldavus (K)

-

Teabe terviklus (T)

- HT.6 Esemeliste pääsuvahendite halduse seire

Teabe konfidentsiaalsus (S)

- HS.31 Lisanõuded ruumide paigutusele

B 2.4 Serveriruum

Serveriruum on mõeldud eelkõige serverite hoiustamiseks, näiteks LAN-server, Unixi server või kodukeskjaama PBX .

Seal võib hoida ka serverit puudutavaid dokumente, väikeses koguses andmekandjaid või teisi riistvara komponente (jaotur, logi printer, konditsioneer).

Serveriruum ei ole sisustatud alalise töökohana. Sinna minnakse harva ja lühiajalisteks töödeks. Silmas on vaja pidada seda, et serveriruumis võib tekkida suurem kahju kui tavalises bürooruumis, sest seal on palju IT-seadmeid ja suur andmete hulk.

Ohud

Serveriruumi IT-turvameetmete puhul arvestatakse järgmiste tüüpiliste ohtudega:

Vääramatu jõud:

- G 1.4 Kahjutuli
- G 1.5 Vesi
- G 1.7 Lubamatu temperatuur ja niiskus
- G 1.16 Kaablijaotusseadmete väljalangemine põlengu tõttu

Organisatsioonilised puudused:

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.6 Volitamata pääs ruumidesse

Tehnilised rikked:

- G 4.1 Toitevõrgu katkestus
- G 4.2 Sisevõrkude katkestus
- G 4.6 Pinge kõikumine / ülepinge / vaegpinge

Ründed:

- G 5.1 IT-seadmete või -tarvikute manipuleerimine ja hävitamine
- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.3 Volitamatu sisenemine hoonesse
- G 5.4 Vargus
- G 5.5 Vandalism

Soovitatavad meetmed

Et turvata teatud IT-varasid, tuleb lisaks sellele moodulile kasutusele võtta veel täiendavad moodulid vastavalt IT-turvameetmete modelleerimise tulemustele.

Et serveriruum välja valida ja sisustada, tuleb rakendada terve rida infrastruktuurseid ja organisatoorseid meetmeid, mida kirjeldatakse moodulis M 1.58 Tehnilised ja organisatsioonilised nõuded serveriruumidele . Teatud meetmete juures on vaja järgida erinevaid lähenemisviise, sõltuvalt sellest, kas serveriruum sisustatakse uude vastvalminud hoonesse, kas see üüritakse või kasutatakse juba olemasolevat hoonet. Teisel juhul on adekvaatse IT- ohutuse realiseerimisvõimalused

sageli palju rohkem piiratud. Etapid, mis on vajalikud serveriruumi kujundamisel kui ka meetmed, mida on vaja sealjuures jälgida, on järgnevalt üles loetletud.

Planeerimine ja kontseptsioon

Serveriruumide planeerimisel on terve rea meetmete abil vaja hoolt kanda piisava füüsilise turvalisuse eest, nagu elektrivarustuse installeerimine, õhukonditsioneeri paigaldamine ja tuleohutus. Serveriruumis ei tohiks võimaluse korral olla veetorusid, sest lekked võivad tekitada suuri kahjusid, mis võivad viia kuni kõigi IT-seadmete väljalangemiseni. Kui käideldavusele esitatakse suuremaid nõudmisi, peab serveriruum tagama piisava varu, mis planeeritakse juba tehnilise infrastruktuuri käigus, et võimaldada ületada üksikuid rikkeid.

Rakendamine

Ainult need inimesed, kes vajavad oma ülesannete täitmiseks otsest ühendust serveri ja muude serveriruumis installeeritud seadmetega, nagu sidejaotus, tulemüür jne, peaksid omama sissepääsu sellesse ruumi. Samuti peab suitsetamiskeeld serveriruumis olema kõikidele üheseltmõistetav.

Kasutamine

Juhul kui serveriruumis isikuid ei viibi, peavad serveriruumid alati lukustatud olema.

Järgmisena tutvustatakse meetmete kogumit „Serveriruumi“ kohta:

Planeerimine ja kontseptsioon

- (L) M 1.3 Juhtmestuse kohandamine
- (L) M 1.7 Tulekustutid
- (M) M 1.10z Turvauksed ja -aknad
- (M) M 1.18z Valve- ja tuletõrjesignalisatsioon
- (L) M 1.24 Veetorude vältimine IT-ruumis
- (L) M 1.26w Toite avariilülitid
- (M) M 1.27 Konditsioneer
- (M) M 1.28 Puhvertoiteallikas
- (M) M 1.31z Tõrgete kaugindikatsioon
- (M) M 1.52z Tehnilise infrastruktuuri varud

- (L) M 1.58 Tehnilised ja organisatsioonilised nõuded serveriruumidele
- (L) M 1.62 Kaablijaotusseadmete tulekaitse

Rakendamine

- (L) M 2.17 Sisenemisreeglid ja reguleerimine
- (L) M 2.21 Suitsetamiskeeld

Kasutamine

- (L) M 1.15 Aknad ja uksed suletud
- (L) M 1.23 Lukustatud uksed

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.1 Lisanõuded juhtmestuse kohandamisele
- HG.2 Tuletõrje-eeskirjade täitmise seire
- HG.4 Võrguhaldussüsteemi turbe regulaarseire
- HG.55 Esemete tõstetud hoidmine serveri- ja arhiiviruumides
- HG.66 Tulekustutite nõue serveri- ja arhiiviruumides
- HG.67 Veetorude keeld serveri- ja arhiiviruumides
- HG.69 Ruumide turvatsoneerimise korraldamine

Teabe käideldavus (K)

- HK.1 Varu-elektrigeneraatori nõue
- HK.11 Serveriruumide ja kaitsekappide temperatuuriseire
- HK.30 Serveriruumi ja andmearhiivi eraldatuse nõue

Teabe terviklus (T)

- HT.6 Esemeliste pääsuvahendite halduse seire
- HT.26 Serveriruumi ja andmearhiivi külastajate logiraamatu pidamine
- HT.44 Lisanõuded turvaustele ja -akendele

Teabe konfidentsiaalsus (S)

- HS.31 Lisanõuded ruumide paigutusele

B 2.5 Andmekandjate arhiiv

Andmetekandjate arhiivis hoitakse igat liiki andmekandjaid. Etalonturbe juhendi alusel ei esitata arhiivi ruumile suuremaid tuleohutusnõudeid. Tuleohutuse võib tagada vastavalt IT-omaniku vajadustele konteineritega, kus andmekandjaid säilitatakse.

Tsentraalandmetekandjate arhiivi ja andmete varundamise arhiivi puhul on soovitatav kasutada andmete kaitsekappe (vaata moodulit B 2.7 Kaitsekapid), et tagada tuleohutus, kaitsta volitamatu juurdepääsu eest andmetele ning tagada volitatud ligipääs. Moodul B 2.5 Andmekandjate arhiiv sobib põhimõtteliselt ka paberi-, filmi- või muude aktide, dokumentide ja ürikute hoiustamiseks, ka siis kui see otseselt selle jaoks mõeldud pole. Mõned soovituslikud meetmed tuleb sellisel juhul vastavalt ümber hinnata.

Ohud

Andmekandjate arhiivi IT-turvameetmete puhul arvestatakse järgmiste tüüpiliste ohtudega:

Vääramatu jõud:

- G 1.4 Kahjutuli
- G 1.5 Vesi
- G 1.7 Lubamatu temperatuur ja niiskus
- G 1.8 Tolm, saastumine

Organisatsioonilised puudused:

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.6 Volitamata pääs ruumidesse

Ründed:

- G 5.3 Volitamatu sisenemine hoonesse
- G 5.4 Vargus
- G 5.5 Vandalism

Soovitatavad meetmed

Et turvata teatud IT-varasid, tuleb lisaks sellele moodulile kasutusele võtta veel täiendavad moodulid vastavalt IT-turvameetmete modelleerimise tulemustele.

Andmekandjate arhiivi jaoks tuleb rakendada mitmeid meetmeid, alustades planeerimise ja kontseptsiooniga, lõpetades igapäevase tööga. Etapid, mis tuleb läbida, samuti meetmed, millele tuleb tähelepanu pöörata, on allpool kirjeldatud.

Planeerimine ja kontseptsioon

Andmekandjate arhiivi põhistruktuur ja seega selle kasutamise peamised raamtingimused määratakse kindlaks planeerimise ja kontseptsiooni loomise käigus. Loomulikult pakub uue hoone sisse seadmine suurimaid valikuvõimalusi. Kui andmekandjaruum planeeritakse juba eksisteerivasse hoonesse, jäävad võimalused kasutuse planeerimisel piiratumaks, eelkõige üüriruumide puhul.

Ruumi valides, kuhu arhiiv sisse seatakse, on kaitseomadused juba suures osas määratletud. Hilisemad muudatused nagu veetorustiku eemaldamine on sageli vaid suurte kulutustega läbiviidavad. Vajalikud tehnilised installeerimised nagu konditsioneeri või valveseadme paigaldus, tuleks võimalusel juba planeerimisel või andmekandjate arhiivi valikul läbi viia.

Rakendamine

Enne andmekandjate arhiiviruumi kasutuselevõttu tuleb kindlaks määrata organisatoorsed reeglid, mis toetavad korraldatud ja turvatud tööd.

Kasutamine

Jooksva töö puhul tuleb vastavat kontrolli läbi viies kindlustada, et ettekirjutatud reeglitest praktikas ka tõepoolest kinni peetakse. Siia kuulub eelkõige põhimõte, et arhiivi pääsevad ainult volitatud isikud ning et arhiiv on lukustatud, kui keegi seal sees ei viibi.

Järgmisena tutvustatakse meetmete kogumit „Andmekandjate arhiivi“ kohta:

Planeerimine ja kontseptsioon

- (M) M 1.7 Tulekustutid
- (M) M 1.10z Turvauksed ja -aknad
- (M) M 1.18z Valve- ja tuletõrjesignalisatsioon
- (M) M 1.24 Veetorude vältimine IT-ruumis
- (M) M 1.27 Konditsioneer

Rakendamine

- (L) M 2.17 Sisenemisreeglid ja reguleerimine
- (L) M 2.21 Suitsetamiskeeld

Kasutamine

- (L) M 1.15 Aknad ja uksed suletud
- (L) M 1.23 Lukustatud uksed

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.2 Tuletõrje-eeskirjade täitmise seire
- HG.55 Esemete tõstetud hoidmine serveri- ja arhiiviruumides
- HG.66 Tulekustutite nõue serveri- ja arhiiviruumides
- HG.67 Veetorude keeld serveri- ja arhiiviruumides
- HG.69 Ruumide turvatsoneerimise korraldamine

Teabe käideldavus (K)

- HK.29 Kaabelduse minimaalsuse nõue andmearhiivides
- HK.30 Serveriruumi ja andmearhiivi eraldatuse nõue

Teabe terviklus (T)

- HT.6 Esemeliste pääsuvahendite halduse seire
- HT.26 Serveriruumi ja andmearhiivi külastajate logiraamatu pidamine
- HT.44 Lisanõuded turvaustele ja -akendele

Teabe konfidentsiaalsus (S)

- HS.31 Lisanõuded ruumide paigutusele

B 2.6 Tehnilise infrastruktuuri ruum

Tehnilise infrastruktuuri ruumi on paigaldatud tavaliselt sellised seadmed, mis ei vaja üldse või vajavad harva teenindamist inimese poolt. Tavaliselt on tegu sisevõrkude jagajatega (nt. elektrikaablite sisenemiruum, kõrgpinge üleandmisruum, keskpinge üleandmisruum, madalpinge peajagaja). Vastavalt olukorrale võivad siin asuda ka elektritoite kaitsed. Samuti on võimalik teiste seadmete üles seadmine (UPS, tähtühendus jne.). Koguni võrguserver võib siin paikneda, kui sellele ei ole eraldi ruumi (moodul B 2.4 Serveriruum).

Ohud

Tehnilise infrastruktuuri ruumi IT-turvameetmete puhul arvestatakse järgmiste tüüpiliste ohtudega:

Vääramatu jõud:

- G 1.4 Kahjutuli
- G 1.5 Vesi
- G 1.7 Lubamatu temperatuur ja niiskus

Organisatsioonilised puudused:

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.6 Volitamata pääs ruumidesse

Tehnilised rikked:

- G 4.1 Toitevõrgu katkestus
- G 4.2 Sisevõrkude katkestus
- G 4.6 Pinge kõikumine / ülepinge / vaegpinge

Ründed:

- G 5.1 IT-seadmete või -tarvikute manipuleerimine ja hävitamine
- G 5.3 Volitamatu sisenemine hoonesse
- G 5.4 Vargus
- G 5.5 Vandalism

Soovitatavad meetmed

Et turvata teatud IT-varasid, tuleb lisaks sellele moodulile kasutusele võtta veel täiendavaid moodulid vastavalt IT-turvameetmete modelleerimise tulemustele. Infrastruktuuri ruumide jaoks tuleb rakendada rida meetmeid, alustades planeerimisega lõpetades igapäevase tööga. Need sammud, mis tuleb läbida, samuti need meetmed, millele tuleb tähelepanu pöörata, on kirjeldatud järgmistes punktides.

Planeerimine ja kontseptsioon

Infrastruktuuri ruumide planeerimisel on vaja paljude erinevate meetmete abil tagada piisav füüsiline turvalisus, nagu elektrivarustuse paigaldamine, konditsioneeri paigaldamine ja tagada tuleohutus. Võimalusel ei tohiks selles, tavaliselt

hõivamata ruumis olla veetorusid, sest lekked võivad tekitada suuri kahjusid, mis võivad viia kuni kõigi IT seadmete väljalangemiseni. Infrastruktuuri ruumidel peaksid kõrgematele kaitsenõuetele vastavalt olema turvauksed ja -aknad, mis on kaitstud ka vägivaldse sissetungi eest, sest need on sageli rünnakute sihiks.

Rakendamine

Ainult need inimesed, kes vastavaid tehnilisi hooldustöid läbi viivad, peaksid omama sissepääsu infrastruktuuri ruumi ja suitsetamiskeeld peaks olema seal iseenesest mõistetav.

Kasutamine

Tehnilise infrastruktuuri ruumid peaksid olema alati põhimõtteliselt lukustatud, kui seal asuvad seadmed ei ole lukustatud kappidesse, et hoida ära volitamatu kasutamine.

Järgmisena tutvustatakse meetmete kogumit „Tehnilise infrastruktuuri ruumi“ kohta:

Planeerimine ja kontseptsioon

- (M) M 1.3 Juhtmestuse kohandamine
- (L) M 1.7 Tulekustutid
- (M) M 1.10z Turvauksed ja -aknad
- (M) M 1.18z Valve- ja tuletõrjesignalisatsioon
- (L) M 1.24 Veetorude vältimine IT-ruumis
- (M) M 1.26w Toite avariilülitid
- (M) M 1.27 Konditsioneer
- (M) M 1.31z Tõrgete kaugindikatsioon

Rakendamine

- (L) M 2.17 Sisenemisreeglid ja reguleerimine
- (L) M 2.21 Suitsetamiskeeld

Kasutamine

- (L) M 1.15 Aknad ja uksed suletud
- (L) M 1.23 Lukustatud uksed

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.1 Lisanõuded juhtmestuse kohandamisele
- HG.2 Tuletõrje-eeskirjade täitmise seire
- HG.4 Võrguhaldussüsteemi turbe regulaarseire
- HG.69 Ruumide turvatsoneerimise korraldamine

Teabe käideldavus (K)

- HK.1 Varu-elektrigeneraatori nõue

Teabe terviklus (T)

-

Teabe konfidentsiaalsus (S)

- HS.31 Lisanõuded ruumide paigutusele

B 2.7 Kaitsekapid

Kaitsekapid on mõeldud igasuguste andmekandjate ladustamiseks või infotehnoloogiliste seadmete majutamiseks („serverikapp“). Kaitsekapp peab kaitsma selles hoitavaid esemeid volitamatu juurdepääsu ja/või tule ning kahjulike ainete (nt tolmu) eest. Kaitsekappi võib kasutada serveriruumi või andmearhiivi asendusena (vt B 2.4 Serveriruum ja B 2.5 Andmekandjate arhiiv) juhul, kui olemasolevad ruumilised või organisatoorsed lahendused ei võimalda vastavate eraldi ruumide kasutamist. Juhul kui ladustada on tarvis ainult andmekandjaid ja seisma pandud IT- seadmeid, tuleks eelistada andmekappi, mis vastaks EN 1047-1 ja EN 1047-2 normidele.

Lisaks eelnevale võib kaitsekappe kasutada ruumide kaitseotstarbe tõstmiseks ka serveriruumides või andmearhiivides. Kaitsekappe soovitatakse kasutada ka juhul, kui serveriruumis hoitakse ühe organisatsiooni mitme erineva valdkonna servereid, mis ei peaks kõikidele administraatoritele võrdselt ligipääsetavad olema.

Eraldiseisvate ruumidega võrreldava turvataseme saavutamiseks on kaitsekapi kasutamise puhul tarvis rakendada terve rida hädavajalikke meetmeid, alustades sobiva toote väljavalimisest kuni paigutamise ja kasutusreeglistiku loomiseni välja.

Ohud

Infosüsteemide etalonturbe seisukohalt loetakse kaitsekappide puhul tüüpilisteks järgmisi ohuallikaid:

Vääramatu jõud:

- G 1.4 Kahjutuli
- G 1.5 Vesi
- G 1.7 Lubamatu temperatuur ja niiskus
- G 1.8 Tolm, saastumine

Organisatsioonilised puudused:

- G 2.4 Turvameetmete ebapiisav järelevalve

Inimvead:

- G 3.21 Mehaaniliste koodlukkude väär kasutamine

Tehnilised rikked:

- G 4.1 Toitevõrgu katkestus
- G 4.2 Sisevõrkude katkestus
- G 4.3 Turvavahendi tõrge
- G 4.4 Keskkonnast tingitud liinihäired

Ründed:

- G 5.1 IT-seadmete või -tarvikute manipuleerimine ja hävitamine
- G 5.4 Vargus
- G 5.5 Vandalism
- G 5.16 Ohud hoolde- ja haldustööde ajal
- G 5.53 Mugavusest tingitud andmekappide väärkasutus

Soovitatavad meetmed

IT-etalonturbe rakendamiseks on soovitatav, et vajalike meetmetepakettide (moodulite) valik toimuks vastavalt modelleerimise käigus selgunud vajadustele. Kaitsekappide valimisel ja kasutuselevõtul tuleb rakendada terve rida erinevaid meetmeid, tegeldes planeerimise, kontseptsiooni ja soetamisega kuni ekspluatatsioonini välja. Järgnevalt anname ülevaate erinevatest kohustuslikest etappidest ja meetmetest, mida iga etapi puhul tuleks rakendada.

Planeerimine ja kontseptsioon

Enne kaitsekapi soetamist tuleb välja töötada kontseptsioon, mis arvestab kapi jaoks planeeritud erinevate kasutusaladega (vt M 2.311 Kaitsekappide planeerimine .

Soetamine

Peamised sammud, mida kaitsekapi valimisel tuleb järgida, on kirjas meetmes M 2.95 Sobivate kaitsekappide soetamine .

Rakendamine

Kaitsekapile peaks olema juurdepääs ainult nendel isikutel, kes tegelevad tehniliste hooldetöödega ning antud isikud peavad saama vastava koolituse, kuidas kaitsekapiga ümber käia. Suitsetamiskeeld peaks kaitsekapiga ruumis olema iseenesestmõistetav. Juhiseid kaitsekapi ülesseadmise kohta leiate meetmest M 1.40 Kaitsekappide sobiv paigutus .

Kasutamine

Kui kapid ei ole ehitatud selliselt, et neid võiks üles seada ka kaitsmata kasutuskeskkonda, peaksid kaitsekappe majutavad ruumid olema üldjuhul alati lukus. Hoolitseda tuleb sellel eest, et kaitsekapid oleksid alati korrektselt suletud. Eriti hoolikas tuleb olla koodlukkude kasutamisel, kindlustamaks nendega korrektse ümberkäimise.

Järgneb ülevaade „Kaitsekapp“ meetmete paketist.

Planeerimine ja kontseptsiooni loomine

- (L) M 1.7 Tulekustutid
- (M) M 1.18z Valve- ja tuletõrjesignalisatsioon
- (L) M 1.24 Veetorude vältimine IT-ruumis
- (M) M 1.27 Konditsioneer
- (L) M 1.28 Puhvertoiteallikas
- (M) M 1.31z Tõrgete kaugindikatsioon
- (M) M 1.41z Kaitse elektromagnetilise kiirguse eest

- (M) M 2.311 Kaitsekappide planeerimine

Soetamine

- (M) M 2.95 Sobivate kaitsekappide soetamine

Rakendamine

- (M) M 1.40 Kaitsekappide sobiv paigutus
- (L) M 2.17 Sisenemisreeglid ja reguleerimine
- (L) M 2.21 Suitsetamiskeeld
- (M) M 3.20 Kaitsekappide kasutamise juhised

Kasutamine

- (L) M 1.15 Aknad ja uksed suletud
- (M) M 2.96 Kaitsekappide lukustamine
- (M) M 2.97 Õige koodlukuprotseduur

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

-

Teabe käideldavus (K)

- HK.11 Serveriruumide ja kaitsekappide temperatuuriseire

Teabe terviklus (T)

- HT.6 Esemeliste pääsuvahendite halduse seire

Teabe konfidentsiaalsus (S)

-

B 2.8 Kaugtöökoht kodus

Tööülesannete täitmisel kodus, väljaspool ettevõtte või ametiasutuse ruume, tuleb tarvitusele võtta turvameetmed, mis peavad aitama tagada, et koduse töökeskkonna turbeaste oleks sama kõrge nagu bürooruumides. Koduse töökoha puhul ei saa eeldada, et infrastruktuurilised lahendused oleksid sama turvalised nagu äriettevõtetes või ametiasutustes. Kodusele töökohale pääsevad tihti ligi ka pereliikmed või külalised. Käesolev moodul püüab kirjeldada erinevaid meetmeid, kuidas koduse töökoha tüüpiliste ohuallikatega ümber käia. Antud moodulit võib rakendada kaugtöö, vabakutseliste töötajate ja FIE-de puhul.

Ohud

Infosüsteemide etalonturbe seisukohalt loetakse koduse töökoha puhul tüüpilisteks järgmisi ohuallikaid:

Vääramatu jõud:

- G 1.5 Vesi

Organisatsioonilised puudused:

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.6 Volitamata pääs ruumidesse
- G 2.14 IT halb tõhuses töötingimuste tõttu
- G 2.47 Failide ja andmekandjate ebaturvaline transport
- G 2.48 Andmekandjate ja dokumentide puudulik hävitamine

Inimvead:

- G 3.6 Koristajad jm väljastpoolt tellitud töötajad

Ründed

- G 5.1 IT-seadmete või -tarvikute manipuleerimine ja hävitamine
- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.3 Volitamatu sisenemine hoonesse
- G 5.69 Varguseoht kodutöökohas
- G 5.70 Pereliikmete või külaliste manipulatsioonid kodutöökohas
- G 5.71 Tundliku informatsiooni konfidentsiaalsuse kadu

Soovitatavad meetmed

Selleks, et tagada kogu loetletud IT-süsteemi turvalisus, tuleb lisaks käesolevale moodulile rakendada veel ka teisi, IT-etalonturbe modelleerimise käigus selguvaid mooduleid.

Koduse töökoha puhul tuleb rakendada erinevaid meetmeid, tegeldes planeerimise ja käitamisega kuni tundlikku infot sisaldavate andmekandjate ja väljatrükkide hävitamiseni välja. Järgnevalt anname ülevaate erinevatest kohustuslikest etappidest ja meetmetest, mida tuleks iga etapi puhul rakendada.

Planeerimine ja kontseptsiooni loomine

Koduse töökoha planeerimise erinevad võimalused võtab kokku meede M 1.44 Kodutöökoha sobiv konfiguratsioon .

Rakendamine

Koduse töökoha kontrollitud kasutamiseks tuleb ära määrata, millist liiki informatsiooni ettevõtte või ametiasutuse ja kodutöökoha vahel edasi tagasi transportida tohib ning millised on turvameetmed, mida selle puhul rakendada tuleb.

Kasutamine

Ka koduse töökoha kasutamisel tuleb kinni pidada tavapärasest töödistsipliinist. Selle hulka kuuluvad töökoha korrashoidmine, tööandja poolt töökeskkonnale kehtestatud reeglite järgimine ja töövahendite turvaline hoidmine. Kodune töökoht peaks olema lukustatud selliselt, et sinna ei saaks kergesti sisse murda.

Väljavahetamine

Eriti just koduse töökoha puhul on oluline jälgida, et andmekandjad ja väljatrükid saaksid korrakohaselt hävitatud, mitte ei visataks lihtsalt olmeprügi hulka.

Planeerimine ja kontseptsiooni loomine

- (M) M 1.19z Sissemurdmiskaitse
- (L) M 1.44 Kodutöökoha sobiv konfiguratsioon
- (M) M 3.9z Ergonoomiline töökoht

Rakendamine

- (L) M 2.112 Kodutööjaamade ja asutuse vahelise dokumentide ja andmekandjate transportimise reguleerimine

Kasutamine

- (M) M 1.15 Aknad ja uksed suletud
- (M) M 1.23 Lukustatud uksed
- (L) M 2.37 Korrastatud töölaud

Väljavahetamine

- (M) M 2.13 Tundlike ressursside jäljetu hävitamine

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele

Kohustuslikud üldmeetmed

- HG.61 Nõuded kodutööarvutile
- HG.68 Valvesignalisatsiooni kohustus

Teabe käideldavus (K)

-

Teabe terviklus (T)

- HT.50 Andmete turvaline haldamine kodu- ja kaugtööl
- HT.63 Sülearvutite krüpteerimine

- HT.67 Pihuarvutite krüpteerimine

Teabe konfidentsiaalsus (S)
-

B 2.9 Arvutuskeskus

Tänapäevaseid ametiasutuste ja ettevõtete strateegilise riistvara kasutuse tendentse iseloomustavad eelkõige kõrgendatud nõuded käideldavusele ning vajadus ühtsete administreerimiskontseptsioonide järele, mis on tihti ajendatud lisaks ka veel survest personalikulusid kokku hoida. Nõuded süsteemi jõudluse osas on kasvanud eriti neis valdkondades, kus on tarvis pidevalt tagada juurdepääs keskandmebaasidele. Kõrgenenud jõudlusvajaduste rahuldamiseks ja vastavate lühiajaliste reservide hoidmiseks on keskmise suurusega ettevõtted, kes siiani kasutasid peamiselt klient-server-süsteeme, oma IT-süsteeme kas arvutuskeskuse abil täiendanud või osaliselt nendega asendanud.

Arvutuskeskuste all peetakse silmas organisatsiooni tööks vajaminevaid suuremaid andmetöötlusseadmeid (arvuti-, salvestus, printimis-, robotsüsteemid jne) koos sinna juurde kuuluvate ruumidega (arvutiruum, arhiiv, ladu, koosviibimisruum jne). Arvutuskeskus on kas kogu aeg inimestega hõivatud (vahetustega töö), või kui inimesi pidevalt juures ei viibi, on sisse seatud telefonivalve (koos või ilma kaugadministreerimise võimaluseta). Reeglina ei ole ühe ettevõtte andmetöötlus üles ehitatud ainult tsentraliseeritud IT-süsteemidele, vaid vastava töö teevad ära mitmed kesksüsteemiga ühenduses olevad detsentraliseeritud IT-süsteemid. Kuna arvutuskeskuses olevate IT-seadmete ja sealt läbi käivate andmete kontsentratsioon on suur, võib tsentraliseeritud andmetöötlusega kaasneda palju ulatuslikum kahju kui hajutatud süsteemi puhul. Suurema andmetöötlussüsteemi rakendamisel tuleb igal juhul lähtuda arvutuskeskust kajastavast moodulist.

Käesolev moodul keskendub keskmise suuruse ja võimsusega arvutuskeskusele. Käsitletavad turvanõuded jäävad serveriruumile või „serveripargile“ ja kõrge turvalisega arvutuskeskustele (nt pankades kasutatavad arvutuskeskused) esitatavate turvanõuete piirimaile. Lisaks siinkohal nimetatud standardsetele turvanõuetele, mis on ennast praktikas juba tõestanud, on enamatel juhtudel tarvis rakendada ka individuaalseid turvameetmeid, mis arvestaksid konkreetsete nõudmiste ja oludega (siia alla kuulub näiteks IT-etalonturbest lähtuv riskianalüüs). Vääramatu jõu ja terrorismi valdkonnast lähtuvaid ohtusid puudutatakse antud moodulite standard-turvameetmetega vaid osaliselt.

Ühelt poolt on käesolev moodul suunatud neile lugejatele, kes soovivad arvutuskeskust kasutusele võtta ja peavad auditi raames kontrollima, kas nende poolt rakendatud standardsed turvameetmed on sobilikud või mitte. Teiselt poolt on arvutuskeskust kajastavat moodulit võimalik kasutada ka neil, kes soovivad olemasolevat IT-süsteemi keskmise suurusega arvutuskeskusesse kokku koondada, kuna antud moodul võimaldab ülevaadet turvameetmetest, mis on vajalikud arvutuskeskuse turvalise töö tagamiseks. Ülevaatlikkuse säilitamiseks on tehnilistest detailidest ja planeerimise suurusandmetest antud moodulis teadlikult loobutud. Täiesti uue arvutuskeskuse ehitamisel peaksid ka suured IT-osakonnad kaaluma kogemustega planeerimismeeskonna kaasamist või kasutama vastava planeerimis- või nõustamisfirma teenuseid. Arvutuskeskuse teenuse sisseostmisel võib käesolevat moodulit kasutada pakutavate teenuste hindamiseks, et välja selgitada, kas vastavad turvaastmed on piisavad või mitte.

Vastupidiselt serveriruumiga (vt B 2.4 Serveriruum) on paljud arvutuskeskuse IT-turvameetmed mitte valikulised, vaid lausa kohustuslikud. Siia alla kuulub näiteks asjakohane valve- ja tuletõrjesignalisatsioon ning eraldiseisev elektritoide. IT-süsteemide turvaliseks käitamiseks on topeltpõrandad ja spetsiaalne, riistvaraliste objektide valvet pakkuv, tulekahju algfaasi tuvastav tuletõrjesüsteem efektiivsed ja

soodsad lahendused. Hoonete enda kustutussüsteemid on suunatud esmajoones hoone kaitsmisele.

Ohud

Infosüsteemide etalonturbe seisukohalt loetakse arvutuskeskuste puhul tüüpilisteks järgmisi ohuallikaid:

Vääramatu jõud:

- G 1.2 IT-süsteemi avarii
- G 1.3 Äike
- G 1.4 Kahjutuli
- G 1.5 Vesi
- G 1.6 Kaablite süttimine
- G 1.7 Lubamatu temperatuur ja niiskus
- G 1.8 Tolm, saastumine
- G 1.11 Keskkonnaõnnetuste mõjud
- G 1.12 Massiüritustest tingitud probleemid
- G 1.13 Tormid
- G 1.16 Kaablijaotusseadmete väljalangemine põlengu tõttu

Organisatsioonilised puudused:

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.2 Reeglite puudulik tundmine
- G 2.4 Turvameetmete ebapiisav järelevalve
- G 2.6 Volitamata pääs ruumidesse
- G 2.11 Liinide väike läbilaskevõime
- G 2.12 Kaablite puudulik dokumenteerimine

Tehnilised rikked:

- G 4.1 Toitevõrgu katkestus
- G 4.2 Sisevõrkude katkestus
- G 4.3 Turvavahendi tõrge

Ründed:

- G 5.3 Volitamatu sisenemine hoonesse
- G 5.4 Vargus
- G 5.5 Vandalism
- G 5.6 Füüsiline rünne
- G 5.16 Ohud hoolde- ja haldustööde ajal
- G 5.68 Volitamata juurdepääs aktiivsetele võrgukomponentidele
- G 5.102 Sabotaaž

Soovitatavad meetmed

Selleks, et tagada kogu loetletud IT-süsteemi turvalisus, tuleb lisaks käesolevale moodulile rakendada veel ka teisi, IT-etalonturbe modelleerimise käigus selguvaid mooduleid.

Arvutuskeskuse valikul ja kujundamisel tuleb täita terve rida infrastruktuurilisi ja organisatoorilisi eeldusi, mille realiseerimist kirjeldatakse meetmes M 1.49 Tehnilised ja organisatsioonilised nõuded arvutuskeskusele . Teatud meetmete puhul on valiku ja kujundamise tegevuskavad erinevad, sõltuvalt sellest, kas arvutuskeskust on tarvis sisse seada uude, alles ehitatavasse hoonesse, või on tegu täiendavate ruumide rentimise või olemasoleva hoone võimaluste ärakasutamisega. Viimasel juhul on adekvaatse IT alase turbe tagamine tihtipeale seotud isegi suuremate takistustega. Järgnevalt anname ülevaate arvutuskeskuse sisseseadmise erinevatest etappidest ja meetmetest, mida tuleks iga etapi puhul rakendada.

Planeerimine ja kontseptsiooni loomine

Arvutuskeskuse planeerimisetapis tuleb tähelepanu pöörata sellele, et tulevaste füüsilist turvalisust tagavate meetmetega, mis puudutavad seadmete ülesseadmiste, voolutoidet, kliimaseadet ja tuleohutust, oleks piisavalt arvestatud. Siia alla kuulub näiteks ka arvestamine asjaoluga, et arvutuskeskuse ruumides ei tohiks olla veetorusid, kuna võimalikud lekked võivad endaga kaasa tuua suuri kahjustusi kuni terve IT-süsteemi avariini välja. Füüsilise kaitse alla kuulub lisaks eelnevale veel ka arvutuskeskuse asukoha valik hoone sees, arvestades võimalikult paljude turvakriteeriumidega, muuhulgas näiteks eraldi tuletõkete ja oluliste ruumide märgistamata jätmisega.

Tehnilisse infrastruktuuri tuleks reeglina sisse arvestada piisav varu, samuti tuleks arvestada varutoiteallika kasutamisega, et üksikute avariidega oleks võimalikult kerge toime tulla. Kahjude ohjamiseks ja kiireks reageerimiseks tuleb kasutusele võtta vastavad ennetavad meetmed. Võimalike kahjustuste tuvastamiseks nende algfaasis tuleb paigaldada sobilikud jälgimissüsteemid, tõrgete kaugindikatsioon ja sobiv kustutussüsteem.

Rakendamine

Arvutuskeskuse serveritele ja muudele sinna üles seatud süsteemidele, nt kommunikatsiooni jaotussüsteemid, tulemüürid jne, tohiks olla juurdepääs vaid neil isikutel, kelle tööülesannete täitmine seda otseselt nõuab. Ruumide koristamine peab olema reguleeritud selliselt, et arvutuskeskusesse pääseb ainult usaldusväärne koristuspersonal ja sedagi ainult järelvalve all. Suitsetamiskeeld peaks olema arvutuskeskuses iseenesestmõistetav, samuti nagu kõige värskemate infrastruktuuriplaanide ja ehitusplaanide olemasolu. Tulekoormuse vähendamiseks tuleb suuri printeripaberi koguseid ladustada väljaspool arvutuskeskust, ruumides, mis ei asu keskusega samas tuletõkketsoonis.

Kasutamine

Kui arvutuskeskuses kedagi ei viibi, peab selle uks olema reeglina alati suletud.

Valmisolek hädaolukorraks

Kuna kaitsemeetmed, mis on jäänud läbi harjutamata, hädaolukorras hästi ei tööta, on vajalik reeglipäraselt läbi viia tuletõrjeõppusi, kuna muuhulgas aitavad need kaasa ka hädaolukorrast teavitamise plaani värskendamisele. Selleks, et olu-

lised andmed oleksid ka pärast suuremat avariid kiiresti kättesaadavad, tuleb neid reeglipäraselt salvestada eraldiseisvasse avariiarhiivi.

Planeerimine ja kontseptsioon

- (M) M 1.49 Tehnilised ja organisatsioonilised nõuded arvutuskeskusele

Voolutoide

- (L) M 1.3 Juhtmestuse kohandamine
- (M) M 1.25 Liigpingekaitse
- (M) M 1.56 Varutoite allikas
- (M) M 1.70 Tsentraalne puhvertoiteallikas

Tuleohutus

- (L) M 1.7 Tulekustutid
- (M) M 1.10z Turvauksed ja -aknad
- (L) M 1.26w Toite avariilülitid
- (M) M 1.47 Eraldi tuletõkked
- (M) M 1.48 Tuletõrjesignalisatsioon
- (M) M 1.50 Kaitse suitsu eest
- (M) M 1.54z Põlengu varajane avastamine / automaatkustutuse tehnoloogia
- (M) M 1.62 Kaablijaotusseadmete tulekaitse

Hoone kaitse

- (L) M 1.12 Kaitstavate hooneosade märgistamata jätmine
- (L) M 1.13z Kaitset vajavate ruumide paigutus
- (L) M 1.18z Valve- ja tuletõrjesignalisatsioon
- (L) M 1.24 Veetorude vältimine IT-ruumis
- (M) M 1.27 Konditsioneer
- (M) M 1.31z Tõrgete kaugindikatsioon
- (M) M 1.52z Tehnilise infrastruktuuri varud
- (M) M 1.53z Videovalve
- (M) M 1.55z Perimeetri kaitse

Rakendamine

- (M) M 1.57 Infrastruktuuri ja hoone uusimad plaanid
- (M) M 2.21 Suitsetamiskeeld
- (M) M 2.212 Organisatsioonilised eeskirjad puhastusteenindusele
- (M) M 2.213 Tehnilise infrastruktuuri hooldus

Kasutamine

- (L) M 1.15 Aknad ja uksed suletud
- (L) M 1.23 Lukustatud uksed
- (M) M 1.71 Tehnilise infrastruktuuri funktsioonikontroll
- (M) M 1.72z Ehitustööde teostamine jooksva töö käigus

- (M) M 1.73 Arvutuskeskuse kaitse volitamata juurdepääsu eest

Valmisolek hädaolukorraks

- (L) M 6.17 Avariiolukorrast teavitamise plaan ja tuleohutuse alased õppused
- (M) M 6.74z Avariiarhiiv

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.1 Lisanõuded juhtmestuse kohandamisele
- HG.2 Tuletõrje-eeskirjade täitmise seire
- HG.4 Võrguhaldussüsteemi turbe regulaarseire
- HG.69 Ruumide turvatsoneerimise korraldamine

Teabe käideldavus (K)

- HK.1 Varu-elektrigeneraatori nõue
- HK.30 Serveriruumi ja andmearhiivi eraldatuse nõue

Teabe terviklus (T)

- HT.6 Esemeliste pääsuvahendite halduse seire

Teabe konfidentsiaalsus (S)

- HS.31 Lisanõuded ruumide paigutusele

B 2.10 Mobiilne töökoht

IT-süsteemide kasutajad muutuvad järjest mobiilsemaks ning tänu üha väiksematele ja võimsamatele seadmetele on töötamine võimalik peaaegu kõikjal. Töökeskkond ei piirdu tihti enam ettevõtte või ametiasutuse ruumidega ning tööülesannete täitmine vaheldub järjest erinevamate kohtade vahel nagu nt hotellituba, ühistransport või kliendi asukoht.

Vahelduva töökeskkonna puhul ei saa eeldada, et infrastruktuurilised lahendused oleksid sama turvalised nagu äriettevõtetes või ametiasutustes. Seetõttu tuleb kasutusele võtta erinevad turvameetmed, mis aitavad viia turbeastme bürookeskkonnaga võimalikult samale tasemele.

Käesolev moodul püüab kirjeldada erinevaid meetmeid, kuidas mobiilse töökoha tüüpiliste ohuallikatega ümber käia.

Ohud

Infosüsteemide etalonturbe seisukohalt loetakse mobiilse töökoha puhul tüüpilisteks järgmisi ohuallikaid:

Vääramatu jõud:

- G 1.15 Muutuvast rakenduskeskkonnast tingitud kahjustused

Organisatsioonilised puudused:

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.4 Turvameetmete ebapiisav järelevalve
- G 2.47 Failide ja andmekandjate ebaturvaline transport
- G 2.48 Andmekandjate ja dokumentide puudulik hävitamine

Inimvead:

- G 3.3 Hooletus turvameetmete suhtes
- G 3.43 Puudulik paroolihooldus
- G 3.44 Teabe hooletu kasutamine

Ründed:

- G 5.1 IT-seadmete või -tarvikute manipuleerimine ja hävitamine
- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.4 Vargus
- G 5.71 Tundliku informatsiooni konfidentsiaalsuse kadu

Soovitatavad meetmed

Vaadeldava IT-süsteemi turvalisuse tagamiseks tuleb lisaks käesolevale moodulile rakendada veel teisigi mooduleid vastavalt infosüsteemide etalonturbe rakendusjuhendi modelleerimise tulemustele.

Mobiilse töökoha kasutamisel tuleb kasutusele võtta terve rida meetmeid. Vastavate meetmete rakendamisel tuleks toetuda, nagu muudelgi juhtudel,

kasututsükli mudelile (life-cycle model).

Planeerimine ja kontseptsiooni loomine

Mobiilse töökoha planeerimise erinevad võimalused, mida võõras töökeskkonnas tuleks järgida, võtab kokku meede M 1.61 Mobiilse töökoha sobiv valimine ja kasutamine .

Rakendamine

Pidevalt muutuva töökoha kasutamiseks tuleb ära määrata, millist liiki informatsiooni ettevõttest või ametiasutusest välja transportida ja töödelda tohib ning millised on turvameetmed, mida selle puhul rakendatakse. Selle käigus tuleb paika panna ka tingimused, mil viisil tohivad mobiilseid IT-süsteeme kasutavad töötajad ligi pääseda oma institutsiooni sisevõrgus olevatele andmetele.

Kasutamine

Mobiilse töökoha kasutamise puhul tuleb lisaks kaasaskantavatele IT-süsteemidele (nt sülearvuti, pihuarvuti, mobiiltelefon) osutada kõrgendatud tähelepanu ka andmetele, mida ringi liikudes töödeldakse. Selle hulka kuuluvad tööandja poolt töökeskkonnale kehtestatud reeglite järgimine ja töövahendite turvaline hoidmine.

Väljavahetamine

Eriti just vahelduva töökoha puhul on oluline jälgida, et andmekandjad ja väljatrükid saaksid korrakohaselt hävitatud, mitte ei satuks olmeprügi hulka.

Alljärgnevalt tutvustatakse meetmete kogumit, mida tuleb rakendada valdkonnas “Mobiilne töökoht”.

Planeerimine ja kontseptsioon

- (L) M 1.61 Mobiilse töökoha sobiv valimine ja kasutamine
- (L) M 2.218 Andmekandjate ja IT-komponentide kaasavõtmise protseduurid
- (L) M 2.309 Mobiilse IT-kasutuse turvapoliitika ja eeskirjad
- (M) M 2.430 Turvapoliitikad ja eeskirjad infoturbe tagamiseks mobiilse töö ajal

Kasutamine

- (L) M 1.15 Aknad ja uksed suletud
- (L) M 1.23 Lukustatud uksed
- (M) M 1.46z Vargusetõrjevahendid
- (L) M 2.37 Korrastatud töölaud
- (M) M 2.389z Avalike pääsupunktide turvaline kasutus
- (L) M 4.251 Töötamine võõraste IT-süsteemidega

Väljavahetamine

- (M) M 2.13 Tundlike ressursside jäljetu hävitamine

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.61 Nõuded kodutööarvutile

Teabe käideldavus (K)

- HK.5 Mobiilseadme aku regulaarvahetus

Teabe terviklus (T)

- HT.50 Andmete turvaline haldamine kodu- ja kaugtööl
- HT.56 Lisanõuded mobiilsele kaugtööarvutile
- HT.63 Sülearvutite krüpteerimine
- HT.67 Pihuarvutite krüpteerimine

Teabe konfidentsiaalsus (S)
-

B 2.11 Nõupidamis-, üritus- ja koolitusruumid

Nõupidamis-, ürituse- ja koolitusruumide eripäraks võrreldes teiste ruumidega on:

- kasutamine vahetuvate inimeste või gruppide poolt,
- ruumide kasutamine nii asutuse oma töötajate kui ka väliste külaliste poolt,
- teatud piiritletud kasutusviis samade isikute poolt kestab tihti vaid lühikest aega, alates mõnest tunnist kuni mõne päevani,
- kaasatoodud IT-süsteeme kasutatakse üheskoos organisatsiooni enda IT-süsteemidega (nt võõras sülearvuti ühendatakse oma projektori külge),
- kasutatav informatsioon on reeglina kas kohapeal olemas (sülearvutis või mobiilse andmekandja peal) või tehakse kättesaadavaks spetsiaalselt sisseseatud testimis- või koolitusvõrgu kaudu. Teatud juhtudel võib olemas olla ka LAN ühendus, mille kaudu on võimaldatud juurdepääs organisatsiooni sisevõrgu andmetele.

Tulenevalt kohati väga erinevast kasutusviisist, on vastavate ruumide ohuallikad teiste ruumidega võrreldes hoopis teistsugused. Lisaks kõikvõimalike üldteada ohtudele tuleb nende ruumide puhul pöörata tähelepanu ka neile ohtudele, mis tekivad ruumis viibivate inimeste „mängutungist“.

Ohud

Infosüsteemide etalonturbe seisukohalt loetakse nõupidamis-, üritus- ja koolitusruumide puhul tüüpilisteks järgmisi ohuallikaid:

Organisatsioonilised puudused:

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.2 Reeglite puudulik tundmine
- G 2.14 IT halb tõhuses töötingimuste tõttu
- G 2.104 Oma ja võõra IT-süsteemi ühildumatus

Inimvead:

- G 3.6 Koristajad jm väljastpoolt tellitud töötajad
- G 3.78 Seadmekaablite halb paigutus ruumis

Tehnilised rikked:

- G 4.1 Toitevõrgu katkestus
- G 4.2 Sisevõrkude katkestus

Ründed:

- G 5.4 Vargus
- G 5.71 Tundliku informatsiooni konfidentsiaalsuse kadu

Soovitatavad meetmed

Selleks, et tagada kogu loetletud IT-süsteemi turvalisus, tuleb lisaks käesolevale moodulile rakendada veel ka teisi, IT-etalonturbe modelleerimise käigus selguvaid mooduleid.

Planeerimine ja kontseptsioon

Selleks, et tagada kogu loetletud IT-süsteemi turvalisus, tuleb lisaks käesolevale moodulile rakendada veel ka teisi, IT-etalonturbe modelleerimise käigus selguvaid mooduleid.
Nõupidamis-, ürituse- ja koolitusruumide kasutusvõimalused on vägagi erinevad. Kuna erinevad kasutusalad nõuavad ka erinevaid turvameetmeid, tuleks esmalt koostada ülevaade, mis hõlmaks vastavate ruumide kõiki võimalikke kasutusvaldkondi (vt M 2.331 Nõupidamis-, ürituse- ja koolitusruumide kavandamine).
Toetudes kasutusala kontseptsioonile, tuleks välja valida sobivad ruumid ning need vastavalt vajadusele sisse seada (vt M 2.332 Nõupidamis-, ürituste- ja koolitusruumide sisustamine).
Juhul kui vajaduste hulka kuuluvad ka LAN ja internetiühendus, tuleb nõupidamis-, ürituse- ja koolitusruumide võrguühendused turvaliseks muuta (vt M 5.124 Võrgupääsu korraldus nõupidamis-, ürituse- ja koolitusruumides).

Rakendamine

Nõupidamis-, ürituse- ja koolitusruumide kasutamiseks tuleb välja töötada oma turvapoliitika ja see nii tehnilisel kui ka organisatoorsel tasandil ellu viia. Kõiki töötajaid tuleb informeerida selle kohta, millised kasutusreeglid on neile kohustuslikud (vt M 2.333 Nõupidamis-, ürituste- ja koolitusruumide turvaline kasutamine).

Kasutamine

Ka nõupidamis-, ürituse- ja koolitusruumide kasutamisel tuleb sisseseade ja olemasoleva tehnikaga hoolikalt ümber käia. Selle hulka kuuluvad organisatsiooni poolt töökeskkonnale kehtestatud reeglitest kinnipidamine ja töövahendite turvaline hoidmine.

Väljavahetamine

Kuna nõupidamis-, ürituse- ja koolitusruumide kasutajad vahetuvad tihti, on väga oluline, et igasugused töömaterjalid nagu andmekandjad ja paberid saaksid korrakohaselt hävitatud, mitte ei jääks lihtsalt kuskile vedelema.

Alljärgnevalt tutvustatakse meetmete kogumit, mida tuleb rakendada valdkonnas “Nõupidamis-, ürituse- ja koolitusruumid”.

Planeerimine ja kontseptsioon

- (L) M 2.331 Nõupidamis-, ürituse- ja koolitusruumide kavandamine
- (L) M 2.332 Nõupidamis-, ürituste- ja koolitusruumide sisustamine
- (M) M 3.9z Ergonoomiline töökoht
- (M) M 5.77z Alamvõrkude rajamine
- (L) M 5.124 Võrgupääsu korraldus nõupidamis-, ürituse- ja koolitusruumides

Rakendamine

- (M) M 2.69 Tüüpsete tööjaamade rajamine
- (L) M 2.204 Ebaturvalise võrkupääsu tõkestamine
- (L) M 2.333 Nõupidamis-, ürituste- ja koolitusruumide turvaline kasutamine
- (L) M 4.252 Koolitusarvuti turvaline konfigureerimine

Kasutamine

- (L) M 1.15 Aknad ja uksed suletud
- (L) M 2.16 Välispersonali ja külastajate valve ja saatmine
- (L) M 4.109z Tööjaamade tarkvara reinstalleerimine
- (M) M 4.293z Avalike pääsupunktide turvaline käitamine

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.2 Tuletõrje-eeskirjade täitmise seire
- HG.4 Võrguhaldussüsteemi turbe regulaarseire
- HG.62 Lisanõuded nõupidamisruumide võrguühendusele

Teabe käideldavus (K)
-
Teabe terviklus (T)
-
Teabe konfidentsiaalsus (S)
-

B 2.12 IT-kaabeldus

IT-kaabelduse alla kuuluvad kõik kommunikatsioonikaablid ja passiivsed komponendid (ristühendused, jätkud, kaablijaotusseadmed), mis on asutuse enda omad (või tema hallata) ja mida kasutatakse oma äranägemise järgi. IT-kaabeldus moodustab organisatsiooni sisekommunikatsioonivõrgu füüsilise aluse. Siia alla kuuluvad nii välisvõrkude ühenduskohad (nt telekommunikatsioonifirma ISDN-ühendus, Interneti-teenuse DSL-ühendus) kui ka sisevõrgu kasutajate ühenduskohad.

Aktiivseid võrgukomponente nagu nt marsruutereid ja kommutaatoreid käesolev peatükk ei käsitle. Samuti jääb käsitluse alt välja WLAN. Mõlema teema kohta on IT-etalonturbe kataloogis olemas eraldi moodulid. Käesolevas moodulis peetakse IT-kaabelduse all silmas füüsilist baasi kommunikatsioonivõrgu ehk Local Area Network (LAN) jaoks, mis ei ole seotud ei kindla tootjafirma ega kindla ettemääratud kasutusalaga. Andmeedastuse jaoks mõeldud IT-kaabeldust ja telekommunikatsiooniteenuste tarbeks vajaminevat PBXi (või kõneside) kaabeldust antud käsitluses teineteisest ei lahutata.

Kinnistute ja hoonete tehnilise infrastruktuuri osana on IT-kaabeldus jaotatud vastavalt kehtivale kaablite struktureerimisviisile primaar-, sekundaar- ja tertsiaarkaabliteks.

Primaarkaabeldusena tähistatakse neid kaableid, mis hooneid omavahel ühendavad. Primaarkaabeldus katab pikki vahemaid, on kõrge edastusvõimsusega ning selle ühenduskohtade arv on väike. Enese poolt kontrollitav primaarkaabeldus on ainult neil asutustel, kelle käsutuses on suured kinnistud koos mitmete hoonetega. Üksikut hoonest käsitledes on hoone primaarkaabelduseks loomulikult peajaotur.

Sekundaarkaabelduse all peetakse silmas kaableid, mis jooksevad hoone jaoturi ja hoone eri korrustel või eri osades olevate jaoturite vahel. Sekundaarkaabelduse leiab eest paljudest suurtes hoonetest.

Tertsiaarkaabelduse moodustavad kaablid, mis ühendavad lõppseadmed ühe keskse jaotuspunkti (nt korruse jaotuspunkti) külge. Need on alati olemas.

Kaablistruktuuri seguvorme esineb tihti neil juhtudel, kus lõppseadmete ühen-

damise keskne jaotuskoht asub otse serveriruumis või tehnilise infrastruktuuri ruumis („Võrguruum“, „Telekommunikatsiooniruum“). Niisugustel juhtudel koosneb sekundaarkaabeldus tihti vaid kommutaatoreid ühendavatest kaablitest. Tertsiaarkaabeldus kulgeb hoone kesksest jaotuspunktist kuni ruumis olevate ühenduspesadeni.

Ohud

Infosüsteemide etalonturbe seisukohalt loetakse IT-kaabelduse puhul tüüpilisteks järgmisi ohuallikaid:

Vääramatu jõud:

- G 1.6 Kaablite süttimine

Organisatsioonilised puudused:

- G 2.11 Liinide väike läbilaskevõime
- G 2.12 Kaablite puudulik dokumenteerimine
- G 2.32 Võrgu ebapiisav võimsus

Inimvead:

- G 3.4 Lubamatud Kaabliühendused
- G 3.5 Liinide juhuslik kahjustamine

Tehnilised rikked:

- G 4.4 Keskkonnast tingitud liinihäired
- G 4.5 Läbikoste
- G 4.21 Tasandusvoolud varjes

Ründed:

- G 5.7 Liinide pealtkuulamine
- G 5.8 Liinide manipuleerimine

Soovitatavad meetmed

Selleks, et tagada kogu loetletud IT-süsteemi turvalisus, tuleb lisaks käesolevale moodulile rakendada veel ka teisi, IT-etalonturbe modelleerimise käigus selguvaid mooduleid.

Antud teemaga on väga tihedalt seotud moodul B 3.302 Marsruuterid ja kommutaatorid ning selle rakendamine peaks toimuma käesoleva mooduliga koostöös. Kui käsiteldavas IT-süsteemis plaanitakse traadita kohtvõrgu kasutamist, tuleb lisaks käesolevale rakendada ka moodulit B 4.6 Traadita kohtvõrgud .

IT-kaabelduse puhul tuleb rakendada erinevaid meetmeid, tegeldes plaanimise ja teostamisega kuni käitamise ja hädaolukorra plaani koostamiseni välja. Järgnevalt anname ülevaate erinevatest kohustuslikest etappidest ja meetmetest, mida tuleks iga etapi puhul rakendada. Muuhulgas tuleb arvestada asjaoluga, et IT-kaabelduse turvalisuse tagamise võimalused on olemasolevasse hoonesse sissekolimisel palju väiksemad kui uue hoone ehitamise puhul.

Planeerimine ja kontseptsioon

Planeerimisfaasis pannakse alus piisava jõudlusega ja turvalise IT-kaabelduse tekkeks. Lähtepunktiks tuleb võtta vajaduste analüüs (vt M 2.395 IT-kaabeldusele esitatavate nõuete analüüs), milles on hinnatud hetkevajadusi ning arvestatud ka institutsiooni võimaliku arengu ja sellega seonduvate vajaduste muutumisega.

Lähtudes eelnevalt väljaselgitatud nõudmistest, pannakse paika võrgu struktuur (vt M 5.2 Võrgu sobiv topograafia) ja sobitatakse kokku hoone võimalustega (vt M 1.21 Liinide õige dimensioneerimine). Kaabelduse mehaanilised ja elektrilised omadused määratakse enamjaolt kaablitüüpide valiku läbi. Planeerimisel tuleks vastavalt võimalustele arvestada ka sellega, kuidas kaableid ja läbi terve maja erinevates kohtades asuvaid lülituskappe võimaliku kuritarvituse eest füüsiliselt kaitsta.

Rakendamine

Tuleohutuse tagamisel on määravaks elemendiks kaablikanalite õige paigutus, sest kanalite puudulik tuletõke võib põhjustada suuri ohtusid. Kaablite paigaldamisel tuleb koostada detailne ja korrektne dokumentatsioon (vt M 5.4 Kaabelduse dokumenteerimine ja märgistus), kuna ilma vastava dokumentatsioonita on hiljem väga raske, kui isegi mitte võimatu, kindlaks teha, kuidas kaablid on veetud ja mida nad omavahel ühendavad. Rikkevaba töö tagamiseks peab IT-kaabeldus olema õigesti paigaldatud (vt M 1.68 Nõuetele vastav installatsioon).

Enne kasutuselevõttu peab aset leidma IT-kaabelduse vastuvõtmine (vt M 5.142 IT-kaabelduse vastuvõtmine), samuti tuleb kontrollida sinna juurdekuuluva dokumentatsiooni kvaliteeti (vt M 5.4 Kaabelduse dokumenteerimine ja märgistus).

Kasutamine

Kasutusloata IT-seadmete sisselülitamise vältimiseks tuleks aktiveerida ainult need ühendused ja pistikupesad, mida tõepoolest ka vajatakse. Sellele lisaks tuleb reeglipäraselt kontrollida, kas vastav aktiveerimine vastab tegelikele vajadustele (vt M 2.20 Liinide kontroll). Täiendavalt tuleb hoolitseda veel selle eest, et igasugused muudatused kajastuksid ka dokumentatsioonis (vt M 5.143 Võrgu dokumentatsiooni pidev edasikirjutamine ja revisjon).

Väljavahetamine

Kui teatud IT-kaabelduse osi ei ole enam tarvis, tuleb need eemaldada (vt M 5.144 IT-kaabelduse demonteerimine).

Valmisolek hädaolukorraks

Juhul kui käideldavusele esitatavad nõuded on kõrged, tuleks kaablid ning olenevalt olukorrast võibolla ka välisühendused planeerida piisava varuga, et ühes suvalises kohas asetleidev rike ei põhjustaks terve süsteemi äralangemist. Selle tagamiseks tuleb planeerida varuga nii hoonetevahelisi kaabliühendusi (vt M 6.103 Primaarkaabelduse liiasus) kui ka hoonetesiseseid kaableid (vt M 6.104 Hoone kaabelduse liiasus).

Alljärgnevalt tutvustatakse meetmete kogumit, mida tuleb rakendada valdkonnas “IT-kaabeldus”.

Planeerimine ja kontseptsioon

- (L) M 1.20 Kaablite valimine füüsiliste/mehaaniliste omaduste järgi
- (L) M 1.21 Liinide õige dimensioneerimine
- (L) M 1.22z Liinide ja jaotuskilpide füüsiline kaitse
- (L) M 1.65z IT kaabelduse uuendamine

- (L) M 1.66z Normidele vastav IT-kaabeldus
- (L) M 2.395 IT-kaabeldusele esitatavate nõuete analüüs
- (L) M 2.396z IT-kaabelduse dokumenteerimise ja märgistuse nõuded

- (L) M 5.2 Võrgu sobiv topograafia
- (L) M 5.3 Sidetehniliselt sobivad kaablitüübid

Rakendamine

- (L) M 1.9 Ruumide ja korruste tuleisolatsioon trassiavades
- (L) M 1.67 Kapisüsteemide dimensioneerimine ja kasutus
- (L) M 1.68 Nõuetele vastav installatsioon
- (L) M 1.69z Kaabeldus serveriruumides
- (L) M 2.19 Neutraalne dokumentatsioon jaotuskilbis
- (L) M 5.4 Kaabelduse dokumenteerimine ja märgistus
- (L) M 5.5 Minimaalselt ohtlikud kaablitrassid
- (L) M 5.142 IT-kaabelduse vastuvõtmine

Kasutamine

- (L) M 1.39 Tasandusvoolude vältimine varjes
- (L) M 2.20 Liinide kontroll
- (L) M 5.143 Võrgu dokumentatsiooni pidev edasikirjutamine ja revisjon

Väljavahetamine

- (L) M 5.1 Tarbetute liinide kõrvaldamine või lühistamine ja maandamine
- (L) M 5.144 IT-kaabelduse demonteerimine

Valmisolek hädaolukorraks

- (L) M 6.103z Primaarkaabelduse liiasus
- (L) M 6.104z Hoone kaabelduse liiasus

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.64 Lisanõuded kaabelduse dokumenteerimisele ja märgistusele

Teabe käideldavus (K)

- HK.31 Kõrgkäideldavuse lisanõuded kaabelduse paigaldusele

Teabe terviklus (T)

- HT.60 Lisanõuded tarbetute liinide kõrvaldamisele

Teabe konfidentsiaalsus (S)

- HS.48 Kõrgkonfidentsiaalsuse lisanõuded IT kaabelduse paigaldusele

B3 IT-süsteemid

Moodulite nimekiri

B 3.101 Server

Serverid on IT-süsteemid, mis võimaldavad teistel IT-süsteemidel (kliendid) võrgu kaudu teenuseid kasutada. Servereid hoitakse tavaliselt hoone keskmes, kõrgemate turvenõuetega, paiknevates ruumides, nagu näiteks serveriruumis või arvutuskeskuses ning neid ei kasutata tööarvutitena. Serverites on võimalik kasutada erinevaid operatsioonisüsteeme, nagu nt Unix/Linux , Microsoft Windows ja Novell Netware . Käesolev moodul vaatleb erinevaid serverite jaoks olulisi turvaaspekte, sõltumata sellest, millist operatsioonisüsteemi serveris parasjagu kasutatakse. Konkreetsetele operatsioonisüsteemidele kehtivad serverite turvaaspektid on eraldi välja toodud IT-etalonturbe kataloogides. Serverikasutuse võrguspetsiifilisi tegureid käsitleb moodul B 4.1 Heterogeensed võrgud .

Ohud

Nagu kõikidel IT-süsteemidel, esineb ka serveril mitmesuguseid ohtusid. Üldjuhul peab paika tõsiasi, et iga üksiku arvuti turvalisus sõltub suuresti tema kasutusalast ehk siis asjaolust, kas seda kasutatakse failiserverina või terminaliserverina ehk autentimisserverina ning iga üksik ohuallikas mõjutab omakorda ka kogu süsteemi turvalisust.

Infosüsteemide etalonturbe seisukohalt loetakse serverite puhul tüüpilisteks järgmisi ohuallikaid:

Vääramatu jõud:

- G 1.1 Personali väljalangemine
- G 1.2 IT-süsteemi avarii

Organisatsioonilised puudused:

- G 2.7 Õiguste volitamata kasutamine
- G 2.9 Halb kohanemine IT muutustega
- G 2.36 Kasutajakeskkonna ebasobiv piiramine

Inimvead:

- G 3.2 Seadme või andmete hävitamine hooletuse tõttu
- G 3.3 Hooletus turvameetmete suhtes
- G 3.5 Liinide juhuslik kahjustamine
- G 3.6 Koristajad jm väljastpoolt tellitud töötajad
- G 3.8 IT-süsteemi väär kasutamine
- G 3.9 IT-süsteemi väär haldus

Tehnilised rikked:

- G 4.1 Toitevõrgu katkestus
- G 4.6 Pinge kõikumine / ülepinge / vaegpinge
- G 4.7 Defektsed andmekandjad
- G 4.10 Keerukad ligipääsuvõimalused võrgustatud IT-süsteemides
- G 4.13 Salvestatud andmete hävimine
- G 4.20 Andmekadu andmekandja täitumise tõttu
- G 4.22 Tüüptarkvara turvaaugud või vead

- G 4.39 Tarkvarakontseptsiooni viga

Ründed:

- G 5.1 IT-seadmete või -tarvikute manipuleerimine ja hävitamine
- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.7 Liinide pealtkuulamine
- G 5.9 IT-süsteemide volitamata kasutamine
- G 5.18 Süstemaatiline paroolide mõistatamine
- G 5.19 Kasutajaõiguste väärkasutus
- G 5.20 Administraatori õiguste väärkasutus
- G 5.21 Trooja hobused
- G 5.23 Viirused
- G 5.26 Sõnumivoo analüüsimine
- G 5.40 Pealtkuulamine ruumis arvuti mikrofoni kaudu
- G 5.71 Tundliku informatsiooni konfidentsiaalsuse kadu
- G 5.75 Ülekoormus siseneva meili tõttu
- G 5.85 Tundliku informatsiooni tervikluse kadu

Soovitatavad meetmed

Selleks, et tagada kogu loetletud IT-süsteemi turvalisus tuleb lisaks käesolevale moodulile rakendada veel teisi, IT-etalonturbe modelleerimise käigus, selguvaid mooduleid.

Eduka serveri ülesehitamiseks tuleb läbida mitmeid etappe, tegeldes kontseptsiooni ja juurutamisega kuni igapäevase töötamiseni välja. Eriti suurt rõhku tuleb kontseptsiooni loomisele ja planeerimisele pöörata juhul, kui serverit hakatakse installeerima uue loodava võrgu tarbeks. Seevastu serveri juurutamisel juba eksisteerivasse võrku võib planeerimisetapp piirduda tihti kõigest sellega, kuidas tagada uue serveri kokkusobivus olemasolevate struktuuridega. Sellele vaatamata tuleb ilmtingimata rakendada serveri hankimise ja töö kohta kehtivaid meetmeid. Järgnevalt anname ülevaate erinevatest etappidest, mis tuleb serveri turvalisuse tagamiseks läbi teha, samuti kirjeldame meetmeid, mida tuleks iga etapi puhul rakendada.

Planeerimine ja kontseptsiooni loomine

Enne tegeliku planeerimistöö algust tuleks võrgu üldstruktuur juba paika panna, st analüüsida, millised on antud juhul operatsioonisüsteemidele esitatavad nõuded (server ja klient). Eriti oluline on siinjuures ära määrata, millised on ülesehitatava serveri kasutuseesmärgid. Selle jaoks tuleb kirjeldada eeldatavad kasutusvaldkonnad ja defineerida kasutusala.

Juhul kui tegemist on uue võrgu ülesehitamisega, tuleks esmalt planeerida, milline saab olema võrgu kui terviku struktuur, otsustades võrgu topograafia ja selle üle, kui keskse ülesandega vastav server peab olema (terminaliserver, „klassikaline“ klient-server-arhitektuur või Peer-to-Peer funktsioonide kasutamine). Siinkohal tuleks abiks võtta moodul B 1.9 Riist- ja tarkvara haldus .

Järgmise sammuna tuleks ära määrata serveri ja kliendi tasandil kasutatavad operatsioonisüsteemid ning vajadusel teha ka täpsem valik erinevate variantide vahel.

Uue võrgu ülesehitamisel tuleb planeerimisjärgus detailselt ära määrata võrgu struktuur, et järgnevatel töödel vajaminev tehniline lähteinfo oleks võimalikult täpne. Ära tuleb määrata vajaminevate serverite arv ning nende koostoimimine. Paika tuleb panna serverite ülesanded ja nende kasutamise viis klientide poolt. Käideldavusele esitatavatest nõuetest lähtudes tuleb ära määrata, mis astmeni peavad võrgu struktuurid olema liiasusega. Siinkohal tuleb määratleda ka infrastruktuuri hädavajalikud eeldused (eelkõige kliimasüsteem ja vooluvarustus, vt M 1.28 Puhvertoiteallikas). Selle kõigega paralleelselt tuleb välja töötada üldine turvapoliitika (vt M 2.316 Serveri turvapoliitika kehtestamine), mida hiljem süsteemi spetsiifiliste ning võrgus kasutatava riist- ja tarkvara detailsemate turvapoliitika reeglitega täiendada (täpsem info on kirjas üksikutes serveri operatsioonisüsteemide moodulites).

Soetamine

Järgmise sammuna tuleb soetada tarkvara ning vajadusel ka lisaks vajaminev riistvara. Kasutusvaldkondadest lähtudes tuleks sõnastada toodetele seatavad nõudmised ning vastavalt nendele teha valik sobilike toodete hulgast. Vajaminevate toodete soetamisega pannakse alus järgmise sammu tööetappidele.

Rakendamine

Kasutajate, täpsemalt administraatorite, mõju serveri turvalisuse tagamisel on määrav. Seepärast peavad kasutajad ja administraatorid saama enne loodava serverisüsteemi tegelikku kasutuselevõttu asjakohase koolituse. Kuna süsteemi planeerimine ja haldamine on keerukas, on eriti soovitatav, et administraatorite koolitus oleks võimalikult põhjalik. Koolituse raames peaksid administraatorid omandama detailseid teadmisi süsteemist, mis võimaldavad neil tagada katkematu ja korrektse halduse. Kasutajate puhul tuleks suurt rõhku pöörata teadmistele, kuidas olemasolevaid turvamehhanisme kasutada. Siinkohal tuleb abiks võtta moodul B 1.13 Infoturbe teadlikkus ja -koolitus .

Pärast organisatsiooniliste ja planeerimist puudutavate eeltööde tegemist saab liikuda edasi serveri installeerimise ja kasutuselevõtu juurde. Siinkohal tuleb arvestada järgmiste asjaoludega:

- Selleks, et kohe algusest peale vältida raskesti parandatavaid vigu, tuleb juba serveri installeerimise ja aluskonfiguratsiooni tegemisel väga hoolas olla. Üldiseid juhiseid selle kohta leiate meetmetest M 2.318 Serveri turvaline installeerimine ning M 4.237 IT-süsteemi turvaline aluskonfiguratsioon . Lisaks üldistele juhistele, mida antud moodul kajastab, tuleb rakendada ka spetsiifilisemaid abinõusid, millekohased soovitused on kirjas vastavates operatsioonisüsteemide kohta käivates moodulites.
- Pärast serverite installeerimist ja aluskonfiguratsioonide tegemist tuleb vajadusel konfigureerida ka hierarhias kõrgemal seisvad haldusstruktuurid. Siinkohal mängib olulist rolli iga üksiku serveri kasutuseesmärk, nt kas failiserver, trükiserver või õhukeste klientide puhul (Thin Client) terminaliserver. Serveri töö kontrolli all hoidmiseks on eriti oluline meede M 2.138 Struktureeritud andmetalletus .
- Pärast seda, kui server on installeeritud ja selle aluskonfiguratsioon tehtud, võib järgmisena installeerida serveri enda tarkvara ja teha vastava aluskonfiguratsiooni. Selleks läbitavad sammud võivad teineteisest vastavalt tarkvara liigile ja kasutusalale kohati suuresti erineda ning osaliselt kajastatakse

neid ka eraldiseisvates moodulites. Üldjuhul on soovitatav serveritarkvara installeerimisel ja konfigureerimisel toimida sarnaselt operatsioonisüsteemi konfigureerimisega:

- installeerimiskontseptsiooni loomine,
- juhul kui on tarvis installeerida mitu sarnase kasutusala ja konfiguratsiooniga serverit: referentsinstallatsiooni loomine,
- installeerimine, aluskonfiguratsiooni tegemine ja täiendite laadimine,
- testimine.

Detailsemad juhised erinevate serverirakenduste turbeks leiate moodulite paketist number 5.

Kasutamine

Pärast esmast installeerimist ja testimisfaasi läbimist minnakse üle tavakasutusele. Turbe seisukohalt tuleb siinkohal arvestada järgmiste asjaoludega:

- Klient-server-võrgud muudavad ennast väga tihti. Iga muutuse korral peab olema tagatud, et muudatuse rakendamine ei osuta turvalisusele negatiivset mõju. Detailsemad juhised, millest tuleb kinni pidada, on ära toodud serveri erinevate operatsioonisüsteemide kohta käivates moodulites. Siinkohal tuleb silmas pidada, et õiguste äravõtmine ning mittevajalike andmete kustutamine peab olema reguleeritud selliselt, et vananenud struktuurid ei tooks endaga kaasa turvaauke. Tõhus abinõu selle tagamiseks on efektiivne ja ulatuslik süsteemihaldus, mis võimaldab igal ajal ligipääsu kõige värskematele andmetele süsteemi seisundi ja õiguste struktuuri kohta (vt M 2.31 Volitatud kasutajate ja õiguste profiilide dokumenteerimine ja M 4.24 Järjekindla süsteemihalduse tagamine).
- Serveri järjekindla turbe tagamise raames on üheks vahendiks süsteemi, st selle üksikkomponentide jälgimine. Asjakohased juhised leiate meetmetest M 4.93 Regulaarne tervikluse kontroll , M 5.8 Võrgu regulaarne turvakontroll ja M 5.9 Serveri logi . Ka andmekaitse tagamine mängib siinkohal tähtsat rolli. Klient-server-süsteemides sagedasti esinevad turvaaugud ning arvukad ründed, mis püüavad vastavaid auke ära kasutada nõuavad süsteemiülematelt, et nad hoiaksid ennast pidevalt kursis süsteemide turvaseisundi ja uute võimalike ohtudega (vt M 2.35 Teabe hankimine turvaaukude kohta) ning rakendaksid õigeaegselt asjakohaseid vastumeetmeid (vt M 2.273 Turvalisust mõjutavate paikade ja värskenduste kiire paigaldamine).

Väljavahetamine

Serverit ei tohi ilma ette teatamata lihtsalt välja lülitada. Kui serverit on tarvis tööst kõrvaldada, tuleb sellest kasutajatele piisava ajavaruga ette teatada ning on terve rida punkte, mida tuleb järgida, vältimaks kasutamise pause ja infokadusid. Vastavad punktid on kirjas moodulis M 2.320 Serveri nõuetekohane kasutuselt kõrvaldamine . Juhul kui serveri teenused on tarvis mõnda teise arvutisse üle viia, järgige moodulit M 2.319 Serveri üleviimine .

Lisaks eelnevale tuleb serveri väljavahetamisel jälgida, et kõvakettale ei jääks alles tundlikku informatsiooni. Kõvaketaste uuesti formaatimine ei ole selle jaoks piisav, kõvakettad tuleb vähemalt üks kord täielikult üle kirjutada. Tuleb silmas pidada, et ei puhtalt loogiline kustutamine ega ka ketaste uuesti formaatimine ins-

talleeritud operatsioonisüsteemide vahenditega ei eemalda kõvaketastelt andmeid ning sobiva tarkvaraga on võimalik andmeid isegi ilma suurema vaevata taastada. Vastavad juhised leiate meetmest M 2.13 Tundlike ressursside jäljetu hävitamine , mida käsitleb hierarhias kõrgemal asuv moodul B 1.1 Organisatsioon , ning meetmest M 4.234 IT-süsteemide ja andmekandjate väljavahetamise kord hierarhias kõrgemal asuvas moodulis B 1.9 Riist- ja tarkvara haldus .

Serveri väljavahetamine tuleb dokumenteerida. Varade nimekirjad ja võrguplaanid tuleb aktualiseerida ning juhul kui väljavahetamisega muutub IT süsteemi struktuur, tuleb ka turvakontseptsiooni vastavalt mugandada.

Valmisolek hädaolukorraks

Vaid reeglipärane ja ulatuslik andmete varundamine suudab kindlalt tagada, et riistvaraliste rikete, avariide ja (tahtlike või tahtmatute) kustutamiste korral on kõiki salvestatud andmeid võimalik teha uuesti kättesaadavaks. Vajalikud meetmed leiate moodulist B 1.4 Andmevarunduspoliitika .

Lisaks jooksva töö salvestamisele mängib tähtsat rolli ka hädaolukordade ennetamine, sest ainult niimoodi on võimalik hädakorral kahjusid vähendada. Juhiseid ootamatuste ennetamise kohta leiate moodulist B 1.3 Hädaplaanimine . Siia alla kuulub ka planeerimine, kuidas turvaintsidentidega ümber käia, mille kohta käiva info leiate moodulist B 1.8 Turvaintsidentide käsitlus . Mõningad serveri kohta käivad ootamatuseplaani puudutavad aspektid on ära toodud meetmes M 6.96 Serveri avariiplaan .

Eeldatakse, et server asub kas serveriruumis (vt moodul B 2.4 Serveriruum), serverikapis (vt moodul B 2.7 Kaitsekapid) või arvutuskeskuses (vt moodul B 2.9 Arvutuskeskus). Serverite operatsioonisüsteemidele rakendatavad meetmed on kirjas vastavates erinevaid operatsioonisüsteeme kajastavates moodulites. Sama kehtib ka ühendatud klientide kohta. Moodulis B 1.9 Riist- ja tarkvara haldus kajastatud meetmed moodustavad kõikidel juhtudel üldise raamistiku serveri toel töötavate võrkude tarbeks.

Lisaks eelnevale tuleb rakendada veel järgmisi täiendavaid meetmeid:

Planeerimine ja kontseptsioon

- (L) M 1.28 Puhvertoiteallikas
- (M) M 2.314z Kõrgkäideldava serveriarhitektuuri kasutamine
- (L) M 2.315 Serveri kasutuselevõtu planeerimine
- (L) M 2.316 Serveri turvapoliitika kehtestamine
- (M) M 4.250z Keskse võrgupõhise autentimisteenuse valimine
- (L) M 4.432 Serveriteenuste turvaline konfiguratsioon
- (L) M 5.10 Piiratud õiguste andmine
- (M) M 5.138z RADIUS serverite kasutamine
- (M) M 5.177 SSL-i/TLS-i kasutamine serveris

Soetamine

- (L) M 2.317 Serveri soetamise kriteeriumid

Rakendamine

- (L) M 2.32z Piiratud kasutajakeskkonna loomine
- (L) M 2.204 Ebaturvalise võrkupääsu tõkestamine
- (L) M 2.318 Serveri turvaline installeerimine
- (L) M 4.7 Algparoolide muutmine
- (L) M 4.15 Turvaline sisselogimine
- (L) M 4.16 Konto- ja/või terminalipääsu piirangud
- (L) M 4.17 Tarbetute kontode ja terminalide blokeerimine
- (M) M 4.40 Arvuti mikrofoni volitamata kasutamise vältimine
- (M) M 4.97z Ainult üks teenus serveri kohta
- (L) M 4.237 IT-süsteemi turvaline aluskonfiguratsioon
- (L) M 4.305 Salvestusvõimaluste piiramine (Quotas)

Kasutamine

- (L) M 2.22z Paroolide deponeerimine
- (L) M 2.273 Turvalisust mõjutavate paikade ja värskenduste kiire paigaldamine
- (L) M 4.24 Järjekindla süsteemihalduse tagamine
- (L) M 4.93z Regulaarne tervikluse kontroll
- (M) M 4.238 Lokaalse paketifiltri rakendamine
- (M) M 4.239 Serveri turvaline käitus
- (M) M 4.240z Serveri testimiskeskkonna rajamine
- (M) M 5.8 Võrgu regulaarne turvakontroll
- (M) M 5.9 Serveri logi

Väljavahetamine

- (L) M 2.319 Serveri üleviimine
- (L) M 2.320 Serveri nõuetekohane kasutuselt kõrvaldamine

Hädaolukorraks valmisolek

- (L) M 6.24 Rikkejärgse buutimismeedia olemasolu
- (L) M 6.96 Serveri avariiplaan

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.6 Arvuti paroolkaitse rangemad reeglid
- HG.24 Paroolide regulaarkontroll parooliskänneriga
- HG.25 Kaugpöörduste kohustuslik logimine
- HG.38 Turvapaikade paigaldatuse regulaarseire

Teabe käideldavus (K)

- HK.27 Puhvertoiteallikas serveri sulgemise tagamiseks

Teabe terviklus (T)

- HT.7 Kasutajate ja nende profiilide perioodiline seire
- HT.14 Süsteemi tegevuslogide krüptoaheldamine
- HT.16 Serverilogi krüptoaheldamine
- HT.51 Lisanõuded teabe hankimisele turvaaukude kohta
- HT.57 Algparoolide muutmise regulaarkontroll
- HT.58 Lisanõuded tarbetute kontode ja terminalide blokeerimisele
- HT.59 Lisanõuded turvalisele sisselogimisele

Teabe konfidentsiaalsus (S)
-

B 3.102 Server Unixi all

Unixi serverid on arvutid, mis töötavad operatsioonisüsteemil Unix ning pakuvad võrgus erinevaid teenuseid, mida teised IT süsteemid võivad kasutada.

Käesolev moodul käsitleb eranditult vaid Unixi all olevate serverite spetsiifilisi ohuallikaid ja turvameetmeid, mistõttu tuleb lisaks käesolevale materjalile järgida ka üldiseid serverile kehtivaid nõudeid, mis on kirjas moodulis B 3.101 Server .

Ohud

Infosüsteemide etalonturbe seisukohalt loetakse Unixi all olevate serverite puhul tüüpilisteks järgmisi ohuallikaid:

Organisatsioonilised puudused:

- G 2.15 Konfidentsiaalsusaugud Unix-süsteemis

Inimvead:

- G 3.10 Failisüsteemide väär eksport Unixis
- G 3.11 Sendmaili väär konfiguratsioon

Tehnilised rikked:

- G 4.11 NIS-serveri ja NIS-klientsüsteemi vahelise autentimisvõimaluse puudumine
- G 4.12 Autentimisvõimaluste puudumine X-serveri ja X-kliendi vahel

Ründed:

- G 5.41 Unix-süsteemi väärkasutus UUCP-ga
- G 5.89 Võrguühenduse ülevõtt

Soovitatavad meetmed

Selleks, et tagada kogu loetletud IT-süsteemi turvalisus, tuleb lisaks käesolevale moodulile rakendada veel ka teisi, IT-etalonturbe modelleerimise käigus selguvaid mooduleid.

Eduka Unixi all oleva serveri ülesehitamiseks tuleb läbida mitmeid etappe, tegeldes kontseptsiooni ja soetamisega kuni igapäevase töötamiseni välja. Järgnevalt anname ülevaate erinevatest kohustuslikest etappidest ja meetmetest, mida iga etapi puhul tuleks rakendada.

Planeerimine ja kontseptsioon

Järgnevalt kirjeldatud meetmed käsitlevad võrgus klientidele teenuseid pakkuva Unixi all oleva serveri turvalist konfigureerimist ja turvalist tööd. Võrgu arhitektuuri üldine planeerimine on paika pandud moodulis B 3.101 Server , milles määratakse täpsemalt ära võrgu üldine arhitektuur ja võrgule kehtiv reeglistik. Nimetatud moodulist tulenevaid serveritele kehtivaid nõudeid tuleb järgida. Mõttekas on server paigutada eraldi serveriruumi. Vajalikud kohustuslikud nõuded leiate moodulist B 2.4 Serveriruum . Serveriruumi puudumisel tuleks kasutada serverikappi, sellisel juhul tutvuge mooduliga B 2.7 Kaitsekapid .

Üheselt tuleb ära määratleda kasutajatunnuste andmise protsess, et priviligeeritud ja mitteprivilegeeritud kasutajatunnuseid oleks võimalik teineteisest selgelt eristada. Lisaks sellele tuleb tagada, et ainukasutajarežiimis ei võimaldataks kellelegi kontrollimatut ligipääsu, kuna vastasel juhul võidakse kõikidest süsteemile kehtestatud turvameetmetest mööda minna.

Soetamine

Serverite arv võrgus, nende kasutamine klientide poolt ja soetatavatele seadetele esitatavad nõuded on üheskoos ära toodud moodulis B 3.101 Server .

Rakendamine

Mõningad järgnevalt kirjeldatud meetmed puudutavad üksikute serverite konfiguratsioone, teisi seevastu tuleb rakendada serverite ja klientide peal, et need tööle hakkaks. Võimalike külgeühendatud klientide puhul tuleb rakendada vastavates moodulites kirjeldatud meetmeid.

Pärast installeerimist tuleb Unixi all oleva serveri konfigureerimise alustamisel lähtuda meetmest M 4.105 Unixi turvaline tüüpinstalleerimine . Siinkohal tuleb vastavalt kasutusalale (võrreldes B 3.101 Server) teha algseaded selliselt, et sisse lülitatakse ainult vajalikud teenused, või nii, et võetakse tarvitusele kirjeldatud meetmed ja lülitatakse sisse süsteemi logi.

Seejärel tuleb jagada ülevaatliku skeemi järgi kasutajafailide, süsteemifailide ning süsteemikataloogide pääsuõigused selliselt, et pääsuõigused saavad ainult need kasutajad ja protsessid, kes neid tõepoolest ka vajavad, kusjuures erilist tähelepanu tuleb siinkohal pöörata setuid ja setgid funktsioonidega antavatele õigustele (vt M 4.19 Unixi süsteemifailide ja -kataloogide atribuutide jaotuse piirangud).

Kasutamine

Unixi all töötava serveri järjepideva turvalisuse tagamiseks on möödapääsmatu, et töö käigus tuleb süsteemi reeglipäraselt võimalike turvaaukude tekke suhtes üle kontrollida, et need saaksid kohe esimesel võimalusel likvideeritud. Kontrolli raames tuleb muuhulgas uurida, kas süsteemi poolt koostatud logides esineb ebakorrapärasusi.

Valmisolek hädaolukorraks

Kuna Unix -süsteemide keerukuse tõttu on ka pärast edukaks osutunud rünnet tihti väga raske saada kahjustuse ulatusest selget ülevaadet, on oluline, et juba eelnevalt oleks paika pandud reeglid, kuidas reaalselt asetleidnud süsteemi tervikluse kao või selle kahtluse korral toimida.

Alljärgnevalt tutvustatakse meetmete kogumit, mida tuleb rakendada valdkonnas „Server Unix“.

Planeerimine ja kontseptsioon

- (L) M 2.33z Unixi ülemarollide jagamine
- (L) M 4.13 Identifikaatorite hoolikas jaotamine
- (L) M 4.18 Monitori- ja ainukasutajarežiimi pääsu reguleerimine
- (M) M 5.16 Võrguteenuste inventuur
- (L) M 5.64z Secure Shell (SSH)

- (L) M 5.83z Turvaline välisvõrguühendus Linux FreeS/WAN abil

Rakendamine

- (L) M 4.9 X Windowsi turvamehhanismid
- (L) M 4.14 Kohustuslik paroolkaitse Unixi all
- (L) M 4.19 Unixi süsteemifailide ja -kataloogide atribuutide jaotuse piirangud
- (M) M 4.20 Unixi kasutajafailide ja -kataloogide atribuutide jaotuse piirangud
- (L) M 4.21 Ülemaõiguste volitamatu võtu vältimine
- (L) M 4.22 Andmete konfidentsiaalsuse kao vältimine Unix-süsteemis
- (M) M 4.23 Käitusfailide turvaline kutsumine
- (L) M 4.105 Unixi turvaline tüüpinstalleerimine
- (L) M 4.106 Süsteemi logimise aktiveerimine (Unix)
- (L) M 5.17 NFSi turvamehhanismid
- (L) M 5.18 NISi turvamehhanismid
- (L) M 5.19 Sendmaili turvamehhanismid
- (L) M 5.20 rlogin, rsh ja rcp turbemehhanismid
- (L) M 5.21 telneti, ftp, tftp, rexeci turvaline kasutamine
- (L) M 5.35 UUCP turvamehhanismid
- (L) M 5.72 Mittevajalike võrguteenuste desaktiveerimine (Unix)

Kasutamine

- (L) M 4.25 Logimine Unix-süsteemis
- (L) M 4.26 Regulaarne turvakontroll Unix-süsteemis

Hädaolukorraks valmisolek

- (L) M 6.31 Protseduurid süsteemi tervikluse kao puhuks

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.6 Arvuti paroolkaitse rangemad reeglid
- HG.24 Paroolide regulaarkontroll parooliskänneriga
- HG.25 Kaugpöörduste kohustuslik logimine
- HG.38 Turvapaikade paigaldatuse regulaarseire
- HG.63 Lisanõuded võrguteenuste inventuurile

Teabe käideldavus (K)

- HK.27 Puhvertoiteallikas serveri sulgemise tagamiseks

Teabe terviklus (T)

- HT.14 Süsteemi tegevuslogide krüptoaheldamine
- HT.16 Serverilogi krüptoaheldamine
- HT.51 Lisanõuded teabe hankimisele turvaaukude kohta
- HT.57 Algparoolide muutmise regulaarkontroll
- HT.58 Lisanõuded tarbetute kontode ja terminalide blokeerimisele

Teabe konfidentsiaalsus (S)
-

B 3.107 Suurarvutid S/390 ja zSeries

IBM S/390- ja zSeries -süsteemid kuuluvad selliste serverisüsteemide hulka, mida liigitatakse üldise nimetaja mainframe (suurarvutid) alla. Suurarvutid on läbi teinud arengu klassikalisest pakktöötlussüsteemist (batch processing) kuni tänapäevase moodsa klient-server-süsteemini välja. Tänapäeval kuuluvad nad saadaolevate serverisüsteemide tippklassi.

Käesolevas moodulis käsitletakse suurarvutite tüüpe IBM zSeries ja IBM S/390. Vastavad zSeries -süsteemid, mille operatsioonisüsteemiks on z/OS, kujutavad endast OS/390-arhitektuuri edasiarendust. Täienduste hulka kuulub zSeries puhul näiteks 64-bitine tugi. Mõlemad süsteemitüübid eksisteerivad kõrvuti, kusjuures OS/390 võib tinglikult nimetada juba vananenud operatsioonisüsteemiks, kuna IBM on selle toe 2004. a. sügisest juba lõpetanud. Kuna käesolev tekst on piisavalt ülevaatlik, kasutatakse riistvara tähistamiseks mõistet „ zSeries “ ning operatsioonisüsteemi tähistamiseks mõistet „z/OS“.

Ajaloost

Aastal 1964 loodud S/360-arhitektuur on olnud aluseks kõikidele järgnevatele edasiarendustele ning seda rakendatakse isegi tänapäeva zSeries -süsteemide tähtsamates osades. Nimevahetus, algul „S/360“, siis „S/370“, siis „S/390“ kuni tänapäevase „ zSeries “ nimeni välja, peegeldab endas süsteemi aluseks olevaks arhitektuuri pidevat edasiarendamist. Tänu oma tagasiühilduvusele toetab see arhitektuur lisaks uutele 64-bitistele rakendustele ka vanemate 24- või 31-bitiste programmide kasutamist.

Vaatamata üha kasvavale jõudlusele on suurarvutite füüsilised mõõdud aegade jooksul tublisti kahanenud. Mainframe arvutisüsteemid on tänapäeval sarnaste mõõtudega nagu tavaliselt arvutuskeskustes kasutusel olevatel süsteemid.

Ülevaade

zSeries süsteemides on olemas mehhanismid, mille abil on võimalik saavutada suur käideldavus ja skaleerituse aste. Kõrge käideldavuse aste saavutatakse sealjuures ilma komponentide liiasust kasutamata. Jõudluse ja käideldavuse tõstmiseks on hetkel võimalik zSeries -süsteemis käitada paralleelselt kuni 16 protsessorit ning üheks klastriks on võimalik kokku ühendada kuni 32 zSeries süsteemi. Seda nimetatakse paralleel- Sysplex -klastriks.

zSeries -riistvara jaoks on saadaval erinevad operatsioonisüsteemid (nt z/OS, VSE, z/VM või TPF). Reeglina tehakse operatsioonisüsteemi valik arvuti suurusest ja kasutusalast lähtudes. Sellele vaatamata kasutatakse kõige sagedamini z/OS-operatsioonisüsteemi. Vältimaks käesoleva mooduli liiga suureks paisumist, keskendutakse järgnevate soovituste jagamisel peamiselt operatsioonisüsteemile z/OS.

Algselt „MVS“ nime kandnud z/OS-operatsioonisüsteemi täiendus nimega Unix System Services lubab lisaks klassikaliste suurarvuti rakendustele kasutada paral-

leelselt ka Unixi all töötavaid rakendusi. Lisaks on zSeries -riistvara jaoks olemas ka Linux i all töötav operatsioonisüsteem.

Tänapäeva z/OS-süsteemide kasutusalad on:

- klassikaline pakktöötlus suurte „ batch -kettide“ jaoks,
- pakktöötlus koos tehingutele suunatud töötlusega (nt IMS või CICS),
- andmebaasi server (nt DB2, IMS DB või Oracle) või
- veebiserver koos rakendustega.

Käesolevas moodulis kirjeldatud tarkvara komponentide puhul on tegu peamiselt IBMi toodetega. Lisaks kirjeldatud toodetele leidub palju ka veel teiste firmade tooteid, mida suurarvutite töökeskkonnas kasutatakse. Vastavaid tooteid jõuab siinkohal käsitleda vaid erandjuhtumitena, kuna vastasel korral paisuks antud moodul liiga suureks.

Operatsioonisüsteem z/OS koosneb süsteemi tuumast (kernel) ning kasutajaprotsesside liidestest. Kommunikatsiooni juhivad ja toetavad erinevad alamsüsteemid.

Tähtsamateks alamsüsteemideks on:

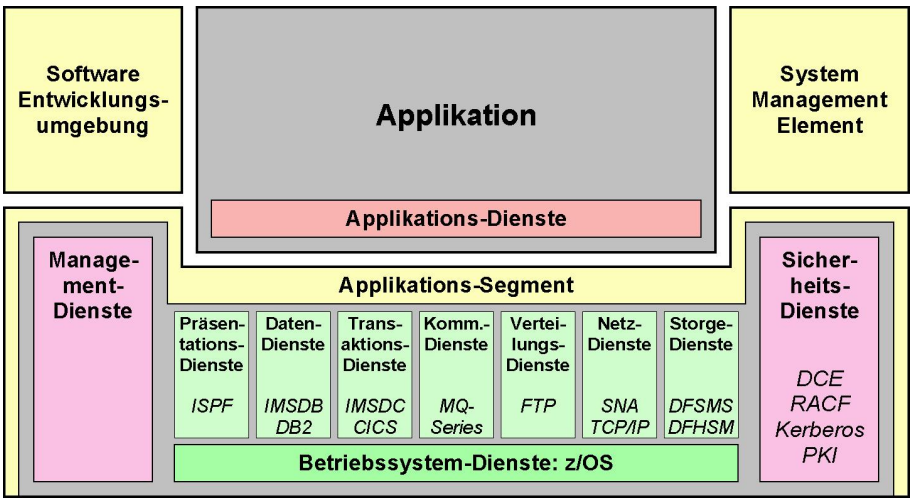
- Job Entry Subsystem (JES) tagaplaanil töötavate protsesside jaoks (pakktöötlus või batch),
- Time Sharing Option (TSO) esiplaanil töötavate protsesside jaoks (interaktiivne) ning
- Unix System Services (Posix -ühilduvusega Unixi alamsüsteem).

Veel kuuluvad alamsüsteemide alla näiteks:

- tehinguhaldur IMS ja selle juurde kuuluv andmebaas tehingutele suunatud andmetöötluse tarbeks,
- tehinguhaldur CICS tehingutele suunatud andmetöötluse tarbeks,
- andmebaas DB2 relatsioonandmebaaside tarbeks ning
- Communications Server (SNA, TCP/IP) võrguühenduste tarbeks.

Turvaliides System Authorization Facility (SAF) võimaldab kaitsta süsteemi ja faile volitamatu juurdepääsu eest. Reaalseid turbefunktsioone täidab seejuures turvatarkvara RACF. Alternatiivsete toodetena väärivad siinkohal äranimetamist veel ka Top Secret ning ACF2 .

Järgnev joonis püüab tugevalt üldistatud moel näidata, millised on operatsioonisüsteemi ülesehituse eri koostisosade omavahelised seosed:



Joonis: z/OS-operatsioonisüsteemi põhimõtteline ülesehitus

Joonis: Software Entwicklungsumgebung- Tarkvaraarenduse keskkond, Applikation- Rakendus, System Management Element- Süsteemihalduse element, Applikations-Dienste- Rakendusteenused, Management Dienste- Haldusteenused, Sicherheits- Dienste (DCE; RACF; Kerberos;PKI)-Turvateenused (DCE; RACF; Kerberos;PKI), Präsentationsdienste ISPF- Esitlusteenus ISPF, Datendienste IMSDB DB2- Andmeteenus IMSDB DB2-, Transkationsdienste IMSDC CICS- transaktiooniteenus IMSDC CICS, Kommdienste MQ Series- kommunikatsiooniteenus MQ seeria, Verteilungdienste FTP- jaotusteenus FTP, Netzdienste SNA TCP/IP- võrguteenus SNA TCP/IP, Storgedienste DFSMS DFHSM- salvestusteenus DFSMS DFHSM, Betriebssystem-Dienste: z/OS- operatsioonisüsteemi teenused: z/OS

Ohud

Üldjuhul sõltub turvalisus suuresti kasutusalast. Ametiasutuse või firmasisene, muudest võrkudest isoleeritud SNA-ühendusega z/OS-süsteem on reeglina vähem ohustatud kui internetti ühendatud veebiteenuseid pakkuv z/OS-süsteem. Lisaks on oluline ka see, kas ligipääs andmetele on võimaldatud ainult nende lugemiseks (nt päringusüsteemid) või on õigus andmeid ka töödelda. Just internetti ühendatud kasutusvaldkonnad, nagu veebiserverid ja veebirakendused, on kunagi „väga turvalisteks“ peetud mainframe -süsteemide ohuallikaid oluliselt kasvatanud.

Tänu mainframe -süsteemide ühendamisele avalikesse võrkudesse on varasemaga võrreldes oskamatust või valest konfiguratsioonist ning poolikult rakendatud protsessidest tulenevad ohud märgatavalt suurenenud.

See kehtib nii väliste ühenduste ja sealt tulenevate võimalike rünnete kui ka sisekeskkonna kohta. Tänapäeva suurarvutisüsteemid on sama palju ohustatud

nagu Unixi või Windowsi all töötavad süsteemid.

Organisatsioonilised puudused:

- G 2.4 Turvameetmete ebapiisav järelevalve
- G 2.27 Ebapiisav või puuduv dokumentatsioon
- G 2.54 Konfidentsiaalsuse kadu jääkinfo kaudu
- G 2.99 zSeriesi süsteemikeskkonna halb või väär konfigureerimine

Inimvead:

- G 3.2 Seadme või andmete hävitamine hooletuse tõttu
- G 3.3 Hooletus turvameetmete suhtes
- G 3.9 IT-süsteemi väär haldus
- G 3.38 Vead konfigureerimisel ja kasutamisel
- G 3.66 Märkide väär teisendus z/OS-i kasutamisel
- G 3.67 z/OS-operatioonisüsteemi puudulik või väär konfiguratsioon
- G 3.68 z/OS-veebiserveri puudulik või väär konfiguratsioon
- G 3.69 Unixi süsteemiteenuste (USS) väär konfigureerimine z/OS-is
- G 3.70 z/OS-i süsteemi failide ebapiisav turve
- G 3.71 z/OS-süsteemide väär süsteemiaeg
- G 3.72 z/OS-i turbesüsteemi RACF väär konfiguratsioon
- G 3.73 z/OS-i süsteemifunktsioonide väär kasutamine
- G 3.74 z/OS-i süsteemiseadistuste puudulik kaitse dünaamiliste muudatuste vastu
- G 3.75 z/OS-i pakktööde puudulik kontroll

Tehnilised rikked:

- G 4.10 Keerukad ligipääsuvõimalused võrgustatud IT-süsteemides
- G 4.22 Tüüptarkvara turvaaugud või vead
- G 4.50 z/OS-operatsioonisüsteemi ülekoormus

Ründed:

- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.10 Kaughooldeportide väärkasutus
- G 5.18 Süstemaatiline paroolide mõistatamine
- G 5.19 Kasutajaõiguste väärkasutus
- G 5.21 Trooja hobused
- G 5.28 Teenuse halvamine
- G 5.57 Võrguanalüüsi utiliidid
- G 5.116 z/OS-i konfiguratsiooni manipuleerimine
- G 5.117 z/OS-i manipuleerimise varjamine
- G 5.118 Suuremate õiguste volitamatu omandamine RACF-is
- G 5.119 Võõraste kasutajatunnuste kasutamine z/OS-is
- G 5.120 Linux/zSeriesi konfiguratsiooni manipuleerimine
- G 5.121 z/OS-süsteemi rünne TCP/IP-ühenduse kaudu
- G 5.122 z/OS-i RACF-i atribuutide väärkasutus

Soovitatavad meetmed

Selleks, et tagada kogu loetletud IT-süsteemi turvalisus, tuleb lisaks käesolevale moodulile rakendada veel ka teisi, IT-etalonturbe modelleerimise käigus selguvaid mooduleid.

Eduka z/OS- mainframe süsteemi ülesehitamiseks tuleb läbida mitmeid etappe, tegeldes strateegilise otsustamise, kontseptsiooni ja installeerimisega kuni igapäevase töötamiseni välja. Siinjuures ei tohi ära unustada süsteemi nõuetekohast kõrvaldamist selle kasutusaja läbisaamisel.

Süsteemi kasutusajaga paralleelselt peab väljatöötatud ootamatuseplaan tagama, et võimalike avariide korral töö ei katkeks. IT-turbehaldus ja läbivaatused peavad tagama, et väljatöötatud reeglistikust ka kinni peetaks.

Järgnevalt anname ülevaate erinevatest kohustuslikest etappidest ja meetmetest, mida tuleks iga etapi puhul rakendada:

Strateegia

Enne iga planeerimise algust leiab aset faas, kus püütakse määratleda strateegiat, mille kujundamisel tuleb suures osas lähtuda omaniku poolt vastavale rakendusele esitatavatest nõuetest. Selle käigus tuleks välja selgitada, kas z/OS-platvorm on sobiv lahendus püstitatud ülesannete täitmiseks.

Lisaks eelnevale tuleb teadvustada, milline on arvutuskeskuse IT-lahenduste varustuse seis. Juhul kui z/OS-platvormi veel ei kasutata, tuleb teha vastavad ettevalmistused süsteemi haldusega tegeleva personali koolituse osas.

Kontseptsioon

Kui strateegiline otsus on langetatud z/OS- mainframe -süsteemi kasuks, peab sellele järgnema süsteemi kasutusala detailne planeerimine. Siinkohal tuleb arvestada järgmiste meetmetega:

- enne zSeries -süsteemide soetamist ja kasutuselevõttu tuleb läbida erinevad planeerimisfaasid (vt M 2.286 zSeries-süsteemide planeerimine ja kasutamine).
- Juhul kui nõuded käideldavuse ja skaleerimise vallas on kõrged, on soovitatav kasutada Sysplex -rööpklastreid (vt M 4.221 Sysplex -rööpklastrid operatsioonisüsteemis z/OS).
- z/OS-süsteemi ning eriti turvasüsteemi RACF (Resource Access Control Facility) jaoks tuleb välja töötada ja kehtestada turvasuunised (vt M 2.288 z/OS-süsteemide turvapoliitika koostamine).
- Tuleb määratleda z/OS-süsteemimääratluse normid (vt M 2.285 z/OS süsteemimääratluste normide määramine).
- Tuleb kehtestada z/OS-süsteemidehaldusega tegeleva personali rollijaotus (vt M 2.295 z/OS-süsteemide haldus).

Rakendamine

Pärast organisatsiooniliste ja planeerimist puudutavate eeltööde tegemist saab liikuda edasi zSeries -riistvara ja z/OS-operatsioonisüsteemi installeerimise juurde. Siinkohal tuleb arvestada järgmiste asjaoludega:

- Tuleb kehtestada z/OS-süsteemide haldusega tegeleva personali rollijaotus (vt M 4.209 z/OS-süsteemide turvaline aluskonfiguratsioon).
- Määrava tähtsusega z/OS-keskkonna turvalisuse tagamisel on turvasüsteemi õige konfiguratsioon (vt M 4.211 z/OS turvasüsteemi RACF kasutamine).
- z/OS-juhtimissüsteemi rakendamisel koos kaugpääsukonsooliga RSF (Remote Support Facility) tuleb järgida soovitusi, mis on toodud meetmes M 4.207 z/OS-süsteemiterminalide kasutamine ja kaitse .

Kasutamine

Pärast esmast installeerimist ja testimisfaasi läbimist minnakse üle tavakasutusele. Turbe seisukohalt tuleb siinkohal arvestada järgmiste asjaoludega:

- z/OS-operatsioonisüsteemi funktsioonide kasutamise eelduseks on z/OS operatsioonisüsteemi turvaline käitamine (vt M 4.210 Operatsioonisüsteemi z/OS turvaline käitus).
- z/OS-operatsioonisüsteemi käitamisfunktsioone toetavad utiliidid, mis nõuavad kõrget autoriseerimise astet, peavad olema kaitstud (vt M 4.215 Turvakriitiliste z/OS-utiliitide kaitse).
- z/OS-süteemi vajalikud hooldetööd on kirjas meetmes M 2.293 zSeries-süsteemide hooldus .
- z/OS-süsteeme või Sysplex -rööpklastreid tuleb töö ajal jälgida (vt M 2.292 z/ OS-süsteemide seire).

Väljavahetamine

Nõuanded z/OS-süsteemide deinstalleerimiseks pärast ettenähtud kasutusea lõppemist leiate meetmest M 2.297 z/OS-süsteemide deinstalleerimine .

Valmisolek hädaolukorraks

Hädaolukorraks valmisoleku kohta käivad soovitused leiate meetmest M 6.93 z/OS süsteemide hädaolukorraks valmisoleku plaan .

IT-turvahaldus ja läbivaatus

IT-turvahaldus peaks saatma z/OS-süsteemi kogu selle kasutusea jooksul. Erilist tähelepanu tuleb pöörata järgnevatele punktidele:

- õiguste jagamise ja nende läbivaatamise käigus tuleb kontrollida, kas vastavad töötajad neid õigusi oma töös vajavad või mitte. Eriti kehtib see kõrgema klassi volituste kohta (vt meede M 2.289 Kitsendavate z/OS kasutajanimede kasutamine).
- z/OS-süsteemi käitamisel tuleb reeglipäraselt kontrollida, kas turvasuunistest peetakse kinni või mitte (vt meede M 2.291 z/OS aruandlus ja auditid).

Järgneb ülevaade „S/390- ja zSeries -suurarvutid“ mooduli meetmete paketist.

Planeerimine ja kontseptsiooni loomine

- (M) M 2.285z z/OS süsteemimääratluste normide määramine
- (M) M 2.286z zSeries -süsteemide planeerimine ja kasutamine
- (M) M 2.287z z/OS-süsteemide pakktööde planeerimine
- (M) M 2.288 z/OS-süsteemide turvapoliitika koostamine
- (L) M 2.295 z/OS-süsteemide haldus
- (M) M 2.296z z/OS-tehingumonitoride põhitegurite arvestamine
- (M) M 3.39w zSeries -platvormi tutvustamine
- (M) M 3.40w Operatsioonisüsteemi z/OS tutvustamine
- (M) M 3.41w zSeries -süsteemide Linuxi ja z/VM tutvustamine
- (M) M 4.221 Sysplex -rööpklastrid operatsioonisüsteemis z/OS

Rakendamine

- (M) M 2.289 (M) Kitsendavate z/OS kasutajanimede kasutamine
- (M) M 2.290z (M) RACF exit -moodulite kasutamine
- (M) M 3.42 (M) z/OS operaatorite koolitus
- (M) M 4.207 z/OS-süsteemiterminalide kasutamine ja kaitse
- (M) M 4.208 z/OS-süsteemide käivitusprotsessi kaitse
- (M) M 4.209 z/OS-süsteemide turvaline aluskonfiguratsioon
- (M) M 4.211 z/OS turvasüsteemi RACF kasutamine
- (M) M 4.212z zSeries -süsteemi Linux 'i kaitse
- (M) M 4.213 Logimisprotsessi kaitse z/OS all
- (M) M 4.216 z/OS-süsteemipiirangute kehtestamine
- (M) M 4.217 z/OS-süsteemide koormuse haldus
- (M) M 4.219 z/OS-tarkvara litsentsivõtmete haldus
- (M) M 4.220 Unixi süsteemiteenuste (USS) kaitse z/OS-süsteemides
- (M) M 5.113z (M) VTAM-seansi halduse funktsiooni kasutamine z/OS all
- (M) M 5.114 (M) z/OS jälitusfunktsioonide kaitse

Kasutamine

- (M) M 2.291 z/OS aruandlus ja auditid
- (M) M 2.292 z/OS-süsteemide seire
- (M) M 2.293 zSeries -süsteemide hooldus
- (M) M 2.294z z/OS paroolide ja RACF käskude sünkroniseerimine
- (M) M 4.210 Operatsioonisüsteemi z/OS turvaline käitus
- (M) M 4.214 Salvestuskandjate haldus z/OS-süsteemides
- (M) M 4.215 Turvakriitiliste z/OS-utiliitide kaitse
- (M) M 4.218 Teave märgistike teisenduse kohta z/OS -süsteemides

Väljavahetamine

- (M) M 2.297 z/OS-süsteemide deinstalleerimine

Valmisolek hädaolukorraks

- (M) M 6.93 z/OS süsteemide hädaolukorraks valmisoleku plaan

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.6 Arvuti paroolkaitse rangemad reeglid
- HG.24 Paroolide regulaarkontroll parooliskänneriga
- HG.25 Kaugpöörduste kohustuslik logimine
- HG.38 Turvapaikade paigaldatuse regulaarseire

Teabe käideldavus (K)

- HK.27 Puhvertoiteallikas serveri sulgemise tagamiseks

Teabe terviklus (T)

- HT.7 Kasutajate ja nende profiilide perioodiline seire
- HT.14 Süsteemi tegevuslogide krüptoaheldamine
- HT.16 Serverilogi krüptoaheldamine

Teabe konfidentsiaalsus (S)
-

B 3.108 Windows Server 2003

Kirjeldus

Tarkvarapakett Windows Server 2003 on Windows 2000 Server operatsioonisüsteemi edasiarendus. Windows Server 2003 on saadaval Standard Edition, Enterprise Edition , Web Edition ning Datacenter Edition versioonis. Eriti laia levikuga on nendest versioonidest Standard Edition . Web-Edition versioon on osa Standard-Edition versioonist ning Enterprise-Edition sisaldab mõningaid spetsiifilisi lisafunktsioone, mis leiavad kasutust spetsiaalselt ainult suurtes kasutajakeskkondades. Selle alla kuulub muuhulgas Fail-over-Cluster funktsioon, terminaliserveri täisversioon, UDDI-andmebaaside võrgutugi, piiramatu hulk VPN- ja RADIUS-ühendusi, uued sertifitseerimisteenused Windows System Resource Manager (WSRM). Kõik nimetatud versioonid on saadaval ka 64-bitises versioonis, mis oma funktsioonide valiku poolest ei erine märkimisväärselt 32-bitistest versioonidest.

Mooduli piiritlemine

Mooduli Windows Server 2003 aluseks on Standard-Edition ja Service Pack 1 . Sellele vaatamata on võimalik antud moodulit ilma probleemideta rakendada ka Web-Edition ning Enterprise-Edition versioonide puhul. Ülejäänud versioonid, nagu nt Datacenter-Edition ja Windows Small Business Server 2003 , sisaldavad endas kasutajaspetsiifilisi lisafunktsioone, mida käesolevas moodulis ei kajastata.

Mitmekülgsete kasutusvõimaluste tõttu on tarvis teemasid teineteisest lahutada ning see seab antud moodulile omad piirid. Ühelt poolt on Windows Server 2003 süsteemi võimalik rakendada puhtalt platvormina serveri poolt pakutavate lisarakenduste jaoks, teiselt poolt saab tänu Windows Server 2003 paljudele kaasasolevatele funktsioonile seda üles ehitada ka kui teatud valdkonna tervikla-hendust.

Teatud Windows-Server 2003 funktsioonide sisselülitamine on hädavajalik vaid kindlate kasutusvaldkondade puhul. Vastavate kasutusvaldkondade kohta annab käesolev moodul mõningaid üldisi juhtnööre. Eelkõige puudutab see funktsioone nagu Network Load Balancing (NLB), kõrge käideldavusega klaster, Active Directory , Application Server , Role Based Access Control (RBAC), sertifitseerimisteenused (PKI) ning Routing ja RAS .

Lähema vaatluse alt jäävad välja Microsofti poolt tasuta kaasapandud lisad, mis ei ole standardpaketi osad. Käsitluse alt jäävad välja näiteks Windows Sharepoint Services (WSS), Windows Software Update Service (WSUS), Rights Management Service (RMS) ning Microsoft Shared Computer Toolkit .

Muuhulgas jäävad käsitluse alt välja ka järgmised standardse paketi osad, mille

kasutamisel tuleb arvestada paljude asjaoludega, mis ei ole üldkehtivad:

- Windows Media Services
- Terminalserver

Ohud

Infosüsteemide etalonturbe seisukohalt loetakse Windows Server 2003 operatsioonisüsteemi all töötavate serveritega võrgu puhul tüüpilisteks järgmisi ohuallikaid:
Organisatsioonilised puudused:

- G 2.7 Õiguste volitamata kasutamine
- G 2.19 Krüpteerimise halb korraldus
- G 2.111 Pääsuõiguste kuritarvitamine teenusepakkuja vahetumisel
- G 2.114 Windowsi Serveri ühtimatud SMB, RPC ja LDAP turbeseadistused
- G 2.115 Standardsete turvagruppide ebapädev kasutamine Windowsi alates Server 2003-st
- G 2.116 Andmekadu andmete kopeerimisel ja teisaldamisel alates Windowsi Server 2003-st

Inimvead:

- G 3.9 IT-süsteemi väär haldus
- G 3.38 Vead konfigureerimisel ja kasutamisel
- G 3.48 Windowsiga töötavate IT-süsteemide väär konfiguratsioon
- G 3.56 IIS-i väär integreerimine süsteemikeskkonda
- G 3.81 Turvamallide väär kasutamine alates Windows Server 2003-st

Tehnilised rikked:

- G 4.13 Salvestatud andmete hävimine
- G 4.22 Tüüptarkvara turvaaugud või vead
- G 4.54 Turbe kadu krüptofailisüsteemi (EFS) kasutamisel
- G 4.55 Andmekadu alates Windows Server 2003 / XP parooli taastamisel

Ründed:

- G 5.7 Liinide pealtkuulamine
- G 5.52 Windows NT administraatoriõiguste väärkasutus
- G 5.71 Tundliku informatsiooni konfidentsiaalsuse kadu
- G 5.79 Windowsi süsteemide administraatoriõiguste volitamatu omandamine
- G 5.83 Krüptograafiliste võtmete paljastamine
- G 5.85 Tundliku informatsiooni tervikluse kadu
- G 5.132 RDP-seansi kompromiteerimine alates Windows Server 2003-st
- G 5.133 Veebipõhiste administreerimisvahendite volitamata kasutamine

Soovitatavad meetmed

Selleks, et tagada kogu loetletud IT-süsteemi turvalisus, tuleb lisaks käesolevale moodulile rakendada veel ka teisi, IT-etalonturbe modelleerimise käigus selguvaid mooduleid.

Kõik otsused Windows Server 2003 versiooni kasuks peaksid põhinema moodulis B 3.101 Server kirjeldatud meetmetel. Käesolev moodul püüab eelnimetatud meetmeid täpsustada ja täiendada.

Server ja kliendid moodustavad ühe funktsionaalse terviku. Seepärast tuleb vaadelda moodulit B 3.201 Klient ja sellel põhinevaid operatsioonisüsteemi kirjeldavaid mooduleid ja käesolevat moodulit kui ühte tervikut.

Planeerimine ja kontseptsiooni loomine

Pärast seda, kui serverikasutuse üldine planeerimisetapp on seljataga ning valik on langenud Windows Server 2003 kasuks, tuleb välja töötada serverikasutuse eri valdkondade spetsiifilised kontseptsioonid, pidades silmas kõiki üldkehtivaid kontseptsioone ja suuniseid. Üldised planeerimist puudutavad tegutsemisjuhised on kirjas meetmes M 2.315 Serveri kasutuselevõtu planeerimine .

Eelnimetatud meetmes mainitud alateemade kohta käivad suunised leiate meetmest M 4.275 Salvestisüsteemide turvaline kasutamine ning M 2.364 Halduse planeerimine alates Windows Server 2003-st .

Planeerimise käigus tuleb langetada tähtsaid otsuseid, millised saavad olema põhilised infrastruktuurilised teenused. Infrastruktuuriliste teenuste kontseptsiooni puudutava otsuse tegemisse tulevad otsapidi sisse ka plaanitud rollide ja IT-etalonturbe abivahendite juhised (vt DNS/WINS/DHCP infrastruktuurilised teenused Windows Server 2003 all teemas Windows Server 2003 abivahendid).

Lisaks eelnevale tuleb planeerida ka serveri kommunikatsiooniprotokollid (M 4.277 Windows Serverite SMB, LDAP ja RPC kommunikatsiooni kaitse , M 5.131 Windows Server 2003 IP-protokollide kaitse).

Täiendavate kõikehõlmavate süsteemidega on võimalik serveri turvalisust tõsta, nt WebDAV ja Encrypting File System (EFS) (vt meede M 5.132 Windows Server 2003 WebDAV turvaline kasutamine , M 4.278 EFS-i turvaline kasutamine Windows Server 2003 keskkonnas), võrgu koormuse tasakaalustamine (Network Load Balancing , NLB), IPSec, kasutaja autentimine Smart Card abil jt. Siinkohal tuleb kindlasti arvestada ka meetmega M 6.99 Windows Serverite tähtsate süsteemikomponentide regulaarne varundus ja M 4.279 Windows Server 2003 laiendatud turvaaspektid .

Kõikide seninimetatud sammude puhul tuleb arvestada meetmetes M 5.10 Piiratud õiguste andmine ning M 5.9 Serveri logi . Spetsiifilisemaid nõuandeid leiate meetmetest M 2.370 Volituste haldamine alates Windows Server 2003-st ja M 2.365 Windows Server 2003 süsteemiseire planeerimine . Nendes meetmetes mainitud soovitusi serveri käitamise kohta tuleb arvestada juba õiguste kontseptsioonide planeerimisel.

Serveri plaanimistööde raames tuleks välja töötada turvapoliitika või olemasolevaid suuniseid vastavalt täiendada. Kõikide seninimetatud etappide puhul tekivad sõltuvalt kasutusalast ja kasutuse kestvusest erisugused võimalikud ohud, samuti individuaalsed lahendused ja tegutsemismeetodid. Erinevused tuleb kokku koguda. Seejärel on võimalik tekkinud olukorda ja ettevõtte või ametiasutuse organisatsioonilist struktuuri arvestades välja mõelda, mil viisil turvapoliitikat peaks täiendama. Ajakohase tegutsemisjuhise leiate meetmest M 2.316 Serveri turvapoliitika kehtestamine .

Soetamine

Pärast serveri kontseptsiooni loomist puudutavate planeerimistööde lõppu ja soetamiskriteeriumite defineerimist (vt M 2.317 Serveri soetamise kriteeriumid) tuleks vastavalt vajaminevate serverite tükiarvule sobilik litsentsmudel välja valida. Siinkohal aitavad Teid IT-etalonturbe abivahendid (vt Sobilike litsentseerimismeetodite valimine Windows XP/Server 2003 all teemas Windows Server 2003 abivahendid).

Rakendamine

Pärast Windows Server 2003 turvameetmete planeerimist tuleb need Windows Server 2003 süsteemi juurutamise st installeerimise ja konfigureerimise käigus ellu rakendada.

Vajaliku turvalisuse astme tagamiseks tuleb Windows-Server-2003-süsteemi turvameetmete ellurakendamisel (ja hiljem ka juba süsteemi käitamise käigus) arvestada järgmiste eeldustega:

- turvariskide ja (potentsiaalsete) kitsaskohtade vähendamiseks tuleb piirata funktsioonide arvukust, (ka serverile ligipääsevate klientide arvukust), nii nagu on planeeritud ja jätta alles ainult hädavajalik (M 4.285 Mittevajalike Windows Server 2003 klientfunktsioonide deinstalleerimine ja M 4.286 Windows Server 2003 Software Restriction Policy rakendamine ning M 4.284 Teenuste rakendamine alates Windows Server 2003-st).
- Konfiguratsioon tuleb teha selline, et serveri turvalisus ja tööfunktsioon oleksid optimaalsed (serveri tugevdamine), et süsteemi allapoole ühilduvus ja süsteemi avatus ei oleks suurem kui vajalik (meede M 4.282 Windows Server 2003 IIS põhikomponentide turvaline konfiguratsioon ja meede M 4.283 Windows NT 4 Serveri ja Windows 2000 Serveri turvaline migratsioon Windows Server 2003-ks).
- IT turbe protsessi igakülgseks toetamiseks tuleb koostada asjakohane kõige värskema infoga dokumentatsioon.

Meedet M 4.237 IT-süsteemi turvaline aluskonfiguratsioon täiendab ja konkretiseerib meede M 4.280 Turvaline põhikonfiguratsioon alates Windows Server 2003-st . Siin selgitatakse terve rida väiksemaid funktsioone ja antakse üldiseid rakendamist puudutavaid tegutsemisjuhiseid, mille abil saaks täita eelpool loetletud eeldusi.

Installeerimise ja konfigureerimise käigus tuleks eelistada abiprogrammidega töötamist, nn assistente. Käsitsi seadistamist tuleks kasutada ainult siis, kui see on hädavajalik. Niimoodi saab ühelt poolt ennetada väärkonfiguratsioonide teket ning teiselt poolt lihtsustab see dokumenteerimist (nt: „konfiguratsioon assistentprogrammi standardseadetega koos järgneva kolme standardist kõrvalekalduva seadistusega. . . “). Dokumentatsiooni ühtset standardit aitavad saavutada administratiivsed abivahendid nagu mallid ja skriptid (M 2.366 Windows Server 2003 turvamallide kasutamine ja M 2.367 Käskude ja skriptide kasutamine alates Windows Server 2003-st).

Kui tegu on serveri esmakordse ülesseadmisega, jooksevad kõik seni loetletud sammud serveri installeerimis- ja ettevalmistusprotsessis üheks kokku. Kindla ja usaldusväärse tööprotsessi tagamiseks tuleks siinkohal rakendada meedet M 4.281 Windows Server 2003 turvaline installeerimine ja ettevalmistus .

Kasutamine

Tavakasutuses on lisaks dokumentatsiooni värskena hoidmisele väga oluline ka administratiivsete mallidega ümberkäimine ja volituste haldamine (M 2.368 Administratiivsete mallide kasutamine alates Windows Server 2003-st ja M 2.370 Volituste haldamine alates Windows Server 2003-st).

Lisaks moodulis B 3.101 Server nimetatud meetmetele M 4.93 Regulaarne tervikluse kontroll ja M 5.8 Võrgu regulaarne turvakontroll , täiendab turvalisuse tagamist veel ka meede M 2.369 Windows Server 2003 turvalisusega seotud hooldustööde regulaarne läbiviimine .

Väljavahetamine

Windows Server 2003 väljavahetamine peaks toimuma vastavalt moodulis B 3.101 Server kirjeldatud meetmetele. Lisaks tuleb üksikute kontode desaktiveerimisel või kustutamisel järgida meedet M 2.371 Kasutamata kasutajatunnuste organiseeritud desaktiveerimine ja kustutamine .

Valmisolek hädaolukorraks

Windows Server 2003 valmisolekut hädaolukordadeks eri aspekte kajastavad meetmed M 6.99 Windows Serverite tähtsate süsteemikomponentide regulaarne varundus ja M 6.76 Avariiplaani koostamine Windowsi süsteemi tõrke puhuks .

Järgneb ülevaade „ Windows Server 2003 “ meetmete paketist.

Planeerimine ja kontseptsiooni loomine

- (L) M 2.232 Windows CA-struktuuri plaaneerimine alates Windows 2000-st
- (L) M 2.364 Halduse planeerimine alates Windows Server 2003-st
- (L) M 2.365 Windows Server 2003 süsteemiseire planeerimine
- (L) M 4.276 Windows Server 2003 kasutamise plaanimine
- (L) M 4.277 Windows Serverite SMB, LDAP ja RPC kommunikatsiooni kaitse
- M 4.278z EFS-i turvaline kasutamine Windows Server 2003 keskkonnas
- M 4.279z Windows Server 2003 laiendatud turvaaspektid
- (L) M 5.131 Windows Server 2003 IP-protokollide kaitse
- (M) M 5.132 Windows Server 2003 WebDAV turvaline kasutamine

Rakendamine

- (M) M 2.366 Windows Server 2003 turvamallide kasutamine
- (L) M 2.367 Käskude ja skriptide kasutamine alates Windows Server 2003-st
- (L) M 4.280 Turvaline põhikonfiguratsioon alates Windows Server 2003-st
- (L) M 4.281 Windows Server 2003 turvaline installeerimine ja ettevalmistus
- (M) M 4.282 Windows Server 2003 IIS põhikomponentide turvaline konfiguratsioon
- (M) M 4.283 Windows NT 4 Serveri ja Windows 2000 Serveri turvaline migratsioon Windows Server 2003-ks
- (M) M 4.284 Teenuste rakendamine alates Windows Server 2003-st
- (L) M 4.285 Mittevajalike Windows Server 2003 klientfunktsioonide deinstalleerimine
- (L) M 4.296 Traadita kohtvõrgu sobiva haldussüsteemi kasutamine
- M 5.90z Protokolli IPSec kasutamine Windowsi keskkonnas

Kasutamine

- (L) M 2.368 Administratiivsete mallide kasutamine alates Windows Server 2003-st
- (L) M 2.369 Windows Server 2003 turvalisusega seotud hooldustööde regulaarne läbiviimine
- (L) M 2.370 Volituste haldamine alates Windows Server 2003-st
- (L) M 4.56 Turvaline kustutus Windows operatsioonisüsteemides

Väljavahetamine

- (L) M 2.371 Kasutamata kasutajatunnuste organiseeritud desaktiveerimine ja kustutamine

Valmisolek hädaolukorraks

- (L) M 6.76 Avariiplaani koostamine Windowsi süsteemi tõrke puhuks
- (L) M 6.99 Windows Serverite tähtsate süsteemikomponentide regulaarne varundus

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.6 Arvuti paroolkaitse rangemad reeglid
- HG.24 z Paroolide regulaarkontroll parooliskänneriga
- HG.25 Kaugpöörduste kohustuslik logimine
- HG.38 Turvapaikade paigaldatuse regulaarseire
- HG.41 Windows Server 2003 laiendatud turvaaspektid

Teabe käideldavus (K)

- HK.18 Windows Server 2003 klasterdamine
- HK.27 = HT.41 Puhvertoiteallikas serveri sulgemise tagamiseks

Teabe terviklus (T)

- HT.7 Kasutajate ja nende profiilide perioodiline seire
- HT.14 Süsteemi tegevuslogide krüptoaheldamine
- HT.16 = HS.55 Serverilogi krüptoaheldamine
- HT.38 = HS.49 Windows Server 2003 krüpteeritud failisüsteemi kasutus

Teabe konfidentsiaalsus (S)

- HS.54 Lisanõuded turvalisele kustutamisele

Lisanõuded turvalisele kustutamisele

B 3.109 Windows Server 2008

Microsofti toode Windows Server 2008 on serverite operatsioonisüsteem, mille turvalisus on sellele eelnenud versioonidega võrreldes märgatavalt paranenud. Redaktsiooniga Windows Server 2008 R2 anti välja ka veel mitmeid parandusi ja täiendusi, mis muudavad Windows 2008 omadustelt võrdväärseks klientsüsteemides kasutatava Windows 7-ga.

Operatsioonisüsteemi Windows Server 2008 saab kasutada erineva otstarbega serverites, nt Windowsi domeenide kontrolleri, Active Directory serveri ja andmebaasiserverina, samuti rakenduste või infrastruktuuriteenuste, nagu DHCP, DNS-i või VPN-i serverina. Kõiki saadaolevaid funktsioone ei ole kindlasti tarvis aktiveerida ning nende valimisel tuleks lähtuda serveri kasutusvaldkondadest. Kuna selles moodulis ei ole võimalik detailselt kirjeldada kõiki kasutusvaldkondi, piirdutakse siinkohal ühise operatsioonisüsteemi platvormi ja olulisemate üldiste turbefunktsioonidega.

Seda moodulit tuleb rakendada alati juhtudel, kus Windows Server 2008 pannakse tööle operatsioonisüsteemina, ning seda ka siis, kui kasutatakse versiooni Windows Server Core. Teenuseid, mille töö on rajatud Windows Server 2008-le, tuleb alati kaitsta ka 5. kihi („Rakendused") asjakohaste moodulite või täiendava riskianalüüsiga.

Kõik selles moodulis kirjeldatud Windows Server 2008 meetmed ja ohud kehtivad samamoodi ka versiooni R2 kohta. Versiooni R2 muudatused ja erinevused on tekstis eraldi välja toodud.

Ohud

Allpool on nimetatud operatsioonisüsteemiga Windows Server 2008 töötavate serverite olulisimad ohud.

Organisatsioonilised puudused

- G 2.7 Õiguste volitamata kasutamine
- G 2.19 Krüpteerimise halb korraldus
- G 2.111 Pääsuõiguste kuritarvitamine teenusepakkuja vahetumisel
- G 2.114 Windowsi Serveri ühtimatud SMB, RPC ja LDAB turbeseadistused
- G 2.115 Standardsete turvagruppide ebapädev kasutamine Windowsi alates Server 2003-st
- G 2.116 Andmekadu andmete kopeerimisel ja teisaldamisel alates Windowsi Server 2003-st
- G 2.156 Ühilduvusprobleemid Active Directory funktsioonitasandi suurendamisel

Inimvead

- G 3.9 IT-süsteemi väär haldus
- G 3.27 Aja väär sünkronisatsioon
- G 3.48 Windowsiga töötavate IT-süsteemide väär konfiguratsioon
- G 3.97 Konfidentsiaalsuse kadu vaatamata draivide krüpteerimisele BitLockeriga alates Windows Vista-st
- G 3.98 BitLockeriga krüpteeritud andmete kadu

Tehnilised rikked

- G 4.13 Salvestatud andmete hävimine
- G 4.22 Tüüptarkvara turvaaugud või vead
- G 4.54 Turbe kadu krüptofailisüsteemi (EFS) kasutamisel

Ründed

- G 5.7 Liinide pealtkuulamine
- G 5.71 Tundliku informatsiooni konfidentsiaalsuse kadu
- G 5.79 Windowsi süsteemide administraatoriõiguste volitamatu omandamine
- G 5.83 Krüptograafiliste võtmete paljastamine
- G 5.85 Tundliku informatsiooni tervikluse kadu
- G 5.132 RDP-seansi kompromiteerimine alates Windows
- G 5.133 Veebipõhiste administreerimisvahendite volitamata kasutamine

Soovitatavad meetmed

Siin kirjeldatavad meetmed täiendavad mooduli B 3.101 Server meetmeid ning keskenduvad operatsioonisüsteemiga Windows Server 2008 töötavate serverite eriaspektidele. Vaadeldava IT-koosluse turvalisuse tagamiseks tuleb tavaliselt peale käesoleva mooduli rakendada veel teisigi mooduleid, mis selguvad IT-etalonturbe rakendusjuhendi põhjal tehtava modelleerimise tulemusel.

Planeerimine ja kontseptsioon

Hoolikas planeerimine on iga serveri puhul ülioluline ja vältimatu tegevus. Sellekohased peamised soovitused on koondatud meetmesse M 4.418 Windows Server 2008 kasutamise planeerimine . Varasemate versioonidega võrreldes tehtud uuendusi kirjeldatakse meetmes M 4.408 Windows Server 2008 uute turbefunktsioonide ülevaade .

Tööandjad kasutavad Windowsi serverite soetamiseks sageli hulgilitsentsilepinguid. Selliste lepingutega seotud toodete aktiveerimiseks on tarvis luua õiged eeldused, mis tagavad süsteemide käideldavuse (vt M 4.336 Hulgilitsentslepinguga Windows süsteemide aktiveerimine alates Windows Server 2008-st). Siia kuuluvad ka reaktiveerimist ettevalmistavad tööd, mida läheb tarvis ennekõike konfiguratsioonimuudatuste korral (M 4.343 Hulgilitsentsilepinguga Windowsi süsteemide reaktiveerimine alates Windows Server 2008-st).

Et süsteemi käitamine oleks turvaline, tuleb juba planeerimisetapis arvestada ka selliste lisaaspektidega nagu süsteemi administreerimise üldnõuete kehtestamine (M 2.364 Halduse planeerimine), grupeerimissuunised (M 2.326 Windows 7 grupeerimissuuniste planeerimine) ja süsteemiseire (M 2.489 Windows Server 2008 süsteemiseire planeerimine).

Olenevalt serveri kasutusvaldkonnast tuleb planeerida veel ka lisavaldkonnad, nt organisatsioonisisene avaliku võtme (public key) infrastruktuur (M 2.332 Nõupidamis-, ürituste- ja koolitusruumide sisustamine) või Windowsil töötavad virtualiseerimislahendused (M 2.490 Hyper-V-ga virtualiseerimise planeerimine).

Soetamine

Enne Windows 2008 serverisüsteemi soetamist tuleb välja selgitada selle nõuded. See ei puuduta mitte üksnes riistvaraliste eelduste väljaselgitamist, vaid ka

õige versiooni väljavalimist (M 4.409 Windows Server 2008 soetamine) ja aktiveerimiseks vajamineva taristuga arvestamist (M 4.336 Hulgilitsentslepinguga Windows süsteemide aktiveeriminen alates Windows Server 2008-st).

Rakendamine

Operatsioonisüsteemi tööleseadmist abistavad tootja mallid (M 2.491 Windows Server 2008 rollide ja turvamallide kasutamine). Nende põhjal tuleb koostada turvaline põhikonfiguratsioon (M 4.280 Turvaline põhikonfiguratsioon alates Windows Server 2003-st). Erinevalt Windowsi paljudest varasematest versioonidest saab siin suures osas kasutusele võtta standardseadistused. Kui aga Windows Server 2008-ga asendatakse mõni vanem Windowsi operatsioonisüsteem, tuleb migratsiooni asjakohasel viisil planeerida (M 4.412 Windows Server 2003 turvaline migreerimine Server 2008-ks) ja teostada.

Nii nagu Windowsi serverite varasemate versioonide puhul, on ka praegu jätkuvalt oluline lokaalselt ühendatud seadmete turvalisus, skriptide ja skriptikeskkondade kasutamine (M 2.367 Käskude ja skriptide kasutamine alates Windows Server 2003-st), süsteemiteenuste konfiguratsioon (M 4.284 Teenuste rakendamine alates Windows Server 2003-st) ning paroolide tagatav piisav kaitse.

Failisüsteemi puhul on tarvis otsustada, kas faili viimase juurdepääsu logimist soovitakse kasutusele võtta või mitte. Selline logi võib lihtsustada turvaintsidentide lahendamist, kuid võib mõjuda halvasti näiteks jõudlusele, mistõttu tuleks kaaluda nii selle plusse kui ka miinuseid (M 4.342 Last Access ajatempli aktiveerimine alates Windows Vistast). Sellised uued funktsioonid nagu kasutajakontode haldus (M 4.340 Windows kasutajakonto haldamise (UAC) kasutamine alates Windows Vistast) ja tervikluse kaitsmise võimalus (M 4.341 Tervikluse kaitse alates Windows Vista) võivad varasemate versioonidega võrreldes aidata suurendada süsteemi turvalisust ning seetõttu tuleks neid ka kasutada. Kui serverit hakatakse kasutama Active Directory funktsioonides, tuleb arvestada ka meetmes M 4.414 Windows Server 2008 Active Directory uuenduste ülevaade esitatud nõuannetega. Tavapärasest suurema kaitsevajaduse korral on soovitatav võtta täiendavaid turbemeetmeid, nagu piiratud kasutajakeskkonnad (M 2.32 Piiratud kasutajakeskkonna loomine), võrgu andmeside lisakaitse (M 4.277 Windows Serverite SMB, LDAP ja RPC kommunikatsiooni kaitse või M 5.90 Protokolli IPSec kasutamine Windowsi keskkonnas) või rakenduste juhtimine AppLockeri tarkvaratööriistaga (M 4.419 Rakenduste juhtimine AppLockeriga alates Windows 7-st). Andmete krüpteerimiseks saab kasutada nii andmekandjatel töötavaid kui ka failisüsteemis toimivaid mehhanisme (M 4.337 BitLockeri Drive Encryption kasutamine ja M 4.147 EFS-i turvaline kasutamine Windows 'i keskkonnas).

Kasutamine

Olulisimad regulaarselt täidetavad tööülesanded on kirjas meetmes M 2.369 Turvalisusega seotud hooldustööde regulaarne läbiviimine ning neid täiendab kasutajakontode ja volituste turvaline haldamine (M 2.370 Volituste haldamine). Süsteemis peaks toimima ka sihipärane seire, et kõiki käideldavusprobleeme ja turvaintsidente saaks tuvastada võimalikult kiiresti (M 4.344 Windows 7 ja Windows Server 2008 süsteemi seire).

Nagu kõikide IT-süsteemide puhul, nii on ka Windowsi serverisüsteemide turbe seisukohalt üliioluline, et tsentraalne paikade haldus toimiks hästi. Selleks otstarbeks on Microsoft loonud tarkvaratööriista Windows Server Update Services

(WSUS) (vt M 4.417 Paikade haldus WSUS-iga alates Windows Server 2008-st).

Nii kasutajad kui ka administraatorid peavad arvesse võtma failide kustutamisega seotud eripärasid (M 4.56 Turvaline kustutus Windows operatsioonisüteemides). Uute biomeetriliste autentimisvõimaluste näol, nt sõrmejälje tuvastamisega, on loodud alternatiiv paroolide sisestamisele (M 4.415 Biomeetriliste autentimisvõimaluste turvaline kasutamine Windowsis).

Kasutusest kõrvaldamine

Windowsi serverite kasutusest kõrvaldamisel tuleb järgida moodulis B 1.0 Infoturbe haldus kirjeldatud meetmeid. Lisaks on tarvis kontod kas desaktiveerida või kustutada (M 2.371 Kasutamata kasutajatunnuste organiseeritud desaktiveerimine ja kustutamine).

Valmisolek hädaolukorraks

Nagu kõikide tsentraalselt töötavate IT-süsteemide puhul, on ka Windowsi serverite jaoks tarvis koostada avariiplaanid (M 6.76 Avariiplaani koostamine Windowsi süsteemi tõrke puhuks). Üks tähtis element hädaolukordadeks valmisoleku puhul on andmete varundamine, mis peaks hõlmama ka operatsioonisüsteemi olulisi valdkondi (M 6.99 Windows Serverite tähtsate süsteemikomponentide regulaarne varundus). Tavapärasemast suuremate käideldavusnõuete korral võib ennetava meetmena abi olla liiasusest (M 6.43 Liiasusega Windowsi serverid).

Planeerimine ja kontseptsioon

- (M) M 2.232 Windows CA-struktuuri plaaneerimine alates Windows 2000-st
- (L) M 2.326 Windows Vista ja Windows 7 grupeerimissuuniste planeerimine
- (L) M 2.364 Halduse planeerimine alates Windows 2003-st
- (L) M 2.489 Windows Server 2008 süsteemiseire planeerimine
- (M) M 2.490 Hyper-V-ga virtualiseerimise planeerimine
- (L) M 4.147z EFS-i turvaline kasutamine Windows 'i keskkonnas
- (M) M 4.277z Windows Serverite SMB, LDAP ja RPC kommunikatsiooni kaitse
- (L) M 4.336 Hulgilitsentslepinguga Windows süsteemide aktiveerimine alates Windows Vistast või Windows Server 2008-st
- (M) M 4.337z BitLockeri Drive Encryption kasutamine
- (L) M 4.340 Windows kasutajakonto haldamise (UAC) kasutamine alates Windows Vistast
- (L) M 4.341 Tervikluse kaitse alates Windows Vista
- (M) M 4.342z Last Access ajatempli aktiveerimine alates Windows Vistast
- (L) M 4.408w Windows Server 2008 uute turbefunktsioonide ülevaade
- (L) M 4.414w Windows Server 2008 Active Directory uuenduste ülevaade
- (M) M 4.418 Windows Server 2008 kasutamise planeerimine

Soetamine

- (L) M 4.409w Windows Server 2008 soetamine

Rakendamine

- (L) M 2.32z Piiratud kasutajakeskkonna loomine
- (M) M 2.367 Käskude ja skriptide kasutamine alates Windows Server 2003-st
- (L) M 2.491 Windows Server 2008 rollide ja turvamallide kasutamine
- (L) M 4.280 Turvaline põhikonfiguratsioon alates Windows Server 2003-st
- (L) M 4.284 Teenuste rakendamine alates Windows Server 2003-st
- (L) M 4.410z Võrgu juurdepääsukaitse kasutamine Windowsis
- (L) M 4.412z Windows Server 2003 turvaline migreerimine Server 2008-ks
- (L) M 4.413z Hyper-V-ga virtualiseerimise turvaline kasutamine
- (L) M 4.419z Rakenduste juhtimine AppLockeriga alates Windows 7-st
- (M) M 5.90z Protokolli IPSec kasutamine Windowsi keskkonnas

Kasutamine

- (M) M 2.368 Administratiivsete mallide kasutamine alates Windows Server 2003-st
- (L) M 2.369 Windows Server 2003 turvalisusega seotud hooldustööde regulaarne läbiviimine
- (L) M 2.370 Volituste haldamine alates Windows Server 2003-st
- (M) M 4.56 Turvaline kustutus Windows operatsioonisüteemides
- (M) M 4.343z Hulgilitsentsilepinguga Windowsi süsteemide reaktiveerimine alates Windows Vistast või Windows Server 2008-st
- (M) M 4.344 Windows Vista, Windows 7 ja Windows Server 2008 süsteemi seire
- (L) M 4.411z DirectAccessi turvaline kasutamine Windowsis
- (L) M 4.415z Biomeetriliste autentimisvõimaluste turvaline kasutamine Windowsis
- (L) M 4.416z Windows Server Core'i kasutamine
- (L) M 4.417 Paikade haldus WSUS-iga alates Windows Server 2008-st

Kasutusest kõrvaldamine

- (L) M 2.371 Kasutamata kasutajatunnuste organiseeritud desaktiveerimine ja kustutamine
- (L) M 2.410 Kataloogiteenuse korrakohane kasutuselt kõrvaldamine

Valmisolek hädaolukorraks

- (L) M 6.76 Avariiplaani koostamine Windowsi süsteemi tõrke puhuks
- (L) M 6.99 Windows Serverite tähtsate süsteemikomponentide regulaarne varundus

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

-

Teabe käideldavus (K)

- M 6.43z Liiasusega Windowsi serverid

Teabe terviklus (T)

-

Teabe konfidentsiaalsus (S)

-

B 3.201 Klient

Käsitlusele tuleb suvalise operatsioonisüsteemiga IT-süsteem, mis võimaldab kasutajate teineteisest eraldamist. Süsteem peaks võimaldama vähemalt ühe administraatori- ja ühe kasutajakeskkonna sisseseadmist. Reeglina on selline IT-süsteem ühendatud võrku ning klient-server-võrgus käsitletakse seda kliendina.

Vastavat IT-süsteemi võib käitada ükskõik millisel platvormil, tegu võib olla kas kõvakettaga varustatud või ilma kõvakettata personaalarvutiga, samuti võib see olla näiteks Unix-Workstation või Apple Macintosh. IT-süsteemi võivad kuuluda disketi-, CD-, DVD-lugejad või muud vahetatavate andmekandjate lugemisseadmed, samuti erinevad lisaseadmed. Juhul kui klient on varustatud veel ka muude andmevahetust võimaldavate liidestega nagu näiteks USB, Bluetooth, WLAN, tuleb ka neid vastavalt institutsiooni turvareeglitele kaitsta, võttes aluseks vastavates moodulites kirjeldatud meetmed.

Käesolev moodul pakub ülevaadet ohuallikatest ja IT-turvameetmetest kõikide klientide kohta, sõltumata nende puhul kasutatud platvormidest või operatsioonisüsteemidest. Konkreetsest operatsioonisüsteemist lähtudes tuleb lisaks järgida ka IT-etalonturbe kataloogi täiendavaid mooduleid.

Ohud

Infosüsteemide etalonturbe seisukohalt loetakse klientide puhul tüüpilisteks järgmisi ohuallikaid:

Organisatsioonilised puudused:

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.7 Õiguste volitamata kasutamine
- G 2.24 Kaitsetus välisvõrgu vastu
- G 2.37 Sideliinide kontrollimatu kasutamine
- G 2.147 Võrdõigusteenustest tulenev puuduv tsentraliseerimine

Inimvead:

- G 3.3 Hooletus turvameetmete suhtes
- G 3.6 Koristajad jm väljastpoolt tellitud töötajad
- G 3.8 IT-süsteemi väär kasutamine
- G 3.17 Arvutikasutajate väär vahetumine

Tehnilised rikked:

- G 4.10 Keerukad ligipääsuvõimalused võrgustatud IT-süsteemides
- G 4.13 Salvestatud andmete hävimine
- M 4.23 Käitusfailide turvaline kutsumine

Ründed:

- G 5.1 IT-seadmete või -tarvikute manipuleerimine ja hävitamine
- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.4 Vargus
- G 5.7 Liinide pealtkuulamine
- G 5.9 IT-süsteemide volitamata kasutamine

- G 5.20 Administraatori õiguste väärkasutus
- G 5.23 Viirused
- G 5.40 Pealtkuulamine ruumis arvuti mikrofoni kaudu
- G 5.71 Tundliku informatsiooni konfidentsiaalsuse kadu
- G 5.85 Tundliku informatsiooni tervikluse kadu

Soovitatavad meetmed

Selleks, et tagada kogu loetletud IT-süsteemi turvalisus, tuleb lisaks käesolevale moodulile rakendada veel ka teisi, IT-etalonturbe modelleerimise käigus selguvaid mooduleid.

Töökohaarvutite puhul tuleks võrgu klientide IT-alase turvalisuse tagamiseks teha läbi järgmised sammud:

Klientide kasutuselevõtu planeerimine

IT-süsteemide turvaliseks kasutamiseks tuleb eelnevalt määrata vastavad raamtingimused. Raamtingimuste määramisse tuleb kaasata juba olemasolevate IT-süsteemide turvanõuded, samuti tuleb juba algusest peale arvestada IT-süsteemi jaoks planeeritud kasutusvaldkondadega (vt M 2.321 Klient-server-võrgu kasutuselevõtu planeerimine). Klientidele kehtiv turvapoliitika tuleks koostada juba enne arvutite ja tarkvara soetamist (vt M 2.322 Klient-server-võrgu turvapoliitika kehtestamine). IT-süsteemide turvalise kasutamise üleüldisi küsimusi lahatakse moodulis B 1.9 Riist- ja tarkvara haldus .

Soetamine

Enne klientide soetamist, mida tehakse reeglina suuremas koguses korraga, tuleb kirja panna sobilike toodete valikukriteeriumid, lähtudes nende vastavast kasutusalast (vt moodul B 1.10 Tüüptarkvara). Ka üksiksüsteemide soetamisel on oluline, et soetatav toode sobiks olemasoleva struktuuriga, vastasel korral võib üksiku süsteemi integreerimine ja töösserakendamine osutuda selle eripäradest tingituna ülemäära töömahukaks.

Juhul kui riist- ja tarkvara ei vasta määratletud turvanõuetele, tuleb rakendada täiendavaid meetmeid. Täiendavad meetmed võivad olla organisatoorset laadi nt, et klienti tohib töös hoida ainult bürooruumis suletud ukse taga, või siis tuleb soetada lisakomponente, et tuvastatud puudujääke korvata (vt meede M 4.41 Sobivate IT-süsteemide turvatoodete valimine).

Juhul kui klientidele esitatavad käideldavuse nõuded on väga kõrged, tuleks nende puhul kasutada puhvertoiteallikat (UPS). Vastavalt vajadusele tuleks rakendada kas nn ühe-töökoha-UPSi, juhul kui käideldavuse kõrgendatud nõuded kehtivad vaid üksikutele klientidele, või siis vastavat eraldi kaitstud vooluringi, nn punast pistikupesa. Täiendavat informatsiooni leiate meetmest M 1.28 Puhvertoiteallikas .

Rakendamine

IT-süsteemide väära kasutamise ja sihiliku väärkasutuse vältimiseks on väga oluline teha põhjalik valik operatsioonisüsteemi ja tarkvara komponentide hulgast ning tagada turvaline installeerimine ja hoolikas konfiguratsioon. Vajalikud meetmed sõltuvad siinkohal suuresti kasutatavast operatsioonisüsteemist. Täpsema info leiate vastavatest moodulitest nagu nt B 3.204 Klient Unixi all või B 3.210 Klient Windowsi all .

Turvaline installeerimine

Turvalisuse nurgakivi pannakse süsteemile juba installeerimise planeerimise faasis. Enne installeerimist tuleks ära määrata, milliseid operatsioonisüsteemi komponente, milliseid rakendusprogramme ja vahendeid (tools) installeerima hakatakse. Langetatud otsused tuleb kirja panna selliselt, et vajadusel oleks võimalik ka hiljem järele kontrollida, millise süsteemikonfiguratsiooni ja tarkvara komponentide valiku kasuks eelnevalt otsustati (vt meede M 4.237 IT-süsteemi turvaline aluskonfiguratsioon).

Installeerimisel tuleks kasutada eranditult vaid kindlatest allikatest pärinevaid andmekandjaid (nt vastava operatsioonisüsteemi või programmi tootja või edasimüüja). Operatsioonisüsteemi installeerimine tuleks, kui vähegi võimalik, läbi viia selliselt, et süsteem ei oleks samal ajal võrku ühendatud (offline -installeerimine). Juhul kui installeerimise käigus on tarvis võrgu kaudu tarkvarapaketi osasid alla laadida, tuleks installeerimise jaoks kasutada sellisel juhul eraldi võrku (testvõrku), mis on ülejäänust võrgust lahus. Tarkvarapakettide hilisem võrgu kaudu lisamine on tungivalt ebasoovitatav. Juhul kui erandkorras on tarvis, et süsteem tuleb installeerida otse töösoleva võrgu külge, tuleb täiendavate lisameetmete abil tagada, et süsteemi ei oleks võimalik installeerimise ajal väljastpoolt rünnata. Juba installeerimise käigus määratakse tihti ära mõningad süsteemi konfiguratsiooni algseaded (eri operatsioonisüsteemide puhul erinevalt).

Turvaline konfigureerimine

Installeerimisele järgneb kliendi aluskonfiguratsiooni tegemine. Selles faasis toimub algse, installeerimise käigus installeerimisprogrammi poolt määratud konfiguratsiooni mugandamine vastavalt kliendi kasutuskeskkonna IT-süsteemi tegelikele oludele ja nõudmistele. Tihti installeeritakse selles faasis juurde lisaprogramme või eemaldatakse teatud programmid standardkonfiguratsioonist, määratakse ära võrgule ligipääsu seaded ja konfigureeritakse kliente kataloogiteenuste jms kasutamise tarbeks. Lisaks eelnevale toimub selles faasis veel ka ebavajalike kasutajatunnuste kustutamine või deaktiveerimine ning reaalsete kasutajate kasutajatunnuste loomine.

Antud etapis toimub ka vajalike rakendusprogrammide installeerimine ja konfigureerimine. Rakendusprogrammide installeerimise ja konfigureerimise käigus tuleb arvestada sarnaste turvaaspektidega nagu operatsioonisüsteemide installeerimise puhul.

Juhul kui on tarvis installeerida ja konfigureerida suurem arv sarnaseid kliente, saab kasutada võimalust, kus vastavaid töid ei pea tegema eraldi iga kliendi juures, luues vastava „üldise" installatsiooni, mis kantakse lõpus üle üksikutele klientidele ning enne töölerakendamist on sellisel juhul tarvis teha veel vaid mõned väiksed muudatused. Niisuguse üldise installatsiooni loomine võib oluliselt suurendada efektiivsust ning vähendada vigade tekkimise riski. Samas jällegi tuleb installeerimise referentsi loomisel olla ülimalt hoolikas. Tehtud seadistused peavad olema arusaadavalt dokumenteeritud.

Oluliseks põhimõtteks klientide konfigureerimisel on asjaolu, et kasutajate poolt tehtavad tavalised vead ei tohi süsteemis tekitada ei tõsiseid rikkeid ega teiste kasutajate andmete kahjustumist, ning et kasutajatel ei tohi olla võimalik puhtalt uudishimust ligi pääseda infole, mis ei ole neile kasutamiseks mõeldud. Rohkem infot leiate meetmest M 4.237 IT-süsteemi turvaline aluskonfiguratsioon .

Pärast seda, kui klient on konfigureeritud, võib arvuti kasutajale üle anda. Juhul

kui kasutajate teadmised arvutis kasutatud operatsioonisüsteemi, üksikute rakendusprogrammide või vahendite (tools) rakendamise kohta ei ole piisavad, tuleb kasutajaid eelnevalt vastavalt koolitada. Üldiseid juhiseid antud valdkonna kohta leiate moodulist B 1.13 Infoturbe teadlikkus ja -koolitus .

Kasutamine

Tänapäevaste klient-süsteemide käitamisel on IT-alase turbe üheks tähtsamaks faktoriks asjaolud, kas turvalisust mõjutavate paikade rakendamine toimub piisavalt operatiivselt, et hoida süsteemi pidevalt kõige ajakohasemal tasemel (vt M 2.273 Turvalisust mõjutavate paikade ja värskenduste kiire paigaldamine), kas viirusetõrjetarkvara on installeeritud ja kas selle täiendite laadimine toimib pidevalt (vt ka moodulit B 1.6 Viirusetõrje kontseptsioon). Lisaks eelnevale on ka reeglipärane andmevarundus (vt lisaks B 1.4 Andmevarunduspoliitika) põhjapanevaks eelduseks sellele, et riistvara rikked ja programmi- või kasutajavead ei tooks endaga kaasa suurt andmekadu.

Üheks võimalikuks vahendiks, kuidas ründeid või väärkasutust tuvastada, on süsteemi jälgimine. Asjakohased juhised leiate meetmetest M 4.93 Regulaarne tervikluse kontroll ja M 5.8 Võrgu regulaarne turvakontroll ning moodulist B 1.9 Riist- ja tarkvara haldus .

Ka klientide puhul on oluline, et administreerimine toimuks turvalisi teid pidi, ning et administraatorite töö oleks kontrollitav. Vastavad olulised aspektid on kirjas meetmes M 4.234 IT-süsteemide ja andmekandjate väljavahetamise kord .

Väljavahetamine

Enne kliendi väljavahetamist peab olema kindel, et kõik kasutajaandmed on varundatud või varusüsteemile üle kantud. Lisaks eelnevale tuleb hoolitseda ka selle eest, et arvuti kõvakettale ei jääks alles tundlikku informatsiooni. Kõvaketaste taasformaatimine ei ole selle jaoks piisav, kõvakettad tuleb vähemalt üks kord täielikult üle kirjutada. Tuleb silmas pidada, et ei puhtalt loogiline kustutamine ega ka ketaste uuesti formaatimine installeeritud operatsioonisüsteemide vahenditega ei eemalda kõvaketastelt andmeid. Sobiva tarkvaraga on installeeritud operatsioonisüsteemide vahenditega kustutatud andmeid võimalik tihti isegi ilma suurema vaevata taastada. Infot turvalise kustutamise kohta leiate meetmetest M 2.13 Tundlike ressursside jäljetu hävitamine ja M 2.309 Mobiilse IT-kasutuse turvapoliitika ja eeskirjad . Pärast kliendi väljavahetamist tuleb vastavad muudatused sisse viia ka varade nimekirja ja võrguplaanidesse.

Valmisolek hädaolukorraks

Hädaolukorraks valmisoleku ulatuse vajadus sõltub tavalise kliendi puhul suuresti selle individuaalsest kasutusvaldkonnast. Tihti piisab kliendi hädaolukorraks valmisoleku täitmiseks reeglipärasest andmevarundusest (vt M 6.32 Regulaarne andmevarundus) ja buutimisvõimelise andmekandja loomisest (vt M 6.24 Rikkejärgse buutimismeedia olemasolu) avariide tarbeks. Klientide puhul, mille käideldavuse nõuded on kõrged, võib olla mõttekas tarvitada lisameetmeid, nt varusüsteemi pidevalt valmis hoida.

Sõltuvalt kasutatavast operatsioonisüsteemist, võib lisaks käesolevale moodulile olla vajalik veel ka täiendavate meetmete rakendamine. Vastava info leiate asjakohastest moodulitest.

Tavalise “Kliendi” puhul tuleb rakendada järgnevaid meetmeid:

Planeerimine ja kontseptsioon

- (L) M 2.23z PC kasutamise juhised
- (L) M 2.321 Klient-server-võrgu kasutuselevõtu planeerimine
- (L) M 2.322 Klient-server-võrgu turvapoliitika kehtestamine
- (L) M 4.41z Sobivate IT-süsteemide turvatoodete valimine
- (M) M 5.66z SSL-i/TLS-i kasutamine kliendis
- (L) M 5.152 Info ja ressursside vahetamine võrdõigusteenuste (p2p) kaudu

Rakendamine

- (L) M 4.40 Arvuti mikrofoni volitamata kasutamise vältimine
- (L) M 4.237 IT-süsteemi turvaline aluskonfiguratsioon

Kasutamine

- (L) M 3.18 PC kasutajate väljalogimiskohustus
- (L) M 4.2 Ekraanilukk
- (L) M 4.3 Viirustõrjeprogrammi regulaarne kasutamine
- (L) M 4.4 Eemaldatavate andmekandjate draivipilude ja väliste andmekandjate nõuetele vastav kasutamine
- (L) M 4.200z USB-salvestuskandjatega ümberkäimine
- (L) M 4.238 Lokaalse paketifiltri rakendamine
- (L) M 4.241 Kliendi turvaline käitus
- (M) M 4.242z Kliendi etaloninstalleeringu loomine
- (L) M 5.45 Veebibrauserite turvaline kasutamine

Väljavahetamine

- (L) M 2.323 Kliendi korrakohane kasutuselt kõrvaldamine

Valmisolek hädaolukorraks

- (L) M 6.24 Rikkejärgse buutimismeedia olemasolu
- (L) M 6.32 Regulaarne andmevarundus

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.6 Arvuti paroolkaitse rangemad reeglid
- HG.7 Ekraaniluku lühem ooteaeg
- HG.24 Paroolide regulaarkontroll parooliskänneriga
- HG.38 Turvapaikade paigaldatuse regulaarseire
- HG.70 Piiratud õigustega personaalne kasutajakonto

Teabe käideldavus (K)
-
Teabe terviklus (T)

- HT.7 Kasutajate ja nende profiilide perioodiline seire

- HT.29 Kombineeritud autentimise nõue

Teabe konfidentsiaalsus (S)

- HS.54 Lisanõuded turvalisele kustutamisele

B 3.202 Autonoomne IT-süsteem

Käsitlusele tuleb IT-süsteem, mis ei ole mitte ühegi teise IT-süsteemiga ühenduses. Vastava lahenduse puhul võib olla tegu ükskõik millise operatsioonisüsteemiga. Vastavat IT-süsteemi võib käitada ükskõik millisel platvormil, tegu võib olla kas kõvakettaga varustatud või ilma kõvakettata personaalarvutiga, samuti võib see olla näiteks Unix -Workstation või Apple Macintosh. IT-süsteemi võivad kuuluda näiteks disketi-, CD-, DVD-lugejad või muud vahetatavate andmekandjate lugemisseadmed, samuti erinevad lisaseadmed. Juhul kui klient on varustatud veel ka muude andmevahetust võimaldavate liidestega nagu näiteks USB, Bluetooth, WLAN, tuleb ka neid vastavalt institutsiooni turvareeglitele kaitsta, võttes aluseks vastavates moodulites kirjeldatud meetmed. Võimalik printer ühendatakse autonoomse IT-süsteemi külge otse.

Käesolev peatükk annab ülevaate erinevatest autonoomse IT-süsteemi puhul tüüpiliseks peetavatest ohuallikatest ja IT-turbe meetmetest. Antud peatükis toodud kirjeldused ei lähtu mitte ühestki kindlast operatsioonisüsteemist. Konkreetsete operatsioonisüsteemide puhul tuleb järgida vastavaid IT-etalonturbe kataloogi täiendavaid mooduleid.

Ohud

Infosüsteemide etalonturbe seisukohalt loetakse autonoomsete IT-süsteemide puhul tüüpilisteks järgmisi ohuallikaid:

Vääramatu jõud:

- G 1.1 Personali väljalangemine
- G 1.2 IT-süsteemi avarii

Organisatsioonilised puudused:

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.7 Õiguste volitamata kasutamine
- G 2.21 Korraldamata kasutajavahetus

Inimvead:

- G 3.3 Hooletus turvameetmete suhtes
- G 3.6 Koristajad jm väljastpoolt tellitud töötajad
- G 3.8 IT-süsteemi väär kasutamine
- G 3.16 Väär pääsuõiguste haldus
- G 3.17 Arvutikasutajate väär vahetumine

Tehnilised rikked:

- G 4.1 Toitevõrgu katkestus
- G 4.7 Defektsed andmekandjad
- G 4.23 Vahetatavate andmekandjate automaattuvastus

Ründed:

- G 5.1 IT-seadmete või -tarvikute manipuleerimine ja hävitamine
- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.4 Vargus
- G 5.9 IT-süsteemide volitamata kasutamine
- G 5.18 Süstemaatiline paroolide mõistatamine
- G 5.19 Kasutajaõiguste väärkasutus
- G 5.20 Administraatori õiguste väärkasutus
- G 5.23 Pahavara

Soovitatavad meetmed

Selleks, et tagada kogu loetletud IT-süsteemi turvalisus, tuleb lisaks käesolevale moodulile rakendada veel ka teisi, IT-etalonturbe modelleerimise käigus selguvaid mooduleid.

Järgneb ülevaade „Autonoomne IT-süsteem“ meetmete paketist. Mõningad järgnevalt loetletud meetmetest tuleb ilmtingimata ellu rakendada ka siis kui vastavat IT-süsteemi kasutab vaid üksainus inimene. Juhul kui vastava IT-süsteemiga töötab mitu inimest, on arvuti administreerimine ja kasutajate teineteisest lahutamine möödapääsmatu. Sellistel juhtudel tuleb arvestada sarnaste ohuallikate ja vastumeetmetega nagu ühiskasutussüsteemi puhul.

Sõltuvalt kasutatavast operatsioonisüsteemist, võib lisaks käesolevale moodulile olla vajalik veel ka täiendavate, teistes moodulites kirjeldatud meetmete rakendamine.

Autonoomselt töötavate töökohaarvutite puhul tuleks IT-alase turvalisuse tagamiseks läbi teha järgmised sammud:

1. Suunised autonoomsete IT-süsteemide kasutamiseks.

Autonoomsete IT-süsteemide turvaliseks kasutamiseks tuleb kehtestada kohustuslikud kasutussuunised. Suunised peaksid näiteks määrama, kes, kunas ja mille jaoks vastavat IT-süsteemi tohib kasutada ning mil moel pääseb erinevatele andmetele ligi. Vastav töö tuleb ära teha mooduli B 1.9 Riist- ja tarkvara haldus ellurakendamisel.

2. Autonoomsete IT-süsteemide turvaline installeerimine

IT-süsteemide väära kasutamise ja sihiliku väärkasutuse vältimiseks on väga oluline teha põhjalik valik operatsioonisüsteemide ja tarkvara komponentide hulgast ning tagada nende turvaline installeerimine. Siinkohal kasutatavad meetmed sõltuvad suuresti konkreetsest operatsioonisüsteemist ja seetõttu toimub nende kehtestamine asjakohaste moodulite rakendamise käigus, nt moodul B 3.204 Klient Unixi all . Eriti oluline on siinkohal meede M 4.15 Turvaline sisselogimine kuna autonoomsete süsteemide tehniline kaitse põhineb suures osas juurdepääsu kontrolli tagamisel. Täiendavad meetmed on vajalikud eelkõige siis, kui ühe IT-süsteemiga töötab mitu kasutajat, kellele kasutajaõigused on erinevad:

- M 2.63 Pääsuvolituste kehtestamine
- M 3.18 PC kasutajate väljalogimiskohustus
- M 4.41 Sobivate IT-süsteemide turvatoodete valimine

3. Installeeritud komponentide turvaline konfiguratsioon.

Sõltuvalt erinevatest turvanõuetest, tuleb vastavad tarkvarakomponendid ka erinevalt konfigureerida. Siinkohal kasutatavad meetmed sõltuvad samuti konkreetsest operatsioonisüsteemist ja seetõttu kuulub nende kehtestamine vastavate moodulite rakendamise alla. Mitme kasutaja puhul, kelle volitused on erinevad, tuleb ka siin rakendada täiendavaid meetmeid. Tähelepanu tuleks pöörata ka meetmele M 4.7 Algparoolide muutmine kuna väga tihti on pääsuõiguste kontrollimine puhas illusioon, sest paroolid on tegelikult kõigile teada.

4. Autonoomsete IT-süsteemide turvaline käitamine

Tänapäevaste klient-süsteemide käitamisel on üheks tähtsamaks IT-turvameetmeks viirusetõrjetarkvara installeerimine ja pidev uuendamine. Võimalike rünnete ja väärkasutuse tuvastamiseks on autonoomsete IT-süsteemide puhul tähtsad eelkõige vastavad organisatsioonilised meetmed. Kuna vastavad meetmed tuleb kehtestada juba moodulite B 1.6 Viirusetõrje kontseptsioon ja B 1.9 Riist- ja tarkvara haldus rakendamise käigus, siis siinkohal neid lähemalt enam ei käsitleta. Spetsiifilisemad meetmed on autonoomsete süsteemide puhul eelkõige M 4.4 Eemaldatavate andmekandjate draivipilude ja väliste andmekandjate nõuetele vastav kasutamine ja M 4.30 Rakendusprogrammide turvavahendite kasutamine .

5. Autonoomsete IT-süsteemide andmevarundus

Tegutsemisplaan ja andmevarunduse vajalik ulatus sõltub IT-süsteemi kasutusalast (vt meede M 6.32 Regulaarne andmevarundus).

Tavalise autonoomse IT-süsteemi puhul tuleb rakendada järgnevaid meetmeid:

Planeerimine ja kontseptsioon

- (L) M 2.23 PC kasutamise juhised
- (L) M 2.63 Pääsuvolituste kehtestamine
- (L) M 4.41 Sobivate IT-süsteemide turvatoodete valimine

Rakendamine

- (L) M 4.7 Algparoolide muutmine
- (L) M 4.15 Turvaline sisselogimine

Kasutamine

- (L) M 2.22 Paroolide deponeerimine
- (L) M 3.18 PC kasutajate väljalogimiskohustus
- (L) M 4.2 Ekraanilukk
- (M) M 4.4 Eemaldatavate andmekandjate draivipilude ja väliste andmekandjate nõuetele vastav kasutamine
- (L) M 4.30 Rakendusprogrammide turvavahendite kasutamine

Valmisolek hädaolukorraks

- (L) M 6.32 Regulaarne andmevarundus

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.6 Arvuti paroolkaitse rangemad reeglid
- HG.24 Paroolide regulaarkontroll parooliskänneriga
- HG.38 Turvapaikade paigaldatuse regulaarseire
- HG.70 Piiratud õigustega personaalne kasutajakonto

Teabe käideldavus (K)
-
Teabe terviklus (T)

- HT.14 Süsteemi tegevuslogide krüptoaheldamine
- HT.29 Kombineeritud autentimise nõue

Teabe konfidentsiaalsus (S)

- HS.54 Lisanõuded turvalisele kustutamisele

B 3.203 Sülearvuti

Sülearvuti (Laptop või Notebook) all peetakse silmas personaalarvutit, mida on võimalik tänu selle ehitusele kergelt transportida ja mobiilselt kasutada. Sülearvuti on oma mõõtmetelt kompaktsem kui töökohaarvuti ning akutoitel on seda võimalik mõnda aega ka ilma vooluvõrguta töös hoida. Sülearvuti on varustatud kõvakettaga ja reeglina veel ka muude salvestusvahenditega nagu disketi-, CD-, DVD-lugejad ning erinevate kommunikatsiooniliidestega (nt Modem, ISDN, LAN, USB, Firewire, WLAN). Sülearvutites on võimalik kasutada kõiki üldlevinud operatsioonisüsteeme nagu nt Windows või Linux, mistõttu tuleb lisaks käesolevale järgida ka klienti käsitlevat moodulit.

Sülearvuti puhul on tüüpiline, et teatud aeg kasutatakse seda arvutivõrgust lahus ning aeg-ajalt ühendatakse see andmete sünkroniseerimiseks ja andmevarunduseks ametiasutuse või ettevõtte võrku. Tihti ühendatakse sülearvuti mobiilse kasutuse raames modemi abil otse välisvõrkudesse, eriti internetti, seega võib öelda, et sülearvuti toimib kaudselt sillana kohtvõrgu ja interneti vahel.

Andmeedastuse seadistamist (modemi, ISDN-kaardi jms abil) siinkohal ei käsitleta (vt B 4.3 Modem). Sülearvuti puhul eeldatakse, et teatud kindla aja jooksul kasutab seda seadet ainult üks kasutaja. Lisaks eelnevale käsitletakse ka kasutaja vahetumist.

Ohud

Infosüsteemide etalonturbe seisukohalt loetakse sülearvutite puhul tüüpilisteks järgmisi ohuallikaid:

Vääramatu jõud:

- G 1.2 IT-süsteemi avarii
- G 1.15 Muutuvast rakenduskeskkonnast tingitud kahjustused

Organisatsioonilised puudused:

- G 2.7 Õiguste volitamata kasutamine
- G 2.8 Ressursside kontrollimatu kasutamine
- G 2.16 Sülearvuti reguleerimata edasiandmine

Inimvead:

- G 3.2 Seadme või andmete hävitamine hooletuse tõttu
- G 3.3 Hooletus turvameetmete suhtes
- G 3.6 Koristajad jm väljastpoolt tellitud töötajad
- G 3.8 IT-süsteemi väär kasutamine
- G 3.38 Vead konfigureerimisel ja kasutamisel
- G 3.76 Vead kaasaskantavate seadmete sünkroniseerimisel

Tehnilised rikked:

- G 4.9 Sisemise toiteallika tühjenemine
- G 4.13 Salvestatud andmete hävimine
- G 4.22 Tüüptarkvara turvaaugud või vead
- G 4.52 Kaasaskantava seadme andmekadu

Ründed:

- G 5.1 IT-seadmete või -tarvikute manipuleerimine ja hävitamine
- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.4 Vargus
- G 5.9 IT-süsteemide volitamata kasutamine
- G 5.18 Süstemaatiline paroolide mõistatamine
- G 5.22 Kaasaskantava IT-süsteemi vargus
- G 5.23 Viirused
- G 5.71 Tundliku informatsiooni konfidentsiaalsuse kadu
- G 5.124 Kaasaskantavate seadmete teabe väärkasutus
- G 5.125 Volitamatu andmeedastus kaasaskantavate seadmetega
- G 5.126 Volitamatu pildistamine ja filmimine kaasaskantavate seadmetega

Soovitatavad meetmed

Selleks, et tagada kogu loetletud IT-süsteemi turvalisus, tuleb lisaks käesolevale moodulile rakendada veel ka teisi, IT-etalonturbe modelleerimise käigus selguvaid mooduleid.

Sülearvuti kasutamisel tuleb rakendada erinevaid meetmeid, tegeldes kontseptsiooni ja soetamisega kuni igapäevase töötamiseni välja. Järgnevalt anname ülevaate erinevatest kohustuslikest etappidest ja meetmetest, mida tuleks iga etapi puhul rakendada.

1. Suunised sülearvutite kasutamiseks

Sülearvutite turvaliseks ja efektiivseks kasutamiseks ametiasutustes või ettevõtetes tuleb välja töötada kontseptsioon, mis arvestab juba olemasolevatele IT-süsteemidele kehtivate turvanõuetega ja lisaks ka nende nõuetega, mis tulenevad sülearvutite jaoks planeeritud kasutusvaldkondadest (vt M 2.36 Sülearvuti väljaandmise ja tagastamise reeglid ja moodul B 3.201 Klient).

Nimetatud kontseptsioonile toetudes tuleb reguleerida sülearvutite kasutamine ja välja töötada vastavad turvajuhised (vt M 2.309 Mobiilse IT-kasutuse turvapoliitika ja eeskirjad). Juhised peaksid näiteks määrama kes, millal ja mille jaoks tohib vastavat IT-süsteemi kasutada ning mil moel ettevõtte või ametiasutuse võrku ligi pääseb. Samuti tuleb määrata, kas ja millisel kujul on mobiilse kasutuse korral lubatud sülearvutit otse internetti ühendada.

2. Sülearvutite soetamine

Sülearvutite soetamisel tuleb lähtuda eelnevalt välja töötatud kontseptsioonist ja sõnastada vajaminevate toodete jaoks kehtivad nõudmised, millest lähtudes tehakse lõplik valik sobilike toodete hulgast (vt M 2.310 Sobivate sülearvutite valimine).

3. Sülearvutite turvaline installeerimine

Sülearvutite väära kasutamise ja sihiliku väärkasutuse vältimiseks on väga oluline teha põhjalik valik operatsioonisüsteemide ja tarkvara komponentide hulgast ning tagada nende turvaline installeerimine. Siinkohal kasutatavad meetmed sõltuvad suuresti konkreetsest operatsioonisüsteemist ja seetõttu toimub nende kehtestamine asjakohaste moodulite rakendamise käigus.

Eriti oluline on siinkohal meede M 4.29 Kaasaskantavatele IT-süsteemidele mõeldud krüpteerimistoote kasutamine , kuna sülearvutite puhul on suur vargu-

se oht ning tavalistest kasutus- ja pääsuõigustest ei ole suurt kasu, juhul kui arvuti langeb varguse ohvriks.

4. Installeeritud komponentide turvaline konfiguratsioon

Sõltuvalt erinevatest turvanõuetest, tuleb vastavad tarkvarakomponendid ka erinevalt konfigureerida. Siinkohal kasutatavad meetmed sõltuvad samuti konkreetsest operatsioonisüsteemist ja seetõttu kuulub nende kehtestamine vastavate moodulite rakendamise alla. Mitme kasutaja puhul, kelle volitused on erinevad, tuleb ka siin rakendada täiendavaid meetmeid. Tähelepanu tuleks pöörata ka meetmele M 4.7 Algparoolide muutmine kuna väga tihti muutub pääsuõiguste kontrollimine puhtalt illusiooniks, sest paroolid on tegelikult kõigile teada.

5. Sülearvutite turvaline käitus

Tänapäevaste sülearvutite käitamisel on üheks tähtsamaks IT-turvameetmeks viirusetõrjetarkvara installeerimine ja selle pidev uuendamine. Sülearvuteid kasutatakse tihti pikema aja jooksul firma või ametiasutuse võrgust lahus või ühendatakse neid ajutiste ühenduste abil internetti. Seetõttu võivad viirusdefinitsioonide failid vananeda ning vastuvõtlikkus erinevatele arvutiviirustele suureneda. Eriti olulised on sülearvutite puhul moodulis B 1.6 Viirusetõrje kontseptsioon ette nähtud meetmed, eelkõige meede M 2.159 Viiruseskanneri värskendamine . Vastavaid meetmeid mitte kasutades võivad sülearvutid ettevõtte või ametiasutuse võrku ühendamisel kujuneda väga ohtlikeks viirusallikateks.

Juhul kui sülearvuteid ühendatakse mobiilse kasutuse raames otse internetti, on piirangutega konfigureeritud Personal Firewall kohustuslik, et arvutit võrgust tulevate rünnete eest kaitsta. Kõikvõimalike rünnete eest kaitsmiseks ei piisa siiski ainult viirusetõrjest üksi. Samamoodi on tähtis, et sülearvuti tarkvara oleks pidevalt uuendatud ning et turvalisust mõjutavate paikade laadimine toimuks võimalikult operatiivselt. Juhul kui sülearvutit on tarvis uuesti ettevõtte või ametiasutuse võrku ühendada ning eelnevalt oli see ühendatud otse internetti, tuleb esmalt värskendatud viirusetõrjetarkvara põhjaliku skaneerimisega kindlaks teha, kas sülearvutis on viiruseid või mitte. Sülearvutit tohib kohtvõrku ühendada alles pärast seda, kui viiruste olemasolu arvutis on välistatud (vt M 5.122 Sülearvuti turvaline ühendamine kohtvõrguga). Eelnev kehtib ka neil juhtudel, kus võrkuühendamine toimub virtuaalse privaatvõrgu (VPN-i) abil, kuna viirused võivad hakata levima ka krüpteeritud juurdepääsude kaudu.

Võrku ühendatud ja mobiilse kasutuse vahel vahetades tuleb andmed sülearvuti ja serveri vahel sünkroniseerida. Sealjuures peab olema tagatud, et alati oleks võimalik tuvastada, kas kõige uuem töödeldud andmete versioon asub parasjagu sülearvutis või võrgus (vt M 4.235 Andmete seisu võrdsustamine sülearvutis).

Võimalike rünnete ja väärkasutuse tuvastamiseks on sülearvutite kasutamise puhul tähtsad eelkõige vastavad organisatsioonilised meetmed. Kuna vastavad meetmed tuleb kehtestada juba mooduli B 1.9 Riist- ja tarkvara haldus rakendamise käigus, siis siinkohal neid lähemalt enam ei käsitleta. Reaalselt kohtvõrku ühendatud sülearvutite kohta käiva ülevaate tagamiseks ja nende konfiguratsiooni pidevaks jälgimiseks on oluline, et kõigi sülearvutite haldamine toimuks ühest kohast (vt M 4.236 Sülearvutite tsentraalne haldus).

Autonoomsete süsteemide puhul on täiendavateks spetsiifilisemateks meetmeteks eelkõige meede M 4.4 Eemaldatavate andmekandjate draivipilude ja väliste andmekandjate nõuetele vastav kasutamine ja M 4.30 Rakendusprogrammide turvavahendite kasutamine .

Sõltuvalt hoone või bürooruumi füüsilistest turvatingimustest, võib olla mõttekas või koguni hädavajalik rakendada meedet M 1.46 Vargusetõrjevahendid . Mobiilse kasutuse korral tuleb olukorrast sõltumata igal juhul rakendada meedet M 1.33 Kaasaskantavate IT-süsteemide hoidmine reisil , et kaitsta sülearvutit varguse eest.

6. Väljavahetamine

Sülearvuti üleandmisel uuele kasutajale, olgu tegu kas tavakasutuse või väljavahetamisega, tuleb silmas pidada, et kõvakettale ei jääks alles tundlikku informatsiooni. Siinkohal tuleb ennekõike järgida meedet M 2.36 Sülearvuti väljaandmise ja tagastamise reeglid ning sõltuvalt olukorrast ka meedet M 4.28 Sülearvuti tarkvara reinstalleerimine kasutaja vahetumisel .

7. Sülearvutite andmevarundus

Tegutsemisplaan ja andmevarunduse vajalik ulatus sõltub sülearvuti kasutusalast (vt M 6.71 Mobiilse IT-süsteemi andmevarundus).

Järgneb ülevaade „Sülearvuti“ meetmete paketist.

Planeerimine ja kontseptsioon

- (L) M 2.36 Sülearvuti väljaandmise ja tagastamise reeglid
- (L) M 2.218 Andmekandjate ja IT-komponentide kaasavõtmise protseduurid
- (L) M 2.309 Mobiilse IT-kasutuse turvapoliitika ja eeskirjad
- (M) M 4.29z Kaasaskantavatele IT-süsteemidele mõeldud krüpteerimistoote kasutamine

Soetamine

- (M) M 2.310z Sobivate sülearvutite valimine

Rakendamine

- (M) M 5.91 Interneti-PC personaalse tulemüüri installeerimine
- (L) M 5.121 Turvaline side mobiilseadme ja töökoha vahel
- (L) M 5.122 Sülearvuti turvaline ühendamine kohtvõrguga

Kasutamine

- (L) M 1.33 Kaasaskantavate IT-süsteemide hoidmine reisil
- (L) M 1.34 Kaasaskantavate IT-süsteemide hoidmine põhiasukohas
- (M) M 1.35z Kaasaskantavate IT-süsteemide ühisladustus
- (M) M 1.46z Vargusetõrjevahendid
- (L) M 4.3 Viirustõrjeprogrammi regulaarne kasutamine
- (L) M 4.27 Sülearvuti paroolkaitse
- (L) M 4.28z Sülearvuti tarkvara reinstalleerimine kasutaja vahetumisel
- (L) M 4.31 Toite tagamine mobiilsel kasutamisel
- (L) M 4.235 Andmete seisu võrdsustamine sülearvutis
- (M) M 4.236z Sülearvutite tsentraalne haldus
- (M) M 4.255 Infrapunaliidese kasutamine

Väljavahetamine

- (L) M 2.306 Kahjudest teatamine

Valmisolek hädaolukorraks

- (L) M 6.71 Mobiilse IT-süsteemi andmevarundus

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.6 Arvuti paroolkaitse rangemad reeglid
- HG.7 Ekraaniluku lühem ooteaeg
- HG.24 Paroolide regulaarkontroll parooliskänneriga
- HG.34 Sülearvutite kasutuse regulaarseire
- HG.38 Turvapaikade paigaldatuse regulaarseire
- HG.70 Piiratud õigustega personaalne kasutajakonto

Teabe käideldavus (K)

- HK.5 Mobiilseadme aku regulaarvahetus

Teabe terviklus (T)

- HT.7 Kasutajate ja nende profiilide perioodiline seire
- HT.29 Kombineeritud autentimise nõue
- HT.63 Sülearvutite krüpteerimine

Teabe konfidentsiaalsus (S)

- HS.54 Lisanõuded turvalisele kustutamisele
- HS.62 Infrapunaliidese ja bluetooth 'i kasutuskeeld

B 3.204 Klient Unixi all

Käsitlusele tuleb Unix-süsteem, mida käitatakse kas stand-alone-režiimis või kliendina võrgus. Süsteemi võivad olla ühendatud terminalid, lugemisseadmed, printerid ja muud seadmed. Lisaks eelnevale võib olla kasutusel veel ka graafiline kasutajaliides X-Window . Ühendatud võivad olla vastavalt ka X-Terminalid ja graafilised sisestusseadmed. Järgneva käsitluse puhul eeldatakse, et reeglina kasutatakse Unix -süsteemi mitme isiku poolt.

Ohud

Infosüsteemide etalonturbe seisukohalt loetakse Unix -süsteemi puhul tüüpilisteks järgmisi ohuallikaid:

Vääramatu jõud:

- G 1.1 Personali väljalangemine
- G 1.2 IT-süsteemi avarii
- G 1.8 Tolm, saastumine

Organisatsioonilised puudused:

- G 2.7 Õiguste volitamata kasutamine
- G 2.9 Halb kohanemine IT muutustega
- G 2.15 Konfidentsiaalsusaugud Unix-süsteemis

Inimvead:

- G 3.2 Seadme või andmete hävitamine hooletuse tõttu
- G 3.3 Hooletus turvameetmete suhtes
- G 3.6 Koristajad jm väljastpoolt tellitud töötajad
- G 3.8 IT-süsteemi väär kasutamine
- G 3.9 IT-süsteemi väär haldus
- G 3.21 Mehaaniliste koodlukkude väär kasutamine
- G 3.23 Andmebaasisüsteemi hooletu haldus

Tehnilised rikked:

- G 4.11 NIS-serveri ja NIS-klientsüsteemi vahelise autentimisvõimaluse puudumine
- G 4.12 Autentimisvõimaluste puudumine X-serveri ja X-kliendi vahel

Ründed:

- G 5.1 IT-seadmete või -tarvikute manipuleerimine ja hävitamine
- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.4 Vargus
- G 5.7 Liinide pealtkuulamine
- G 5.8 Liinide manipuleerimine
- G 5.9 IT-süsteemide volitamata kasutamine
- G 5.18 Süstemaatiline paroolide mõistatamine
- G 5.19 Kasutajaõiguste väärkasutus

- G 5.20 Administraatori õiguste väärkasutus
- G 5.21 Trooja hobused
- G 5.23 Viirused
- G 5.41 Unix-süsteemi väärkasutus UUCP-ga
- G 5.89 Võrguühenduse ülevõtt

Soovitatavad meetmed

Selleks, et tagada kogu loetletud IT-süsteemi turvalisus, tuleb lisaks käesolevale moodulile rakendada veel ka teisi, IT-etalonturbe modelleerimise käigus selguvaid mooduleid.

Unixi all olevate klientide puhul tuleb rakendada erinevaid meetmeid, tegeldes kontseptsiooni ja käitamisega kuni valmisolekuks hädaolukordadeni välja. Järgnevalt anname ülevaate erinevatest kohustuslikest etappidest ja meetmetest, mida tuleks iga etapi puhul rakendada.

Planeerimine ja kontseptsioon

Juba enne Unix -süsteemi esmakordset kasutamist, olenemata, kas seda plaanitakse rakendada kliendina, terminali- või rakendusserveri või autonoomse süsteemi funktsioonides, tuleb vastu võtta terve rida otsuseid, mis panevad aluse süsteemi korrapärasele ja turvalisele kasutusele. Juba päris alguses tehtud vigu on tihti võimalik vaid suure vaevaga likvideerida.

Üheselt tuleb määratleda kasutajatunnuste andmise protsess nii, et privilegeeritud ja mitteprivilegeeritud kasutajatunnuseid oleks võimalik teineteisest selgelt eristada. Lisaks eelmainitule tuleb tagada, et ainukasutajarežiimis (Single-User-Mode) ei võimaldataks kellelegi kontrollimatut ligipääsu, kuna vastasel juhul võidakse kõikidest süsteemile kehtestatud turvameetmetest mööda minna.

Rakendamine

Unix -süsteemi installeerimisel tuleb võtta tarvitusele terve rida meetmeid, (eriti oluline on meede M 4.105 Unixi turvaline tüüpinstalleerimine), mille ülesandeks on süsteemi „karastamine“ ehk turvaaukude sulgemine, mis pärast tüüpinstalleerimist reeglina veel alles on. Siia alla kuulub muuhulgas ka ainult tõesti vajalike võrguteenuste sisselülitamine (vt M 5.72 Mittevajalike võrguteenuste desaktiveerimine (Unix)) ning süsteemi logi aktiveerimine.

Seejärel tuleb jagada ülevaatliku skeemi järgi kasutajafailide, süsteemifailide ning süsteemikataloogide pääsuõigused selliselt, et pääsuõigused saavad ainult need kasutajad ja protsessid, kes neid tõepoolest ka vajavad, kusjuures erilist tähelepanu tuleb siinkohal pöörata setuid ja setgid funktsioonidega antavatele õigustele (vt M 4.19 Unixi süsteemifailide ja -kataloogide atribuutide jaotuse piirangud).

Kasutamine

Unix -süsteemi turvalisust puudutava ülevaate tagamiseks on ülimalt oluline, et olemasolevad kasutajaprofiilid ja nende volitused saaksid operatiivselt dokumenteeritud, et vastavat dokumentatsiooni pidevalt uuendataks ja reeglipäraselt kontrollitaks, kas dokumentatsioon vastab reaalsele olukorrale. Süsteemi turvalisust tuleb reeglipäraselt kontrollida ning kontrolli raames tuleb muuhulgas uurida, kas süsteemi poolt koostatud logides esineb ebakorrapärasusi.

Valmisolek hädaolukorraks

Kuna Unix -süsteemide keerukuse tõttu on ka peale edukaks osutunud rünnet tihti väga raske saada kahjustuse ulatusest selget ülevaadet, on oluline, et juba eelnevalt oleks paika pandud reeglid, kuidas reaalselt asetleidnud süsteemi terviklikkuse kao või selle kahtluse korral toimida.
Alljärgnevalt tutvustatakse meetmete kogumit, mida tuleb rakendada valdkonnas „Klient Unixi all“.

Võimalike külgeühendatud arvutite puhul (nt kliendid Windows NT või Windows 95 all) tuleb rakendada vastavates moodulites kirjeldatud meetmeid.

Lisaks eelnevale tuleb rakendada veel järgmisi täiendavaid meetmeid:

Planeerimine ja kontseptsioon

- (L) M 2.33z Unixi ülemarollide jagamine
- (L) M 4.13 Identifikaatorite hoolikas jaotamine
- (L) M 4.18 Monitori- ja ainukasutajarežiimi pääsu reguleerimine
- (M) M 4.41z Sobivate IT-süsteemide turvatoodete valimine
- (M) M 5.64z Secure Shell (SSH)

Rakendamine

- (L) M 2.32z Piiratud kasutajakeskkonna loomine
- (L) M 4.9 X Windowsi turvamehhanismid
- (L) M 4.14 Kohustuslik paroolkaitse Unixi all
- (L) M 4.16 Konto- ja/või terminalipääsu piirangud
- (L) M 4.17 Tarbetute kontode ja terminalide blokeerimine
- (L) M 4.19 Unixi süsteemifailide ja -kataloogide atribuutide jaotuse piirangud
- (M) M 4.20 Unixi kasutajafailide ja -kataloogide atribuutide jaotuse piirangud
- (L) M 4.21 Ülemaõiguste volitamatu võtu vältimine
- (L) M 4.22z Andmete konfidentsiaalsuse kao vältimine Unix-süsteemis
- (M) M 4.23 Käitusfailide turvaline kutsumine
- (L) M 4.105 Unixi turvaline tüüpinstalleerimine
- (L) M 4.106 Süsteemi logimise aktiveerimine (Unix)
- (L) M 4.370z Anoubise kasutamine Windowsis
- (L) M 5.17 NFSi turvamehhanismid
- (L) M 5.18 NISi turvamehhanismid
- (L) M 5.19 Sendmaili turvamehhanismid
- (L) M 5.20 rlogin, rsh ja rcp turbemehhanismid
- (L) M 5.21 telneti, ftp, tftp, rexeci turvaline kasutamine
- (L) M 5.35 UUCP turvamehhanismid
- (L) M 5.72 Mittevajalike võrguteenuste desaktiveerimine (Unix)

Kasutamine

- (L) M 4.25 Logimine Unix-süsteemis
- (L) M 4.26 Regulaarne turvakontroll Unix-süsteemis

Valmisolek hädaolukorraks

- (L) M 6.31 Protseduurid süsteemi tervikluse kao puhuks

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.6 Arvuti paroolkaitse rangemad reeglid
- HG.7 Ekraaniluku lühem ooteaeg
- HG.70 Piiratud õigustega personaalne kasutajakonto

Teabe käideldavus (K)
-
Teabe terviklus (T)

- HT.7 Kasutajate ja nende profiilide perioodiline seire

Teabe konfidentsiaalsus (S)
-

B 3.208 Interneti-PC

Interneti kasutamine informatsiooni hankimise ja kommunikatsiooni eesmärgil on tänapäeva avaliku halduse ja eramajanduse sektoris iseenesest mõistetavaks muutunud. Ka internetikaubanduse ja e-valitsuse funktsioonid muutuvad üha tähtsamaks. Mugavaim lahendus terve ühe asutuse töötajate jaoks on see, kui juurdepääs Internetile võimaldatakse otse töökohaarvutist. Töökohaarvuti on aga üldjuhul ühendatud kohtvõrku (LAN), mis tähendab, et vastav olukord võib põhjustada asutuse jaoks teatud turvariske.

Turvaprobleemide vältimiseks või muudest, kasutuse spetsiifikast tulenevatest põhjustest lähtudes leidub üha rohkem asutusi ja ettevõtteid, kes seavad sisse eraldiseisvad „Interneti-PCd“. Interneti-PC all peetakse silmas arvutit, mis kasutab internetiühendust, kuid ei ole ühendatud institutsiooni sisevõrguga. Juhul kui sisse on seatud mitu Interneti-PCd, võivad need omavahel ka ühenduses olla, näiteks kasutada ühist internetiühendust. Enamasti on Interneti-PCde ülesandeks töötajatele internetiteenuste võimaldamine sellisel moel, et kohtvõrk ei oleks sealjuures ohustatud.

Käsitlusele tuleb Interneti-PC, milles kasutatakse kas Windows või Linux operatsioonisüsteemi. Interneti kasutamisel lähtutakse enamlevinud veebilehitsejatest nagu Internet Explorer, Netscape Navigator või Opera, ning meiliklientidest nagu nt Microsoft Outlook, Outlook Express, Netscape Messenger või KMail. Vastavalt kasutusalale võivad olla installeeritud ka muid internetiteenuseid, näiteks News , Instant Messaging või Internet-Banking , pakkuvad programmid.

Ohud

Infosüsteemide etalonturbe seisukohalt loetakse Interneti-PCde tüüpilisteks järgmisi ohuallikaid:

Vääramatu jõud:

- G 1.2 IT-süsteemi avarii

Organisatsioonilised puudused:

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.2 Reeglite puudulik tundmine
- G 2.21 Korraldamata kasutajavahetus

Inimvead:

- G 3. 1 Andmete konfidentsiaalsuse või tervikluse kadu kasutaja vea tõttu
- G 3.3 Hooletus turvameetmete suhtes
- G 3.9 IT-süsteemi väär haldus
- G 3.38 Vead konfigureerimisel ja kasutamisel

Tehnilised rikked:

- G 4.22 Tüüptarkvara turvaaugud või vead

Ründed:

- G 5.1 IT-seadmete või -tarvikute manipuleerimine ja hävitamine
- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.21 Trooja hobused
- G 5.23 Viirused
- G 5.43 Makroviirused
- G 5.48 IP-aadressi võltsimine
- G 5.78 DNS-i võltsimine
- G 5.87 Veebilehe võltsimine
- G 5.88 Aktiivsisu väärkasutus
- G 5.103 Veebimeili väärkasutus
- G 5.143 Man-in-the-Middle tüüpi rünne

Soovitatavad meetmed

Selleks, et tagada kogu loetletud IT-süsteemi turvalisus, tuleb lisaks käesolevale moodulile rakendada veel ka teisi, IT-etalonturbe modelleerimise käigus selguvaid mooduleid.

Juhul kui ettevõte või ametiasutus plaanib installeerida kas ühe või mitu Interneti-PCd, tuleks IT-etalonturbe seisukohalt läbi teha järgmised sammud:

1. Kontseptsiooni loomine

Esmalt tuleb selgeks teha kasutusala üldpõhimõtted, nt milliseid internetiteenuseid kasutama hakatakse ning kes saab olema Interneti-PC administreerimise eest vastutav.

2. Kasutussuuniste väljatöötamine

Interneti-PCde turvaliseks kasutamiseks tuleb kehtestada kohustuslikud kasutussuunised. Suunised peaksid näiteks määrama, kes, kunas ja mille jaoks vastavat Interneti-PCd kasutada tohib ning mil moel andmeid Interneti-PC ja kohtvõrgu vahel edastatakse.

3. Turvaline installeerimine (vt M 4.151 Internet-PC turvaline installeerimine)

Internetiühendus kujutab endast Interneti-PCle installeeritud rakenduste ja sinna arvutisse salvestatud andmete jaoks täiendavat ohuallikat. Seepärast on eriti oluline, et operatsioonisüsteem ja tarkvara komponendid saaksid hoolikalt valitud ja turvaliselt installeeritud.

4. Installeeritud komponentide turvaline konfiguratsioon

Sõltuvalt erinevatest turvanõuetest tuleb vastavad tarkvarakomponendid ka erinevalt konfigureerida. Eriti puudutab see veebibrauserit (vt M 5.93 Veebibrauseri turve Internet-PC kasutamisel), meiliklienti (vt M 5.94 Meilikliendi turve Internet-PC kasutamisel) ning olenevalt olukorrast ka spetsiaalset E-Business -tarkvara.

5. Interneti-PCde turvaline käitamine (vt M 4.152 Internet-PC turvaline käitus)

Interneti-PCde käitamisel on üheks tähtsamaks IT-turvameetmeks reeglipärane turvalisust mõjutavate paikade ja täiendite võimalikult kiire paigaldamine. Võimalike rünnete ja väärkasutuse tuvastamiseks tuleks Interneti-PCde kasutamise puhul süsteemi lisaks kõigele ka jälgida.

6. Interneti-PCde andmevarundus (vt M 6.79 Andmete varundamine Internet-PCde kasutamisel).

Tegutsemisplaan ja andmevarunduse vajalik ulatus sõltub Interneti-PC kasutusalast.

Käesolev moodul annab soovitusi Interneti-PC kontseptsiooni loomise, konfiguratsiooni ja käitamise kohta. Siinjuures on oluline meeles pidada, et standardse töökohaarvuti jaoks, millel kasutatakse reeglina mitut erinevat rakendust ja millega töödeldakse tundlikku informatsiooni, ei piisa käesolevas materjalis nimetatud meetmetest. Käesolev meetmete pakett keskendub eranditult vaid spetsiaalsele kasutusalale, milleks on „Interneti-PC“. Standardsetele töökohaarvutitele kehtivad IT-turvasuunised leiate mooduli paketi nr 3 teistest, klienti käsitlevatest moodulitest.

Alljärgnevalt tutvustatakse meetmete kogumit, mida tuleb rakendada valdkonnas „Interneti-PC“.

Planeerimine ja kontseptsioon

- (M) M 4.41z Sobivate IT-süsteemide turvatoodete valimine
- (M) M 5.66z SSL-i/TLS-i kasutamine kliendis
- (M) M 5.92 Internet-PC turvaline Internetiga ühendamine

Rakendamine

- (L) M 4.151 Internet-PC turvaline installeerimine
- (M) M 5.91 Interneti-PC personaalse tulemüüri installeerimine
- (L) M 5.98 Kulukate sissehelistusnumbrite kasutamise tõkestamine

Kasutamine

- (L) M 2.313 Turvaline sisselogimine internetiteenustesse
- (L) M 4.3 Viirustõrjeprogrammi regulaarne kasutamine
- (L) M 4.152 Internet-PC turvaline käitus
- (L) M 5.59 DNS võltsimise tõrje
- (L) M 5.93 Veebibrauseri turve Internet-PC kasutamisel
- (L) M 5.94 Meilikliendi turve Internet-PC kasutamisel
- (M) M 5.95 E-kaubanduse turve Internet-PC kasutamisel
- (L) M 5.96 Veebmeili turvaline kasutamine

Valmisolek hädaolukorraks

- (L) M 6.79 Andmete varundamine Internet-PCde kasutamisel

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.6 Arvuti paroolkaitse rangemad reeglid

Teabe käideldavus (K)
-
Teabe terviklus (T)
-
Teabe konfidentsiaalsus (S)
-

B 3.209 Klient Windows XP all

Käsitlusele tulevad töökoha personaalarvutid, mille operatsioonisüsteemiks on Windows XP Professional. Windows XP on operatsioonisüsteemile Windows 2000 järgnenud toode. Operatsioonisüsteemi turvalisus mängib ühes IT-süsteemis vägagi tähtsat rolli, kuna operatsioonisüsteemi enda kitsaskohad võivad mõjutada kõikide rakenduste turvalisust terves võrgus. Käesolev moodul kirjeldab turvameetmeid, mida tuleks rakendada Windows XP ga töötava töökohaarvuti puhul. Meetmed keskenduvad esmajoones Windows XP all töötav kliendi planeerimisele ja käitamisele domeeni keskkonnas, Windows XP installeerimist üksikusse töökohaarvutisse käsitletakse vaid väga lühidalt. Serverit puudutavad turvameetmed, mis on klientide käitamisel domeeni keskkonnas olulised, leiate servereid kajastavate moodulite paketist nr 3.

Ohud

Nagu kõikidel IT-süsteemidel, esineb ka Microsoft Windows XP all töötavatel klientidel mitmesuguseid ohtusid. Toimunud rünnete puhul on tihti olnud tegu kas ühe või mitme süsteemikomponendi väärkonfiguratsiooni oskusliku ärakasutamisega. Seetõttu on väga oluline, et süsteemi ja selle komponentide konfigureerimine oleks korrektne. Üldjuhul peab paika tõsiasi, et iga üksiku arvuti turvalisus sõltub suuresti tema kasutusalast ning iga üksik ohuallikas mõjutab omakorda ka kogu süsteemi turvalisust. Tuleb silmas pidada, et arvutite puhul, mis ei ole võrku ühendatud, läheb rünnete teostamiseks (vt loetelu „Ründed“) tarvis otsest juurdepääsu seadmele (konsoolile).

Üksikute Windows XP operatsioonisüsteemi all töötavate arvutite puhul loetakse infosüsteemide etalonturbe seisukohalt tüüpilisteks järgmisi ohuallikaid.

Vääramatu jõud:

- G 1.2 IT-süsteemi avarii
- G 1.4 Kahjutuli
- G 1.5 Vesi
- G 1.8 Tolm, saastumine

Organisatsioonilised puudused:

- G 2.7 Õiguste volitamata kasutamine
- G 2.9 Halb kohanemine IT muutustega

Inimvead:

- G 3.2 Seadme või andmete hävitamine hooletuse tõttu
- G 3.3 Hooletus turvameetmete suhtes
- G 3.6 Koristajad jm väljastpoolt tellitud töötajad
- G 3.8 IT-süsteemi väär kasutamine
- G 3.9 IT-süsteemi väär haldus
- G 3.22 Registri väär modifitseerimine
- G 3.48 Windowsiga töötavate IT-süsteemide väär konfiguratsioon

Tehnilised rikked:

- G 4.1 Toitevõrgu katkestus
- G 4.7 Defektsed andmekandjad
- G 4.23 Vahetatavate andmekandjate automaattuvastus

Ründed:

- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.4 Vargus
- G 5.7 Liinide pealtkuulamine
- G 5.9 IT-süsteemide volitamata kasutamine
- G 5.18 Süstemaatiline paroolide mõistatamine
- G 5.21 Trooja hobused
- G 5.23 Viirused
- G 5.43 Makroviirused
- G 5.52 Windows NT administraatoriõiguste väärkasutus
- G 5.71 Tundliku informatsiooni konfidentsiaalsuse kadu
- G 5.79 Windowsi süsteemide administraatoriõiguste volitamatu omandamine
- G 5.83 Krüptograafiliste võtmete paljastamine
- G 5.85 Tundliku informatsiooni tervikluse kadu

Soovitatavad meetmed

Selleks, et tagada kogu loetletud IT-süsteemi turvalisus, tuleb lisaks käesolevale moodulile rakendada veel ka teisi, IT-etalonturbe modelleerimise käigus selguvaid mooduleid.

Nagu eelpool mainitud, esineb võrguühendustega arvutitel spetsiifilisi ohtusid, mistõttu on osa meetmeid kajastatud üksikasjalikumalt kui teisi. Eelkõige kuuluvad kohustuslike meetmete hulka võrgust tulenevate rünnete vastu kaitsmine ning vastavate meetmete rakendamisel tuleb olla eriti hoolas. Kõrge turvastandardi hoidmisel on oluliseks abiks klientide efektiivne tsentraalne haldamine. Ühesed konfigureerimisnõuded lihtsustavad oluliselt tööd konfiguratsiooni soovimatute muudatuste jälgimisel, turvanõuete muudatusi on võimalik palju kiiremini kõikide klientide juures rakendada, samuti jõuavad tarkvarauuendused soovitud sihtkohta palju kiiremini. Suuremat osa riistvara/tarkvara puudutavatest meetmetest on võimalik ellu rakendada tsentraalse halduse jaoks välja töötatud grupipoliitika kaudu. Juhul kui organisatsioonis planeeritakse kasutada Microsoft Active Directory, tuleb selle kasutust hoolikalt ette planeerida.

Erijuhtumit kujutab endast Windows XP all töötavate klientide haldamine Windows NT domeenikeskkonnas. Sellisel juhul on tsentraalseks halduseks võimalik kasutada ainult Windows NT süsteemisuuniseid. Kuna vastava lahenduse tehnilised võimalused on väga piiratud, ei soovitata Windows XP puhul süsteemisuuniseid kasutada. Windows XP all töötavate klientide haldamiseks tuleks kaaluda Active Directory grupipoliitika kasutamist.

Windows XP all olevaid kliente saab lisaks domeenidele ka töögruppidena kasutada. Vastaval juhul toimub kogu turbe haldamine lokaalselt, st iga kliendi juures eraldi. Erinevatel arvutitel vabakasutusse antud ressursse on tsentraalse haldusega väga raske kontrollida ja jälgida. Problemaatiliseks osutub ka andmevarundus.

Võrguühenduse kaudu on siiski võimalik ka teatud võrgupõhiseid funktsioone rakendada, nt turvamallide kasutamine konfigureerimiseks ja operatsioonisüsteemi automaatne täiendite laadimine Software Update Service funktsiooni abil.

Windows XP all oleva klientide edukaks ja turvaliseks konfigureerimiseks tuleb läbida mitmeid etappe, tegeldes kontseptsiooni ja installeerimisega kuni igapäevase töötamiseni välja. Järgnevalt anname ülevaate erinevatest kohustuslikest etappidest ja meetmetest, mida iga etapi puhul tuleks rakendada.

Planeerimine ja kontseptsioon

Pärast otsuse langetamist hakata klientides kasutama operatsioonisüsteemi Windows XP-d, tuleb esmalt planeerida, milline saab olema selle kasutusala (vt M 2.324 Windows XP, Vista ja Windows 7 kasutuselevõtu planeerimine). Sellega paralleelselt tuleb välja töötada uus turvapoliitika (vt M 2.325 Windows XP, Vista ja Windows 7 turvapoliitika kavandamine), mis peab võimalikud olemasolevad turvasuunised Windows XP konteksti ümber tõstma ning defineerima Windows XP spetsiifilised täiendused.

Võrguühendusega kasutajakeskkonna puhul on soovitatav kasutada tsentraalset haldussüsteemi. Selleks võib näiteks kasutada Microsoft Active Directory funktsioone. Turvasuuniste suhteliselt lihtsat tsentraalset rakendamist võimaldab eelkõige grupipoliitikate kasutamine. Windows XP kasutamisel võrguühenduseta üksiksüsteemis on soovitatav kasutada lokaalseid grupipoliitikaid. Vastavad soovitused grupipoliitika, konfiguratsiooni ning Windows XP süsteemi halduse kohta leiate meetmest M 2.326 Windows XP, Vista ja Windows 7 grupeerimissuuniste planeerimine .

Planeerimisetapis on tarvis tähelepanu pöörata ka veel teistele aspektidele. Eelkõige puudutavad need Windows XP süsteemi turvalist konfigureerimist. Olulised on siinkohal järgmised meetmed:

- M 4.244 Windowsi klientoperatsioonisüsteemide turvaline süsteemikonfiguratsioon
- M 4.245 Windowsi Group Policy Objects alusseadistused
- M 4.246 Süsteemiteenuste konfigureerimine Windows XP, Windows Vista ja Windows 7 keskkondades
- M 4.247 Windowsi klientoperatsioonisüsteemide piiratud kasutajaõigused
- M 5.123 Võrgusuhtluse kaitse Windowsis

Juhul kui ettevõte või ametiasutus plaanib kasutada Windows XP poolt võimaldatavat kaugpöördumist, tuleb planeerimisetapis teha sobivate tehnoloogiate hulgast valik ja kaaluda nendega seotud erinevaid turvaaspekte (vt M 2.327 Kaugpääsu turve Windows XP-s, Vistas ja Windows 7-s).

Windows XP kasutamisel sülearvutites tuleb juba planeerimisetapis arvestada vastavate turvakaalutlustega. Antud valdkonna spetsiifilisemad tahud võtab kokku meede M 2.328 Windows XP kasutuselevõtt mobiilsel arvutil .

Konfigureerimisvigade vältimiseks pakub Windows XP mõningaid haldustööriistu, mida on võimalik kasutada juba planeerimis- ja testimisfaasis, ning pole vähimatki kahtlust, et vastavad funktsioonid saavad turvalisusele ainult kasuks tulla.

Tähtsamate tööriistade ülevaate leiate moodulist M 4.243 Windowsi klientoperatsioonisüsteemide haldustööriistad .

Rakendamine

Rakendamisfaasis tuleb võtta tarvitusele kõik meetmed, mis aitavad ette valmistada ja tagada turvalist käitamist. Siia alla kuuluvad ennekõike süsteemi turvaline installeerimine ja turvaline aluskonfiguratsioon.

Pärast organisatoorsete ja planeerimist puudutavate eeltööde tegemist saab edasi liikuda Windows XP süsteemide installeerimise juurde. Hooletus on installeerimise käigus täiesti lubamatu. Asjakohased soovitused on kokku võetud meetmes M 4.248 Windowsi klientoperatsioonisüsteemide turvaline installimine . Erinevad asjaolud, mida on Windows XP installeerimise käigus vaja jälgida, peavad olema välja töötatud juba eelnevalt planeerimisfaasis.

Kasutamine

Pärast esmast installeerimist ja testimisfaasi läbimist minnakse üle tavakasutusele. Turbe seisukohalt tuleb siinkohal arvestada järgmiste asjaoludega:

- Windows XP all töötav süsteem muudab ennast reeglina iga päev. Iga muutuse korral peab olema tagatud, et muudatuse rakendamine ei osuta turvalisusele negatiivset mõju. Juhised, millest tuleb kinni pidada, on kokku võetud meetmes M 4.146 Windows'i klient-operatsioonisüsteemide turvaline käitus .
- Windows XP võrgu järjekindla turbe tagamise raames on üheks vahendiks süsteemi, st selle üksikkomponentide jälgimine. Siinkohal mängib tähtsat rolli ka andmekaitse tagamine.
- Windows XP all töötavaid süsteeme ohustavad, nagu ka kõiki teisi IT-süsteeme, üldlevinud turvariskid. Võimalike rünnete tõenäosuse vähendamiseks on oluline, et Windows XP all töötavate süsteemide tarkvarauuenduste laadimine toimuks pidevalt. Vastavad soovitused leiate meetmest M 4.249 Windowsi klientsüsteemide ajakohastamine .
- Juba kasutuses olevate Windows XP süsteemide puhul tuleb arvestada Service Pack 2 lisamisel tekkivate mõjudega (vt M 2.329 Windows XP SP2 kasutuselevõtt).
- Oluline faktor Windows XP süsteemide turvalisuse tagamisel jooksva töö käigus on reeglipärane kehtivate turvasätete ja üldkehtivate turvapoliitikate kontrollimine. Juhised, millest siinkohal tuleb kinni pidada, on kokku võetud meetmes M 2.330 Windows XP, Windows Vista ja Windows 7 turvapoliitika ja selle elluviimise regulaarne kontroll .
- Mõningad Windows XP poolt pakutavad haldustööriistad on turvalisusest lähtudes vägagi soovitatavad, kuna muuhulgas on nende abil võimalik ka konfigureerimisvigu vältida. Lisaks sellele saab neid tööriistu kasutada ka vigade analüüsimiseks ja revisjoni läbiviimiseks (vt M 4.243 Windowsi klientoperatsioonisüsteemide haldustööriistad).

Väljavahetamine/seismapanek

Windows XP all töötava töökohaarvuti seismapanemisel tuleb hoolt kanda selle eest, et salvestatud andmed ei satuks valedesse kätesse ning et andmete väärkasutus oleks välistatud. Salvestatud andmete alla kuuluvad muuhulgas ka paroolid, Cookies , ajutised internetifailid jne. Samal ajal tuleb jälgida, et salvestatud andmete arhiveerimisel säiliks ka võimalus andmetele ligipääsuks, näiteks juhul, kui töökohaarvuti senine kasutaja on organisatsioonist lahkunud. Samad nõudmised kehtivad ka juhul, kui töökohaarvuti kasutaja vahetub.

Valmisolek hädaolukorraks

Lisaks jooksva töö salvestamisele on tähtis ka hädaolukordade ennetamine, sest ainult niimoodi on võimalik häda korral kahjusid vähendada. Hädaolukordade kohta käivad juhised leiate M 6.76 Avariiplaani koostamine Windowsi süsteemi tõrke puhuks . Juhised andmevarunduse kohta leiate M 6.78 Andmete varundamine Windowsi klientsüsteemides .

Alljärgnevalt tutvustatakse meetmete kogumit, mida tuleb rakendada valdkonnas „Klient Windows XP all“.

Planeerimine ja kontseptsioon

- (L) M 2.324 Windows XP, Vista ja Windows 7 kasutuselevõtu planeerimine
- (L) M 2.325 Windows XP, Vista ja Windows 7 turvapoliitika kavandamine
- (L) M 2.326 Windows XP, Vista ja Windows 7 grupeerimissuuniste planeerimine
- (L) M 2.327 Kaugpääsu turve Windows XP-s, Vistas ja Windows 7-s
- (L) M 2.328 Windows XP kasutuselevõtt mobiilsel arvutil
- (L) M 4.147z EFS-i turvaline kasutamine Windows 'i keskkonnas
- (M) M 4.243z Windowsi klientoperatsioonisüsteemide haldustööriistad
- (L) M 4.244 Windowsi klientoperatsioonisüsteemide turvaline süsteemikonfiguratsioon
- (L) M 4.245 Windowsi Group Policy Objects alusseadistused
- (L) M 4.246 Süsteemiteenuste konfigureerimine Windows XP, Windows Vista ja Windows 7 keskkondades
- (L) M 4.247 Windowsi klientoperatsioonisüsteemide piiratud kasutajaõigused
- (L) M 5.123 Võrgusuhtluse kaitse Windowsis

Rakendamine

- (L) M 2.32z Piiratud kasutajakeskkonna loomine
- (L) M 3.28 Windowsi klientoperatsioonisüsteemide turvamehhanismide koolitus kasutajatele
- (L) M 4.57 CD-ROMi automaattuvastuse blokeerimine
- (L) M 4.149 Windows'i faili- ja ühiskasutusõigused
- (L) M 4.248 Windowsi klientoperatsioonisüsteemide turvaline installimine
- (M) M 5.89 Turvalise kanali konfigureerimine Windowsis
- (M) M 5.90z Protokolli IPSec kasutamine Windowsi keskkonnas

Kasutamine

- (L) M 2.329 Windows XP SP2 kasutuselevõtt
- (L) M 2.330 Windows XP, Windows Vista ja Windows 7 turvapoliitika ja selle elluviimise regulaarne kontroll
- (M) M 4.56 Turvaline kustutus Windows operatsioonisüteemides
- (L) M 4.146 Windows'i klient-operatsioonisüsteemide turvaline käitus
- (L) M 4.148 Windows 2000/XP süsteemi seire
- (L) M 4.249 Windowsi klientsüsteemide ajakohastamine

Valmisolek hädaolukorraks

- (L) M 6.76 Avariiplaani koostamine Windowsi süsteemi tõrke puhuks

- (L) M 6.78 Andmete varundamine Windowsi klientsüsteemides

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.6 Arvuti paroolkaitse rangemad reeglid
- HG.7 Ekraaniluku lühem ooteaeg
- HG.38 Turvapaikade paigaldatuse regulaarseire
- HG.70 Piiratud õigustega personaalne kasutajakonto

Teabe käideldavus (K)
-
Teabe terviklus (T)

- HT.7 Kasutajate ja nende profiilide perioodiline seire

Teabe konfidentsiaalsus (S)
-

B 3.210 Klient Windows all

Käesolev moodul käsitleb Windows Vista versiooni Enterprise, lühidalt Windows Vista Enterprise. Vajadusel näidatakse selle erinevusi versioonidest Windows Vista Business ja Windows Vista Ultimate.

Windows Vista on Microsofti operatsioonisüsteemi Windows XP Professional/Home Edition järeltulija. Windows Vista klientoperatsioonisüsteemi turvalisus on oluline kogu infosüsteemi turvalisuse jaoks. Klientoperatsioonisüsteemi nõrgad kohad ohustavad kõiki IT-süsteeme ja lõpuks kogu infosüsteemi.

Käesoleva mooduli põhirõhk on klientide kasutamisel domeeniümbruses. Eraldi tuuakse välja erandjuhud, mis kehtivad Windows Vista kasutamisel eraldiseisvatele või töögrupis olevatele arvutitele.

Serveri spetsiifilisi turbemeetmed klientsüsteemi domeenis kasutamise korral on kirjeldatud moodulites nagu B 3.108 Windows Server 2003 .

Microsofti operatsioonisüsteemiga kliendid on oma laialdase leviku tõttu ründajatele atraktiivne märklaud. Seda näitavad arvukalt avaldatud artiklid turvaaukudest ja rünnakutest. Võrreldes eelnevate versioonidega on Microsoft Windows Vistasse sisestatud mõningad muudatused, mis peaksid parandama kliendi turbeastet. Lisaks on Microsoft varasemate Windowsi versioonide turbeelemente edasi arendanud ja need seejärel Windows Vistas kasutusele võtnud. Näiteks Windows XP SP2 turbekeskus. Mõned Windows Vistale omased turbeelemendid:

- BitLocker Drive Encryption kõvaketta krüpteerimiseks, et kaitsta konfidentsiaalseid faile (ainult Windows Vista Enterprise ja Ultimate);
- kasutajakontode kontroll (User Account Control, UAC) süsteemiterviklikkuse turbeks halduskontodega töötamisel;
- Internet Explorer 7 (IE7) kaitserežiim kaitseks pahavara allalaadimise ja installeerimise eest internetis surfates (eeldab UAC olemasolu). Kaitserežiim sisaldab veel teisigi turbetunnuseid kasutaja- ja süsteemiandmete kaitseks ja terviklikkuse säilitamiseks;
- File and Registry Virtualization vanemate rakenduste, mida enne Windows Vistat sai kasutada ainult halduskonto all, turvaliseks käituseks tavakasutaja poolt (eeldab UAC olemasolu).

Uute ja muudetud turbeelementide kõrval iseloomustavad Windows Vistat muutunud toimimisviisid ja nõuded aktiveerimisel.

Ohud

Moodsaid IT-süsteeme ohustavad igapäevases kasutuses mitmed tegurid. Tihti tulenevad edukad rünnakud sellest, et kasutatakse ära ühe või mitme süsteemiosa väärkonfiguratsiooni või süsteemiarhitektuuri kontseptsioonilisi nõrkusi.

Üldiselt sõltub üksikute IT-süsteemide ohustatus nende kasutuskohast, ja selle ohuga tuleb arvestada kogu süsteemi puhul. Tuleb arvesse võtta, et võrguta IT-süsteemide korral on kõikideks rünnakuteks vaja lokaalset ligipääsu IT-süsteemile (vt „Ründed").

Operatsioonisüsteemi Windows Vista all paiknevate IT-süsteemide etalonturbe tagamisel arvestatakse järgnevate ohtudega.

Vääramatud jõud

- G 1.2 IT-süsteemi avarii

- G 1.4 Kahjutuli
- G 1.5 Vesi
- G 1.8 Tolm, saastumine

Organisatsioonilised puudused

- G 2.7 Õiguste volitamata kasutamine
- G 2.9 Halb kohanemine IT muutustega
- G 2.19 Krüpteerimise halb korraldus
- G 2.62 Turvaintsidentide puudulik käsitlus
- G 2.146 Vista klientsüsteemide kasutuskõlblikkuse kaotus tingituna reaktiveerimise tegemata jätmisest enne SP1

Inimvead

- G 3.2 Seadme või andmete hävitamine hooletuse tõttu
- G 3.3 Hooletus turvameetmete suhtes
- G 3.6 Koristajad jm väljastpoolt tellitud töötajad
- G 3.8 IT-süsteemi väär kasutamine
- G 3.9 IT-süsteemi väär haldus
- G 3.22 Registri väär modifitseerimine
- G 3.48 Windowsiga töötavate IT-süsteemide väär konfiguratsioon
- G 3.97 Konfidentsiaalsuse kadu vaatamata draivide krüpteerimisele BitLockeriga alates Windows Vista-st
- G 3.98 BitLockeriga krüpteeritud andmete kadu

Tehnilised vead

- G 4.1 Toitevõrgu katkestus
- G 4.7 Defektsed andmekandjad
- G 4.23 Vahetatavate andmekandjate automaattuvastus
- G 4.73 Windows Vista ja Windows 7 ühilduvusprobleemidest tingitud tarkvarafunktsioonide pärssimine

Ründed

- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.4 Vargus
- G 5.7 Liinide pealtkuulamine
- G 5.9 IT-süsteemide volitamata kasutamine
- G 5.18 Süstemaatiline paroolide mõistatamine
- G 5.23 Viirused
- G 5.52 Windows NT administraatoriõiguste väärkasutus
- G 5.71 Tundliku informatsiooni konfidentsiaalsuse kadu
- G 5.79 Windowsi süsteemide administraatoriõiguste volitamatu omandamine
- G 5.83 Krüptograafiliste võtmete paljastamine
- G 5.85 Tundliku informatsiooni tervikluse kadu

Soovitatavad meetmed

Vaadeldava IT-koosluse turvalisuse tagamiseks tuleb vastavalt infosüsteemide etalonturbe rakendusjuhendi modelleerimise tulemusele lisaks käesolevale moodulile rakendada veel teisigi mooduleid.

Windows Vista süsteemid on üldjuhul kindla IT-koosluse osa. Sellest tulenevad erilised ründevõimalused. Juba aluskonfiguratsioonis võimaldab Windows Vista kasutada mõningaid turbemeetmeid. Teised turbemeetmed tuleb vastutavatel isikutel eraldi rakendada. Active Directory (AD) toetab keskset konfiguratsiooni ja tehniliste turbemeetmete läbiviimist.

Kohtades, kus keskne konfiguratsioon Active Directory' ga ei ole võimalik, tuleb tehnilised meetmed igal kliendil seadistada lokaalse infoturbe kaudu. Selleks võib luua konfiguratsioonifailid, mis kantakse sobivate vahenditega kliendile ja installeeritakse seal.

Konfiguratsiooni kirjeldamisel lähtutakse AD-funktsioonitasandil „Windows Server 2003 " olevast Windows Server 2003 domeenistruktuurist.

Windows Vista turvaliseks konfigureerimiseks tuleb tarvitusele võtta hulk meetmeid, alustades kontseptsioonist ja installeerimisest ning lõpetades käitusega. Järgnevalt on välja toodud sammud ja meetmed, mida tuleb iga vastava sammu juures järgida.

Planeerimine ja kontseptsioon

Windows Vista kasutamisel tuleb valida sobiv versioon ja selle kasutuselevõttu tuleb planeerida (vt M 2.324 Windows Vista ja Windows 7 kasutuselevõtu planeerimine ja M 2.440 Windows Vista ja Windows 7 sobiva versiooni valimine). Siinkohal tuleb eristada, kas kasutajakeskkond on täiesti uuena loodud või uuendatakse juba olemasolevat keskkonda Windows Vistale. Windows Vista kasutamiseks tuleb välja töötada vastav infoturbe poliitika. Võimalik on juba olemasolev infoturbe poliitika Windows Vistaga kohandada või töötada välja täiesti uus, Windows Vista omadustele vastav turbepoliitika (vt M 2.325 Windows Vista ja Windows 7 turvapoliitika kavandamine).

Domeenikeskkonnas on keskse haldustööriistaga, nagu seda on Active Directory , võimalik luua ja hallata erinevaid turbeseadeid. Võimalik on teiste turbeseadete keskne loomine ja sobivate vahenditega klientidele edastamine. Meetmes M 2.326 Windows Vista ja Windows 7 grupeerimissuuniste planeerimine antakse juhiseid ja soovitusi klientide konfigureerimiseks Windows Vista all.

Windows Vista toetab kliendi kaugadministreerimist ja võimaldab kaugadministreerimisega ligipääsu teistele süsteemidele. Kui soovitakse seda võimalust kasutada, tuleb sellele mõelda juba plaanimisfaasis, et volitamata isikutel ei oleks võimalik kliendil registreeruda. Olulisi aspekte on kirjeldatud meetmes M 2.327 Kaugpääsu turve Windows Vistas ja Windows 7-s .

Kui Windows Vistat soovitakse kasutada mobiilarvutil, tuleb juba plaanimisel arvestada erinevate turvaaspektidega. Windows Vista spetsiifilisi aspekte kirjeldatakse meetmes M 2.442 Windows Vista ja Windows 7 kasutamine kaasaskantavates arvutites .

Windows Vista kasutamisel on väga oluline süsteemi aktiveerimine. Taustainformatsiooni saab meetmest M 4.336 Hulgilitsentslepinguga Windows süsteemide aktiveerimine alates Windows Vistast või Windows Server 2008-st .

Rakendamine

Rakendamisel võetakse kõik meetmed, mis valmistavad ette turvalise kasutamise. Siia hulka kuuluvad meetmed süsteemi installeerimiseks ja aluskonfiguree-

rimiseks.

Pärast organisatoorsete ja plaaniliste eeltööde teostamist võib alustada Windows Vista süsteemide installeerimisega. Installatsioon tuleb teostada hoolikalt. Kõik olulised soovitused on kokku võetud meetmes M 4.248 Windowsi klientoperatsioonisüsteemide turvaline installimine . Windows Vista konfiguratsiooniks vajalikud aspektid tuleb välja selgitada juba kasutuse plaanimise juures.

Kasutamine

Rakendamist testitakse ideaaljuhul testinstallatsiooni abil. Pärast edukat testfaasi installitakse Windows Vista klientidele ja minnakse üle tavakasutusele. Infosüsteemide turbest lähtuvalt tuleb arvestada järgmiste aspektidega.

- Windows Vista süsteemi kasutab suur hulk kasutajaid, kellel on erinevad nõudmised ja vajadused. See tähendab, et luua ja hallata tuleb vastav hulk kasutajaprofiile.
- Tavakasutuse olulised aspektid on kokku võetud meetmes M 4.146 Windows'i klient-operatsioonisüsteemide turvaline käitus .
- Windows Vista turbe säilitamise üks võimalusi on süsteemi või süsteemi üksikute osade monitooring. Olulised soovitused selleks leiate meetmest M 4.344 Windows Vista, Windows 7 ja Windows Server 2008 süsteemi seire .
- Nagu teisigi IT-süsteeme, ohustavad ka Windows Vistat üldised turvariskid. Selleks, et vähendada eduka rünnaku võimalusi arvestatavale tasemele, tuleb Windows Vista süsteemi hoida alati ajakohasel tasemel. Vastavad soovitused leiate meetmest M 4.249 Windowsi klientsüsteemide ajakohastamine .
- Kasutuses olevate Windows Vista süsteemide korral tuleb arvestada mõjudega, mis võivad tuleneda remondipakkide (Service Pack) ja kuumlappide (Hotfixes) installeerimisest.
- Kehtivate turbeseadistuste ja üldise infoturbe kontroll on oluline panus Windows Vista turvalisuseks jooksvas käituses. Sellekohased olulised aspektid on kokku võetud meetmes M 2.330 Windows Windows Vista ja Windows 7 turvapoliitika ja selle elluviimise regulaarne kontroll .
- Windows Vista pakub mõningaid haldustööriistu, mille kasutamine on soovitatav ka infoturbe seisukohast, kuna nende abiga on võimalik vältida turvalisust mõjutavaid konfiguratsioonivigu. Need tööriistad on kasulikud veaanalüüsi, näiteks auditi korral (vt M 4.243 Windowsi klientoperatsioonisüsteemide haldustööriistad).
- Käituses olev Windows Vista süsteem tuleb teatud juhtudel reaktiveerida. Vihjeid ja soovitusi reaktiveerimiseks leiab meetmest M 4.343 Hulgilitsentsilepinguga Windowsi süsteemide reaktiveerimine alates Windows Vistast või Windows Server 2008-st .

Väljavahetamine/kõrvaldamine

Lauaarvutitelt, mis osakonnast välja viiakse või mis sealt kõrvaldatakse, tuleb kustutada kõik lokaalselt salvestatud kasutajaandmed. See kehtib ka vigaste ja seetõttu väljavahetatud andmekandjate kohta. Kui andmekandjalt ei ole enam võimalik andmeid usaldusväärselt kustutada, tuleb see hävitada. Soovitusi selle kohta leiab meetmest B 1.15 Andmete kustutamine ja hävitamine .

Tuleb jälgida, et kinni peetaks arhiveerimisaegadest. Sellega kindlustatakse ligipääs andmetele ka siis, kui algselt salvestav IT-süsteem välja vahetatakse.

Valmisolek hädaolukorraks

Jooksvas töös on turvalisuse tagamise kõrval tähtis osa ka hädaolukordadeks valmistumisel. Juhised hädaolukorra valmisolekuks leiate meetmest M 6.76 Avariiplaani koostamine Windowsi süsteemi tõrke puhuks . Soovitusi varukoopiate tegemiseks leiate meetmest M 6.78 Andmete varundamine Windowsi klientsüsteemides .

Alljärgnevalt tutvustatakse meetmete kogumit, mida tuleb rakendada valdkonnas „Klient Windows Vista all".

Planeerimine ja kontseptsioon

- (L) M 2.324 Windows Vista ja Windows 7 kasutuselevõtu planeerimine
- (L) M 2.325 Windows Vista ja Windows 7 turvapoliitika kavandamine
- (L) M 2.326 Windows Vista ja Windows 7 grupeerimissuuniste planeerimine
- (L) M 2.327 Kaugpääsu turve Windows XP-s, Vistas ja Windows 7-s
- (L) M 2.440 Windows Vista ja Windows 7 sobiva versiooni valimine
- (L) M 2.441 Uue tarkvara ühilduvuse kontroll koostööks Windows Vista ja Windows 7-ga
- (M) M 2.442 Windows Vista ja Windows 7 kasutamine kaasaskantavates arvutites
- (L) M 4.147z EFS-i turvaline kasutamine Windows 'i keskkonnas
- (M) M 4.243z Windowsi klientoperatsioonisüsteemide haldustööriistad
- (L) M 4.244 Windowsi klientoperatsioonisüsteemide turvaline süsteemikonfiguratsioon
- (L) M 4.245 Windowsi Group Policy Objects alusseadistused
- (L) M 4.246 Süsteemiteenuste konfigureerimine Windows Vista ja Windows 7 keskkondades
- (L) M 4.247 Windowsi klientoperatsioonisüsteemide piiratud kasutajaõigused
- (M) M 4.336 Hulgilitsentslepinguga Windows süsteemide aktiveerimine alates Windows Vistast või Windows Server 2008-st
- (M) M 4.337z BitLockeri Drive Encryption kasutamine
- (M) M 4.338 Windows Vista ja Windows 7 failide ja registri virtualiseerimise kasutamine
- (L) M 4.339 Vahetavate andmekandjate volitamata kasutamise tõkestamine Windows Vistas ja Windows 7-s
- (L) M 4.340 Windows kasutajakonto haldamise (UAC) kasutamine alates Windows Vistast
- (L) M 4.341 Tervikluse kaitse alates Windows Vista
- (M) M 4.342z Last Access ajatempli aktiveerimine alates Windows Vistast
- (M) M 5.123 Võrgusuhtluse kaitse Windowsis

Rakendamine

- (L) M 2.32z Piiratud kasutajakeskkonna loomine
- (L) M 3.28 Windowsi klientoperatsioonisüsteemide turvamehhanismide koolitus kasutajatele
- (L) M 4.149 Windows'i faili- ja ühiskasutusõigused
- (L) M 4.248 Windowsi klientoperatsioonisüsteemide turvaline installimine
- (M) M 5.89 Turvalise kanali konfigureerimine Windowsis

- (M) M 5.90z Protokolli IPSec kasutamine Windowsi keskkonnas

Kasutamine

- (L) M 2.330 Windows Windows Vista ja Windows 7 turvapoliitika ja selle elluviimise regulaarne kontroll
- (L) M 2.443 Windows Vista SP1 kasutuselevõtt
- (M) M 4.56 Turvaline kustutus Windows operatsioonisüteemides
- (L) M 4.146 Windows'i klient-operatsioonisüsteemide turvaline käitus
- (L) M 4.249 Windowsi klientsüsteemide ajakohastamine
- (M) M 4.343z Hulgilitsentsilepinguga Windowsi süsteemide reaktiveerimine alates Windows Vistast või Windows Server 2008-st
- (M) M 4.344 Windows Vista, Windows 7 ja Windows Server 2008 süsteemi seire

Valmisolek hädaolukorraks

- (L) M 6.76 Avariiplaani koostamine Windowsi süsteemi tõrke puhuks
- (L) M 6.78 Andmete varundamine Windowsi klientsüsteemides

B 3.211 Mac OS X-ga töötav klientsüsteem

Selles moodulis kirjeldatakse Apple'i klientoperatsioonisüsteemi Mac OS X. X tootenimes Mac OS X märgib Rooma numbrit kümme, kuid seda võib mõista ka kui viidet tähele x, mis sisaldub sellistes nimedes nagu Unix, Linux ja AIX ning teistes Unixi derivaatides.

Mac OS X rajaneb Apple'i vabavaralisel Unixi-põhisel operatsioonisüsteemil nimega Darwin. Darwin on vabavara kernel, mille aluseks on FreeBSD. Suurim erinevus FreeBSD ja Mac OS X vahel seisneb selles, et FreeBSD-s puudub graafiline kasutajaliides Aqua.

Operatsioonisüsteemi Mac OS X saab ja tohib installida ainult Apple'i IT-süsteemidesse. Mac OS-i rakendatakse muudetud kujul ka teistes Apple'i toodetes, nt iPhone'is, iPadis ja iPod touchis. Selles moodulis keskendutakse küll peamiselt klientsüsteemide versioonile Snow Leopard (Mac OS 10.6), kuid seda saab kasutada kõikide Mac OS X versioonide puhul, mis sisaldavad siin kirjeldatud tarkvarakomponente (nt FileVault alates versioonist 10.3, Dashboard alates versioonist 10.4 või Time Machine alates versioonist 10.5).

Infokoosluse turbe tagamiseks on ülioluline, et operatsioonisüsteem oleks piisavalt turvaline. Operatsioonisüsteemi kitsaskohad võivad ohustada kõiki võrgus töötavaid rakendusi. See moodul keskendub peamiselt selliste Mac OS X-ga töötavate IT-süsteemide turbele, mida kasutatakse kas üksikrežiimis (stand alone system) või klientsüsteemina klient-server-võrgus.

Ohud

Operatsioonisüsteemiga Mac OS X töötavate IT-süsteemide puhul loetakse IT-etalonturbe seisukohalt tüüpilisteks järgmisi ohuallikaid.

Vääramatu jõud

- G 1.2 IT-süsteemi avarii
- G 1.4 Kahjutuli
- G 1.5 Vesi
- G 1.8 Tolm, saastumine

Organisatsioonilised puudused

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.9 Halb kohanemine IT muutustega
- G 2.19 Krüpteerimise halb korraldus

Inimvead

- G 3.2 Seadme või andmete hävitamine hooletuse tõttu
- G 3.3 Hooletus turvameetmete suhtes
- G 3.6 Koristajad jm väljastpoolt tellitud töötajad
- G 3.8 IT-süsteemi väär kasutamine
- G 3.9 IT-süsteemi väär haldus
- G 3.108 Mac OS X väär konfiguratsioon
- G 3.109 FileVault-krüpteerimise väär kasutamine

Tehnilised rikked

- G 4.7 Defektsed andmekandjad

Ründed

- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.7 Liinide pealtkuulamine
- G 5.9 IT-süsteemide volitamata kasutamine
- G 5.18 Süstemaatiline paroolide mõistatamine
- G 5.21 Trooja hobused
- G 5.23 Viirused
- G 5.40 Pealtkuulamine ruumis arvuti mikrofoni kaudu
- G 5.71 Tundliku informatsiooni konfidentsiaalsuse kadu
- G 5.83 Krüptograafiliste võtmete paljastamine
- G 5.85 Tundliku informatsiooni tervikluse kadu

Soovitatavad meetmed

Vaadeldava IT-koosluse turvalisuse tagamiseks tuleb peale käesoleva mooduli rakendada veel teisigi mooduleid, mis selguvad IT-etalonturbe rakendusjuhendi põhjal tehtava modelleerimise tulemusel. Selle hulka kuulub moodul B 3.201 Klient . Kui Mac OS X-t kasutatakse sülearvutis, tuleb lisaks arvestada mooduliga B 3.203 Sülearvuti .

Selles moodulis kajastatakse meetmeid, mis aitavad tagada Mac OS X-ga töötava klientsüsteemi turvalisuse tavapärase turbevajaduse korral. Siin käsitletakse ainult selliseid rakendusi, mis on olemas Mac OS X standardkonfiguratsiooni korral.

Mac OS X-ga töötavate klientsüsteemide turvaliseks konfigureerimiseks tuleb võtta mitmeid meetmeid, mis puudutavad planeerimist, kontseptsiooni loomist, installimist ja turvalist käitamist. Järgnevalt on esitatud ülevaade erinevatest kohustuslikest etappidest ja meetmetest, mida iga etapi puhul tuleks võtta.

Planeerimine ja kontseptsioon

Mac OS X-ga töötavate klientsüsteemide kasutuselevõtule mis tahes institutsioonis peavad alati eelnema kasutusvaldkonna planeerimine ja turvaomaduste kohandamine sisenõuetega, nagu on kirjeldatud meetmes M 2.478 Mac OS X turvalise kasutuse planeerimine . Selleks tuleb muu hulgas kindlaks määrata Mac OS X kasutuselevõtu eeldused, koostada nii kasutamise kui ka haldamise kontseptsioon ning välja töötada juhised andmete nõuetekohase varundamise ja krüpteerimise kohta. Meetmes M 4.375 Sandbox 'i funktsioonide kasutamine Mac OS X-s kirjeldatakse meetodit, kuidas piirata rakenduste volitusi. Siinkohal tuleb arvestada, et asjakohaste ettevalmistustööde raames on tarvis langetada otsus, millised funktsioonid pannakse tööle liivakastis (sandbox) ja millised pääsuõigused nendele rakendustele antakse. Lisaks on vaja planeerida Mac OS X-s töötavate programmide pääsuõiguste juhtimist, sest olenevalt kasutusvaldkonnast tuleb klientsüsteemile selleks otstarbeks teha tavapärasest rangem konfiguratsioon. Teemakohased juhised leiate meetmest M 4.378 Programmide pääsuõiguste piiramine MAC OS X-s . Kuna IT-süsteemide turbes on oluline roll paroolide tugevusel, tuleks eeltööde raames kokku leppida paroolidele esitatavad nõuded. Võtma peaks vähemalt meetme M 4.376 Paroolisuuniste kindlaksmääramine Mac OS X-s .

Rakendamine

Mac OS X-ga töötavate klientsüsteemide installimisel tuleb võtta mitmeid meetmeid, mis suurendavad süsteemi turvalisust. Süsteemi turvalisust suurendab nn karastamine, mille eesmärk on sulgeda väga sageli pärast tüüpinstallimist esinevad turvaaugud. Vastavad soovitused leiate meetmest M 4.371 Mac OS X-ga töötavate klientsüsteemide konfigureerimine . Seejärel tuleks iga kasutajakonto puhul võtta meede M 4.374 Kasutajakontode juurdepääsukaitse Mac OS X-s , et suurendada iga konto turbeastet. Mac OS X funktsioon Personal Firewall ei suuda mitte mingil juhul asendada turvalüüsi, kuid sellest hoolimata on soovitatav see siiski aktiveerida ja sobivalt konfigureerida. Sellekohased juhised leiate meetmest M 5.166 Mac OS X isikliku tulemüüri konfiguratsioon . Kasutaja kausta krüpteerimiseks on võimalik kasutada meedet M 4.372 FileVaulti kasutamine Mac OS X-s .

Selleks et Mac OS X-ga töötav klientsüsteem ei lubaks võrgu kaudu liiga palju teenuseid kasutada, s.t ei pakuks liiga palju pidepunkte enda ründamiseks, tuleks võimalikult suur hulk võrguteenuseid välja lülitada (vt M 5.165 Mac OS X mittevajalike võrguteenuste desaktiveerimine). Samuti võib kasuks tulla mittevajaliku riistvara desaktiveerimine, nt selleks, et välistada arvutitesse paigaldatud mikrofonide ja kaamerate väärkasutus (vt M 4.373 Mittevajaliku riistvara desaktiveerimine Mac OS X-s).

Kasutamine

Mac OS X klientsüsteemide tõrgeteta töö tagamiseks tuleb teha regulaarseid kontrolle ja logifailide analüüse. Siinkohal tuleks tähelepanu pöörata eelkõige mis tahes ebareeglipärasustele. Sellekohast teavet leiate meetmetest M 4.25 Logimine Unix-süsteemis ja M 4.26 Regulaarne turvakontroll Unix-süsteemis . Kui konfidentsiaalseid andmeid on tarvis transportida või salvestada väljapoole kasutaja kausta, tuleks töötajaid teavitada meetmest M 4.379 Andmete turvaline talletamine ja transportimine Mac OS X-s ning korraldada asjakohaseid koolitusi. Administraatoreid tuleb teavitada ka meetmest M 4.377 Mac OS X digisignatuuride kontrollimine , et nad oskaksid iga uue rakenduse puhul kontrollida digisignatuuri kehtivust.

Kasutusest kõrvaldamine

Nii väljavahetamise kui ka seismapaneku puhul on oluline tagada, et kolmandatel isikutel puuduks juurdepääs konfidentsiaalsetele andmetele. Kui andmekandja või IT-süsteem kõrvaldatakse kasutusest, ei tule turvaliselt kustutada mitte üksnes kõik vahetatavatel andmekandjatel olevad andmed, vaid ka lokaalselt salvestatud kasutajaandmed. Andmete turvalise kustutamise kohta Mac OS X-s leiate lisateavet meetmest M 6.148 Mac OS X süsteemi kasutusest kõrvaldamine .

Valmisolek hädaolukorraks

Tavapärase töörežiimi võimalikult kiireks taastamiseks riistvara rikke või andmete kaotsimineku korral tuleks võtta meetmeid M 6.146 Andmete varundamine ja taastamine Mac OS X klientsüsteemides ja M 6.147 Süsteemiparameetrite taastamine Mac OS X-s . Meetmest M 4.380 Apple Software Restore'i kasutamine Mac OS X-s leiate lisateavet selle kohta, kuidas luua süsteemist identseid koopiaid. Selliseid süsteemikujutisi saab kasutada näiteks Mac OS X-ga töötava klientsüsteemi taastamiseks või standardse kujutise (image) laadimiseks kõikides-

se Mac OS X klientsüsteemidesse läbi võrgu.

Alljärgnevalt tutvustatakse meetmete kogumit, mida tuleb rakendada valdkonnas „Mac OS X-ga töötav klientsüsteem”.

Planeerimine ja kontseptsioon

- (L) M 2.478 Mac OS X turvalise kasutuse planeerimine
- (L) M 2.479 Mac OS X turvapoliitika planeerimine
- (M) M 4.374 Kasutajakontode juurdepääsukaitse Mac OS X-s
- (M) M 4.375z Sandbox 'i funktsioonide kasutamine Mac OS X-s
- (L) M 4.376 Paroolisuuniste kindlaksmääramine Mac OS X-s
- (M) M 4.378z Programmide pääsuõiguste piiramine MAC OS X-s
- (L) M 5.64z Secure Shell (SSH)

Rakendamine

- (L) M 4.106 Süsteemi logimise aktiveerimine (Unix)
- (M) M 4.371 Mac OS X-ga töötavate klientsüsteemide konfigureerimine
- (M) M 4.372 FileVaulti kasutamine Mac OS X-s
- (M) M 4.373 Mittevajaliku riistvara desaktiveerimine Mac OS X-s
- (M) M 5.165 Mac OS X mittevajalike võrguteenuste desaktiveerimine
- (L) M 5.166z Mac OS X isikliku tulemüüri konfiguratsioon
- (M) M 5.167 Mac OS X kaugpöörduste turvalisus

Kasutamine

- (L) M 4.25 Logimine Unix-süsteemis
- (M) M 4.26 Regulaarne turvakontroll Unix-süsteemis
- (L) M 4.377z Mac OS X digisignatuuride kontrollimine
- (M) M 4.379 Andmete turvaline talletamine ja transportimine Mac OS X-s

Kasutusest kõrvaldamine

- (M) M 6.148 Mac OS X süsteemi kasutusest kõrvaldamine

Valmisolek hädaolukorraks

- (L) M 4.380w Apple Software Restore'i kasutamine Mac OS X-s
- (L) M 6.31 Protseduurid süsteemi tervikluse kao puhuks
- (L) M 6.146 Andmete varundamine ja taastamine Mac OS X klientsüsteemides
- (L) M 6.147 Süsteemiparameetrite taastamine Mac OS X-s

B 3.212 Windows 7-ga töötav klientsüsteem

Käesolevas moodulis käsitletakse klientoperatsioonisüsteemi Microsoft Windows 7 versiooni Enterprise (lühidalt Windows 7 Enterprise). Kui see on vajalik, kirjeldatakse ka erinevusi versioonidest Windows 7 Professional ja Windows 7 Ultimate.

Windows 7 on Microsofti operatsioonisüsteemi Windows Vista järeltulija. IT-koosluse turbe tagamiseks on ülioluline, et klientsüsteemis töötav operatsioonisüsteem, nt Windows 7, oleks piisavalt turvaline. Klientsüsteemi operatsioonisüsteemi võimalikud turvaaugud ohustavad kõikide IT-süsteemide, andmete ja lõppkokkuvõttes ka kogu infokoosluse turvet.

Selles moodulis keskendutakse klientsüsteemide kasutamisele domeenikeskkonnas. Lisaks märgitakse tekstis eraldi ära olulised kõrvalekalded, mis kehtivad Windows 7 kasutamisel kas eraldiseisvates töökohaarvutites või töörühma kuuluvates arvutites.

Microsoft on Windows 7-s selle eelkäijaversioonidega võrreldes teinud mitmeid muudatusi, mille eesmärk on suurendada turbeastet. Lisaks selle on Microsoft edasi arendanud ja Windows 7-sse üle võtnud ka varasemates Windowsi versioonides kasutusel olnud turvafunktsioone. Nende hulka kuuluvad näiteks Windows XP-st koos Service Pack 2-ga ja Windows Vistast tuntud turvakeskus (security center), mis on Windows 7-s edasi arendatud tegevuskeskuseks (action center).

Windows 7 erifunktsioonide hulka kuuluvad muu hulgas järgmised funktsioonid:

- AppLocker: installatsiooni kaitse ja kinnitamata tarkvara käivitamise kaitse (ainult versioonides Windows 7 Enterprise ja Ultimate);
- BitLocker To Go: vahetatavate andmekandjate krüpteerimine administraatorivolitusteta kasutajate poolt.

Serveritele kehtivaid turbemeetmeid, mida tuleb võtta klientide käitamisel domeenikeskkonnas, kirjeldatakse serverimoodulites B 1.0 Infoturbe haldus , B 3.108 Windows Server 2003 ja B 3.109 Windows Server 2008 .

Ohud

Moodsate IT-süsteemide igapäevatööga on seotud suur hulk ohte. Õnnestunud rünnete puhul on sageli olnud tegu kas ühe või ka mitme süsteemikomponendi väärkonfiguratsiooni või süsteemi arhitektuuri kontseptsiooniliste nõrkuste oskuslikku ärakasutamisega. Microsofti operatsioonisüsteemiga töötavad klientsüsteemid on ründajatele oma suure leviku tõttu atraktiivsed sihtmärgid. Seda tõestavad suur hulk avalikustatud turvaauke ja ründeid.

Alljärgnevalt on nimetatud Windows 7-ga töötavate IT-süsteemide tüüpilised ohud.

Vääramatu jõud

- G 1.2 IT-süsteemi avarii

Organisatsioonilised puudused

- G 2.7 Õiguste volitamata kasutamine
- G 2.9 Halb kohanemine IT muutustega
- G 2.19 Krüpteerimise halb korraldus

- G 2.62 Turvaintsidentide puudulik käsitlus

Inimvead

- G 3.2 Seadme või andmete hävitamine hooletuse tõttu
- G 3.3 Hooletus turvameetmete suhtes
- G 3.8 IT-süsteemi väär kasutamine
- G 3.9 IT-süsteemi väär haldus
- G 3.22 Registri väär modifitseerimine
- G 3.48 Windowsiga töötavate IT-süsteemide väär konfiguratsioon
- G 3.97 Konfidentsiaalsuse kadu vaatamata draivide krüpteerimisele BitLockeriga alates Windows Vista-st
- G 3.98 BitLockeriga krüpteeritud andmete kadu
- G 3.112 Image'ite volitamata või väär rakendamine Windows DISM-i kasutamisel

Tehnilised rikked

- G 4.1 Toitevõrgu katkestus
- G 4.7 Defektsed andmekandjad
- G 4.23 Vahetatavate andmekandjate automaattuvastus
- G 4.54 Turbe kadu krüptofailisüsteemi (EFS) kasutamisel
- G 4.55 Andmekadu alates Windows Server 2003 / XP parooli taastamisel
- G 4.73 Windows Vista ja Windows 7 ühilduvusprobleemidest tingitud tarkvarafunktsioonide pärssimine

Ründed

- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.4 Vargus
- G 5.7 Liinide pealtkuulamine
- G 5.9 IT-süsteemide volitamata kasutamine
- G 5.18 Süstemaatiline paroolide mõistatamine
- G 5.23 Viirused
- G 5.52 Windows NT administraatoriõiguste väärkasutus
- G 5.71 Tundliku informatsiooni konfidentsiaalsuse kadu
- G 5.79 Windowsi süsteemide administraatoriõiguste volitamatu omandamine
- G 5.83 Krüptograafiliste võtmete paljastamine
- G 5.85 Tundliku informatsiooni tervikluse kadu

Soovitatavad meetmed

Vaadeldava IT-koosluse turvalisuse tagamiseks tuleb peale käesoleva mooduli rakendada veel teisigi mooduleid, mis selguvad IT-etalonturbe rakendusjuhendi põhjal tehtava modelleerimise tulemusel.

Windows 7 puhul töötab teatud hulk turvamehhanisme isegi juba aluskonfiguratsioonis. Samas on ka selliseid turvamehhanisme, mille puhul on tarvis, et vastutavad isikud need tööle seadistaks. Tehniliste turvameetmete tsentraalseks konfigureerimiseks ja võtmiseks saab kasutada Active Directoryt (AD).

Olukordades, kus AD-d ei ole tsentraalseks konfigureerimiseks võimalik kasutada, tuleb tehnilisi meetmeid võtta detsentraalselt, s.t kohapeal igas klientsüsteemis eraldi, rakendades lokaalset turvapoliitikat. Selleks saab konfiguratsioonifailid koostada tsentraalselt ning need sobivate mehhanismidega klientsüsteemidesse üle kanda ja seal installida.

Järgnevate konfiguratsioonide kirjeldamisel on aluseks võetud Windows Server 2003/2008 domeenistruktuur selle AD funktsioonitasandil „Windows Server 2003/2008".

Windows 7-ga töötavate klientsüsteemide turvaliseks konfigureerimiseks tuleb võtta mitmeid meetmeid, mis käsitlevad näiteks kontseptsiooni väljatöötamist ja selle rakendamist (installimist/konfigureerimist) ning käitamist. Järgnevalt on esitatud ülevaade erinevatest kohustuslikest etappidest ja meetmetest, mida iga etapi puhul tuleks võtta.

Planeerimine ja kontseptsioon

Windows 7 kasutuselevõtul tuleb esmalt välja valida sobiv tooteversioon (vt M 2.440 Windows Vista ja Windows 7 sobiva versiooni valimine) ja planeerida selle kasutusotstarve (vt M 2.324 Windows Vista ja Windows 7 kasutuselevõtu planeerimine). Siinkohal tuleb eristada, kas Windows 7 jaoks luuakse täiesti uus kasutuskeskkond või hakatakse seda juurutama juba olemasolevas kasutuskeskkonnas (migratsioon). Windows 7 kasutamiseks tuleb välja töötada sobiv turvapoliitika. Selleks võib kasutada kas juba olemasolevat turvapoliitikat ja seda Windows 7 omadustele kohandada või luua täiesti uus, spetsiaalselt Windows 7 omadustest lähtuv turvapoliitika (vt M 2.325 Windows Vista ja Windows 7 turvapoliitika kavandamine).

Domeenikeskkonnas saab erinevaid turvaseadistusi koostada ja hallata mõne tsentraalselt toimiva haldustööriistaga, nt Active Directoryga. Teistel juhtudel saab turvaseadistusi koostada tsentraalselt ning need sobivate mehhanismidega klientsüsteemidesse üle kanda. Juhiseid ja soovitusi Windows 7-ga töötavateklientsüsteemide konfigureerimise kohta leiate meetmest M 2.326 Windows Vista ja Windows 7 grupeerimissuuniste planeerimine .

Windows 7 toetab ka klientsüsteemide kaughaldust ning sisaldab muu hulgas lahendusi, mis võimaldavad Windows 7 kaughalduse funktsioonil teistele süsteemidele ligi pääseda. Seetõttu tuleb juba planeerimisetapis kindlaks määrata, kuidas seda funktsiooni hakatakse kasutama, et volitamata isikud ei saaks end klientsüsteemidesse sisse logida. Sellekohased olulised aspektid leiate meetmest M 2.327 Kaugpääsu turve Windows Vistas ja Windows 7-s .

Windows 7 kasutamisel sülearvutites tuleb juba planeerimisetapis arvestada asjakohaste turvaaspektidega. Windows Vistat ja Windows 7-t puudutavad erinõuded on kirjas meetmes M 2.442 Windows Vista ja Windows 7 kasutamine

kaasaskantavates arvutites .

Rakendamine

Rakendamisel tuleb võtta kõiki meetmeid, mis aitavad turvalist käitamist ette valmistada. Siia alla kuuluvad ennekõike süsteemi turvaline installimine ja turvaline aluskonfiguratsioon.

Pärast organisatsiooniliste ja planeerimist puudutavate eeltööde tegemist saab edasi liikuda Windows 7 süsteemide installimise juurde. Installimisel tuleb olla ülimalt hoolikas, vt M 4.248 Windowsi klientoperatsioonisüsteemide turvaline installimine . Erinevad aspektid, mida Windows 7 installimise käigus tuleb jälgida, peavad olema välja töötatud juba planeerimisfaasis.

Kui Windows 7 keskkonnas soovitakse turvaliselt kasutada Windowsi vanematele versioonidele kirjutatud tarkvara, on tarvis tunda selleks vajaminevat erinevat tehnoloogiat (nt VirtualPC XP-Mode, vt M 4.424z Kodugrupi funktsiooni kasutamine Windows 7-s).

Operatsioonisüsteemis Windows 7 on väga palju standardseid funktsioone, mis on suunatud eeskätt kodukasutajatele. Siia kuuluvad näiteks kodu töögrupp, mis võimaldab lokaalvõrgus teenuseid kasutusse lubada ja neile ligi pääseda. Institutsioonide puhul, kus on oluline, et Windows 7-ga töötavate klientsüsteemide töö oleks võrgu piires turvaline, tuleb selliste funktsioonide kasutust piirata (vt M 4.423 Kodugrupi funktsiooni kasutamine Windows 7-s).

Enne püsivat kasutuselevõttu tuleb Windows 7 aktiveerida. Selgitused leiate meetmest M 4.336 Hulgilitsentslepinguga Windows süsteemide aktiveerimine alates Windows Vistast või Windows Server 2008-st .

Kasutamine

Ideaaljuhul peaks kasutuselevõtt toimuma katsetuskeskkonnas. Windows 7 tuleks installida klientsüsteemidesse ning seda tohib tavakasutusse lubada alles pärast katsete edukat läbimist. Turbe seisukohalt tuleb siinkohal arvestada järgmiste asjaoludega:

- Juhised, millest tuleb tavakasutuse puhul kinni pidada, on kokku võetud meetmesse M 4.146 Windows'i klient-operatsioonisüsteemide turvaline käitus .
- Windows 7-ga töötavate süsteemide turbe tagamises on oluline süsteemi, s.t selle üksikkomponentide seire. Sellekohased soovitused leiate meetmest M 4.344 Windows Vista, Windows 7 ja Windows Server 2008 süsteemi seire .
- Nagu kõiki teisi IT-süsteeme, ohustavad ka Windows 7-ga töötavaid IT-süsteeme mitmed turvariskid. Et vähendada rünnete eduka toimepaneku tõenäosus vastuvõetavale tasemele, tuleb Windows 7-ga töötavatesse süsteemidesse laadida pidevalt tarkvaravärskendusi. Asjakohased soovitused leiate meetmest M 4.249 Windowsi klientsüsteemide ajakohastamine .
- Turvaseadistuste tsentraalseks konfigureerimiseks, jälgimiseks, hooldusseadistuste tegemiseks ja probleemide kõrvaldamiseks on Windows 7-s olemas spetsiaalne tegevuskeskus (action center). Tegevuskeskuse turvalise töö tagamiseks tuleb võtta meedet M 4.420 Windows 7 tegevuskeskuse turvaline kasutamine .
- Windows 7-ga töötavate süsteemide turvalisust tavakasutuse raames aitab tagada kehtivate turvasätete ja üldkehtiva turvapoliitika reeglipärane kontrol-

limine. Juhised, millest siinkohal tuleb kinni pidada, on kogutud meetmesse M 2.330 Windows Windows Vista ja Windows 7 turvapoliitika ja selle elluviimise regulaarne kontroll .

- Windows 7-s on mõned haldustööriistad, mille kasutamist võib turbe seisukohalt julgelt soovitada, sest need aitavad muu hulgas vältida näiteks konfigureerimisel tehtavaid vigu. Samuti võib neid tööriistu kasutada vigade analüüsimiseks ja revisjoni tegemiseks (vt M 4.243 Windowsi klientoperatsioonisüsteemide haldustööriistad).Windows 7-ga töötavat süsteemi on teatud juhtudel tarvis uuesti aktiveerida. Reaktiveerimist käsitlevad juhised ja soovitused leiate meetmest M 4.343 Hulgilitsentsilepinguga Windowsi süsteemide reaktiveerimine alates Windows Vistast või Windows Server 2008-st
- Windows 7 puhul ei saa kasutada mitte üksnes alates Windows Vistast kasutusele võetud kõvaketta krüpteerimise lahendust (vt M 4.337 BitLockeri Drive Encryption kasutamine), vaid ka vahetatavate andmekandjate krüpteerimist BitLocker To Go-ga. Selle rakenduse turvalise kasutuse aspektid on kirjas meetmes M 4.422 BitLocker To Go kasutamine alates Windows 7-st .

Kasutusest kõrvaldamine

Klientsüsteemidest, mis eemaldatakse või kõrvaldatakse kasutusest, tuleb ära kustutada sinna lokaalselt salvestatud kasutajaandmed. Sama kehtib ka defektsete andmekandjate kohta, mis uute vastu välja vahetatakse. Kui aga andmekandjatel olevate andmete turvaline kustutus osutub võimatuks, tuleb andmekandjad sobival viisil hävitada. Asjakohased soovitused leiate moodulist B 1.0 Infoturbe haldus .

Siinkohal tuleb arvestada, et arhiveeritud andmetele peab kogu arhiveerimisaja kestel säilima juurdepääs, seda ka siis, kui salvestav IT-süsteem kõrvaldatakse kasutusest.

Valmisolek hädaolukorraks

Tavakasutuse turbe tagamise kõrval on oluline ka piisav valmisolek hädaolukorraks. Lisateavet leiate meetmest M 6.76 Avariiplaani koostamine Windowsi süsteemi tõrke puhuks . Juhised andmevarunduse kohta leiate meetmest M 6.78 Andmete varundamine Windowsi klientsüsteemides .

Alljärgnevalt tutvustatakse meetmete kogumit, mida tuleb rakendada valdkonnas „Windows 7-ga töötav klientsüsteem".

Planeerimine ja kontseptsioon

- (L) M 2.324 Windows Vista ja Windows 7 kasutuselevõtu planeerimine
- (L) M 2.325 Windows Vista ja Windows 7 turvapoliitika kavandamine
- (L) M 2.326 Windows Vista ja Windows 7 grupeerimissuuniste planeerimine
- (M) M 2.327 Kaugpääsu turve Windows Vistas ja Windows 7-s
- (L) M 2.440 Windows Vista ja Windows 7 sobiva versiooni valimine
- (L) M 2.441 Uue tarkvara ühilduvuse kontroll koostööks Windows Vista ja Windows 7-ga
- (M) M 2.442 Windows Vista ja Windows 7 kasutamine kaasaskantavates arvutites

- (L) M 4.147z EFS-i turvaline kasutamine Windows ’i keskkonnas
- (M) M 4.243z Windowsi klientoperatsioonisüsteemide haldustööriistad
- (L) M 4.244 Windowsi klientoperatsioonisüsteemide turvaline süsteemikonfiguratsioon
- (L) M 4.245 Windowsi Group Policy Objects alusseadistused
- (L) M 4.246 Süsteemiteenuste konfigureerimine Windows Vista ja Windows 7 keskkondades
- (L) M 4.247z Windowsi klientoperatsioonisüsteemide piiratud kasutajaõigused
- (L) M 4.336 Hulgilitsentslepinguga Windows süsteemide aktiveerimine alates Windows Vistast või Windows Server 2008-st
- (M) M 4.337z BitLockeri Drive Encryption kasutamine
- (L) M 4.338 Windows Vista ja Windows 7 failide ja registri virtualiseerimise kasutamine
- (M) M 4.339 Vahetavate andmekandjate volitamata kasutamise tõkestamine Windows Vistas ja Windows 7-s
- (L) M 4.340 Windows kasutajakonto haldamise (UAC) kasutamine alates Windows Vistast
- (L) M 4.341 Tervikluse kaitse alates Windows Vista
- (M) M 4.342z Last Access ajatempli aktiveerimine alates Windows Vistast
- (M) M 4.425 Vaulti ja Cardspace’i funktsiooni kasutamine Windows 7-s
- (M) M 5.123 Võrgusuhtluse kaitse Windowsis

Rakendamine

- (L) M 2.32z Piiratud kasutajakeskkonna loomine
- (L) M 3.28 Windowsi klientoperatsioonisüsteemide turvamehhanismide koolitus kasutajatele
- (L) M 4.149 Windows’i faili- ja ühiskasutusõigused
- (L) M 4.248 Windowsi klientoperatsioonisüsteemide turvaline installimine
- (L) M 4.419z Rakenduste juhtimine AppLockeriga alates Windows 7-st
- (L) M 4.421 Windows PowerShelli turve
- (M) M 4.423 Kodugrupi funktsiooni kasutamine Windows 7-s
- (M) M 4.424z Vanemate tarkvarade turvaline kasutamine alates Windows 7-st
- (L) M 5.89 Turvalise kanali konfigureerimine Windowsis
- (M) M 5.90z Protokolli IPSec kasutamine Windowsi keskkonnas

Kasutamine

- (M) M 2.330 Windows Windows Vista ja Windows 7 turvapoliitika ja selle elluviimise regulaarne kontroll
- (L) M 4.56 Turvaline kustutus Windows operatsioonisüteemides
- (L) M 4.146 Windows’i klient-operatsioonisüsteemide turvaline käitus
- (L) M 4.249 Windowsi klientsüsteemide ajakohastamine
- (M) M 4.343z Hulgilitsentsilepinguga Windowsi süsteemide reaktiveerimine alates Windows Vistast või Windows Server 2008-st
- (M) M 4.344 Windows Vista, Windows 7 ja Windows Server 2008 süsteemi seire

- (L) M 4.420 Windows 7 tegevuskeskuse turvaline kasutamine
- (M) M 4.422z BitLocker To Go kasutamine alates Windows 7-st

Valmisolek hädaolukorraks

- (L) M 6.76 Avariiplaani koostamine Windowsi süsteemi tõrke puhuks
- (L) M 6.78 Andmete varundamine Windowsi klientsüsteemides

B 3.213 Klient Windows 8 keskkonnas

Kirjeldus

Windows 8-ga tõi Microsoft turule klientoperatsioonisüsteemi, milles on ühelt poolt edasi arendatud Windows 7 tehnoloogiaid ja komponente, teiselt poolt on aga võetud siht klaviatuurita kaasaskantavatele seadmetele, mille kasutamine seisneb ekraani puudutamises ning mida saab seega kasutada andmesisestuseks.

See nõuab rakenduste jaoks uut kasutuskontseptsiooni. Peale selle on Microsoft klassikaliste töölaua rakenduste kõrval Windows 8-s kasutamiseks ette näinud ka mobiilsete rakenduste klassi e nn „äpid". Äppe on seega võimalik juhtida puudutamisega. Lisaks kujutavad need ekraanil kuvafunktsioone „plaatidena". Mõnesid rakendusi, eelkõige Windows 8-ga kaasas olevat Internet Explorerit, saab kasutada kahes Windows 8 variandis. Töölaua rakendus ja äpp võivad seejuures olla installeeritud paralleelselt samasse süsteemi ning neid võib kasutada vaheldumisi. Paljud muud rakendused on siiski kasutatavad kas ainult töölaua variandi või äpina.

Pärast Windows 8 turuletoomist on Microsoft operatsioonisüsteemi sisse viinud mõningaid parandusi, millega lisandub versiooni number 8.1. See moodul lähtub eeldusest, et kasutatakse Windows 8.1 versiooni. Kui kirjeldatud turvameetmete puhul on Windows 8 jaoks erinevusi, on need tekstis välja toodud.

Mooduli struktuur lähtub mooduli B 3.212 Windows 7-ga töötav klientsüsteem keskkonnas struktuurist, nii et Windows 7 üleviimise projektis Windows 8-le on võimalik olemasolevate turvasuuniste vähene kohandamine. Erilist tähelepanu tuleb sel juhul pöörata integreeritud Trusted Platform Modules'i (TPM) toetusele ning pilve funktsioonide integreerimisele operatsioonisüsteemi, sest nende valdkondade jaoks tuleb tavaliselt koostada ja dokumenteerida uued turvahinnangud. Sama kehtib ka äppide kasutamise suhtes asutuses ning rakenduste laiendatud kaitsemehhanismide suhtes. Selle kohta leiate suuniseid mooduli abivahendites.

Ohud

Allpool on nimetatud operatsioonisüsteemiga Windows Server 8 töötava klientsüsteemi olulisimad ohud.

Vääramatu jõud

- G 1.2 IT-süsteemi avarii

Töökorralduslikud puudused

- G 2.7 Õiguste volitamata kasutamine
- G 2.9 Halb kohanemine IT muutustega

IT-muudatuste puudulik kohandamine

- G 2.19 Krüpteerimise halb korraldus
- G 2.63 Fakside kontrollimatu kasutamine

Turvaintsidentide puudulik käsitlus

- G 2.202 Lock-in-efek
- G 2.203 Integreeritud pilve-funktsioon
- G 2.204 TPM-i kasutamine

Inimvead

- G 3.2 Seadme või andmete hävitamine hooletuse tõttu
- G 3.3 Hooletus turvameetmete suhtes
- G 3.6 Koristajad jm väljastpoolt tellitud töötajad
- G 3.8 IT-süsteemi väär kasutamine
- G 3.9 IT-süsteemi väär haldus
- G 3.22 Registri väär modifitseerimine
- G 3.48 Windowsiga töötavate IT-süsteemide väär konfiguratsioon
- G 3.97 Konfidentsiaalsuse kadu vaatamata draivide krüpteerimisele BitLockeriga alates Windows Vista-st
- G 3.98 BitLockeriga krüpteeritud andmete kadu
- G 3.112 Image'ite volitamata või väär rakendamine Windows DISM-i kasutamisel

Tehnilised rikked

- G 4.1 Toitevõrgu katkestus
- G 4.7 Defektsed andmekandjad
- G 4.22 Tüüptarkvara turvaaugud või vead
- G 4.23 Vahetatavate andmekandjate automaattuvastus
- G 4.54 Turbe kadu krüptofailisüsteemi (EFS) kasutamisel
- G 4.55 Andmekadu alates Windows Server 2003 / XP parooli taastamisel
- G 4.73 Tarkvara funktsioonide kahjustamine Windowsi versioonide ühilduvusprobleemide tõttu

Ründed

- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.4 Vargus
- G 5.9 IT-süsteemide volitamata kasutamine
- G 5.18 Süstemaatiline paroolide mõistatamine
- G 5.23 Pahavara
- G 5.52 Windows NT administraatoriõiguste väärkasutus
- G 5.71 Tundliku informatsiooni konfidentsiaalsuse kadu
- G 5.79 Windowsi süsteemide administraatoriõiguste volitamatu omandamine
- G 5.83 Krüptograafiliste võtmete paljastamine
- G 5.85 Tundliku informatsiooni tervikluse kadu

Soovitatavad meetmed

Vaadeldava IT-koosluse turvalisuse tagamiseks tuleb peale käesoleva mooduli rakendada veel teisigi mooduleid, mis selguvad IT-etalonturbe rakendusjuhendi põhjal tehtava modelleerimise tulemusel.

Teatud hulk turvamehhanisme töötavad Windows 8 puhul ka selle aluskonfiguratsioonis. Samas leidub ka selliseid turvamehhanisme, mille puhul on tarvis, et vastutavad isikud seadistaksid need esmalt tööle. Tehniliste turvameetmete tsentraalseks konfigureerimiseks ja võtmiseks saab kasutada Active Directory't (AD).
Olukordades, kus AD-d ei saa tsentraalseks konfigureerimiseks kasutada, tuleb tehnilisi meetmeid võtta detsentraalselt, st kohapeal igas klientsüsteemis eraldi, rakendades lokaalset turvapoliitikat. Selleks saab konfiguratsioonifailid koostada tsentraalselt ning need sobivate mehhanismidega klientsüsteemidesse üle kanda ja seal installeerida.

Windows 8 keskkonnas töötavate klientide turvaliseks konfigureerimiseks tuleb võtta mitmeid meetmeid, alustades nt teostuse kontseptsiooniga (installeerimine/konfigureerimine) kuni käitamiseni. Järgnevalt on esitatud ülevaade erinevatest kohustuslikest etappidest ja meetmetest, mida tuleks iga etapi puhul võtta.

Planeerimine ja kontseptsioon
Windows-kliendi turvaline rakendamine eeldab hoolikat planeerimist. Sealjuures tuleb arvesse võtta aspekte, mida on kirjeldatud meetmes M 2.324 Windows Vista ja Windows 7 kasutuselevõtu planeerimine . Mobiilse rakenduse korral tuleb järgida järgmisi aspekte (M 2.442 Windows Vista ja Windows 7 kasutamine kaasaskantavates arvutites).

Kõigepealt tuleb kasutuskeskkonna jaoks välja valida õige Windowsi versioon (M 2.440 Windows Vista ja Windows 7 sobiva versiooni valimine). Tööandjad kasutavad Windowsi litsentside soetamiseks sageli hulgilitsentsilepinguid. Selliste lepingutega seotud toodete aktiveerimiseks on tarvis luua õiged eeldused, mis tagavad süsteemide kättesaadavuse (M 4.336 Hulgilitsentslepinguga Windows süsteemide aktiveerimine alates Windows Vistast või Windows Server 2008-st).
Planeerimisetapis tuleb välja töötada ka turvanõuded Windows 8 kasutamiseks ja dokumenteerida need turvasuuniste kujul (M 2.325 Windows Vista ja Windows 7 turvapoliitika kavandamine . Turvasuuniste planeerimine Windows-klientidel alates Windows XP-st). Kasutada tuleks Windowsi oma kaitsefunktsioone, eriti kasutajakontode haldust (M 4.340 Windows kasutajakonto haldamise (UAC) kasutamine alates Windows Vistast) ja tervikluse kaitset (M 4.341 Tervikluse kaitse alates Windows Vista). Töökeskkonnas ei tohiks võimaluse korral kasutada olemasolevaid funktsioone paroolide kohapealseks salvestamiseks (M 4.425 Vaulti ja Cardspace'i funktsiooni kasutamine Windows 7-s).

Windowsi domeenides tuleks turvanõudeid konfigureerida ja klientidele kasutada

anda nii tsentraalselt kui võimalik (M 2.326 Windows Vista ja Windows 7 grupeerimissuuniste planeerimine ja M 4.245 Windowsi Group Policy Objects alusseadistused).

Kui kliendid kantakse üle varasemast Windowsi versioonist, tuleb eelnevalt kontrollida kasutatavate rakenduste ühilduvust (M 2.441 Uue tarkvara ühilduvuse kontroll koostööks Windows Vista ja Windows 7-ga). Seejuures tuleb arvesse võtta Windowsi eripärasid Legacy tarkvara käsitlemisel M 4.338 Windows Vista ja Windows 7 failide ja registri virtualiseerimise kasutamine).

Suurenenud kaitsevajaduse korral on kliendil soovitatav kasutada krüpteerimismehhanisme. Windows 8 annab selle jaoks kaasa EFS-i (M 4.147z EFS-i turvaline kasutamine Windows 'i keskkonnas nas) ja BitLockeri (M 4.337z BitLockeri Drive Encryption kasutamine). Kui klientsüsteemi teabe töötlemise kontrollitavusele on olemas erinõuded, tuleks failijuurdepääsu jaoks aktiveerida ajatemplid (M 4.342z Last Access ajatempli aktiveerimine alates Windows Vistast).

Soetamine
Windows 8 soetamise käigus tuleb selgeks teha mõned küsimused, muu hulgas rakendatavate redaktsioonide ja 32- või 64-bitilise variandi valikuga seonduv. Juhtnööre leiab selle jaoks meetmest M 2.559 Windows 8 soetamine .

Teostus
Kui kasutatakse Windows-kliente, tuleb arvesse võtta erinevaid kaitseaspekte (M 4.248 Windowsi klientoperatsioonisüsteemide turvaline installimine). Klientsüsteemide manipuleerimine peaks olema raskendatud, kui buutimine turvatakse asjakohaselt, kõiki loodud kasutajakontosid kaitstakse asjakohase tugevusega paroolidega ja kasutajakeskkonda piiratakse asjakohaselt (M 2.32z Piiratud kasutajakeskkonna loomine).
Järgmised kaitsemeetmed seisnevad selles, et turvatakse registrit, piiratakse PowerShelli (M 4.421 Windows PowerShelli turve) ja kaitstakse suhtlemist domeeniga (M 5.89 Turvalise kanali konfigureerimine Windowsis). Kui kasutatakse vanemat tarkvara, on vajalikud täiendavad kaitsemeetmed (M 4.424z Kodugrupi funktsiooni kasutamine Windows 7-s).

Selleks et kaitsta töödeldavaid andmeid lubamatu juurdepääsu eest, peavad faili- ja ühiskasutusõigused olema antud üksnes piirangutega (M 4.149 Windows'i faili- ja ühiskasutusõigused). Seejuures tuleb lahutada või vähemalt reguleerida kodurühmade kasutamist (M 4.423 Kodugrupi funktsiooni kasutamine Windows 7-s).

Eriti Windows 8-sse integreeritud pilve-funktsioonid peidavad endas tahtmatu andmevoo ohtu süsteemi kasutamise kaudu. Sellekohased vastumeetmed on toodud meetmes M 4.472 Andmete kokkuhoid Windows 8 puhul .

Andmekaitse tagamine Windows 8 puhul
Suurenenud kaitsevajaduse korral võib suhtlust kaitsta IPSec'iga (M 5.90z Protokolli IPSec kasutamine Windowsi keskkonnas). AppLockeriga saab kontrollida rakenduste teostamist ja sel moel saavutatakse parem kaitse pahavara ja manipulatsioonide vastu (M 4.419z Rakenduste juhtimine AppLockeriga alates Windows 7-st).

Klientsüsteemide kasutajaid tuleb kasutajasüsteemi turvalisusega seotud aspektide suhtes asjakohaselt koolitada (M 3.28 Windowsi klientoperatsioonisüsteemide turvamehhanismide koolitus kasutajatele).

Kasutamine
Windows 8 klientide turvalisema kasutamise meetmed on toodud meetmes M 4.146 Windows'i klient-operatsioonisüsteemide turvaline käitus . Võttes arvesse aina uusi avaldatud turvaauke, on eriti oluline süsteeme pidevalt uuendada (M 4.249 Windowsi klientsüsteemide ajakohastamine).
Tööga seotud ülesanded hõlmavad eriti klientide järelevalvet (M 4.344 Windows Vista, Windows 7 ja Windows Server 2008 süsteemi seire) ja nende turvalisuse regulaarset kontrollimist M 2.330 Windows Windows Vista ja Windows 7 turvapoliitika ja selle elluviimise regulaarne kontroll).

Andmed võivad ka seeläbi kolmandate isikute kätte sattuda, et neid ei kustutata täielikult, kui puuduvad vastavad vastumeetmed (M 4.56 Turvaline kustutus Windows operatsioonisüsteemides). Andmete turvaliseks vahetamiseks vahetatavate andmekandjatega võib kasutada täiendavalt krüpteerimislahendust BitLocker To Go (M 4.422z BitLocker To Go kasutamine alates Windows 7-st).

Valmisolek hädaolukorraks
Tõrge klientsüsteemides ei ole paljudel juhtudel kriitiline, sest asutuses on piisavalt asendusseadmeid. Kui siiski vajatakse eririistvara või -tarkvara või kui kliente kasutatakse mobiilselt, võib valmisolek hädaolukorraks muutuda kulukamaks. Seetõttu tuleb ka hädaolukorra planeerimisel võtta klientsüsteeme asjakohaselt arvesse (M 6.76 Avariiplaani koostamine Windowsi süsteemi tõrke puhuks). Seejuures on keskne abinõu eelkõige tugevdada regulaarselt kliendipoolseid programme ja andmeid (M 6.78 Andmete varundamine Windowsi klientsüsteemides).

Planeerimine ja kontseptsioon

- (L) M 2.324 Windows Vista ja Windows 7 kasutuselevõtu planeerimine
- (L) M 2.325 Windows Vista ja Windows 7 turvapoliitika kavandamine
- (L) M 2.326 Windows Vista ja Windows 7 grupeerimissuuniste planeerimine
- (M) M 2.327 Kaugpääsu turve Windows Vistas ja Windows 7-s
- (L) M 2.440 Windows Vista ja Windows 7 sobiva versiooni valimine
- (L) M 2.441 Uue tarkvara ühilduvuse kontroll koostööks Windows Vista ja Windows 7-ga
- (M) M 2.442 Windows Vista ja Windows 7 kasutamine kaasaskantavates arvutites

- (L) M 4.147z EFS-i turvaline kasutamine Windows 'i keskkonnas
- (M) M 4.243z Windowsi klientoperatsioonisüsteemide haldustööriistad
- (L) M 4.244 Windowsi klientoperatsioonisüsteemide turvaline süsteemikonfiguratsioon
- (L) M 4.245 Windowsi Group Policy Objects alusseadistused
- (L) M 4.246 Süsteemiteenuste konfigureerimine Windows Vista ja Windows 7 keskkondades
- (L) M 4.247 Windowsi klientoperatsioonisüsteemide piiratud kasutajaõigused
- (L) M 4.336 Hulgilitsentslepinguga Windows süsteemide aktiveerimine alates Windows Vistast või Windows Server 2008-st
- (M) M 4.337z BitLockeri Drive Encryption kasutamine
- (L) M 4.338 Windows Vista ja Windows 7 failide ja registri virtualiseerimise kasutamine
- (M) M 4.339 Vahetavate andmekandjate volitamata kasutamise tõkestamine Windows Vistas ja Windows 7-s
- (L) M 4.340 Windows kasutajakonto haldamise (UAC) kasutamine alates Windows Vistast
- (L) M 4.341 Tervikluse kaitse alates Windows Vista
- (M) M 4.342z Last Access ajatempli aktiveerimine alates Windows Vistast
- (M) M 4.425 Vaulti ja Cardspace'i funktsiooni kasutamine Windows 7-s
- (M) M 5.123 Võrgusuhtluse kaitse Windowsis

Rakendamine

- (L) M 2.32z Piiratud kasutajakeskkonna loomine
- (L) M 3.28 Windowsi klientoperatsioonisüsteemide turvamehhanismide koolitus kasutajatele
- (L) M 4.149 Windows'i faili- ja ühiskasutusõigused
- (L) M 4.248 Windowsi klientoperatsioonisüsteemide turvaline installimine
- (L) M 4.419z Rakenduste juhtimine AppLockeriga alates Windows 7-st
- (L) M 4.421 Windows PowerShelli turve
- (M) M 4.423 Kodugrupi funktsiooni kasutamine Windows 7-s
- (M) M 4.424z Vanemate tarkvarade turvaline kasutamine alates Windows 7-st
- (L) M 5.89 Turvalise kanali konfigureerimine Windowsis
- (M) M 5.90z Protokolli IPSec kasutamine Windowsi keskkonnas

Kasutamine

- (M) M 2.330 Windows Windows Vista ja Windows 7 turvapoliitika ja selle elluviimise regulaarne kontroll
- (L) M 4.56 Turvaline kustutus Windows operatsioonisüsteemides
- (L) M 4.146 Windows'i klient-operatsioonisüsteemide turvaline käitus
- (L) M 4.249 Windowsi klientsüsteemide ajakohastamine
- (L) M 4.343z Hulgilitsentsilepinguga Windowsi süsteemide reaktiveerimine alates Windows Vistast või Windows Server 2008-st

- (M) M 4.344 Windows Vista, Windows 7 ja Windows Server 2008 süsteemi seire
- (L) M 4.420 Windows 7 tegevuskeskuse turvaline kasutamine
- (M) M 4.422z BitLocker To Go kasutamine alates Windows 7-st

Valmisolek hädaolukorraks

- (L) M 6.76 Avariiplaani koostamine Windowsi süsteemi tõrke puhuks
- (L) M 6.78 Andmete varundamine Windowsi klientsüsteemides

B 3.301 Turvalüüs (tulemüür)

Turvalüüs (nimetatakse sageli ka tulemüüriks) on riist- ja tarkvaratehnilistest komponentidest koosnev süsteem IP-võrkude omavaheliseks turvaliseks ühendamiseks. Selleks piiratakse kommunikatsiooni tehnilisi võimalusi vastavalt kehtivale infoturbepoliitikale. Võrguühenduse turvalisus tähendab seejuures eranditult üksnes volitatud süsteemi juurdepääsu või soovitud andmevooge erinevate võrkude vahel.

Turvalüüsid seatakse üles kahe erineva usaldusväärse võrgu keskses ühenduskohas. Seejuures ei kujuta erinevad usaldusväärsed võrgud endast ilmtingimata mitte üksnes kombinatsiooni Internet-Intranet, vaid hoopis sagedamini võib ka kahel organisatsioonisisesel võrgul olla erineva astme turvavajadus nt. büroo suhtevõrgu eraldamine personaliosakonna võrgust, kuhu kantakse üle erilist kaitset vajavaid isikuandmeid.

Mõiste „turvalüüs“ kasutamine tavapärase definitsiooni „tulemüür“ asemel viitab tõsiasjale, et tänapäeval ei kasutata võrguühenduste turvamiseks enam mitte ühte vahendit, vaid tegemist on paljude IT-süsteemidega, mis kõik täidavad erinevaid ülesandeid, nt. pakettide filtreerimine, viirusetõrje või võrgus järelevalve teostamine (“Intrusion Detection”).

Käesolevas moodulis kirjeldatakse eranditult turvalüüsile spetsiifilisi ohte ja meetmeid. Lisaks sellele vaadeldakse veel ka nende IT-süsteemide spetsiifilisi ohte ja meetmeid, mille abil turvalüüs üles ehitatakse. Sageli realiseeritakse turvalüüsi komponendid Unix -süsteemil. Niisugusel juhul tuleb täiendavalt silmas pidada ISKE moodulis B 3.102 Server Unixi all loetletud ohte ja meetmeid.

Ohud

Turvalüüsi IT-etalonturbe korral eeldatakse alljärgnevate tüüpiliste ohtude olemasolu:
Organisatsioonilised puudused:

- G 2.24 Kaitsetus välisvõrgu vastu
- G 2.101 Turvalüüsi ebapiisav hädaolukorra ennetamise plaan

Inimvead:

- G 3.3 Hooletus turvameetmete suhtes
- G 3.9 IT-süsteemi väär haldus
- G 3.38 Vead konfigureerimisel ja kasutamisel

Tehnilised rikked:

- G 4.10 Keerukad ligipääsuvõimalused võrgustatud IT-süsteemides
- G 4.11 NIS-serveri ja NIS-klientsüsteemi vahelise autentimisvõimaluse puudumine
- G 4.12 Autentimisvõimaluste puudumine X-serveri ja X-kliendi vahel
- G 4.20 Andmekadu andmekandja täitumise tõttu
- G 4.22 Tüüptarkvara turvaaugud või vead
- G 4.39 Tarkvarakontseptsiooni viga

Ründed:

- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.9 IT-süsteemide volitamata kasutamine
- G 5.18 Süstemaatiline paroolide mõistatamine
- G 5.24 Sõnumite korduv sisestamine
- G 5.25 Maskeerimine
- G 5.28 Teenuse halvamine
- G 5.39 Sissetung arvutitesse modemi kaudu
- G 5.48 IP-aadressi võltsimine
- G 5.49 Lähtemarsruutimise väärkasutus
- G 5.50 ICMP-protokolli väärkasutus
- G 5.51 Marsruutimisprotokollide väärkasutus
- G 5.78 DNS-i võltsimine
- G 5.143 Man-in-the-Middle tüüpi rünne

Soovitatavad meetmed

Selleks, et tagada kogu loetletud IT-süsteemi turvalisus, tuleb lisaks käesolevale moodulile rakendada veel ka teisi, IT-etalonturbe modelleerimise käigus selguvaid mooduleid.

Turvalüüs ei kaitse sisevõrgus toimuvate rünnakute eest. Seetõttu tuleb turvalüüsi ülesehitamisel rakendada oma töötajate võimalike rünnakute ärahoidmiseks kõiki nõutavaid turvameetmeid. Juhul kui sisevõrguks on Unix -võrk või PC-võrk, tuleb rakendada vastavates moodulites kirjeldatud turvameetmeid .

Turvalüüs tuleks paigaldada eraldiasuvasse serveriruumi. Vajalikud kohustuslikud nõuded leiate moodulist B 2.4 Serveriruum . Vajaliku serveriruumi puudumisel võib turvalüüsi alternatiivselt üles seada ka kaitsekapis (vaata moodul B 2.7 Kaitsekapid). Juhul kui turvalüüsi ise ei hallata, vaid sellega tegeleb teenusepakkuja, tuleb rakendada moodulit B 1.11 Väljasttellimine (Outsourcing) . Iseäranis tuleb silmas pidada soovitusi, mida antakse moodulis M 5.116z Meiliserveri integreerimine turvalüüsi koostisse .

Turvalüüsi edukaks ülesehitamiseks tuleb rakendada arvukalt meetmeid, alates kontseptsiooni väljatöötamisest ja lõpetades komponentide käitlemisega. Seejuures läbiviidavad etapid, nagu ka igal etapil järgitavad meetmed, on loetletud alljärgnevalt.

1. Turvalüüsiga võrguühenduse kontseptsioon (vt M 2.70 Turvalüüsi (tulemüüri) kontseptsiooni väljatöötamine):

- turvaeesmärkide kindlaksmääramine
- võrgustruktuuri kohandamine
- peamised eeldused

2. Turvalüüsi poliitika (vt M 2.71 Turvalüüsi (tulemüüri) turvapoliitika):

- Kommunikatsiooninõuete väljavalimine

- Teenuste väljavalimine (enne teenuste väljavalimist tuleb läbi lugeda moodulis M 5.39 Protokollide ja teenuste ohutu kasutamine toodud selgitused ja ääretingimused.)
- Organisatsioonilised eeskirjad

3. Turvalüüsi turvaeeskirjad (vt M 2.299 Turvalüüsi (tulemüüri) turvapoliitika koostamine)

- Eeskirjad ja viited turvalüüsi või tema üksikute komponentide turvaliseks käitlemiseks ja administreerimiseks.

4. Turvalüüsi komponentide soetamine:

- Turvalüüsi peamise ülesehituse väljavalimine (vt M 2.73 Sobiva turvalüüsi (tulemüüri) põhistruktuuri väljavalimine)
- Soetamiskriteeriumid (vt M 2.74 Sobiva paketifiltri valimine ja M 2.75 Sobiva rakenduslüüsi valimine)

5. Turvalüüsi ülesehitamine:

- Filtreerimisreeglite paikapanemine ja teostamine (vt M 2.76 Sobivate filtreerimisreeglite valimine ja kehtestamine)
- IT-etalonturbe meetmete rakendamine turvalüüsi komponentide jaoks
- Sisevõrgu infosüsteeme kontrollivate IT-etalonturbe meetmete rakendamine
- Raamtingimuste järgimine protokollide ja teenuste turvaliseks kasutamiseks (vt M 5.39 Protokollide ja teenuste ohutu kasutamine)
- Täiendavate komponentide sidumine (vt M 2.77 Serverite integreerimine tulemüüri)

6. Turvalüüsi kasutamine: (vt M 2.78 Turvalüüsi (tulemüüri) turvaline kasutamine)

- Regulaarne kontroll
- Muudatustega kohandamine ja testimine
- Turvalüüsi operatsioonide logimine (vt M 4.47 Turvalüüsi operatsioonide logimine)
- Hädaolukorraks valmisoleku plaanimine turvalüüsi jaoks (vt B 1.3 Hädaplaanimine)
- Andmevarundus (vt B 1.4 Andmevarunduspoliitika)

7. Turvalüüsiga ühendatud kliendi tegevus

Klient peab – lisaks kliendi-moodulites kirjeldatud meetmetele – järgima täiendavalt meedet, mis on toodud moodulis M 5.45 Veebibrauserite turvaline kasutamine .

Turvalüüsi kasutamisest loobumiseks võib olla erinevaid põhjuseid. Nendeks võivad olla turvalüüsi ülesehitamisega seotud kulud või administratsiooni hõivatus,

aga ka tõsiasi, et olemasolevaid riske ei osata hinnata. Juhul kui siiski soovitakse saada internetiühendust, võib alternatiivina kasutada eraldiseisvat (Stand-alone) süsteemi (M 5.46 Autonoomsüsteemide installeerimine interneti kasutamiseks).

Alljärgnevalt tutvustatakse meetmete kogumit, mida tuleb rakendada valdkonnas „Turvalüüs“.

Planeerimine ja kontseptsioon

- (L) M 2.70 Turvalüüsi (tulemüüri) kontseptsiooni väljatöötamine
- (L) M 2.71 Turvalüüsi (tulemüüri) turvapoliitika
- (L) M 2.299 Turvalüüsi (tulemüüri) turvapoliitika koostamine
- (L) M 2.301z Turvalüüsiteenuse väljasttellimine
- (L) M 2.476 Interneti turvalise ühendamise kontseptsioon

Soetamine

- (L) M 2.73 Sobiva turvalüüsi (tulemüüri) põhistruktuuri väljavalimine
- (L) M 2.74 Sobiva paketifiltri valimine
- (L) M 2.75 Sobiva rakenduslüüsi valimine
- (L) M 2.176z Sobiva internetiteenuse pakkuja valimine

Rakendamine

- (L) M 2.76 Sobivate filtreerimisreeglite valimine ja kehtestamine
- (L) M 2.77 Serverite integreerimine tulemüüri
- (L) M 3.43 Turvalüüsi administraatorite koolitus
- (M) M 4.224z Virtuaalsete privaatvõrkude integreerimine turvalüüsidesse

Kasutamine

- (L) M 2.78 Turvalüüsi (tulemüüri) turvaline kasutamine
- (M) M 2.302z Turvalüüside kõrge käideldavuse tagamine
- (L) M 4.47 Turvalüüsi operatsioonide logimine
- (L) M 4.100 Tulemüür ja aktiivsisu
- (M) M 4.101 Tulemüürid ja krüpteerimine
- (L) M 4.222 Turvaprokside õige konfigureerimine
- (M) M 4.223 Proksiserverite integreerimine turvalüüsi koostisesse
- (M) M 4.225z Logiserveri kasutamine turvalüüsis
- (L) M 4.226z Viirusskannerite integreerimine turvalüüsi koostisse
- (L) M 4.227 Lokaalse NTP -serveri kasutamine aja sünkroniseerimiseks
- (L) M 5.39 Protokollide ja teenuste ohutu kasutamine
- (L) M 5.46 Autonoomsüsteemide installeerimine interneti kasutamiseks
- (L) M 5.59 DNS võltsimise tõrje
- (L) M 5.70 Aadressi tõlkimine - Network Address Translation (NAT)
- (M) M 5.71z Sissetungi tuvastuse ja sellele reageerimise süsteemid
- (M) M 5.115z Veebiserveri integreerimine turvalüüsi koostisse
- (M) M 5.116z Meiliserveri integreerimine turvalüüsi koostisse

- (M) M 5.117z Andmebaasiserveri integreerimine turvalüüsi koostisse
- (M) M 5.118z DNS-serveri integreerimine turvalüüsi koostisse
- (M) M 5.119z Veebi-, rakendus- ja andmebaasiserveritega veebirakenduse integreerimine turvalüüsi koostisesse
- (M) M 5.120 ICMP-protokolli käsitlus turvalüüsis

Väljavahetamine

- (L) M 2.300 Turvalüüsi turvaline kõrvaldamine või selle komponentide asendamine

Valmisolek hädaolukorraks

- (L) M 6.94 Turvalüüside hädaolukorraks valmisoleku plaan

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.6 Arvuti paroolkaitse rangemad reeglid
- HG.24 Paroolide regulaarkontroll parooliskänneriga
- HG.25 Kaugpöörduste kohustuslik logimine
- HG.27 Tulemüüri ründekatsete kaugindikatsioon
- HG.38 Turvapaikade paigaldatuse regulaarseire
- HG.73 Võrgu aktiivkomponentide turvalise paigutuse regulaarseire

Teabe käideldavus (K)
-
Teabe terviklus (T)

- HT.7 Kasutajate ja nende profiilide perioodiline seire
- HT.13 Tulemüüri konfiguratsioonimuudatuste krüptoaheldamine

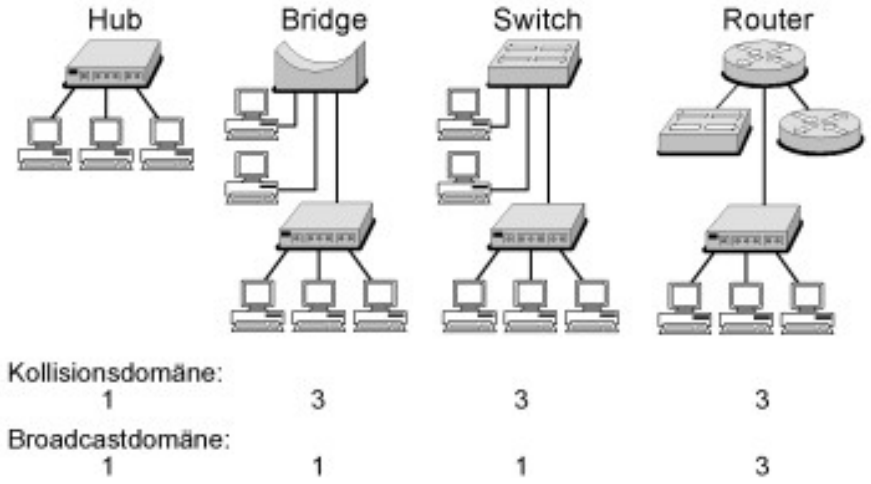
Teabe konfidentsiaalsus (S)
-

B 3.302 Marsruuterid ja kommutaatorid

Võrkude osatähtsus IT-infrastruktuuri osana suureneb üha enam, kuna tänapäeval on mitmekordistunud rakenduste kasutamine koht- või kaugvõrkude osas. Tuleb tagada võrkude käideldavus, terviklus ja konfidentsiaalsus. Need IT-turvalisuse kolm põhitingimust peavad olema nõuetekohaselt täidetud ka kõikide rakenduste korral.

Võrk koosneb aktiivsest ja passiivsest võrgutehnikast. Passiivse võrgutehnika all mõistetakse esmajoones struktureeritud kaabeldust, mille juurde kuuluvad pistikupaneeli abil konfigureeritavad kaablijagajad (Patch-Felder), kaitsekapid ja töökohal paiknevad pistikupesad. Aktiivseks võrgutehnikaks on näiteks jaoturid, sillad, kommutaatorid ja marsruuterid. Kaasaegsetes võrkudes asendavad kommutaatorid sageli jaotureid ja sildu. Aktiivse võrgutehnika (marsruuterite ja kommutaatorite) ühe või mitme komponendi rike võib viia kogu IT-infrastruktuuri töökorrast väljalangemiseni. Kuna need komponendid on IT-infrastruktuuri põhialuseks, peavad marsruuterid ja kommutaatorid olema kaitstud volitamata juurdepääsu ja manipulatsioonide eest.

Marsruuterite tööpõhimõtet on kirjeldatud moodulis M 2.276 Marsruuteri funktsionaalne kirjeldus . Meede M 2.277 Kommutaatori funktsionaalne kirjeldus kirjeldab kommutaatori tööpõhimõtet. Järgnevalt selgitatakse lühidalt alloleval joonisel kujutatud võrgu aktiivkomponentide olulisemaid funktsionaalseid erinevusi.



Hub-Jaotur, Bridge- Sild, Switch-Kommutaator, Router- Marsruuter
Kollidiondomäne-Põrkedomeen (Collision Domain)
Broadcastdomäne- Levidomeen (Broadcast Domain)
Joonis: Jaotur, sild, kommutaator ja marsruuter

Põrkedomeen

Põrkedomeeni all mõistetakse võrgujuurdepääsu protokolli CSMA/CD (Carrier Sense Multipe Access with Collision Detection) üksikut segmenti. Kõik seadmed, mis on ühendatud ühes ja samas segmendis, on põrkedomeeni koostisosadeks. Juhul kui kaks seadet üritavad andmepaketti samaaegselt võrku edastada, räägitakse põrkest. Mõlemad seadmed ootavad pärast põrke toimumist juhusliku valiku abil kindlaksmääratud aja ning proovivad andmepaketti seejärel uuesti võrku saata. Ooteaja tõttu väheneb seadmete käsutuses olev efektiivne läbilaskevõime.

Levidomeen

Levisaadetised pole suunatud mitte teatud kindlale lõppseadmele, vaid kõikidele üksteise „naabruses“ asuvatele lõppseadmetele. Need võrguseadmed, mis võtavad vastu teiste seadmete poolt edastatud levisaadetisi, moodustavad üheskoos levidomeeni. Levidomeeni kuuluvad seadmed ei pea paiknema ühes ja samas põrkedomeenis. IP-protokolli korral räägitakse sel juhul ka IP-alamvõrgust. Nii näiteks moodustavad levidomeeni IP-aadressiga 192.168.1.1 kuni 192.168.1.254 jaamad IP-alamvõrgus, mille alamvõrgumaskiks on 255.255.255.0.

Jaotur

Jaoturid töötavad OSI esimesel kihil (nn. füüsiline kiht, mis edastab andmed füüsilise bitikihina). Kõik külgeühendatud seadmed asuvad ühes ja samas põrkedomeenis ning seega ka samas levidomeenis. Jaoturid asendatakse tänapäeval kommutaatoritega.

Sild

Sillad ühendavad võrke OSI teisel kihil (lülikihil) ja segmenteerivad põrkedomeene. Silla iga segment või port moodustab eraldiseisva põrkedomeeni. Kõik külgeühendatud jaamad on tavaliselt levidomeeni koostisosadeks. Sildu võib kasutada ka erinevate topograafiaga võrkude (Ethernet, Token Ring , FDDI, jne.)

ühendamiseks OSI teisel kihil (transparent bridging, translational bridging). Peamiselt kasutatakse sildasid võrgukoormuse jagamiseks. Võrgukoormuse vähendamine saavutatakse seeläbi, et kahe võrgusegmendi vahel keskseks üleminekuks olev sild ei edasta enam kõiki andmepakette. Sillal on sisemine MAC-aadressitabel, millest tuleneb, missuguses ühendatud segmendis asuvad vastavad MAC-aadressid. Näiteks kui sild saab allsegmendist A andmepaketi allsegmendi B jaama jaoks, siis saadetakse andmepakett edasi. Seevastu kui sild võtab allsegmendist A vastu andmepaketi, mis on määratud allsegmendi A jaamale, ei edastata seda alamsegmenti B. Sellega saavutatakse allsegmendi B koormuse vähendamine. Kaasajal asendatakse sillad kommutaatoritega.

Lülikihi (OSI teise kihi) kommutaator

Tavapärased lülikihi kommutaatorid (Layer-2-Switches) ühendavad võrke OSI teisel kihil. Iga kommutaatori port kujutab endast eraldi põrkedomeeni. Tavaliselt on kõik külgeühendatud jaamad levidomeeni koostisosadeks. See tähendab, et lülikihi kommutaator võrdleb sihtaadresse (MAC-aadresse) oma tabelis olevate MAC-aadressidega ning otsustab võrdlustulemuste põhjal, missugusesse porti sissetulnud andmepaketid edastatakse.

Vaatamata sarnasele tööviisile on lülikihi kommutaatoril sildadega võrreldes kaks olulist erinevust:

- Kommutaator ühendab omavahel reeglina oluliselt rohkem alamsegmente kui sild.
- Kommutaatori ülesehitus põhineb spetsialiseeritud integraallülitusel (Application Specific Interface Circuits – ASIC), mistõttu ta on võimeline andmepakette sillast oluliselt kiiremini ühest segmendist teise saatma. Kommutaatori erinevaid tehnoloogiaid on kirjeldatud meetmes M 2.277 Kommutaatori funktsionaalne kirjeldus . Mõnikord nimetatakse kommutaatoreid ka mitmepordilisteks sildadeks (Multiport Bridges).

Marsruuterid

Marsruuterid töötavad OSI kolmandal kihil (võrgukihil) ja edastavad andmepakette vastavalt IP-päises olevate sihtaadresside (IP-aadressid) alusel. Marsruuteri iga liides kujutab endast eraldi levidomeeni ning seega ka põrkedomeeni. Marsruuterid võivad võrke ühendada erinevate topograafiate alusel. Marsruutereid kasutatakse kohtvõrkude segmenteerimiseks või nende omavaheliseks ühendamiseks kaugvõrkude kaudu. Marsruuter tuvastab sobiva ühenduse lähtesüsteemi (lähtevõrgu) ja sihtsüsteemi (sihtvõrgu) vahel. Enamikel juhtudel toimub see andmepaketi edasisaatmisega järgmisele marsruuterile, niinimetatud järgmisele hüppele (Next Hop). Üksikasjalikumaid aspekte kirjeldatakse meetmes M 2.276 Marsruuteri funktsionaalne kirjeldus .

Marsruuterid peavad igat IP-paketti enne edasisaatmist analüüsima. See toob endaga kaasa viivitusi ning „klassikaliste“ kommutaatoritega võrreldes ka väiksema andmete läbilaskevõime.

Kolmanda ja neljanda kihi kommutaatorid

Kolmanda ja neljanda kihi kommutaatorid on kommutaatorid, mis on täiendavalt võimelised ka marsruutima. Teise kihi kommutaatorid otsustavad andmepaketi MAC-päises oleva MAC sihtaadressi põhjal, missugusesse porti andmepaketid edasi saadetakse. Kolmanda kihi kommutaator käsitleb andmepakette esimesel korral samamoodi nagu marsruuter (IP-sihtaadressid IP-päises). Kõik järgnevad saatja poolt sellele vastuvõtjale lähetatud andmepaketid suunatakse siiski OSI teisele kihile (MAC-sihtaadress MAC-päises). Seetõttu saavutab niisugune kommutaator tavapärasest marsruuterist tunduvalt suurema andmete läbilaskevõime.

Veel üheks erinevuseks marsruuteri ja kolmanda kihi kommutaatori vahel on portide arv eraldiseisvate lõppseadmetega ühendamiseks. Kolmanda kihi kommutaatori portide arv on tavaliselt oluliselt suurem.

Tänu marsruutimisele võivad kolmanda või neljanda kihi kommutaatorid asendada kohtvõrkudes tavapäraseid kohtvõrgust-kohtvõrku (LAN-to-LAN) marsruutereid.

Eristamine

Käesolevas moodulis kirjeldatakse marsruuterite ja kommutaatorite kasutamisega seotud ohte ja meetmeid. Erinevad tootjad on võtnud kasutusele tähistused „teise kihi kommutaator“, „kolmanda kihi kommutaator“ või „neljanda kihi kommutaator“, mis raskendab marsruuterite eristamist kommutaatoritest. Kuna marsruuterite ja kommutaatorite funktsioonid on muutunud sarnaseks, siis võib suuremat osa kirjeldatud meetmetest rakendada nii marsruuterite kui ka kommutaatorite korral.

Saadaval on suur valik erinevate tootjate pakutavaid marsruutereid ja kommutaatoreid. Meetmete ja ohtude kirjeldused on käesolevas moodulis sõnastatud tootjatest võimalikult sõltumatul kujul.

Lisaks üleüldistele aspektidele ja infrastruktuurilistele meetmetele tuleb marsruuterite ja kommutaatorite kasutamisel silmas pidada ka moodulit B 4.1 Heterogeensed võrgud . Võrgu aktiivkomponentide sidumisel kõikehõlmavasse võrgu- ja süsteemihaldusesse on oluline järgida moodulit B 4.2 Võrgu- ja süsteemihaldus . Marsruuteri kasutamisel paketifiltrina või väljavaliku tegijana tuleb täiendavalt silmas pidada ka ISKE mooduleid B 3.301 Turvalüüs (tulemüür) ja B 4.4 Virtuaalne privaatvõrk (VPN) .

Lisaks spetsiaalselt selleks otstarbeks valmistatud seadmetega pakuvad ka erinevad operatsioonisüsteemid (näiteks erinevad Unixi -derivaadid) marsruutimise funktsionaalsust. See tähendab, et marsruuter võib koosneda vastavast arvutist, millel on kaks või enam võrgukaarti ja tavaline operatsioonisüsteem. Väiksemate kohtvõrkude korral võib see teatud asjaoludel olla hinna poolest soodsaks alternatiiviks. Lisaks käesolevas moodulis kirjeldatud turvameetmetele tuleb niisugu se marsruuteri kasutamise korral järgida ka olemasoleva operatsioonisüsteemi (Unix, Windows 2000 jne) turvameetmeid.

Ohud

Lisaks ohtudele, mis kehtivad üldiselt enamiku IT-süsteemide korral, on aktiivsete võrgukomponentide jaoks veel arvukalt spetsiifilisi ohte.

Need ohud põhinevad sageli kasutatavate protokollide, nagu näiteks TCP, UDP, IP või ICMP, teadaolevatel kitsaskohtadel. Nii näiteks võivad dünaamiliste marsruutimisprotokollide kitsaskohtade tõttu marsruuterite marsruutimistabelid teisene-

da. Veel ühe ohuna tuleb nimetada sageli puuduvat või ebapiisavat autentimisvõimalust võrgu aktiivkomponentidel.

Võrgu aktiivkomponente tarnitakse sageli mitteturvalise vaikimisi konfiguratsiooniga (vaata G 4.49 Marsruuterite ja kommutaatorite ebaturvalised vaikesätted), mida peaks seadme kasutuselevõtmisel üle kontrollima. Erineva turvavajadusega alamvõrkude turvaliseks eraldamiseks soovitatakse aeg-ajalt virtuaalsete võrkude (VLAN) kasutamist. Siiski on teada mõningad ründemeetodid, mis võimaldavad ületada virtuaalsete võrkude vahelisi piire ning teistele virtuaalsetele võrkudele õigustamatult ligi pääseda (vaata G 5.115 Virtuaalsete kohtvõrkude vaheliste piiride ületamine).

Alljärgnevalt on ülevaatlikult välja toodud marsruuterite ja kommutaatorite kasutamisega seotud ohud:

Organisatsioonilised puudused:

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.3 Puuduvad, puudulikud või ühildumatud ressursid
- G 2.4 Turvameetmete ebapiisav järelevalve
- G 2.22 Logiandmete analüüsimata jätmine
- G 2.27 Ebapiisav või puuduv dokumentatsioon
- G 2.44 Ühildamatud võrgu aktiiv- ja passiivkomponendid
- G 2.54 Konfidentsiaalsuse kadu jääkinfo kaudu
- G 2.98 Marsruuterite ja kommutaatorite kasutamise väär kavandamine

Inimvead:

- G 3.64 Marsruuterite ja kommutaatorite väär konfiguratsioon
- G 3.65 Marsruuterite ja kommutaatorite väär haldamine

Tehnilised rikked:

- G 4.49 Marsruuterite ja kommutaatorite ebaturvalised vaikesätted

Ründed:

- G 5.4 Vargus
- G 5.51 Marsruutimisprotokollide väärkasutus
- G 5.66 IT-süsteemide volitamatud võrguühendused
- G 5.112 ARP-protokolli tabelitega manipuleerimine
- G 5.113 MAC-aadresside võltsimine
- G 5.114 Genereeriva puu (Spanning Tree) väärkasutus
- G 5.115 Virtuaalsete kohtvõrkude vaheliste piiride ületamine

Soovitatavad meetmed

Käesolevas moodulis käsitletud turvameetmed tuginevad võrgu aktiivkomponentide elueale. Alljärgnevalt kirjeldatakse meetmeid, mis on jaotatud järgnevatesse tsüklitesse:

- Marsruuterite ja kommutaatorite kasutamise planeerimine ja kontseptsioon

Marsruuterite ja kommutaatorite kasutamist tuleb hoolikalt kavandada. Marsruuterite ja kommutaatorite tööpõhimõtted on kirjeldatud meetmetes M 2.276 Marsruuteri funktsionaalne kirjeldus ja M 2.277 Kommutaatori funktsionaalne kirjeldus . Marsruuterite ja kommutaatorite kasutamise tüüpstsenaariumid, mis võivad abiks olla planeerimisel ja kontseptsiooni väljatöötamisel, on ära toodud meetmes M 2.278 Marsruuterite ja kommutaatorite kasutamise tüüpstsenaariumid .

- Marsruuterite ja kommutaatorite turvastrateegia koostamine

Enne võrgu aktiivkomponentide hankimist (vt M 2.280 Sobivate marsruuterite ja kommutaatorite ostmis- ja valimiskriteeriumid) tuleb seadmete turvaliseks kasutamiseks koostada ja dokumenteerida vastav turvastrateegia (vt M 2.279 Marsruuterite ja kommutaatorite turvapoliitika koostamine). Sellele järgnevalt võib välja valida sobivad võrguelemendid ning integreerida need turvaliselt olemasolevasse võrguinfrastruktuuri. Kõnealuses etapis on oluline administraatorite koolitamine marsruuterite ja kommutaatorite turvalise halduse alal (vt M 3.38 Marsruuterite ja kommutaatorite koolitus administraatoritele).

- Marsruuterite ja kommutaatorite konfigureerimine ja kasutuselevõtmine

Marsruuterite ja kommutaatorite konfigureerimisel ja kasutuselevõtmisel tuleb silmas pidada mitmeid olulisi turvameetmeid. Võrgukomponentide ebaturvalised vaikesätted kujutavad endast sageli suurt turvariski. Seetõttu peab konfiguratsiooni enne seadmete kasutuselevõtmist üle kontrollima ja vajadusel muutma.

Marsruuterite ja kommutaatorite kasutamisel on suur tähtsus süsteemi turvalisel ülesehitamisel (vt M 4.201 Marsruuterite ja kommutaatorite turvaline lokaalne aluskonfiguratsioon ja M 4.202 Marsruuterite ja kommutaatorite turvaline võrgualuskonfiguratsioon). Marsruuterite kasutuselevõtmisel tuleb lisaks eelnevale tähelepanu pöörata ka marsruutimisprotokollide turvalisusele. Kasutamise eesmärgist lähtudes tuleb marsruuteritel konfigureerida ka pääsuloendid (vt M 5.111 Marsruuterite pääsuloendite konfigureerimine). Siinjuures, aga ka tavapärase töö korral, tuleb süsteemi konfiguratsioon hoolikalt dokumenteerida (vt M 2.281 Marsruuterite ja kommutaatorite süsteemikonfiguratsiooni dokumenteerimine).

Marsruutereid kasutatakse sageli ka virtuaalsete privaatvõrkude (VPN) turvaliseks rajamiseks. Virtuaalvõrkude kommutaatoritele ülesehitamisel tuleb järgida teatavaid turvaaspekte. Kokkuvõtvalt on meetmes M 4.203 Marsruuterite ja kommutaatorite konfigureerimise kontroll-loend ära toodud kontrollnimekiri marsruuterite ja kommutaatorite turvaliseks konfigureerimiseks.

- Marsruuterite ja kommutaatorite turvaline kasutamine

Juhised marsruuterite ja kommutaatorite turvaliseks kasutamiseks on kirjas meetmetes M 2.282 Marsruuterite ja kommutaatorite seire , M 2.283 Marsruuterite ja kommutaatorite tarkvara hooldus ja M 6.91 Marsruuterite ja kommutaatorite andmete varundus ja taaste . Marsruuterite ja kommutaatorite protokollimise aspekte kirjeldatakse moodulis M 4.205 Marsruuterite ja kommutaatorite töö logimine . Rikke korral olulised turvaaspektid on ära toodud meetmes M 6.92 Marsruuterite ja kommutaatorite hädaolukorraks valmisoleku plaan .

- Turvaaspektid marsruuterite ja kommutaatorite väljavahetamine

Salvestatud konfiguratsiooniandmed ja logifailid marsruuteritel ja kommutaatoritel sisaldavad informatsiooni võrgustruktuuri kohta. Võrgu aktiivkomponentide väljavahetamisel tuleb järgida juhiseid meetmes M 2.284 Marsruuterite ja kommutaatorite turvaline tööst kõrvaldamine .

Alljärgnevalt tutvustatakse meetmete kogumit, mida tuleb rakendada valdkonnas "Marsruuterid ja kommutaatorid".

Planeerimine ja kontseptsioon:

- (M) M 2.276z Marsruuteri funktsionaalne kirjeldus
- (M) M 2.277z Kommutaatori funktsionaalne kirjeldus
- (M) M 2.278z Marsruuterite ja kommutaatorite kasutamise tüüpstsenaariumid
- (M) M 2.279 Marsruuterite ja kommutaatorite turvapoliitika koostamine

Soetamine:

- (M) M 2.280 Sobivate marsruuterite ja kommutaatorite ostmis- ja valimiskriteeriumid

Rakendamine:

- (L) M 1.43 Võrgu aktiivkomponentide turvaline paigutus
- (M) M 3.38 Marsruuterite ja kommutaatorite koolitus administraatoritele
- (M) M 4.201 Marsruuterite ja kommutaatorite turvaline lokaalne aluskonfiguratsioon
- (M) M 4.202 Marsruuterite ja kommutaatorite turvaline võrgualuskonfiguratsioon
- (M) M 4.203 Marsruuterite ja kommutaatorite konfigureerimise kontrolloend
- (M) M 5.111 Marsruuterite pääsuloendite konfigureerimine

Kasutamine:

- (M) M 2.281 Marsruuterite ja kommutaatorite süsteemikonfiguratsiooni dokumenteerimine
- (M) M 2.282 Marsruuterite ja kommutaatorite seire
- (M) M 2.283 Marsruuterite ja kommutaatorite tarkvara hooldus
- (M) M 4.204 Marsruuterite ja kommutaatorite turvaline haldus
- (M) M 4.205 Marsruuterite ja kommutaatorite töö logimine
- (M) M 4.206 Kommutaatori portide turvamine
- (M) M 5.112 Marsruutimisprotokollide turvaaspektide arvestamine

Väljavahetamine:

- (M) M 2.284 Marsruuterite ja kommutaatorite turvaline tööst kõrvaldamine

Valmisolek hädaolukorraks:

- (M) M 6.91 Marsruuterite ja kommutaatorite andmete varundus ja taaste
- (M) M 6.92 Marsruuterite ja kommutaatorite hädaolukorraks valmisoleku plaan

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.6 Arvuti paroolkaitse rangemad reeglid
- HG.25 Kaugpöörduste kohustuslik logimine
- HG.73 Võrgu aktiivkomponentide turvalise paigutuse regulaarseire

Teabe käideldavus (K)
-
Teabe terviklus (T)
-
Teabe konfidentsiaalsus (S)
-

B 3.303 Salvestisüsteemid ja salvestivõrgud

Salvestisüsteemid võimaldavad institutsioonidel salvestada nende digitaalseid andmeid. Kuna digitaalsete andmete maht aina suureneb ning koos sellega kasvab ka andmestruktuuride hävimise oht, muutub tänapäevaste salvestisüsteemide kasutuselevõtt institutsioonides aina päevakohasemaks.

Andmete pideva muutumise kõrval võib täheldada ka pidevat muutust salvestisüsteemidele esitatavates nõuetes, mis avaldub ennekõike alljärgnevas:

- Institutsiooni andmetele tuleb tagada kõikjal pidev juurdepääs ning seda koraga väga erinevateks otstarveteks. Seetõttu esitatakse tänapäevastele salvestisüsteemidele väga suuri käideldavusnõudeid.
- Tööprotsesside ümberkorraldused, mis soodustavad tööülesannete jaotamist eri rühmade ja meeskondade vahel, suurendavad pidevalt nende rakendusprogrammide loetelu, mis peavad andmetele juurde pääsema.
- Institutsiooni hallatava teabe aina suurenev digitaliseerimine muudab aina olulisemaks erinevate vastavusnõuete järgmise (compliance).
- Salvestisüsteemidelt oodatakse, et need oleksid paindlikud, et neid süsteeme saaks pidevalt muutuvate vajadustega kohandada ja et vajamineva salvestiruumi saaks kasutusse anda tsentraalselt.

Vanemates salvestisüsteemides kasutati lahendusi, kus andmekandja on ühendatud otse serveri külge. Niinimetatud omasalvestisüsteemid (Direct Attached Storage, DAS) ei suuda aga praegusi ega ka tulevasi vajadusi enam rahuldada. Nimetatud süsteemide puudustena võib nimetada veel ka kulutuste järsku suurenemist seoses riistvara ja administreerimisega. Pealegi ei suuda uued tehnoloogiad, nt andmete elusalt migreerimine, ei salvestisüsteemide siseselt ega ka salvestisüsteemide vahel DAS-iga koostööd teha. Direct-Attached-Storage-lahendusi ei õnnestu muu hulgas ka efektiivselt hallata. Seetõttu nähakse tsentraalselt toimivate salvestisüsteemide kasutuselevõttu juba mõnda aega kui möödapääsmatut lahendust, mis on ka praktikas juba laialt levinud.

Selles moodulis käsitletakse järgmist:

- salvestilahendused: salvestilahendus koosneb vähemalt ühest või mitmest salvestivõrgust ja ühest salvestisüsteemist.
- Salvestivõrgud: salvestivõrgud võimaldavad ühelt poolt salvestisüsteemidele juurde pääseda ning teisalt andmeid erinevate salvestisüsteemide vahel replikeerida.
- Salvestisüsteemid: salvestisüsteemi all peetakse silmas tsentraalselt toimivat lahendust, mis osutab teistele süsteemidele salvestiruumi teenust. Samas võimaldab salvestisüsteem paljudel teistel süsteemidel (nt virtuaalsetel ja füüsilistel serveritel, klientidel) kasutada üheaegselt olemasolevat salvestiruumi.

Salvestivõrgu abil võivad mitu serverit, või vajadusel ka lõppseadet kasutada ühist salvestit. Niisuguse süsteemi eeliseks on madalad halduskulud ja andmeva-

runduse lihtsustumine. Kuna mitmest omavahel ühendatud üksusest koosnevad salvestisüsteemid kasutavad tavaliselt spetsiaalset salvestivõrku, siis nimetatakse neid süsteeme kirjanduses sageli “salvestivõrguks”. Salvestusprotsessis pole tegev mitte üksnes võrk, vaid koostööd peavad tegema ka paljud teised komponendid. Seetõttu käsitleb käesolev moodul salvestisüsteeme ja salvestivõrke üheskoos. Edaspidi nimetatakse salvestisüsteemiks keskset instantsi, mis lubab teistel süsteemidel kasutada oma salvestusruumi. Salvestissüsteemiga ühendatud andmevarundusseadmeid käsitletakse moodulis B 1.12 Arhiveerimine . Andmevarunduse kontseptuaalseid aspekte selgitatakse moodulis B 1.4 Andmevarunduspoliitika .

Salvestisüsteemide kasutuselevõtmine võimaldab organisatsioonis salvestusmahu koondamist, mis tähendab alljärgnevat:

- Salvestimaht „eemaldatakse” lokaalsetest serveritest ja koondatakse tsentraalsetesse salvestisüsteemidesse .
- Salvestusruumi suurenenud v ajadust saab tänu tsentraalse salvestusmahu paindlikule kasutamisele rahuldada ilma riistvara ümberehituseta.
- Rakendused saavad salvestusruumi ja selles sisalduvat informatsiooni ühiselt kasutada .

Salvestissüsteeme on kahte tüüpi: võrgumälu (Network Attached Storage – NAS) ja salvestivõrk (Storage-Area-Network – SAN). Lihtsustatult käsitletuna kujutavad NAS-süsteemid endast spetsiaalseid võrgu servereid. Ligipääs salvestile on “failipõhine”. Seevastu SAN-süsteemide näol on tegemist kettavõrgu serveriga ühendamise spetsiaalse viisiga, mis tagab küll suure jõudluse, kuid on tehniliselt keerukas. Ligipääs salvestile on “plokipõhine”.

Network-Attached-Storage -süsteemid kasutavad ühenduses olevate arvutite andmevahetuseks olemasolevat Ethernet -kohtvõrku, millel on TCP/IP protokoll nagu NFS (Network File System Protokoll) või CIFS (Common Internet File System). Kõnealused süsteemid töötavad sageli nagu tavalised failiserverid, mistõttu paljud pakkujad kasutavad niisuguste süsteemide jaoks mõistet „registraator (Filer)“. Sellest tulenevalt peab NAS-süsteemide korral rakendama täiendavalt moodulit B 3.101 Server .

Storage Area Network -süsteemid on reeglina spetsiaalselt selleks otstarbeks loodud võrgud, mis ühendavad salvestisüsteemid serveritega. Tüüpiline SAN koosneb ühest või mitmest kettasüsteemist, salvestisüsteemi aktiivsetest elementidest (SAN-kommutaatoritest), teistest salvestisüsteemidest (nt. lintsalvestitest) ja ühendatud serveritest. SAN-süsteemide spetsiaalsele võrgule või kombineeritud salvestisüsteemidele tuleb rakendada moodulit B 4.1 Heterogeensed võrgud .

Nende kahe laialt levinud salvestisüsteemi ja salvestivõrgu kõrval leidub aga ka teisi variante.

Salvestisüsteemid, mis võimaldavad andmetele juurde pääseda nii NAS- kui ka SAN-süsteemidega, kannavad sageli nimetust kas hübriidsalvestisüsteem (Hybrid Storage) või ka kombineeritud salvestisüsteem (Unified Storage). Teenuste osutamisel võib seda käitada nii NAS- kui ka SAN-süsteemina. Kombineerutud käitamine on võimalik tänu vastavatele süsteemikomponentidele ja nende konfiguratsioonile. Nii on võimalik, et üks ja sama salvestisüsteem suudab

juurdepääsu teatud rakendustele pakkuda läbi Ethernet-ühenduse, töötades nn filer'ina ja osutada seeläbi failiteenuseid CIFS- ja NFS-protokolliga ja pakkuda läbi Fibre Channel'i, Fibre Channel over Ethernet'i või iSCSI teistele serveritele ka salvestimahtusid.

Seetõttu tuleb hübriidsüsteemide puhul rakendada ka mooduleid B 3.101 Server ja B 4.1 Heterogeensed võrgud .

Object Storage (sageli ka Object based Storage) võimaldab traditsiooniliste ploki- ja failipõhiste juurdepääsude kõrval rakendada andmete suhtes objektipõhist juurdepääsu.

Objektikesksed salvestilahendused salvestavad andmeid andmekandjatele koos nende juurde kuuluvate metaandmetega mitte failide, vaid objektidena. Objekti saab eksimatult identifitseerida objekti ID (räsiväärtus) põhjal, mis sisaldab muu hulgas ka objekti metaandmeid. Juurdepääs objektipõhisele mälule toimub läbi juhtiva rakenduse. Rakendus pääseb objektipõhisesse salvestisüsteemi kas spetsiaalse liidese (Application Programming Interface (API)) ja selle võimalike käskudega või otse IP-ga. Juhtudel, kus juurdepääsuks kasutatakse API-d, peab vastav rakendus toetama objektipõhise salvestisüsteemi tootjapõhist API-d. Object-Storage-tüüpi lahendusi kasutatakse sageli arhiveerimisel ja dokumendihalduses.

Objektipõhiste salvestilahenduste puhul tuleb kindlasti rakendada ka mooduleid B 3.101 Server ja B 5.24 Veebiteenused .

Ohud

Salvestisüsteemide IT-etalonturbe jaoks eeldatakse järgmiste tüüpiliste ohtude olemasolu:

Vääramatu jõud:

- G 1.2 IT-süsteemi avarii
- G 1.9 Tugevast magnetväljast tingitud andmekadu

Organisatsioonilised puudused:

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.4 Turvameetmete ebapiisav järelevalve
- G 2.5 Hoolduse puudumine või puudulikkus
- G 2.7 Õiguste volitamata kasutamine
- G 2.26 Ebapiisavad või puuduvad tarkvara katsetamis- ja teavitusprotseduurid
- G 2.27 Ebapiisav või puuduv dokumentatsioon
- G 2.37 Sideliinide kontrollimatu kasutamine
- G 2.48 Andmekandjate ja dokumentide puudulik hävitamine
- G 2.54 Konfidentsiaalsuse kadu jääkinfo kaudu
- G 2.67 Pääsuõiguste puudulik haldus

- G 2.82 Arhiivisüsteemi asukoha halb planeerimine
- G 2.103 Töötajate ebapiisav koolitamine
- G 2.109 Salvestisüsteemi ebapiisav või puuduv planeerimine
- G 2.182 Salvestisüsteemide puuduv või ebapiisav käitamise kontseptsioon
- G 2.183 Puuduv või puudulik tsoonide kontseptsioon
- G 2.184 XXX
- G 2.185 Tarkvara puuduv või puudulik hooldus (Maintenance) ja paigaldus (Patch Level Management)
- G 2.186 Salvestisüsteemidega seotud vastutusalade puuduv või puudulik reguleerimine või rollide ebaselge piiritlemine
- G 2.187 Salvestisüsteemide puuduv või puudulik simultaanteeninduse halduskontseptsioon

Inimvead:

- G 3.9 IT-süsteemi väär haldus
- G 3.16 Väär pääsuõiguste haldus
- G 3.24 Andmete juhuslik manipuleerimine
- G 3.38 Vead konfigureerimisel ja kasutamisel
- G 3.79 SAN salvestivõrgu ressursside vale jaotamine

Tehnilised rikked:

- G 4.13 Salvestatud andmete hävimine
- G 4.53 Salvestite ebaturvalised vaikesätted
- G 4.95 Salvestisüsteemi komponendi rike
- G 4.96 Salvestisüsteemi komponendi tõrge

Ründed:

- G 5.1 IT-seadmete või -tarvikute manipuleerimine ja hävitamine
- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.4 Vargus
- G 5.7 Liinide pealtkuulamine
- G 5.8 Liinide manipuleerimine
- G 5.10 Kaughooldeportide väärkasutus
- G 5.18 Süstemaatiline paroolide mõistatamine
- G 5.20 Administraatori õiguste väärkasutus
- G 5.28 Teenuse halvamine
- G 5.57 Võrguanalüüsi utiliidid
- G 5.89 Võrguühenduse ülevõtt
- G 5.102 Sabotaaž
- G 5.129 Andmete manipuleerimine salvestisüsteemi kaudu
- G 5.130 Salvestisüsteemi konfiguratsiooni manipuleerimine
- G 5.185 Füüsiline juurdepääs salvestusvõrgu kommutaatoritele (SAN-switch'idele)
- G 5.186 Juurdepääs teiste teenusetarbijate andmetele WWN-Spoofing'uga
- G 5.187 Võrgu loogiliste lahutuspiiride ületamine
- G 5.189 Salvestipõhiste replikeerimismeetodite konfidentsiaalsuse kadu

Soovitatavad meetmed

Salvestisüsteemi kindlustamiseks tuleb lisaks käesolevale moodulile rakendada veel teisi mooduleid, vastavalt infosüsteemide etalonturbe kohase modelleerimise tulemustele.

Salvestisüsteemi edukaks ülesehitamiseks ja kasutamiseks peab võtma kasutusele mitmeid meetmeid. Kõigepealt tuleb langetada strateegiline otsus, missugust tüüpi süsteem välja valitakse. Kontseptsiooni väljatöötamisele järgneb installeerimine ja kasutuselevõtmine. Pärast kasutusaja lõppemist peab rakendama meetmeid süsteemi eeskirjadekohaseks kõrvaldamiseks.

Paralleelselt kasutusajaga tuleb hädaolukorraks valmisoleku abil tagada süsteemi töö jätkumine ka hädaolukorras. Sellega kaasnevalt peavad IT-turvameeskond ja audit garanteerima, et reeglistikust tõepoolest ka kinni peetakse.

Seejuures läbiviidavad etapid, samuti rakendatavad meetmed, millele tuleb igas etapis tähelepanu pöörata, on loetletud alljärgnevalt:

Planeerimine ja kontseptsioon

Pärast süsteemile esitatavate nõuete analüüsimist peaksid vastutavad isikud langetama otsuse, mis tüüpi salvestilahendusi hakatakse institutsioonis tulevikus kasutama. Selleks tuleb esmalt välja selgitada, milline tehnoloogia täidab kõige paremini salvestisüsteemile esitatud nõudeid (vt M 2.362 Sobiva salvestisüsteemi valik ja M 2.351 Salvestisüsteemide planeerimine).

Lähtepunktiks tuleks üldjuhul võtta tsentraalset salvestamisfunktsiooni pakkuv rakendus. Selline lähtepunkt võimaldab mõistlikul moel sõnastada nii salvestisüsteemile kui ka -võrgule, st kogu salvestilahendusele tervikuna esitatavad turbenõuded. Olulised aspektid, millele salvestisüsteemi planeerimisel tähelepanu pöörata, on muu hulgas salvestisüsteemi eeldatav laiendamine selle kasutustsükli vältel ja salvestisüsteemi jõudlusnäitajad. Siin on oluline, et tsentraalsete salvestikomponentide planeerimisel arvestataks ka juba oodatavate arengute ja laienemisprognoosidega, mille tulemusel valitaks sellised IT-komponendid, mis suudavad rahuldada institutsiooni vajadusi ka pikemas perspektiivis. Salvestisüsteemile esitatavad nõuded peaksid kajastuma ka selle turvapoliitikas (vt M 2.525 Salvestisüsteemide turvapoliitika väljatöötamine).

Kui vajaduste analüüs näitab, et salvestilahendus peab võimaldama simultaanteenindust, tuleb välja töötada reeglid, kuidas lahutada erinevaid teenusetarbijaid üksteisest korrektselt (vt M 2.525 Salvestisüsteemide turvapoliitika väljatöötamine). Suurte käideldavus- ja skaleeritavusnõuete korral on soovitav kasutusele võtta kõrgkäideldav salvestilahendus (vt M 2.354 Kõrge käideldavusega SAN-konfiguratsiooni kasutamine). Täiendava meetmena suurte turbenõuete, eriti mis puudutavad salvestatud andmete konfidentsiaalsuse ja tervikluse tagamist, on soovitatav kasutada krüpteerimismehhanisme ja juurutada tsoonide kontseptsioon (vt M 4.448 Krüpteeringu kasutamine salvestisüsteemides ja M 4.449 Tsoonide kontseptsiooni juurutamine).

Vajaminevate salvestusmahtude hindamise ja planeerimise kõrval on väga oluline ka salvestilahenduse kiire ja korrektne ülesehitamine (vt M 1.59 Arhiivisüsteemide asjakohane rajamine). Siin on oluline kriitiliselt hinnata, kas serveriruumid või arvutuskeskus on salvestilahenduse jaoks tehnilise ja töökorralduse poole pealt sobivad paigalduskohad või mitte. Tegelik paigaldamine peab toimuma rakendamise etapis.

Salvestisüsteemi planeerimise käigus tuleb välja töötada ka asjakohane andmevarunduspoliitika. Selleks tuleb institutsiooni andmevarunduspoliitikasse (B 1.4

Andmevarunduspoliitika) sisse viia väljavalitud salvestilahendust käsitlevad tehnilised ja töökorralduslikud muudatused.

Soetamine

Kui organisatsioon on defineerinud oma peamised nõuded salvestisüsteemile, tuleb võimalikud pakkujad ja tarnijad üle kontrollida (M 2.355 Salvestisüsteemi tarnija valik).

Salvestisüsteemi riistvarakomponentide tarnijatega sõlmitakse teeninduslepingud, milles lepitakse kokku realistlikes reageerimisaegades, nii et need oleksid kooskõlas süsteemi käideldavusega ja esitatavate nõuetega (M 2.356 Lepingud SAN teenusepakkujatega).

Rakendamine

Pärast organisatoorsete ja planeerimisalaste ettevalmistustööde lõppemist võib alustada kohtvõrgu salvesti (NAS-süsteemi) installeerimisega või vastavate võrgu- ja salvestikomponentidega ning salvestivõrgu (SAN-süsteemi) ülesehitamisega.

Seejuures tuleb silmas pidada järgmisi meetmeid:

Salvestisüsteemi autentimismehhanismide põhikonfiguratsioon peab olema turvaline (vt M 4.274 Salvestissüsteemide turvaline aluskonfiguratsioon).

Salvestisüsteem tuleb paigutada kaitstud haldusvõrku (M 2.357 Salvestisüsteemide haldusvõrgu ehitus).

Käesolevas etapis kooskõlastatakse turvalisusest tulenevad nõuded süsteemi tegevusest lähtuvate nõuetega. Kõik NAS- või SAN-süsteemiga seotud administraatorid peavad läbima kasutuselevõetud lahenduse alase koolituse (vt M 3.54 Salvestisüsteemide administraatorite koolitus).

Salvestivõrgu salvesti (SAN-süsteemi) ülesehitamisel ühendatakse server salvestisüsteemi komponentidega, vastavalt kirjalikule spetsifikatsioonile ja plaanidele (vt M 5.130 Salvestisvõrgu (SAN-i) kaitse segmenteerimise abil).

Testimisetapi tulemuste põhjal koostatakse süsteemi dokumentatsioon. Dokumenteerida tuleb kogu kasutuselevõetud riist- ja tarkvara, samuti kõik installeerimistegevused ja individuaalsed konfiguratsioonid (vt M 2.358 Salvestisüsteemide süsteemisätete dokumenteerimine).

Kasutamine

Pärast esmakordset installeerimist ja testimist minnakse üle tavapärasele tegevusele. Turvalisusest lähtuvalt peab seejuures tähelepanu pöörama järgmistele asjaoludele:

- Salvestisüsteemi funktsionaalsuse kasutamine eeldab salvestisüsteemi turvalist tööd. Salvestisüsteemi tegevust toetavad teeninduprogrammid peavad olema kaitstud ning kõrge autentimistasemega (vt M 4.275 Salvestisüsteemide turvaline kasutamine).
- Salvestisüsteeme tuleb jooksva töö käigus pidevalt jälgida ja hooldada. (vt M 2.359 Salvestisüsteemide seire ja haldamine).
- Lisaks järelevalvele ja hooldusele, mis peavad tagama ennekõike süsteemi tehnilise kasutatavuse, tuleb jälgida ka täiendavaid, turvalisuse seisukohalt olulisi aspekte (vt M 2.360 Salvestisüsteemide turvaaudit ja aruanded).
- Juhtudel, kus SAN-Fabricule esitatavad tervikluse nõuded on tavapärasest suuremad, on soovitav kasutada laiendatud turbefunktsioonidega salvestiprotokolle (vt M 4.447 SAN-Fabricu tervikluse tagamine).

Väljavahetamine

Soovitused üksikkomponentide ja terviksüsteemide väljavahetamiseks pärast tavakasutamise lõppemist on kirjas meetmes M 2.361 Salvestisüsteemide kasutuselt kõrvaldamine .

Valmisolek hädaolukorraks

Salvestisüsteemid nõuavad olemasolevate IT-hädaolukorraplaanide ümbertöötamist ja kohandamist (vt M 6.98 Salvestisüsteemide valmisolek hädaolukorraks).

Alljärgnevalt tutvustatakse meetmete kogumit, mida tuleb rakendada valdkonnas “Salvestissüsteemid ja salvestisvõrgud”:

Planeerimine ja kontseptsioon

- (L) M 2.351 Salvestisüsteemide planeerimine
- (M) M 2.354z Kõrge käideldavusega SAN-konfiguratsiooni kasutamine
- (L) M 2.362 Sobiva salvestisüsteemi valik
- (L) M 2.525 Salvestisüsteemide turvapoliitika väljatöötamine
- (L) M 2.528z Teenusetarbijate turvaline lahutamine salvestisüsteemides
- (L) M 2.529w Salvestisüsteemide modelleerimine
- (L) M 3.92w Salvestisüsteemide kasutamise põhiterminid
- (M) M 4.448z Krüpteeringu kasutamine salvestisüsteemides
- (M) M 4.449z Tsoonide kontseptsiooni juurutamine

Soetamine

- (L) M 2.355 Salvestisüsteemi tarnija valik
- (L) M 2.356 Lepingud SAN teenusepakkujatega

Rakendamine

- (L) M 1.59 Arhiivisüsteemide asjakohane rajamine
- (M) M 2.357 Salvestisüsteemide haldusvõrgu ehitus
- (L) M 2.358 Salvestisüsteemide süsteemisätete dokumenteerimine
- (L) M 2.526 Salvestisüsteemi käitamise planeerimine
- (L) M 3.54 Salvestisüsteemide administraatorite koolitus
- (M) M 4.80 Kaug-võrguhalduse turvalised pääsumehhanismid
- (L) M 4.274 Salvestissüsteemide turvaline aluskonfiguratsioon
- (M) M 5.130 Salvestisvõrgu (SAN-i) kaitse segmenteerimise abil

Kasutamine

- (L) M 2.359 Salvestisüsteemide seire ja haldamine
- (M) M 2.360 Salvestisüsteemide turvaaudit ja aruanded
- (M) M 2.527 Turvaline kustutamine SAN-keskkonnas
- (L) M 4.275 Salvestisüsteemide turvaline kasutamine
- (L) M 4.447 SAN-Fabricu tervikluse tagamine

Väljavahetamine

- (M) M 2.361 Salvestisüsteemide kasutuselt kõrvaldamine

Valmisolek hädaolukorraks

- (L) M 6.1 Käideldavusnõuete inventuur
- (L) M 6.98 Salvestisüsteemide valmisolek hädaolukorraks

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.6 Arvuti paroolkaitse rangemad reeglid
- HG.38 Turvapaikade paigaldatuse regulaarseire
- HG.50 Virtuaalsed salvestivõrgud ja pordipõhine tsoneerimine
- HG.72 Lisanõuded lepingutele SAN teenusepakkujatega

Teabe käideldavus (K)

- HK.17 Lisanõuded kõrgkäideldavusega salvestivõrkudele
- HK.19 Liiasuse nõue salvestivõrkudes

Teabe terviklus (T)

- HT.37 Andmete krüpteerimise nõue transpordil ja salvestamisel
- HT.57 Algparoolide muutmise regulaarkontroll
- HT.58 Lisanõuded tarbetute kontode ja terminalide blokeerimisele
- HT.59 Lisanõuded turvalisele sisselogimisele
- HT.69 Lisanõuded salvestivõrgu administreerimiskonfiguratsiooni seirele
- HT.70 Lisanõuded salvestisüsteemide haldusvõrgule

Teabe konfidentsiaalsus (S)
-

B 3.304 Virtualiseerimine

IT-süsteemide virtualiseerimisel käitatakse ühel füüsilisel arvutil üht või mitut virtuaalset IT-süsteemi. Sellist füüsilist arvutit nimetatakse virtualiseerimisserveriks. Mitmeid selliseid virtualiseerimisserverid saab tihti koondada üheks virtuaalseks taristuks. Sellises virtuaalses taristus saab virtualiseerimisservereid ja nendel käitatavaid virtuaalseid IT-süsteeme koos hallata.

IT-süsteemide virtualiseerimine loob mitmesuguseid eeliseid IT-töö korraldamiseks IT-koosluses. Serveri ressursside efektiivsema kasutamisega on võimalik kokku hoida riistvarale, elektrienergiale ja konditsioneerimisele tehtavaid kulutusi. Sellega seotud tsentraliseerimise ja konsolideerimise, samuti IT-süsteemide lihtsustatud valmisoleku tõttu on võimalik vähendada ka personalile ja haldusele tehtavaid kulutusi. Virtualiseerimise võimalused aga muudavad IT-koosluste haldamise keerukamaks. Kuna virtualiseerimistehnika kasutamine puudutab IT-koosluse erinevaid valdkondi ja tegevusalasid, tuleb ühendada erinevate valdkondade teadmisi ja kogemusi.

Konkreetse IT-koosluse kaitsevajaduse kindlaksmääramisel tuleb arvesse võtta virtualiseerimisserverite ja virtuaalsete IT-süsteemide kasutamist. Tuleb silmas pidada, et virtualiseerimisserveri kaitsevajadust mõjutab sellel rakendatavate virtuaalsete IT-süsteemide kaitsevajadus. Virtualiseerimisserveri või ühe virtuaalse IT-süsteemi probleemid võivad avaldada mõju kõikidele teistele virtualiseerimisserveril käitatavatele virtuaalsetele IT-süsteemidele.

Käesolevas moodulis kirjeldatakse, kuidas on IT-koosluses võimalik juurutada IT-süsteemide virtualiseerimist ning millistel tingimustel on virtuaalseid infrastruktuure IT-koosluses võimalik turvaliselt käitada.

Temaatiline piiritlemine

Käesolevas moodulis käsitletakse ainult täielike IT-süsteemide virtualiseerimist, teisi tehnikaid, mida on osaliselt samuti võimalik siduda sõnaga „virtualiseerimine” (rakenduste virtualiseerimine terminalserveri abil, Storage -virtualiseerimine jne), ei käsitleta käesolevas moodulis. Selles võetakse vaatluse alla virtualiseerimisserverid ja virtuaalsed IT-süsteemid, milles funktsioneerivad operatsioonisüsteemid, mida kasutatakse tihti ka otse füüsilistel IT-süsteemidel.

Tarkvaraarenduses kasutatakse mõisteid virtuaalne masin ja virtuaalse masina monitor (VMM) mõnikord ka teatud kindlate käituskeskkondade jaoks, näiteks Java või Dot-NET (Microsoft NET) kasutamisel. Taolisi käituskeskkondi käesolevas moodulis samuti ei käsitleta.

Ohud

Virtualiseerimisserverite ja virtuaalsete IT-süsteemide turvalist käitamist mõjutavad mõned uued organisatsioonilised ja tehnilised ohud, mis on tingitud virtualiseerimisserveri mitmesugustest funktsioonidest ja virtuaalsete IT-süsteemidega manipuleerimise võimalusest. See on seotud sellega, et tekib uus taristu osa, nimelt IT-objektide virtualiseerimise taristu. Samuti võivad virtuaalsed IT-süsteemid üle minna uude seisundisse. Nii võib väljalülitatud süsteem olla siiski aktiivne , kui

see on külmutatud üksnes virtualiseerimistarkvara abil. Lisaks sellele ammenduvad virtuaalsete IT-süsteemide elutsüklid tavaliselt oluliselt kiiremini.

Infosüsteemide etalonturbes peetakse virtuaalsete infrastruktuuride kasutamisel tüüpiliseks järgmisi ohtusid:

Organisatsioonilised puudused

- G 2.29 Tarkvara testimine tootmisandmetega
- G 2.32 Võrgu ebapiisav võimsus
- G 2.37 Sideliinide kontrollimatu kasutamine
- G 2.60 Võrgu- ja süsteemihalduse puuduv või ebasobiv strateegia
- G 2.148 Virtualiseerimise puudulik planeerimine
- G 2.149 Virtuaalsete IT-süsteemide ebapiisav salvestusvõimsus
- G 2.150 Külastaja tööriistade väär integreerimine virtuaalsetes IT-süsteemides
- G 2. 151 Virtuaalsetel IT-süsteemidel kasutatavate rakenduste ebapiisav tootjatugi

Inimvead

- G 3.16 Väär pääsuõiguste haldus
- G 3.28 Võrgu aktiivkomponentide ebasobiv konfiguratsioon
- G 3.36 Sündmuste väär tõlgendamine
- G 3.79 SAN salvestivõrgu ressursside vale jaotamine
- G 3.99 Virtualiseerimisserveri valed võrguühendused
- G 3.100 Virtuaalsete IT-süsteemide snapshot'ide ebakompetentne kasutamine
- G 3.101 Külastaja tööriistade väär kasutamine virtuaalsetes IT-süsteemides
- G 3.102 Aja vale sünkroniseerimine virtuaalsetes IT-süsteemides

Tehnilised rikked

- G 4.74 IT-komponentide tõrge virtualiseeritud keskkonnas
- G 4.75 Virtualiseerimiskeskkondade võrgutaristu rike
- G 4.76 Virtualiseerimissüsteemide haldusserverite tõrge
- G 4.77 Külastaja tööriistade valest funktsioonist virtuaalses keskkonnas tingitud ressursside kitsaskohad
- G 4.78 Virtuaalsete masinate väljalangemine lõpetamata andmevarundusprotsesside tõttu

Ründed

- G 5.29 Andmekandjate volitamata kopeerimine
- G 5.133 Veebipõhiste administreerimisvahendite volitamata kasutamine
- G 5.147 Volitamata lugemine või segamine virtualiseerimisvõrgus
- G 5.148 Virtualiseerimisfunktsioonide kuritarvitamine
- G 5.149 Külalistööriistade kuritarvitamine virtuaalsetes IT-süsteemides
- G 5.150 Virtuaalsete IT-süsteemide hüperviisori kompromiteerimine

Soovitatavad meetmed

IT-koosluse turvalisuse tagamiseks tuleb lisaks käesolevale moodulile rakendada veel teisigi mooduleid vastavalt infosüsteemide etalonturbe rakendusjuhendi modelleerimise tulemustele. Virtualiseerimisserverite ja virtuaalsete IT-süsteemide modelleerimisel on vajalik silmas pidada järgmist:

- Moodulit B 3.304 Virtualiseerimine tuleb rakendada igale virtualiseerimisserverile või igale virtualiseerimisserverite grupile. Virtualiseerimisserver on füüsiline IT-süsteem (klient või server), millel toimub IT-süsteemide käitamine. Lisaks moodulile B 3.304 Virtualiseerimine tuleb virtualiseerimisserverile rakendada ka kolmandasse kihti kuuluvaid serveri või kliendi mooduleid.
- Lisaks füüsilistele IT-süsteemidele ja virtualiseerimisserveritele tuleb (virtuaalsed masinad, VM-d) infosüsteemide etalonturbe kataloogi moodulite abil modelleerida ka virtuaalsed IT-süsteemid. VM-de modelleerimine toimub põhimõtteliselt sarnaselt füüsiliste IT-süsteemide modelleerimisega, st et kaasatakse olulise tähtsusega moodulid kihtidest 3 ja 5. Kuna praktika näitab, et seatakse sisse palju VM-e, on nende otstarbekas modelleerimine tihti võimalik vaid sobivate gruppide moodustamise teel.
- Gruppide moodustamiseks kehtivad VM-de puhul samad reeglid nagu füüsiliste IT-süsteemide puhul. Põhimõtteliselt võib grupiks liita ka sellised VM-d, mis töötavad erinevatel füüsilistel IT-süsteemidel. Täiendavaid nõuandeid virtuaalsete IT-süsteemide modelleerimiseks leidub meetmes M 2.392 Virtualiseerimisserverite ja virtuaalsete IT-süsteemide modelleerimine .

Planeerimine ja kontseptsioon

Virtuaalse infrastruktuuri planeerimisel tuleb kinni pidada tervest reast raamtingimustest. Lisaks kasutatavale virtualiseerimistehnikale ja vastavatele toodetele (vt M 1.74 Virtuaalse taristu planeerimine) ning virtualiseerimisel kõne alla tulevate süsteemide sobivusele (M 2.444 Virtuaalsete IT-süsteemide ressursside planeerimine) tuleb kindlasti planeerida ka tulevane võrgustruktuur (M 5.153 Võrgu planeerimine virtuaalsete taristute jaoks). Peale selle tuleb kohandada terve rida organisatsioonilisi eeskirju.

Kuna virtualiseerimisserverid sobivad eriti katse- ja arenduskeskkondade üleehitamiseks, tuleks koostada detailsed eeskirjad nendes keskkondades töödeldud andmetega ümberkäimiseks (M 2.82 Tüüptarkvara testimisplaani väljatöötamine).

Soetamine

Virtualiseerimisserveri riistvara valikul tuleb tähelepanu pöörata asjaolule, et soetataks süsteemid, mis sobivad valitud virtualiseerimislahendusega. Süsteemid peavad olema küllalt hea töövõimega, et tagada kõigi planeeritud virtuaalsete IT-süsteemide piisav jõudlus (M 2.445 Sobiva riistvara valimine virtualiseerimiskeskkondade jaoks).

Rakendamine

Virtuaalse infrastruktuuri rajamine või virtualiseerimisserveri installeerimine võib toimuda organisatsiooni harjumuspäraseid protseduure kasutades (B 3.101 Server). Virtualiseerimisprojekti keerukuse astet ei tohiks siiski alahinnata, seepärast tuleb arvestada mõningate omapäradega võrkude konfigureerimisel (M

5.154 Virtuaalse taristu võrgu turvaline konfiguratsioon) ja virtualiseerimisserverite administratiivpääsude (M 2.446 Haldustoimingute jaotus virtualiseerimisserverite puhul) loomisel.

Virtuaalsete süsteemide valmisolekuks virtualiseerimisserveritel tuleb virtuaalsete IT-süsteemide installeerimise organisatsioonilisi meetmeid (M 2.447 Virtuaalsete IT-süsteemide turvaline kasutamine) täiendada tehniliste meetmetega (M 4.346 Virtuaalsete IT-süsteemide turvaline konfigureerimine), et tagada nende häireteta talitlus.

Tegelikel virtualiseerimisserveritel tuleks võimalusel kasutada vaid virtualiseerimistehnika hulka kuuluvaid teenuseid. Teisi teenuseid tuleks pakkuda virtualiseeritud instantsides (või süsteemidel väljaspool virtuaalset taristut).

Kasutamine

Meetmed M 2.448 Virtuaalsete taristute funktsiooni ja konfiguratsiooni kontroll ja M 4.349 Virtuaalse taristu turvaline kasutamine moodustavad põhialuse nii virtualiseerimisserverite kui ka virtuaalsete IT-süsteemide turvaliseks talitluseks. Lisaks selle tuleb järgida meedet M 4.348 Aja sünkroniseerimine virtuaalsetes IT-süsteemides .

Valmisolek hädaolukorraks

Virtualiseerimisserverite ettevalmistamisel hädaolukorraks tuleks arvestada asjaoluga, et mida rohkem IT-süsteeme ühel virtualiseerimisserveril rakendatakse, seda suurem on potentsiaalne kahju. Seetõttu peab kõigi virtuaalsete süsteemide üldine kaitsevajadus põhinema virtualiseerimiskomponentide kaitsevajadusel (M 6.138 Hädaolukorraks valmisoleku plaani koostamine virtualiseerimiskomponentide tõrke puhuks).

Alljärgnevalt tutvustatakse turvameetmete kogumit, mida tuleb rakendada valdkonnas „Virtualiseerimine“ :

Planeerimine ja kontseptsioon

- (L) M 1.74 Virtuaalse taristu planeerimine
- (M) M 2.82 Tüüptarkvara testimisplaani väljatöötamine
- (M) M 2.314z Kõrgkäideldava serveriarhitektuuri kasutamine
- (L) M 2.392 Virtualiseerimisserverite ja virtuaalsete IT-süsteemide modelleerimine
- (L) M 2.444 Virtuaalsete IT-süsteemide ressursside planeerimine
- (L) M 2.477 Virtuaaltaristu planeerimine
- (L) M 3.70w Sissejuhatus virtualiseerimisse
- (M) M 3.71 Virtuaalkeskkondade administraatorite koolitamine
- (M) M 5.153 Võrgu planeerimine virtuaalsete taristute jaoks

Soetamine

- (L) M 2.445 Sobiva riistvara valimine virtualiseerimiskeskkondade jaoks

Rakendamine

- (M) M 2.83 Tüüptarkvara testimine
- (M) M 2.446 Haldustoimingute jaotus virtualiseerimisserverite puhul

- (L) M 2.447 Virtuaalsete IT-süsteemide turvaline kasutamine
- (M) M 3.72w Virtualiseerimistehnika põhimõisted
- (M) M 4.97z Ainult üks teenus serveri kohta
- (L) M 4.346 Virtuaalsete IT-süsteemide turvaline konfigureerimine
- (M) M 4.347z Virtuaalsete IT-süsteemide snapshot'ide desaktiveerimine
- (M) M 5.154 Virtuaalse taristu võrgu turvaline konfiguratsioon

Kasutamine

- (M) M 2.448 Virtuaalsete taristute funktsiooni ja konfiguratsiooni kontroll
- (L) M 2.449z Konsooli kaudu virtuaalsetele IT-süsteemidele juurdepääsu minimaalne kasutamine
- (M) M 4.348 Aja sünkroniseerimine virtuaalsetes IT-süsteemides
- (L) M 4.349 Virtuaalse taristu turvaline kasutamine

Valmisolek hädaolukorraks

- (M) M 6.138 Hädaolukorraks valmisoleku plaani koostamine virtualiseerimiskomponentide tõrke puhuks

B 3.305 Terminaliserver

Terminaliserverid võimaldavad kesksete ressursside kasutamist mitme kliendi poolt. Ressurssideks võivad olla serveri operatsioonisüsteemi koostisosad, standardrakendused või käsurida. Nii saab võimaldada ligipääsu rakendustele, ilma et need peaks kliendil installeerima. Reeglina pääseb terminaliserveril paiknevatele rakendustele korraga ligi mitu võrgus paiknevat klienti.

Terminaliserverid kujutavad endast kesksel koondatud stsenaariumit klientserveri arhitektuuris. Rakendused installeeritakse suure jõudlusega terminaliserveritele, millelt kliendid saavad neid käivitada ja juhtida. Neid sisendeid ja väljundeid saab vastava klienttarkvaraga hallata võrdlemisi lihtsalt varustatud töökohaarvutitel (Fat Clients). Peale selle on olemas lahendused, mis toimivad spetsiaalsete terminalidega (Thin Clients).

Selles moodulis näidatakse süstemaatiliselt, kuidas koostada institutsioonisiseselt terminaliserveri kasutuskontseptsiooni ja kuidas on võimalik tagada selle realiseerimist ja sidumist ülejäänud süsteemiga. Seda tuleb kasutada vaadeldud informatsioonikogumi igal terminaliserveril.

Mooduli piiritlemine

Selle mooduli sisuks on terminaliserverite puhul esinevad ohud ja rakendatavad meetmed. Arvestada tuleb mooduliga B 3.101 Server . Kui terminaliserveri kliendil teostatakse iseseisvat operatsioonisüsteemi, mida ei saada serverilt, tuleb järgida moodulit B 3.102 Server Unixi all . Terminaliserverite teenuseid saavad kasutada mitmed operatsioonisüsteemid, näiteks Unix või Linux, Windows ja z/OS .

Üksikud teostused erinevad üksteisest mitmete punktide poolest, näiteks:

- kasutatava edastusprotokolli poolest,
- nõudmiste poolest võrgu ülekandekiirusele,
- nõudmiste poolest serveri kiirusele,
- jaotatud ressursside kasutamise poolest ja
- eelkõige erineva konfiguratsiooni ja halduse tõttu, selle teenuse taga töötavas operatsioonisüsteemis.

Terminaliserveri turvalisusest lähtuvalt on oluline kasutada lisaks mooduleid, mis kehtivad vastavale operatsioonisüsteemile.

Ohud

Infosüsteemide etalonturbe seisukohast on terminaliserverit kasutava võrgu põhilisteks ohuallikateks:

Vääramatud jõud

- G 1.2 IT-süsteemi avarii

Organisatsioonilised puudused

- G 2.7 Õiguste volitamata kasutamine
- G 2.32 Võrgu ebapiisav võimsus
- G 2.36 Kasutajakeskkonna ebasobiv piiramine

- G 2.153 Terminaliserveri keskkonna edastuskanalite piisamatu turve
- G 2.154 Ebasobivad rakendused terminaliserveritel kasutamiseks

Inimvead

- G 3.9 IT-süsteemi väär haldus
- G 3.16 Väär pääsuõiguste haldus
- G 3.38 Vead konfigureerimisel ja kasutamisel

Tehnilised rikked

- G 4.10 Keerukad ligipääsuvõimalused võrgustatud IT-süsteemides
- G 4.12 Autentimisvõimaluste puudumine X-serveri ja X-kliendi vahel
- G 4.22 Tüüptarkvara turvaaugud või vead
- G 4.33 Autentimise puudumine või puudulikkus
- G 4.35 Ebaturvaline krüptoalgoritm
- G 4.81 Laiendatud õigused terminaliserveril programmdialoogi kaudu
- G 4.82 Terminaliserveri rivist väljalangemine ja mitte kättesaadavus

Ründed

- G 5.19 Kasutajaõiguste väärkasutus
- G 5.23 Viirused
- G 5.112 ARP-protokolli tabelitega manipuleerimine
- G 5.161 Võltsitud vastused XDMCP-levisaatele terminaliserveritel
- G 5.162 X-Windowsi seansside ümberjuhtimine

Soovitatavad meetmed

Vaadeldava IT-koosluse turvalisuse tagamiseks tuleb lisaks käesolevale moodulile rakendada veel teisigi mooduleid vastavalt infosüsteemide etalonturbe rakendusjuhendi modelleerimise tulemusele.

Terminaliserveri edukaks ülesehituseks tuleb teostada rida meetmeid, alustades kontseptsiooniga, sealt edasi serveri hankimine ja kuni käitamiseni välja. Järgnevalt on ära toodud sammud, mida seejuures läbitakse ning meetmed, mida vastava sammu juures jälgida tuleb.

Planeerimine ja kontseptsiooni loomine

Terminaliserveri plaanimisel tuleb arvestada mitmete raamtingimustega. Esimese sammuna tuleks täiendada infoturbe suuniseid detailse terminaliserveri suunise võrra (vt M 2.464 Infoturbesuuniste loomine terminaliserveri kasutamiseks). Siin kirjalikult äratoodud meetmed ja sihid peavad peegeldama turvalise terminaliserveri keskkonna tingimusi ja nõudeid. Olemasoleva klient-server-arhitektuuri migratsioonil terminaliserveri toega keskkonda tuleb enne teostust põhjalikult kontrollida, kas teisaldatavad rakendused on selleks sobilikud (vt M 2.466 Migratsioon terminaliserveri arhitektuurile).

Mitme kasutajaga keskkonnas nagu terminaliserveri süsteem on olulise tähtsusega klientide eraldamine üksteisest ja riskantsetest süsteemifunktsioonidest. Et kindlustada tõrgetevaba käitust ja tagada seansisiseste andmete konfidentsiaalsus, tuleb laiali jagada piiravad õigused (vt M 5.163 Piirav õiguste jaotus terminaliserveritel).

Terminaliserverit saab kasutada juhtudel, kus kliendid pääsevad ligi sisudele ebaturvalistes võrkudes, näiteks veebilehekülgedel, mis sisaldavad aktiivsisusid. Kliendi asemel suhtleb ebaturvalise võrgu kaudu terminaliserver ja kliendile edastatakse ainult sisud. Terminaliserverit, mis kliendi asemel siseneb ebaturvalisse võrku, nimetatakse graafiliseks tulemüüriks (vt M 4.365 Terminaliserveri kasutamine graafilise tulemüürina).

Soetamine

Kui seni klient serveril põhineval võrguarhitektuuril kasutatud rakendused soovitakse teha terminaliserveril kesksel kättesaadavaks, tuleb enne teisaldamist kontrollida litsentsiõigusi puudutavaid lepinguid ja vajadusel muretseda uus tarkvara (vt M 2.486 Veebirakenduste arhitektuuri dokumenteerimine).

Rakendamine

Terminaliserveri infrastruktuuri haldamine vajab eelneva kogemuseta administraatorite ja kasutajate korral selgitamist. Kõiki isikuid, kes töötavad terminaliserveri süsteemiga, tuleb koolitada (vt M 3.81 Koolitamine terminaliserveri turvaliseks kasutamiseks).

Kasutamine

Kasutajatel ei tohi olla võimalik muuta terminaliserveri kasutajakeskkonda ja nad võivad pääseda ligi ainult ressurssidele, millele neil peab ligipääs olema (vt M 4.367 Klientrakenduste turvaline kasutamine terminaliserveril). Kui ühendus terminaliserveri ja tema klientide vahel toimub ebaturvalise võrgu kaudu, tuleb kasutusele võtta meetmed, et kommunikatsiooni ei oleks võimalik pealt kuulata, muuta ega häirida (vt M 5.164 Terminaliserveri turvaline kasutamine kaugvõrgust).

Väljavahetamine

Kui terminaliserver, terminaliserveriga ühendatud klient või terminaliserveri keskkonna infrastruktuurikomponent tahetakse kasutuselt kõrvaldada, tuleks arvestada meetmega M 2.469 Terminaliserveri keskkonnast komponentide korrastatud eemaldamine .

Valmisolek hädaolukorraks

Kuna terminaliserveri keskkonna rivist väljalangemisest on mõjutatud suur hulk kasutajaid, tuleb kasutusele võtta meetmed, mis rivist väljalangemise korral vähendaksid kahju. Terminaliserveri võrgustiku kaudu on võimalik täita ka kõrgeid nõudeid kättesaadavusele (vt M 6.142 Redundantsete (ressurssi osaliselt või täielikult dubleerivate) terminaliserverite kasutamine).

Kui terminaliserveri klient langeb rivist välja, ei ole vastaval kasutajal võimalik terminaliserveril paiknevatele rakendustele ligi pääseda. Seetõttu on ilma oma operatsioonisüsteemita (Thin Clients) terminalide korral vaja võtta kasutusele varumehhanismid (vt M 6.143 Terminaliserveri kliendi kasutuselevõtt katkestuse järgselt).

Kui rakendused installeeritakse ennetavalt nii terminaliserveril kui ka klient-PC-l, saab hädaolukorras ajutiselt käituses hoida hädakäitust (M 6.144 Terminaliserveri kliendi konfiguratsioon duaalseks kasutamiseks tava klient PC-na).

Alljärgnevalt tutvustatakse meetmete kogumit, mida tuleb rakendada valdkonnas “Terminaliserver”:

Planeerimine ja kontseptsiooni loomine

- (L) M 2.464 Infoturbesuuniste loomine terminaliserveri kasutamiseks
- (L) M 2.465 Terminaliserveri vajalike ressursside analüüs
- (L) M 2.466 Migratsioon terminaliserveri arhitektuurile
- (L) M 2.467 Terminaliserveri regulaarsete taaskäivitustsüklite plaanimine
- (M) M 4.250z Keskse võrgupõhise autentimisteenuse valimine
- (M) M 4.365z Terminaliserveri kasutamine graafilise tulemüürina
- (L) M 5.64z Secure Shell (SSH)
- (L) M 5.162 Ribalaiuse planeerimine terminaliserverite kasutamisel
- (L) M 5.163 Piirav õiguste jaotus terminaliserveritel

Soetamine

- (L) M 2.468z Tarkvaralitsentsid terminaliserveri keskkonnas

Rakendamine

- (L) M 3.81 Koolitamine terminaliserveri turvaliseks kasutamiseks
- (L) M 4.9 X Windowsi turvamehhanismid
- (L) M 4.106 Süsteemi logimise aktiveerimine (Unix)
- (M) M 4.366 Liikuvate kasutajaprofiilide turvaline konfiguratsioon terminaliserveri keskkonnas
- (L) M 5.72 Mittevajalike võrguteenuste desaktiveerimine (Unix)

Kasutamine

- (L) M 2.273 Turvalisust mõjutavate paikade ja värskenduste kiire paigaldamine
- (L) M 4.3 Viirustõrjeprogrammi regulaarne kasutamine
- (M) M 4.367 Klientrakenduste turvaline kasutamine terminaliserveril
- (M) M 4.368 Terminaliserveri keskkonna regulaarne audit
- (M) M 5.164 Terminaliserveri turvaline kasutamine kaugvõrgust

Väljavahetamine

- (L) M 2.469 Terminaliserveri keskkonnast komponentide korrastatud eemaldamine

Valmisolek hädaolukorraks

- (M) M 6.142z Redundantsete (ressurssi osaliselt või täielikult dubleerivate) terminaliserverite kasutamine
- (M) M 6.143 Terminaliserveri kliendi kasutuselevõtt katkestuse järgselt
- (M) M 6.144z Terminaliserveri kliendi konfiguratsioon duaalseks kasutamiseks tava klient PC-na

B 3.401 Kodukeskjaam (PBX)

Kodukeskjaama all mõeldakse ISKE rakendusjuhendis PBX telefoni keskjaama. Kodukeskjaama (PBX) abil on võimalik ühendada majasisesed telefonid omavahel ning liita nad avaliku telefonivõrguga (public switched telephone network , PSTN). Sõltuvalt lõppseadmetest võib lisaks kõnetelefonidele kasutada ka muid teenuseid. Nii on kodukeskjaama abil võimalik edastada andmeid, tekste, graafikuid ja liikuvaid pilte.

Infot vahendatakse seejuures analoogselt või digitaalselt traadiga või traadita edastusmeediumi kaudu. Sõltuvalt ühendusest ja kasutatud andmevõrkudest võivad asutuse sideseadmed olla järgmised.

Tavapärased keskjaamad

Tavapäraste keskjaamade puhul kasutatakse ühenduse loomiseks ja ülekandeks olenevalt olemasolevast tehnikast eraldi võrku. Keskjaama külge võivad olla ühendatud näiteks telefonid, faksiaparaadid, modemid ja telefonide automaatvastajad.

VoIP-süsteem

Voice over IP (VoIP) ehk IP-kõne korral kasutatakse lõppseadmete keskjaamaga ühendamiseks mitte eraldi keskjaama infrastruktuuri, vaid ühendus luuakse IP-andmevõrguga oma kaabli kaudu. VoIP-i korral suhtlevad lõppseadmed keskjaamaga või teiste VoIP-seadmetega IP-l põhinevate signalisatsioonide ja meediatransportlogide kaudu. Avalikku telefonivõrku ühendamine toimub asutuse pääslarakenduse kaudu.

Hübriidsüsteem / Hübriidjaam

Kuna VoIP-ide tähtsus üha kasvab, pakutakse kodukeskjaamu, mis ühendavad tavatelefone VoIP-telefonidega. Niinimetatud hübriidjaamadel on lisaks tavapärastele keskjaamadele ühendus andmevõrku, kus IP-telefonid suhtlevad kodukeskjaamaga. Hübriidjaama abil saab korraga käitada tavapäraseid digitaal- või analoogtelefone ja VoIP-telefone. Samuti on hübriidjaamaga võimalik samm-sammult migreeruda VoIP-infrastruktuuri.

IP-ühendus

VoIP-i kasutamisel võib RSTN-ühendus olla asutusevälisel teenuspakkujal. Majasisene VoIP-süsteem suhtleb ka asutusevälise teenusepakkujaga interneti (IP) kaudu. Sellist varianti nimetatakse IP-seadmeühenduseks.

Üldiselt võiks öelda, et kuna suured kodukeskjaamapakkujad vahetavad tavapärase telefonivõrgu välja ühtsel IP-l põhinevate lahendustega (next generation network), siis ei ole enam võimalik andme- ja keeletranspordi vahel vahet teha. Sellel on mõju ka majasisese telefoniseadme ja keskjaamateenuse pakkuja vahelisele liidesele.

Käesolevas moodulis vaadeldakse eelkõige tavapäraseid kodukeskjaamu ähvardavaid ohte ja nendega toimetulemise meetmeid. Moodulis kirjeldatut võib vaadelda kui kõigi keskjaamade kohta käivat teavet, olenemata hiljem kasutatavast tehnoloogiast. Kõiki tavapärasest keskjaamast erinevaid valdkondi on lisaks käsit-

letud vastavates moodulites, nagu nt VoIP (B 4.7 IP-kõne (VOIP)) või mobiilsed ja traadita süsteemid (nt B 3.404 Mobiiltelefon).

Järgneb ülevaade ohtude paketist valdkonnas „Kodukeskjaam”:

Ohud

Infosüsteemide etalonturbe seisukohalt loetakse kodukeskjaama puhul tüüpilisteks järgmisi ohuallikaid:

Vääramatu jõud

- G 1.2 IT-süsteemi avarii
- G 1.10 Laivõrgu tõrge

Organisatsioonilised puudused

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.2 Reeglite puudulik tundmine
- G 2.5 Hoolduse puudumine või puudulikkus

Inimvead

- G 3.7 Käsitsemisvea tõttu tekkinud kodukeskjaama (PBX) rike
- G 3.9 IT-süsteemi väär haldus
- G 3.16 Väär pääsuõiguste haldus

Ründed

- G 5.10 Kaughooldeportide väärkasutus
- G 5.11 Kodukeskjaamas (PBX) salvestatud andmete konfidentsiaalsuse kadu
- G 5.12 Telefonikõnede ja andmesaadetiste pealtkuulamine
- G 5.13 Pealtkuulamine kodukeskjaama (PBX) lõppseadmete ruumides
- G 5.14 Telefoniteenuste vargus
- G 5.15 Kodukeskjaama rakenduste väärkasutus
- G 5.16 Ohud hoolde- ja haldustööde ajal
- G 5.42 Inimestega manipuleerimine (Social Engineering)
- G 5.44 Kodukeskjaama (PBX) kaughooldusportide väärkasutus
- G 5.71 Tundliku informatsiooni konfidentsiaalsuse kadu

Soovitatavad meetmed

Selleks, et tagada kogu loetletud info turvalisus, tuleb lisaks käesolevale moodulile rakendada veel ka teisi, IT-etalonturbe modelleerimise käigus selguvaid mooduleid.

Siia kuulub näiteks moodul B 4.5 IT-süsteemi kohtvõrguühendus ISDN kaudu , milles käsitletakse IT-süsteemi ISDN-i kaudu, mida saab kasutada kõigi ISDN-i kaudu realiseeritavate välisühenduste puhul. Samuti tuleks järgida vastavaid lõike

moodulitest B 3.204 Klient Unixi all , B 4.6 Traadita kohtvõrgud ja B 4.7 IP-kõne (VOIP) . Kodukeskjaama kesksed seadmed tuleks kõik üles seada ühte ruumi, mis vastab kas serveriruumile (B 2.4 Serveriruum) või tehnilise infrastruktuuri ruumile (B 2.6 Tehnilise infrastruktuuri ruum) esitatavatele nõuetele. Kodukeskjaama kaabeldustööde kohta leiate infot moodulist B 2.2 Elektrotehniline kaabeldus .

Kodukeskjaama puhul tuleb rakendada erinevaid meetmeid, tegeldes soetamisplaani ja käitamisega kuni hädaolukorraks valmisoleku plaanini välja. Järgnevalt anname ülevaate erinevatest kohustuslikest etappidest ja meetmetest, mida tuleb iga etapi puhul rakendada.

Planeerimine ja kontseptsioon

Kodukeskjaama planeerimisel tuleks järgida moodulis M 2.471 Kodukeskjaama rakendamise planeerimine toodud meetmeid. Keskjaama kasutuselevõtuks ja korrektseks kasutamiseks tuleks koostada juhend (M 2.472 Kodukeskjaama (PBX) turvajuhendi koostamine).

Soetamine

Peamised sammud, mida kodukeskjaama valimisel tuleb järgida, on kirjas meetmes M 2.105 Kodukeskjaama soetamine .

Rakendamine

Installeerimise käigus tuleb tootja poolt eelseadistusega määratud paroolid kindlasti ära muuta, kuna vastasel korral saavad suvalised ründajad keskjaama manipuleerida. Samuti tuleb turvaliseks muuta kõik liidesed. Konfigureerimisel tuleb lähtuda põhireeglist, et kõik mittevajalikud funktsioonid tuleb välja lülitada, sest nende tööshoidmine toob endaga kaasa vaid tarbetuid riske (vt M 5.14 Sisemiste kaugpöörduste turve ja M 5.15 Väliste kaugpöörduste turve).

Ruumi, kus kodukeskjaam asub, võivad siseneda vaid isikud, kellel on volitus teostada kodukeskjaama tehnilisi hooldustöid.

Kasutamine

Kodukeskjaama juures tehtavad haldustööd tuleks võimalusel logida, et hiljem oleks võimalik järele vaadata, kuidas on turvalisust puudutavaid seadistusi muudetud, vt M 4.5 Kodukeskjaama (PBX) haldustööde logi . Kõrgete turvanõuete korral tuleb kodukeskjaamas kasutatavat konfiguratsiooni regulaarselt revideerida (vt M 4.6 Kodukeskjaama (PBX) konfiguratsiooni läbivaatus). Kuna vägagi tihti on turvalisuse kadu seotud lõppseadme väärkasutusega, tuleks töötajaid informeerida seadme korrektsest kasutamisest. Samuti tuleks neid regulaarselt teavitada seadme kasutamisega seotud võimalikest ohtudest (vt M 3.82 Kodukeskjaama turvalise kasutamise koolitus).

Valimisolek hädaolukorraks

Kodukeskjaama hädaolukorraks valmisolek eeldab selleks vajalike meetmete rakendamist. Lisaks tuleb keskjaama konfiguratsiooniandmeid regulaarselt varundada, et võimaliku avarii korral oleks võimalik jaam kiiresti töökorda seada ja vajalikul moel konfigureerida (vt M 6.145 Kodukeskjaama (PBX) hädaolukorraks valmisolek).

Alljärgnevalt tutvustatakse meetmete kogumit, mida tuleb rakendada valdkonnas „Kodukeskjaam”:

Planeerimine ja kontseptsioon

- (L) M 2.27z Kodukeskjaama (PBX) hooldus
- (L) M 2.470 Kodukeskjaama nõudlusanalüüsi läbiviimine
- (L) M 2.471 Kodukeskjaama rakendamise planeerimine
- (L) M 2.472 Kodukeskjaama (PBX) turvajuhendi koostamine
- (L) M 2.473 Kodukeskjaama (PBX) teenusepakkuja valimine

Soetamine

- (L) M 2.105w Kodukeskjaama soetamine

Rakendamine

- (L) M 4.7 Algparoolide muutmine
- (M) M 4.10 Kodukeskjaama (PBX) terminalide paroolikaitse
- (M) M 4.11 Kodukeskjaama (PBX) liideste turve
- (M) M 4.369 Telefoni automaatvastaja turvaline kasutamine
- (L) M 5.14 Sisemiste kaugpöörduste turve
- (L) M 5.15 Väliste kaugpöörduste turve

Kasutamine

- (L) M 3.82 Kodukeskjaama turvalise kasutamise koolitus
- (M) M 4.5 Kodukeskjaama (PBX) haldustööde logi
- (M) M 4.6 Kodukeskjaama (PBX) konfiguratsiooni läbivaatus.

Väljavahetamine

- (M) M 2.474 Kodukeskjaama (PBX) komponentide turvaline kasutuselt kõrvaldamine

Valmisolek hädaolukorraks

- (M) M 6.26 Kodukeskjaama (PBX) konfiguratsiooniandmete regulaarne varundus
- (M) M 6.145 Kodukeskjaama (PBX) hädaolukorraks valmisolek

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.6 Arvuti paroolkaitse rangemad reeglid
- HG.13 Lisanõuded andmete kaugedastuse hädaolukorraplaanile
- HG.25 Kaugpöörduste kohustuslik logimine
- HG.38 Turvapaikade paigaldatuse regulaarseire

Teabe käideldavus (K)
-
Teabe terviklus (T)

- HT.7 Kasutajate ja nende profiilide perioodiline seire
- HT.57 Algparoolide muutmise regulaarkontroll
- HT.58 Lisanõuded tarbetute kontode ja terminalide blokeerimisele
- HT.59 Lisanõuded turvalisele sisselogimisele

Teabe konfidentsiaalsus (S)

-

B 3.402 Faks

NB! Käesolev moodul kuulub rakendamisele ainult siis kui faksi kasutatakse andmekogu andmete käitlemisel!

Käesolevas punktis käsitletakse andmete edastamist faksi kujul. Faksi saatev seade loeb algmaterjali punkt punkti haaval sisse, edastab selle ning vastuvõttev seade väljastab selle sisseloetud kujul. Käesolevate IT-etalonturbe meetmete valikul ei ole eraldi arvestatud erinevate edastusstandarditega (nt CCITT grupp nr 3). Antud moodulis käsitletakse faksiseadmete tehnilise baasina eranditult vaid laiatarbekaubana tuntud eraldiseisvaid faksiaparaate, mitte paigaldatavaid faksikaarte ega ka faksiservereid (vt B 5.6 Faksiserver).

Ohud

Infosüsteemide etalonturbe seisukohalt loetakse faksi kaudu toimiva andmeedastuse puhul tüüpilisteks järgmisi ohuallikaid:

Organisatsioonilised puudused:

- G 2.20 Kulumaterjalide ebapiisav või vale varu

Inimvead:

- G 3.14 Faksi juriidilise siduvuse ülehindamine

Tehnilised rikked:

- G 4.14 Spetsiaalse faksipaberi pleekumine
- G 4.15 Faksi saatmine vääral aadressil

Ründed:

- G 5.7 Liinide pealtkuulamine
- G 5.30 Faksiaparaadi või -serveri volitamata kasutamine
- G 5.31 Saabuvate fakside volitamata lugemine
- G 5.32 Faksiaparaadi ja -serveri jääkinfo lugemine
- G 5.33 Väära identiteedi kasutamine faksi saatmisel
- G 5.34 Faksi sihtaadressiklahvide ümberprogrammeerimine
- G 5.35 Faksisaadetistest tulenev ülekoormus

Soovitatavad meetmed

Selleks, et tagada kogu loetletud IT-süsteemi turvalisus, tuleb lisaks käesolevale moodulile rakendada veel ka teisi, IT-etalonturbe modelleerimise käigus selguvaid mooduleid.

Faksiaparaatide puhul tuleb rakendada erinevaid meetmeid, tegeldes soetamise ja käitamisega kuni hädaolukorraks valmisoleku plaanini välja. Järgnevalt on välja toodud erinevad kohustuslikud etapid ja meetmed, mida iga etapi puhul tuleks rakendada.

Soetamine

Peamised sammud, mida faksiaparaadi valimisel tuleb järgida, on välja toodud meetmes M 2.49 Sobivate faksiaparaatide hankimine

Rakendamine

Faksiaparaadi installeerimisel tuleb jälgida, et seade saaks üles seatud nii, et selle kasutamine ja käsitsemine oleks võimalikult otstarbekohane. Aparaati kasutama hakkavad töötajad peavad saama koolituse, kuidas aparaadiga ümber käia.

Kasutamine

Kasutamise vältel tuleb hoolitseda selle eest, et faksiaparaadi kulumaterjale oleks alati varutud piisaval hulgal, et ükski sissetulev faks ei läheks kaduma ainuüksi seetõttu, et teatud ajahetkel on paber või tooner otsa saanud. Üldjuhul on mõttekas faksid varustada sobiva faksiplangiga, mis muudab nende hilisema identifitseerimise lihtsamaks. Faksiaparaadi võimalikku väärkasutust aitab tuvastada saatmis- ja vastuvõtuprotokollide regulaarne läbivaatamine ning aeg-ajalt tuleks kontrollida ka klahvide alla programmeeritud aadresse, et vältida fakside saatmist kogemata valel aadressil.

Väljavahetamine

Kulumaterjalide ja varuosade väljavahetamisel tuleb arvestada, et teatud seadmetes jäävad saadetud või vastuvõetud faksid vahekilede, trumlite või ka paberi peale alles. Seepärast ei tohi vastavaid materjale lihtsalt niisama olmeprügi hulka visata, vaid tuleb korraldada nende jäätmekäitlus kindlustamaks, et volitamata isikutel ei oleks hiljem võimalik neile ligi pääseda.

Alljärgnevalt tutvustatakse meetmete kogumit, mida tuleb rakendada valdkonnas „Faksiaparaat“:

Soetamine

- (L) M 2.49z Sobivate faksiaparaatide hankimine

Rakendamine

- (L) M 1.37 Faksiaparaadi õige paigutus
- (L) M 2.47 Faksi eest vastutaja
- (L) M 3.15 Kõigi töötajate juhendamine faksi kasutamise alal
- (M) M 4.36z Faksi adressaatnumbrite blokeerimine
- (M) M 4.37z Faksi saatjanumbrite blokeerimine

Kasutamine

- (M) M 2.48z Faksioperaator
- (M) M 2.51z Sissetulnud fakside kopeerimine
- (L) M 2.52 Faksimaterjalide varude jälgimine ja täiendamine
- (M) M 2.53z Faksi desaktiveerimine õhtul
- (M) M 4.43z Automaatse ümbrikusüsteemiga faksiaparaat
- (M) M 5.24z Sobiva faksiblanketi kasutamine
- (L) M 5.25 Saate- ja vastuvõtulogide kasutamine
- (M) M 2.26z Süsteemiülema ja ta asetäitja määramine
- (M) M 2.27z Kodukeskjaama (PBX) hooldus

- (M) M 2.28z Väline sidealase konsultatsiooni teenus

- (L) M 5.29 Sihtaadresside ja logide perioodiline kontroll

Väljavahetamine

- (L) M 2.50 Faksimaterjalide ja varuosade õige hävitamine

Valmisolek hädaolukorraks

- (L) M 6.39 Faksitoodete tarnijate loend asendushangeteks

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed
-
Teabe käideldavus (K)
-
Teabe terviklus (T)

- HT.35 Tavalise faksiteenuse kasutuskeeld

Teabe konfidentsiaalsus (S)
-

B 3.404 Mobiiltelefon

Kirjeldus

Selles moodulis käsitletakse mobiiltelefone, mis põhinevad GSM-standardil (Global System for Mobile communication, D- ja E-võrgud), UMTS- (Universal Mobile Telecommunications System) ja LTE-tehnoloogial (Long Term Evolution). Kuna LTE puhul kasutatakse helistamiseks andmepakettidel põhinevat andmevahetust, tuleb selle tehnoloogia korral täiendavalt arvestada ka mooduliga B 4.7 IP-kõne (VOIP) . Kui mobiiltelefoni puhul on tegemist nutitelefoniga, tuleb arvestada ka mooduliga B 3.405 Pihuarvuti (PDA) ning vajaduse korral ka mooduliga B 3.203 Sülearvuti . Mobiiltelefonide puhul, mis kasutavad VPN-tehnoloogiaid, nt selleks, et ühendada end institutsiooni võrguga, tuleks arvestada ka mooduliga B 4.4 Virtuaalne privaatvõrk (VPN) .

Mobiilivõrguga ühenduse loomiseks läheb mobiiltelefonil tarvis SIM-kaarti (SIM - Subscriber Identity Module). SIM-kaardi abil on võimalik eristada mobiilivõrgus kasutajat ja seadet.

Mobiiltelefon on varustatud rahvusvaheliselt üheselt loetava seerianumbriga (IMEI - International Mobile Equipment Identity). Abonent identifitseeritakse SIM-kaardile salvestatud numbri (IMSI - International Mobile Subscriber Identity) abil. IMSI number omistatakse abonendile teenusepakkuja poolt pärast lepingu sõlmimist. Tuleb meeles pidada, et tegu ei ole abonendile omistatavate telefoninumbritega (MSISDN) (vähemalt üks). Nende kahe lahutamisega on võimalik, et abonent saab oma SIM-kaardiga kasutada erinevaid mobiilsideseadmeid.

SIM-kaardile salvestatakse muu hulgas ka abonendiga seotud GSM-mobiiltelefoni telefoninumber (MSISDN). Samuti on sinna salvestatud krüptograafilised algoritmid, mida kasutatakse autentimisel ja kasutajaandmete krüpteerimisel (mobiiltelefoni ja baasjaama vahel).

Ohud

IT-etalonturbe seisukohalt loetakse mobiiltelefonide kasutamise puhul tüüpilisteks järgmisi ohuallikaid:
Organisatsioonilised puudused

- G 2.2 Reeglite puudulik tundmine
- G 2.4 Turvameetmete ebapiisav järelevalve
- G 2.7 Õiguste volitamata kasutamine
- G 2.200 Ebapiisav planeerimine mobiil- ja nutitelefonide ning tahvel- ja pihuarvutite soetamisel
- G 3.3 Hooletus turvameetmete suhtes

- G 3.43 Puudulik paroolihooldus
- G 3.44 Teabe hooletu kasutamine
- G 3.45 Sidepartnerite puudulik autentimine
- G 3.77 Infoturbe vähene aktsepteerimine
- G 3.123 Mobiil- ja nutitelefonide ning tahvel- ja pihuarvutite keelatud kasutamine eraotstarbel
- G 4.32 Sõnumi kaotsiminek
- G 4.41 Mobiilsidevõrgu rike
- G 4.42 Mobiiltelefoni või PDA tõrge
- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.4 Vargus
- G 5.27 Sõnumi salgamine
- G 5.94 SIM-kaardi kuritarvitamine
- G 5.95 Pealtkuulamine ruumis mobiiltelefonidega
- G 5.96 Mobiiltelefoni ehituse muutmine
- G 5.97 Volitamata andmeedastus mobiiltelefonide kaudu
- G 5.98 Mobiilikõnede pealtkuulamine
- G 5.99 Mobiiltelefonikõnede ühenduseandmete analüüs
- G 5.126 Volitamatu pildistamine ja filmimine kaasaskantavate seadmetega
- G 5.192 Helistaja või SMS-i saatja telefoninumbri võltsimine

Soovitatavad meetmed

Vaadeldava IT-koosluse turvalisuse tagamiseks tuleb tavaliselt peale käesoleva mooduli rakendada veel teisigi mooduleid, mis selguvad IT-etalonturbe rakendusjuhendi põhjal tehtava modelleerimise tulemusel. Mobiiltelefonide puhul tuleb võtta erinevaid meetmeid, mis on muu hulgas seotud nt planeerimise, kasutamise ja hädaolukordadeks valmisolekuga. Järgnevalt on esitatud ülevaade erinevatest kohustuslikest etappidest ja meetmetest, mida iga etapi puhul tuleks võtta.

Planeerimine ja kontseptsioon

Mobiiltelefonide turvalise kasutuse tagamiseks tuleks koostada asjakohased turvasuunised (vt M 2.188 Mobiiltelefonide kasutamise eeskirjad ja turvasuunised). Ettevõttel või ametiasutusel, kes varustab oma töötajaid töötelefonidega, mida kasutakse tihti ning mille omanikud pidevalt vahetuvad, võib olla mõttekas hoida mobiiltelefone ühes keskses kohas (vt M 2.190 Mobiilikogu sisseseadmine).

Rakendamine

Mobiiltelefonidesse on ka sisse ehitatud mitmeid turvamehhanisme, kuid need on erinevate mobiiltelefonide, SIM-kaartide ja võrguoperaatorite puhul erinevad. Täpsema ülevaate nimetatud turvamehhanismidest koos kasutamisjuhistega leiate meetmest M 4.114 Mobiiltelefonide turvamehhanismide rakendamine .

Kasutamine

Mobiiltelefonide nõuetekohane ja turvaline kasutamine eeldab teatud meetmete võtmist, mille alla kuulub nt toite tagamine ning vajaduse korral ka mobiiltelefoni numbrituvastuse tõkestamine (vt M 4.114 Mobiiltelefonide turvamehhanismide rakendamine ja M 5.79 Kaitse mobiiltelefoni numbri tuvastamise vastu). Kui seadmeid kasutatakse ka andmeedastuseks, tuleb täiendavalt tagada funkt-

sioonide turve ja ennetada andmeedastuse väärkasutust (vt M 5.81 Turvaline andmeedastus mobiiltelefoni kaudu). Telefoni võimaliku kaotuse korral tuleb väärkasutuse ja liigsete kulutuste vältimiseks SIM-kaart viivitamatult sulgeda (vt M 2.189 Mobiiltelefoni blokeerimine kaotamise korral). Töötajaid tuleb teavitada mobiiltelefonide kasutamisega seotud spetsiifilistest ohtudest (vt M 2.558 Töötajate mobiil- ja nutitelefonide ning tahvel- ja pihuarvutite infoturbe teadlikkuse suurendamine).

Ressursside väljavahetamine

Kuna mobiiltelefonid sisaldavad sageli ka konfidentsiaalseid andmeid, peab olema täpselt reguleeritud, kuidas need seadmed kasutusest kõrvaldatakse. Asjakohaseid soovitusi leiate meetmest M 4.465 Mobiil- ja nutitelefonide ning tahvel- ja pihuarvutite kasutuselt kõrvaldamine . Juhul kui seadmetes kasutatakse ka eemaldatavaid mälukaarte, võtke ka meedet M 2.13 Tundlike ressursside jäljetu hävitamine , kus kirjeldatakse, kuidas kõrvaldada kastutusest eemaldatavaid mälukaarte.

Valmisolek hädaolukorraks

Olulisemad juhised, kuidas mobiiltelefoni tõrkeid ja võimalikku kaotamist ennetada, on kokku võetud meetmesse M 6.72 Ettevaatusabinõud mobiiltelefoni tõrgete puhuks .

Järgneb ülevaade meetmete paketist „Mobiiltelefon".

Planeerimine ja kontseptsioon

- (L) M 2.188 Mobiiltelefonide kasutamise eeskirjad ja turvasuunised
- (M) M 2.190z Mobiilikogu sisseseadmine

Rakendamine

- (L) M 4.114 Mobiiltelefonide turvamehhanismide rakendamine
- (L) M 2.189 Mobiiltelefoni blokeerimine kaotamise korral
- (L) M 2.558 Töötajate mobiil- ja nutitelefonide ning tahvel- ja pihuarvutite infoturbe teadlikkuse suurendamine
- (L) M 4.115 Mobiiltelefonide toite tagamine
- (L) M 4.255 Infrapunaliidese kasutamine
- (M) M 5.78z Kaitse mobiiltelefonide järgi asukoha määramise eest
- (M) M 5.79z Kaitse mobiiltelefoni numbri tuvastamise vastu
- (M) M 5.80z Kaitse mobiiltelefonidega pealtkuulamise eest siseruumides
- (M) M 5.81 Turvaline andmeedastus mobiiltelefoni kaudu

Ressursside väljavahetamine

- (L) M 2.13 Tundlike ressursside jäljetu hävitamine

- (L) M 4.465 Mobiil- ja nutitelefonide ning tahvel- ja pihuarvutite kasutuselt kõrvaldamine

Valmisolek hädaolukorraks

- (L) M 6.72 Ettevaatusabinõud mobiiltelefoni tõrgete puhuks

B 3.405 Nutitelefonid, tahvel- ja pihuarvutid

Kirjeldus

Selles moodulis käsitletakse kaasaskantavaid lõppseadmeid, mida kasutatakse andmete sisestamiseks ja töötlemiseks ning sidevahendina. Tootevalikus on palju seadmeid, mis erinevad üksteisest nii mõõtmete kui ka funktsioonide poolest. Nende hulka kuuluvad muu hulgas järgmised:

- märkmik, aadresside ja päevaplaanide haldamiseks.
- Ilma oma klahvistikuta PDAd, mille andmesisestus toimib ekraani kaudu (pulga abil). Peamiseks kasutusalaks on kohtumiste ja aadresside haldamine ning väikesemahuliste märkmete tegemine.
- PDAd, mille andmesisestus toimib kas sisseehitatud klahvistiku ja/või puutetundliku ekraani abil. Vastavad seadmed võimaldavad lisaks kohtumiste, aadresside ning väiksemahuliste märkmete sisestamisele ja haldamisele ka e-postiga ümber käia.
- Integreeritud mobiiltelefonidega PDAd, niinimetatud nutitelefonid (Smartphones), omavad juba sissehitatud liidest andmeedastuse tarbeks. Nutitelefonide kasutamise korral tuleb täiendavalt rakendada ka moodulit B 3.404 Mobiiltelefon .
- Ülemineku „päris“ sülearvutite vahel moodustavad nn „ sub-notebooks “, mis on oma mõõtmetelt oluliselt väiksemad kui tavalised sülearvutid ning võimaldavad seetõttu näiteks enda külge ühendada vähem lõppseadmeid ning on varustatud vähemate liidestega, kuid sobivad sellele vaatamata muuhulgas näiteks esitlustel kasutamiseks. „Sub-sülearvutite“ kasutamisel tuleb täiendavalt rakendada moodulit B 3.203 Sülearvuti .

Üleminekuid eri tüüpi seadmete vahel on raske määratleda ning tänu tehnika arengule on need pidevas muutuses. Aina rohkem ja rohkem leiab aset PDA ja mobiiltelefoni funktsioonide kombineerimist.

Tüüpiliseks kasutajapoolseks ootuseks PDA suhtes on kontori standardrakenduste mobiilne kasutusvõimalus. Osaliselt on turul saada ka selleks otstarbeks mugandatud erinevaid tekstitöötlus-, tabelarvutus-, meili- ja kalendermärkmiku programme. PDAsid kasutatakse aga ka üha enam turvariskidega seotud rakendustes näiteks autentimise loakaardina võrkudele juurdepääsu tagamisel (nt ühekordsete paroolide genereerimiseks), patsiendiandmete salvestamiseks või kliendi andmebaaside pidamiseks.

Käesolevas peatükis käsitletakse ainult neid IT-turbeaspekte, mis on olulised PDA kasutajatele. Eesmärgiks on näidata, kuidas luua süsteemselt kontseptsioon organisatsioonisiseseks PDAde kasutamiseks ning kuidas tagada selle ellurakendamine.

Ohud

Infosüsteemide etalonturbe seisukohalt loetakse PDAde kasutamise puhul tüüpilisteks järgmisi ohuallikaid:

Vääramatu jõud:

- G 1.15 Muutuvast rakenduskeskkonnast tingitud kahjustused

Organisatsioonilised puudused:

- G 2.2 Reeglite puudulik tundmine
- G 2.4 Turvameetmete ebapiisav järelevalve
- G 2.7 Õiguste volitamata kasutamine
- G 2.200 Ebapiisav planeerimine mobiil- ja nutitelefonide ning tahvel- ja pihuarvutite soetamisel

Inimvead:

- G 3.3 Hooletus turvameetmete suhtes
- G 3.43 Puudulik paroolihooldus
- G 3.44 Teabe hooletu kasutamine
- G 3.45 Sidepartnerite puudulik autentimine
- G 3.76 Vead kaasaskantavate seadmete sünkroniseerimisel
- G 3.123 Mobiil- ja nutitelefonide ning tahvel- ja pihuarvutite keelatud kasutamine eraotstarbel

Tehnilised rikked:

- G 4.42 Mobiiltelefoni või PDA tõrge
- G 4.51 Pihuarvutite puudulikud turbemehhanismid
- G 4.52 Kaasaskantava seadme andmekadu

Ründed:

- G 5.1 IT-seadmete või -tarvikute manipuleerimine ja hävitamine
- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.9 IT-süsteemide volitamata kasutamine
- G 5.22 Kaasaskantava IT-süsteemi vargus
- G 5.23 Viirused
- G 5.123 Ruumide pealtkuulamine kaasaskantavate seadmetega
- G 5.124 Kaasaskantavate seadmete teabe väärkasutus
- G 5.125 Volitamatu andmeedastus kaasaskantavate seadmetega
- G 5.126 Volitamatu pildistamine ja filmimine kaasaskantavate seadmetega
- G 5.117 z/OS-i manipuleerimise varjamine
- G 5.193 Nutitelefonide, tahvel- ja pihuarvutite ebapiisav kaitse pahavara eest
- G 5.194 GSM-koodide smugeldamine telefonifunktsioonidega lõppseadmetesse

Soovitatavad meetmed

Vaadeldava IT-koosluse turvalisuse tagamiseks tuleb lisaks käesolevale moodulile rakendada veel teisigi mooduleid vastavalt IT-etalonturbe rakendusjuhendi modelleerimise tulemustele.

Nutitelefonide, tahvelarvutite ja PDA-de turbe tagamiseks tuleb võtta mitmeid meetmeid, mille hulka kuuluvad nt kontseptsiooni koostamine, soetamine ja

kasutamine. Järgnevalt antakse ülevaade erinevatest kohustuslikest etappidest ja meetmetest, mida iga etapi puhul tuleks võtta.

Planeerimine ja kontseptsioon
Nutitelefonide, tahvelarvutite ja PDA-de turvaliseks ja efektiivseks kasutamiseks ametiasutustes või ettevõtetes tuleb välja töötada kontseptsioon, mis arvestab juba olemasolevatele IT-süsteemidele kehtivate turbenõuetega ja lisaks ka nende nõuetega, mis tulenevad seadmete planeeritud kasutusvaldkondadest (vt M 2.303 Pihuarvutite kasutamise strateegia määramine). Strateegia põhjal tuleb nutitelefonide, tahvelarvutite ja PDA-de kasutamiseks välja töötada konkreetsed suunised ja turvapoliitika (vt M 2.304 Pihuarvutite turvapoliitika ja kasutamise reeglid). Nutitelefonidesse, tahvelarvutitesse ja PDA-desse saab salvestada palju erinevaid rakendusi. Rakendused tuleb välja valida ja nende kasutamine peab olema turvaline (vt M 4.467 Nutitelefonide, tahvel- ja pihuarvutite rakenduste valimine).

Soetamine
Nutitelefonide, tahvelarvutite ja PDA-de soetamisel tuleks lähtuda kontseptsioonis määratletud nõuetest ja valida nende põhjal välja sobivad tooted (vt M 4.305 Salvestusvõimaluste piiramine (Quotas)). Samuti tuleks kontrollida, kas nutitelefonide, tahvelarvutite ja PDA-de turbe tagamiseks on tarvis soetada täiendavaid turbelahendusi (vt M 4.231 Lisavahendite kasutamine pihuarvutite turbeks).

Rakendamine
Kaasaskantavaid lõppseadmeid nagu sülearvuteid, nutitelefone, tahvelarvuteid ja PDA-sid kasutatakse sageli nii internetis kui ka institutsiooni sisevõrkudes hoitavate andmete allalaadimiseks ka väljaspool kontorit. Siinkohal tuleks arvestada täiendavate andmete kaitsmist puudutavate turbeaspektidega (vt M 5.121 Turvaline side mobiilseadme ja töökoha vahel).

Kasutamine
Olenevalt erinevatest turvanõuetest tuleb vastavad tarkvarakomponendid (nutitelefonid, tahvelarvutid, PDA-d, sünkroniseerimistarkvara, tsentraalse seadmehalduse tarkvara) ka erinevalt konfigureerida. See puudutab eeskätt lõppseadmeid endid (vt M 4.228 Pihuarvutite turvamehhanismide rakendamine), sünkroniseerimiskeskkonda (vt M 4.229 Pihuarvutite turvaline kasutamine) ja spetsiaalselt seadmete haldamiseks kasutatavat tarkvara (vt M 4.230 Pihuarvutite tsentraalne haldus). Nutitelefonide, tahvelarvutite ja PDA-de turvaliseks kasutamiseks peavad ka nendega ühenduses olevad töökohaarvutid ning eelkõige sünkroniseerimisliides olema turvaliselt konfigureeritud. Standardsetele töökoha-PC-dele kehtivad turbesuunised leiate moodulite paketti nr 3 kuuluvatest moodulitest, milles käsitletakse erinevaid kliente.

Ressursside väljavahetamine
Igas institutsioonis peaks töötajatele olema täpselt teada, kuidas ja kellele tuleb nutitelefonide, tahvelarvutite ja PDA-de võimalikest tõrgetest, defektidest ja vargusest teatada (vt M 2.306 Kahjudest teatamine). Samuti tuleb töökorraldust puudutavate meetmetega tagada, et nutitelefonide ning tahvel- ja pihuarvutite kasutuselt kõrvaldamisel järgitaks asjakohaseid nõudeid (vt M 4.465 Mobiil- ja nutitelefonide ning tahvel- ja pihuarvutite kasutuselt kõrvaldamine).

Valmisolek hädaolukorraks

Nutitelefon, tahvelarvuti või PDA võib väga erinevatel põhjustel kas rikki minna või töötada ainult osaliselt. Seetõttu tuleks võtta meetmeid, mis ennetaksid sellis-te olukordade tekkimist ja minimeeriksid nende võimalikke tagajärgi (vt M 6.95 Pihuarvutite andmevarundus ja muud tõrgete vältimise meetodid). Samuti tuleks arvestada soovitustega, mis tagavad, et seadmete kaotamise või varguse korral ei läheks kõik seadmesse salvestatud andmed jäädavalt kaduma ega satuks va-ledesse kätesse (vt M 6.159 Nutitelefonide ning tahvel- ja pihuarvutite kaotuste ja varguste ennetamine).

Alljärgnevalt tutvustatakse meetmete kogumit, mida tuleb rakendada vald-konnas„Pihuarvuti“:

Planeerimine ja kontseptsioon

- (L) M 2.218 Andmekandjate ja IT-komponentide kaasavõtmise protseduurid
- (L) M 2.303 Pihuarvutite kasutamise strateegia määramine
- (L) M 2.304 Pihuarvutite turvapoliitika ja kasutamise reeglid
- (M) M 4.467 Nutitelefonide, tahvel- ja pihuarvutite rakenduste valimine
- (M) M 4.468 Isikliku ja tööalase kasutamise lahutamine nutitelefonides ning tahvel- ja pihuarvutites

Soetamine

- (L) M 2.305 Sobivate pihuarvutite valimine
- (M) M 4.231 Lisavahendite kasutamine pihuarvutite turbeks

Rakendamine

- (L) M 5.121 Turvaline side mobiilseadme ja töökoha vahel

Kasutamine

- (L) M 1.33 Kaasaskantavate IT-süsteemide hoidmine reisil
- (L) M 2.558 Töötajate mobiil- ja nutitelefonide ning tahvel- ja pihuarvutite infoturbe teadlikkuse suurendamine
- (L) M 4.3 Viirustõrjeprogrammi regulaarne kasutamine
- (L) M 4.31 Toite tagamine mobiilsel kasutamisel
- (L) M 4.228 Pihuarvutite turvamehhanismide rakendamine
- (L) M 4.229 Pihuarvutite turvaline kasutamine
- (M) M 4.230z Pihuarvutite tsentraalne haldus
- (M) M 4.232z Lisasalvestuskaartide turvaline kasutamine
- (L) M 4.255 Infrapunaliidese kasutamine
- (L) M 4.466 Viirusetõrjeprogrammide kasutamine nutitelefonides ning tahvel- ja pihuarvutites
- (L) M 4.469 GSM-koodide sissesmugeldamise tõkestamine telefonifunkt-sioonidega lõppseadmetes
- (L) M 5.173z Lühi-URL-ide ja QR-koodide kasutamine
- (M) M 5.176 Nutitelefonide, tahvel- ja pihuarvutite turvaline ühendamine asutuse võrguga

Väljavahetamine

- (L) M 2.306 Kahjudest teatamine
- (L) M 4.465 Mobiil- ja nutitelefonide ning tahvel- ja pihuarvutite kasutuselt kõrvaldamine

Valmisolek hädaolukorraks

- (L) M 6.95 Pihuarvutite andmevarundus ja muud tõrgete vältimise meetodid
- (L) M 6.159 Nutitelefonide ning tahvel- ja pihuarvutite kaotuste ja varguste ennetamine

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.6 Arvuti paroolkaitse rangemad reeglid
- HG.7 Ekraaniluku lühem ooteaeg
- HG.24 Paroolide regulaarkontroll parooliskänneriga
- HG.35 Pihuarvutite kasutuse regulaarseire
- HG.71 Lisanõuded mobiiltelefoni/pihuarvuti soetusele ja käitlusele

Teabe käideldavus (K)

- HK.5 Mobiilseadme aku regulaarvahetus

Teabe terviklus (T)

- HT.56 Lisanõuded mobiilsele kaugtööarvutile
- HT.67 Pihuarvutite krüpteerimine

Teabe konfidentsiaalsus (S)

- HS.54 Lisanõuded turvalisele kustutamisele
- HS.62 Infrapunaliidese ja bluetooth 'i kasutuskeeld
- HS.63 Häälteabe kõnepõhine edastuskeeld

B 3.406 Printerid, koopiamasinad ja multifunktsionaalsed seadmed

Büroosisustuse standardvarustusse kuulub tavalisel koopiamasin ning IT-töökohtades printer. Töö tulemused tuleb tihti välja printida, läbi töötada ja arhiveerida. Paljudel juhtudel ei ole mõttekas iga töökoha juurde eraldi printerit installeerida. Seetõttu hallatakse prindiservereid, koopiamasinaid ja multifunktsionaalseid seadmeid, mille peal töötajad oma dokumente välja prindivad või hoopis tsentraalselt paljundavad.

Printimisülesannete saatmist otse töökohaarvutist võrguprinterisse tihti enam ei soovitata. Tsentraalne prindiserver, mis võtab ülesanded vastu ja jagab need vabade printerite vahel, pakub enamasti palju rohkem eeliseid kui puudusi. Seetõttu loetakse reeglina ka prindiserverid printimise infrastruktuuri osaks.

Paberipõhiste seadmete võrku integreerimine ei piirdu paljudel juhtudel ainult printeritega. Näitena võib tuua dokumendiskännerid, mille kasutusõigus antakse paljudele töötajatele korraga, et töötajad saaksid paberdokumente digitaliseerida. Printeriga ühendatult võib skännerit kasutada näiteks nagu tavalist koopiamasinat.

Käesolev moodul käsitleb võrguühendusega printerite, prindiserverite, dokumendiskännerite, koopiamasinate ja multifunktsionaalsete seadmete turvet. Multifunktsionaalsete seadmete alla liigitatakse seadmed, mis suudavad täita mitut erinevat paberi töötlemisega seotud ülesannet nagu nt printimine, paljundamine, skaneerimine või ka faksimine. Ülevaatlikkuse säilimiseks kõiki erinevaid seadmetüüpe järgnevalt eraldi välja ei tooda. Kuna aga näiteks digitaalsete koopiamasinate turvalisust puudutavad soovitused on sarnased võrguühendusega printeritega, kehtivad vastavad soovitused analoogselt ka neile seadmetele.

Ohud

Nagu kõikidel IT-süsteemidel, esineb ka printerite, digitaalsete koopiamasinate, võrku ühendatavate skännerite ja multifunktsionaalsete seadmete puhul mitmesuguseid ohtusid. **Infosüsteemide etalonturbe seisukohalt loetakse eelnimetatud süsteemidel tüüpilisteks järgmisi ohuallikaid:**

Organisatsioonilised puudused:

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.6 Volitamata pääs ruumidesse
- G 2.8 Ressursside kontrollimatu kasutamine
- G 2.15 Konfidentsiaalsusaugud Unix-süsteemis
- G 2.20 Kulumaterjalide ebapiisav või vale varu
- G 2.122 Mitmefunktsiooniliste seadmete ebasobiv kasutamine

Inimvead:

- G 3. 1 Andmete konfidentsiaalsuse või tervikluse kadu kasutaja vea tõttu
- G 3.3 Hooletus turvameetmete suhtes
- G 3.6 Koristajad jm väljastpoolt tellitud töötajad
- G 3.44 Teabe hooletu kasutamine
- G 3.86 Printerite, koopiamasinate ja multifunktsionaalsete seadmete reguleerimata ja hooletu kasutus

Tehnilised rikked:

- G 4.43 Dokumenteerimata funktsioonid
- G 4.64 Printerite, koopiamasinate ja multifunktsionaalsete seadmete keerukus
- G 4.65 Printerite ja multifunktsionaalsete seadmete kommunikatsiooni ebapiisav turve
- G 4.66 Printeritest, koopiaseadmetest ja multifunktsionaalsetest seadmetest tingitud negatiivne mõju tervisele ja keskkonnale

Ründed:

- G 5.1 IT-seadmete või -tarvikute manipuleerimine ja hävitamine
- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.71 Tundliku informatsiooni konfidentsiaalsuse kadu
- G 5.140 Printerite, koopiamasinate ja multifunktsionaalsete seadmete jääkinfo lugemine

Soovitatavad meetmed

Selleks, et tagada kogu loetletud IT-süsteemi turvalisus, tuleb lisaks käesolevale moodulile rakendada veel ka teisi, IT-etalonturbe modelleerimise käigus selguvaid mooduleid.

Prindiserverite puhul on reeglina tegu tavaliste IT-süsteemidega, mida kasutatakse vastava serveri funktsioonides. Nimetatud lahenduse korral tuleb täiendavalt rakendada moodulit B 3.101 Server ning vastava operatsioonisüsteemi serverit käsitlevat moodulit.

Täiendavat, operatsioonisüsteeme käsitlevat informatsiooni leidub vastavates moodulites.

Printerite, koopiamasinate ja multifunktsionaalsete seadmete puhul tuleks IT-alase turvalisuse tagamiseks arvestada ennekõike järgmiste valdkondadega:

- info ja kommunikatsiooni krüpteerimine (digitaalsete andmete kaitse),
- süsteemikaitse (seadmete kaitse) ning
- juurdepääs dokumentidele (väljaprinditud dokumentide kaitse).

Planeerimine ja kontseptsioon

Võrguprinterite, koopiamasinate ja multifunktsionaalsete seadmete turve vajab hoolikat planeerimist (vt M 2.397 Printerite, koopiamasinate ja multifunktsionaalsete seadmete kasutamise planeerimine). Täpsema info tüüpiliste printimislahenduste koostisosade ja koostamise kohta leiate meetmest M 4.304 Printerite haldamine . Võrguprinterite turvanõuded tuleb integreerida organisatsiooni üldisesse turvastrateegiasse.

Paljude printeritega seoses üleskerkivate probleemide puhul ei piisa ainult tehnilistest lahendustest. Töötajad peavad teadma, kuidas printeritega turvaliselt ümber käia, ning neid tuleb kohustada järgima turvanõudeid (vt M 2.397 Printerite, koopiamasinate ja multifunktsionaalsete seadmete kasutamise planeerimine).

Lisaks tüüpilistele printeritele tuleb arvestada ka sarnaste seadmete olemasoluga. Siia alla kuuluvad näiteks multifunktsionaalsed seadmed (M 5.146 Multifunktsionaalsete seadmete lahutamine võrgust) ning dokumendiskännerid (M 4.303 Võrgutoega dokumendiskännerite kasutamine).

Soetamine

Kasutusvaldkondadest lähtudes tuleks sõnastada toodetele seatavad nõudmised ning vastavalt nendele teha valik sobilike toodete hulgast (vt M 2.399 Printerite, koopiamasinate ja multifunktsionaalsete seadmete soetamise ning väljavalimise kriteeriumid).

Rakendamine

Pärast seda kui kõik planeerimistööd on tehtud, tuleb hakata tegelema seadmete kasutuselevõtuga. Siinjuures sõltub palju asjaolust, kuhu vastavaid seadmeid soovitakse üles panna (vt M 1.32 Printerite ja koopiamasinate turvaline paigutus) ning kuidas piiratakse töötajate juurdepääsu neile (M 4.301 Juurdepääsu piiramine printeritele, koopiamasinatele ja multifunktsionaalsetele seadmetele).

Nagu kõiki IT-süsteeme, tuleks ka võrguprintereid, koopiamasinaid ja skännereid volitamata kasutuse eest kaitsta (vt M 4.299 Autentimine printerite, koopiamasinate ja multifunktsionaalsete seadmete kasutamisel). Kuid ka nende vahendite turvalisusele, mida kasutatakse (digitaalse) informatsiooni salvestamiseks ja hoidmiseks, tuleb pöörata piisavalt tähelepanu. Infot sellekohaste soovituste kohta leiate meetmest M 4.300 Printerite, koopiamasinate ja multifunktsionaalsete seadmete infoturve .

Lisaks printerite riistvarale on turvalise töö tagamiseks tähtsad ka erinevad tarkvarakomponendid nagu prindiserverid ja selle kliendid. Sõltuvalt kasutatavast operatsioonisüsteemist ja printimislahendusest tuleb rakendada vastavaid meetmeid ja mooduleid nagu nt M 5.145 Turvaline CUPSi kasutamine või B 5.17 Samba .

Kasutamine

Tavakasutuse raames on lisaks tähtsamate asetleidnud sündmuste logimisele (vt M 4.302 Printerite, koopiamasinate ja multifunktsionaalsete seadmete logimine) tähtis ka seadmete varustamine vajaminevate kulumaterjalidega (vt M 2.52 Faksimaterjalide varude jälgimine ja täiendamine).

Väljavahetamine

Printerite, koopiamasinate, skännerite ja multifunktsionaalsete seadmete mällu jääb tihtipeale konfidentsiaalset infot. Seadmete väljavahetamisel tuleb arvestada meetmega M 2.400 Printerite, koopiamasinate ja multifunktsionaalsete seadmete turvaline kasutuselt kõrvaldamine .

Valmisolek hädaolukorraks

Infot võrguühendusega printerite, koopiaseadmete, dokumendiskännerite ja multifunktsionaalsete seadmete kaitsmise kohta leiate ka meetmest M 6.105 Printerite, koopiamasinate ja multifunktsionaalsete seadmete hädaolukorraks valmisoleku plaan .

Alljärgnevalt tutvustatakse meetmete kogumit, mida tuleb rakendada valdkonnas „Printerid, koopiamasinad ja multifunktsionaalsed seadmed“:

Planeerimine ja kontseptsioon

- (L) M 2.397 Printerite, koopiamasinate ja multifunktsionaalsete seadmete kasutamise planeerimine
- (L) M 2.398 Printerite, koopiamasinate ja multifunktsionaalsete seadmete kasutusjuhised

Soetamine

- (L) M 2.399w Printerite, koopiamasinate ja multifunktsionaalsete seadmete soetamise ning väljavalimise kriteeriumid

Rakendamine

- (M) M 1.32 Printerite ja koopiamasinate turvaline paigutus
- (M) M 4.299z Autentimine printerite, koopiamasinate ja multifunktsionaalsete seadmete kasutamisel
- (M) M 4.300z Printerite, koopiamasinate ja multifunktsionaalsete seadmete infoturve
- (L) M 4.301 Juurdepääsu piiramine printeritele, koopiamasinatele ja multifunktsionaalsetele seadmetele
- (L) M 5.145 Turvaline CUPSi kasutamine

Kasutamine

- (L) M 2.52 Faksimaterjalide varude jälgimine ja täiendamine
- (L) M 4.302 Printerite, koopiamasinate ja multifunktsionaalsete seadmete logimine
- (L) M 4.303 Võrgutoega dokumendiskännerite kasutamine
- (M) M 4.304z Printerite haldamine
- (L) M 5.146 Multifunktsionaalsete seadmete lahutamine võrgust

Väljavahetamine

- (L) M 2.13 Tundlike ressursside jäljetu hävitamine
- (L) M 2.400 Printerite, koopiamasinate ja multifunktsionaalsete seadmete turvaline kasutuselt kõrvaldamine

Valmisolek hädaolukorraks

- (L) M 6.105 Printerite, koopiamasinate ja multifunktsionaalsete seadmete hädaolukorraks valmisoleku plaan

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed
-
Teabe käideldavus (K)

- HK.5 Mobiilseadme aku regulaarvahetus

Teabe terviklus (T)
-
Teabe konfidentsiaalsus (S)

- HS.59 Eraldi printer kõrgkonfidentsiaalsetele andmetele
- HS.60 Juuresolekunõue kõrgkonfidentsiaalsete dokumentide paljundamisel
- HS.61 Lisanõuded printerite, koopiamasinate ja multifunktsionaalsete seadmete ja nende komponentide kasutuselt kõrvaldamisele
- HS.62 Infrapunaliidese ja bluetooth 'i kasutuskeeld

B 3.407 Integreeritud süsteem

Kirjeldus

Integreeritud süsteemid on andmeid töötlevad süsteemid, mis on integreeritud suuremasse süsteemi või tootesse, kus need võtavad üle juhtimis-, reguleerimis- ja andmetöötlusega seotud ülesanded ning kasutaja neid sageli otse ei tajugi. Kui integreeritud süsteemi varustatuse tase on madal, st selle ressursid, mis puudutavad salvesteid, CPU-d ja energiat, on äärmiselt piiratud, ning kui sellel ei ole kasutajaliidest, on tegemist sügavalt integreeritud süsteemiga. Selliste sügavalt integreeritud süsteemide näidete hulka kuuluvad südamestimulaatorid ja autode ning lennukite alamsüsteemid.

Integreeritud süsteeme leidub nii kõrgetehnoloogia valdkonnas, nt lennunduses ja kosmoseuuringutes, meditsiinitehnikas, telekommunikatsioonis ja autotööstuses, kui ka tarbe- ja kodumasinate valdkonnas.

Integreeritud süsteemi iseloomustab, et sellel on erinevalt nt arvutist üks või enam täpselt määratletud ülesannet. See moodustab tark- ja riistvaraliselt funktsionaalse terviku, mis täidab üksnes neid määratletud ülesandeid. Integreeritud süsteemide tarkvara tähistatakse kui püsivara ning see on enamasti salvestatud välkmälusse, EPROM-ile, EEPROM-ile või ROM-ile ja kasutaja ei saa seda välja vahetada või siis saab seda teha üksnes spetsiaalsete vahendite või funktsioonide abil. See koosneb peamiselt Bootloader'ist, operatsioonisüsteemist ja rakendusest, kusjuures spetsialiseeritud süsteemid loobuvad operatsioonisüsteemist. Integreeritud süsteemid on küll otstarbekohased seadmed, kuid vastupidiselt puhtale riistvara rakendamisele (ASIC) siiski universaalsed arvutid. Platvormidena tulevad kõne alla erinevad CPU-arhitektuurid või paindlikud kõrgintegreeritud Field Programmable Gate Array (FPGA) moodulid.

Integreeritud süsteemides ei ole kasutusliidest ning need ei kasuta erilisi lisaseadmeid, nt funktsionaalseid nuppe, pöördlülitit ja vastava kasutuseesmärgi jaoks välja töötatud ekraane. Väljastusüksuste valik ulatub lihtsast signaallambist LCD-de kaudu kuni keerukate kokpiti-ekraanideni. Integreeritud süsteemid suhtlevad sageli andmesiinide kaudu, mis on heterogeenselt ühendatud keerukatesse süsteemidesse. Peale selle võivad mitmete erinevate ja mitme kanaliga sisend- ja väljundportide kaudu olla ühendatud lisakomponendid, nagu andurid ja käivitid. Mõnedel integreeritud süsteemide liikidel on veebiliides, mille abil saab brauseri kaudu teostada konfiguratsiooniseadistusi.

Integreeritud süsteemidele esitatavad nõudmised sõltuvad rakendustest, kuid neid saab iseloomustada järgmiselt:

- vastupidav, tõrgeteta töötamine;
- riist- ja tarkvara keerukus, mis on kohandatud rakendusele;
- reaktsiooniaeg enamasti määratletud etteantud aja piires;
- mitmed erinevad liidesed (andmesiin, analoogsed ja digitaalsed I/O-pordid);
- vahetu koostalitlus andurite ja käivititega.

Kõnealune moodul käsitleb peamiselt integreeritud süsteeme ja seda saab kasutada paljude erinevate integreeritud süsteemide jaoks. Operatsiooni- ja näidikusüsteemide või spetsiifiliste riist- ja tarkvara-arhitektuuride eraldi turbefunktsioonidesse lähemalt ei süveneta.

Integreeritud süsteemide erirakendus on kiipkaardid. Kaartidel on tavaliselt protsessor, töömälu ja I/O-liidesed. Ka kiipkaartide puhul käsitletakse selles moodulis küll põhilisi turvalisusega seotud aspekte, kuid ei vaadelda konkreetseid aspekte.

Moodulit saab põhiliselt kasutada IT-kooslusena koos ühe või enama integreeritud süsteemiga, kui need vastavad järgmistele kriteeriumidele:

- integreeritud süsteem soetatakse eraldi ja see ei ole ümbritseva süsteemi integreeritud koostisosa.
- Integreeritud süsteemi valiku-, soetamise ja valmistamise protsesse on võimalik kontrollida ja mõjutada.
- Selle mooduli meetmete elluviimine on võimalik ja kontrollitav.
- Integreeritud süsteem ei paku otsest kasutaja sekkumist.

Ohud

IT-etalonturbe seisukohalt loetakse integreeritud süsteemide puhul tüüpilisteks alljärgnevaid ohuallikaid.

Vääramatu jõud

- G 1.2 IT-süsteemi avarii
- G 1.8 Tolm, saastumine

Töökorralduslikud puudused

- G 2.29 Tarkvara testimine tootmisandmetega
- G 2.27 Ebapiisav või puuduv dokumentatsioon
- G 2.29 Tarkvara testimine tootmisandmetega
- G 2.206 Mitteküllaldased turvanõuded integreeritud süsteemide väljatöötamisel
- G 2.207 Kaitsmata sisend- ja väljundliidesed integreeritud süsteemides
- G 2.208 Integreeritud süsteemide elektrooniliste komponentide mitteküllaldane füüsiline kaitse

Tehnilised rikked

- G 4.22 Tüüptarkvara turvaaugud või vead
- G 4.33 Autentimise puudumine või puudulikkus
- G 4.39 Tarkvarakontseptsiooni viga
- G 4.43 Dokumenteerimata funktsioonid

Ründed

- G 5.1 IT-seadmete või -tarvikute manipuleerimine ja hävitamine
- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.16 Ohud hoolde- ja haldustööde ajal
- G 5.23 Pahavara
- G 5.141 Andmevargus kaasaskantavate andmekandjatega

Soovitatavad meetmed

Vaadeldava IT-koosluse turvalisuse tagamiseks tuleb peale selle mooduli rakendada veel teisigi mooduleid, mis selguvad IT-etalonturbe rakendusjuhendi põhjal tehtava modelleerimise tulemusel.

Planeerimine ja kontseptsioon

Hoolikas planeerimine ja kontseptsioon on integreeritud süsteemide jaoks vältimatu. Kui integreeritud süsteem töötatakse välja ise või tellitakse, tuleb arvesse võtta turvalise arenduse põhimõtteid (vt M 2.378z Süsteemiarendus). Arendustööriistad peavad olema veatud ja nende manipuleerimine ei tohi olla tuvastamatult võimalik (vt M 2.567 Usaldusväärsete arendustööriistade valik). Suurenenud kaitsevajaduse korral nõutava turbeastme tagamiseks integreeritud süsteemi jaoks tuleb läbi viia kontrollimine tunnustatud kriteeriumide kohaselt (vt M 2.65 IT-süsteemi kasutajate eraldatuse kontroll).

Integreeritud süsteemi turbefunktsioonid ja raamid turbefunktsioonide jaoks on piiratud juba kontsepti kindlaksmääramisega. Tarkvara-riistvara jaotamise kohta põhimõttelise otsuse tegemisel tuleb arvesse võtta tarkvaraliste ja riistvaraliste teostuste erinevaid turbefunktsioone (vt M 4.482 Integreeritud süsteemide funktsioonide riistvaraline teostamine). Süsteemi stabiilsuse suurendamiseks tuleks vajaduse korral kasutada riistvaral või tarkvaral põhinevat salvesti kaitset (vt M 4.484 Salvesti kaitse integreeritud süsteemides). Kasutatav operatsioonisüsteem peaks hetke tehnika taseme kohaselt olema tõrkekindel ja sellel ei tohi olla palju ründepunkte (vt M 4.485 Turvaline operatsioonisüsteem integreeritud süsteemide jaoks). Selleks et tagada programmide ja kasutajaandmete usaldusväärsus, tuleks kasutada krüptoprotseduure (vt M 4.90w Krüptoprotseduuride kasutamine ISO/OSI etalonmudeli eri kihtides). Riistvaralises turvamoodulis (Trusted Platform Module) saab turvaliselt luua ja salvestada võtmeid ning seega autentida turvalisemalt andmeid ja komponente (vt M 4.483 Krüptograafiliste protsessorite ja kaasprotsessorite (Trusted Platform Module) kasutamine integreeritud süsteemides).

Juba planeerimisetapis tuleb kindlaks määrata eeskirjad hilisemaks kasutamiseks (vt M 2.562 Integreeritud süsteemide kasutamise eeskirjad).

Soetamine

Enne integreeritud süsteemi soetamist tuleb välja selgitada selle nõuded. Kriteeriumide nimekiri peab hõlmama ka vajalikke turbefunktsioone. Soetatud süsteemid või komponendid peavad vastama täpselt standardile ja soetamise protsess peab toimuma nii, et seda ei saaks manipuleerida (vt M 2.563 Usaldusväärse tarne- ja logistikaketi ning pädeva tootja valimine integreeritud süsteemide jaoks).

Teostus

Integreeritud süsteeme tuleb arendamise ajal ja enne tavatöö režiimis kasutuselevõttu nõutavas ulatuses katsetada (vt M 2.568 Tarkvara testimisprotseduurid). Neid tuleb kaitsta füüsilise manipuleerimise eest (vt M 4.487 Urkimiskaitse (tuvastamine, takistamine, tõrje) integreeritud süsteemides). Kasutada võib ainult vajalikke füüsikalisi ja loogilisi liideseid ja juurdepääs tohib olla võimalik üksnes

pärast edukat autentimist (vt M 4.488 Mittekasutatavate liideste ja teenuste inaktiveerimine integreeritud süsteemides). Buutimisprotsess ei tohi olla kahjustatav (vt M 4.489 Kaitstud ja autenditud buutimisprotsess integreeritud süsteemides).

Kasutamine

Kui integreeritud süsteemi kasutatakse ebasoodsates tingimustes, tuleks seda asjakohaselt kaitsta (vt M 1.81 Integreeritud süsteemide füüsiline kaitse). Konfiguratsiooni parameetrite ja püsivara muutusi tuleb hoolikalt kavandada, läbi viia ja dokumenteerida (vt M 2.34 IT-süsteemi muutuste dokumenteerimine ja M 4.78 Konfiguratsioonimuudatuste hoolikas teostamine ning M 4.177 Tarkvarapakettide tervikluse ja autentsuse tagamine).

Töörežiimis ei tohi integreeritud süsteem sisaldada koodielemente, mis ei ole süsteemi funktsioonide osad (vt M 4.491 Silumisvõimaluste tõkestamine integreeritud süsteemides). Krüptomuutujad ei tohi olla kahjustatavad (vt M 4.34z Krüpteerimise, kontrollsummade ja digitaalallkirjade rakendamine ja M 2.46 Krüpteerimise õige korraldus). Kui integreeritud on veebiserver, tohib installeerida ja aktiveerida ainult vajalikke komponente ja funktsioone ning konfigureerida tuleb samaväärsed turvamehhanismid nagu büroo veebiserverite korral (vt M 4.492 Integreeritud veebiserveri turvaline konfiguratsioon ja kasutamine).

Integreeritud süsteemi järjekindla turbe tagamisel on väga oluline nii süsteemi kui ka selle üksikkomponentide seire. Turbega seotud sündmused integreeritud süsteemi kasutamisel tuleb dokumenteerida tehniliste võimaluste raames (vt M 2.565 Turbega seotud sündmuste protokollimine integreeritud süsteemides). Lisaks peaksid integreeritud süsteemi kõik seadmemoodulid valdama ja kasutama kättesaadavusele ja terviklusele esitatavate kõrgendatud nõudmistega kooskõlas olevaid integreeritud enesetesti seadmeid (vt M 4.490 Seadmemoodulite funktsiooni automaatseire (BIST) integreeritud süsteemides).

Kasutusest kõrvaldamine

Integreeritud süsteemi kasutusest kõrvaldamise korral ei tohi konfidentsiaalne teave riistvara, tarkvara ja andmete kohta sattuda volitamata isikute kätte (vt M 2.566 Integreeritud süsteemi turvaline kasutusest kõrvaldamine).

Valmisolek hädaolukorraks

Tavapärasest suuremate kättesaadavuse nõuete korral peaksid olemas olema mehhanismid, et taastada viimast töökonfiguratsiooni ja tarneolekut (vt M 6.163 Integreeritud süsteemide taastamine).

Kui integreeritud süsteemis on konfidentsiaalseks liigitatud teavet, peab süsteemis olema kustutamisvõimalus hädaolukorras (vt ka M 6.163 Integreeritud süsteemide taastamine).

Planeerimine ja kontseptsioon

- (L) M 2.378z Süsteemiarendus
- (L) M 2.562 Integreeritud süsteemide kasutamise eeskirjad
- (L) M 4.34z Krüpteerimise, kontrollsummade ja digitaalallkirjade rakendamine
- (L) M 4.482 Integreeritud süsteemide funktsioonide riistvaraline teostamine
- (L) M 4.483 Krüptograafiliste protsessorite ja kaasprotsessorite (Trusted Platform Module) kasutamine integreeritud süsteemides

- (L) M 4.484 Salvesti kaitse integreeritud süsteemides
- (L) M 4.485 Turvaline operatsioonisüsteem integreeritud süsteemide jaoks
- (L) M 4.486z Integreeritud süsteemide vastupanuvõime külgkanalrünnete vastu

Soetamine

- (L) M 2.66z Sertifikaatidega arvestamine IT soetamisel
- (L) M 2.563 Usaldusväärse tarne- ja logistikaketi ning pädeva tootja valimine integreeritud süsteemide jaoks
- (L) M 2.564 Integreeritud süsteemide soetamise kriteeriumid

Teostus

- (L) M 2.568 Tarkvara testimisprotseduurid
- (L) M 4.487z Urkimiskaitse (tuvastamine, takistamine, tõrje) integreeritud süsteemides
- (L) M 4.488 Mittekasutatavate liideste ja teenuste inaktiveerimine integreeritud süsteemides
- (L) M 4.489 Kaitstud ja autenditud buutimisprotsess integreeritud süsteemides

Kasutamine

- (L) M 1.81 Integreeritud süsteemide füüsiline kaitse
- (L) M 2.34 IT-süsteemi muutuste dokumenteerimine
- (L) M 2.565 Turbega seotud sündmuste protokollimine integreeritud süsteemides
- (L) M M 4.78 Konfiguratsioonimuudatuste hoolikas teostamine
- (M) M 4.177 Tarkvarapakettide tervikluse ja autentsuse tagamine
- (L) M 4.490 Seadmemoodulite funktsiooni automaatseire (BIST) integreeritud süsteemides
- (L) M 4.491 Silumisvõimaluste tõkestamine integreeritud süsteemides
- (M) M 4.492 Integreeritud veebiserveri turvaline konfiguratsioon ja kasutamine

Kasutusest kõrvaldamine

- (L) M 2.566 Integreeritud süsteemi turvaline kasutusest kõrvaldamine

Valmisolek hädaolukorraks

- (L) M 6.163 Integreeritud süsteemide taastamine

B4 Võrgud

Moodulite nimekiri

B 4.1 Heterogeensed võrgud

Kohtvõrk moodustub kaablitest (st passiivsetest võrgukomponentidest nagu kaabel ja kaabliühendused) ning aktiivsetest võrgukomponentidest ehk võrguühendustest. Kohtvõrku võib integreerida nii erinevaid kaabeldusvariante kui ka erinevaid aktiivseid võrgukomponente. Aktiivseteks võrgukomponentideks loetakse kõiki neid võrgu koostisosi, mis vajavad oma (võrgu-) voolutoidet. Siia alla kuuluvad muuhulgas järgurid, sillad, kommutaatorid, marsruuterid ja tulemüürid. Passiivseteks võrgukomponentideks loetakse kõiki neid võrgu koostisosi, mis ei vaja eraldi (võrgu-) voolutoidet. Siia alla kuuluvad näiteks kaablid, jaotuskapid, kaablijaotusseadmed, pistikühendused.

Kuna detailsemad kaabelduse kohta käivad kirjeldused on juba eelnevalt kokku võetud moodulisse B 2.2 Elektrotehniline kaabeldus , rakendusi puudutavad perifeersed seadmed moodulite komplekti nr 3, keskendub käesolev moodul peamiselt aktiivsete võrgukomponentide, nende aluseks oleva topoloogia, konfiguratsiooni, sobilike komponentide valikukriteeriumide, edastusprotokollide valiku ning selle kõige juurde kuuluva võrguhalduse kirjeldamisele.

Käsitlusele tulevad ainult LAN-tehnoloogiad, nt võrguprotokollid Ethernet, Token Ring või FDDI, täpsemalt sinna juurde kuuluvad võrgukomponendid nagu sillad, kommutaatorid või marsruuterid. Vastavaid tehnoloogiad võidakse sõltuvalt olukorrast kasutada ka laivõrgus. WAN-ühendusega seotud küsimustega käesolevas moodulis siiski ei tegelda. Muuhulgas viitame siinkohal moodulile B 3.301 Turvalüüs (tulemüür) .

IT-etalonturbe seisukohalt kohtvõrgu turvalisuse tagamiseks käesolevast moodulist üksi ei piisa. Lisaks aktiivsetele võrgukomponentidele ja võrguhalduseks kasutatavale tarkvarale tuleb tähelepanu pöörata ka füüsilisele kaabeldusele ning võrgus kasutatavatele serverisüsteemidele. Seetõttu on lisaks käesolevale vaja tingimata läbi töötada veel ka eelpool nimetatud moodulid.

Käesolev moodul annab juhtnööre, kuidas oleks võimalik heterogeenset võrku analüüsida ning selle põhjal turvakontseptsioone välja töötada ja töösse rakendada. Seega on antud moodul suunatud organisatsiooni sellele üksusele, mis vastutab võrgu kasutamise eest ning kus on olemas vastavad erialased teadmised.

Ohud

Infosüsteemide etalonturbe seisukohalt loetakse heterogeense võrgu puhul kokkuvõtlikult tüüpilisteks järgmisi ohuallikaid:
Vääramatu jõud:

- G 1.2 IT-süsteemi avarii
- G 1.3 Äike
- G 1.4 Kahjutuli
- G 1.5 Vesi
- G 1.7 Lubamatu temperatuur ja niiskus
- G 1.8 Tolm, saastumine

Organisatsioonilised puudused:

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.2 Reeglite puudulik tundmine
- G 2.4 Turvameetmete ebapiisav järelevalve

- G 2.7 Õiguste volitamata kasutamine
- G 2.9 Halb kohanemine IT muutustega
- G 2.22 Logiandmete analüüsimata jätmine
- G 2.27 Ebapiisav või puuduv dokumentatsioon
- G 2.32 Võrgu ebapiisav võimsus
- G 2.44 Ühildamatud võrgu aktiiv- ja passiivkomponendid
- G 2.45 Võrgu konseptuaalsed puudused
- G 2.46 Maksimaalse lubatava kaabli- või siinipikkuse või ringi suuruse ületamine

Inimvead:

- G 3.2 Seadme või andmete hävitamine hooletuse tõttu
- G 3.3 Hooletus turvameetmete suhtes
- G 3.5 Liinide juhuslik kahjustamine
- G 3.6 Koristajad jm väljastpoolt tellitud töötajad
- G 3.8 IT-süsteemi väär kasutamine
- G 3.9 IT-süsteemi väär haldus
- G 3.28 Võrgu aktiivkomponentide ebasobiv konfiguratsioon
- G 3.29 Ebasobiv või puuduv segmentimine
- G 3.43 Puudulik paroolihooldus

Tehnilised rikked:

- G 4.1 Toitevõrgu katkestus
- G 4.10 Keerukad ligipääsuvõimalused võrgustatud IT-süsteemides
- G 4.31 Võrgukomponentide rike või tõrge

Ründed:

- G 5.1 IT-seadmete või -tarvikute manipuleerimine ja hävitamine
- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.4 Vargus
- G 5.5 Vandalism
- G 5.6 Füüsiline rünne
- G 5.7 Liinide pealtkuulamine
- G 5.8 Liinide manipuleerimine
- G 5.9 IT-süsteemide volitamata kasutamine
- G 5.18 Süstemaatiline paroolide mõistatamine
- G 5.20 Administraatori õiguste väärkasutus
- G 5.28 Teenuse halvamine
- G 5.66 IT-süsteemide volitamatud võrguühendused
- G 5.67 Võrguhaldusfunktsioonide volitamatu käivitamine
- G 5.68 Volitamata juurdepääs aktiivsetele võrgukomponentidele

Soovitatavad meetmed

Selleks, et tagada kogu loetletud IT-süsteemi turvalisus, tuleb lisaks käesolevale moodulile rakendada veel ka teisi, IT-etalonturbe modelleerimise käigus selguvaid mooduleid.

Olgu siinkohal veelkord meelde tuletatud, et IT-etalonturbe seisukohalt saab tõhusast kohtvõrgu kaitsest rääkida vaid sel juhul, kui lisaks käesolevale moodulile töötatakse läbi ka moodulid B 2.2 Elektrotehniline kaabeldus , B 3.101 Server ning vajadusel ka kindlaid operatsioonisüsteeme käsitlevad moodulid ning moodul B 4.2 Võrgu- ja süsteemihaldus .

Lisaks tuleks võrgu aktiivkomponendid paigutada tehnilise infrastruktuuri ruumidesse (nt jaoturruumidesse), mis tähendab mooduli B 2.6 Tehnilise infrastruktuuri ruum rakendamist.

Võrguadministraatori töökoht peaks olema samuti kaitstud kõrgendatud turvameetmetega. Lisaks moodulis B 2.3 Bürooruum kajastatud nõuetele tuleb paika panna ka reeglistik kasutatava operatsioonisüsteemi tarbeks (tutvuge vastavate moodulitega moodulite komplektist nr 3).

Heterogeense võrgu turvaliseks kasutamiseks tuleb rakendada terve rida erinevaid meetmeid, alates võrgu hetkesituatsiooni analüüsimisest, võrguhalduse kontseptsiooni väljatöötamisest kuni lõpliku töötamiseni välja. Järgnevalt anname ülevaate erinevatest kohustuslikest etappidest ja meetmetest, mida iga etapi puhul tuleks rakendada.

1.Võrgu hetkeolukorra analüüsimine (vt M 2.139 Olemasoleva võrgukeskkonna läbivaatus ja M 2.140 Võrgu hetkeolukorra analüüsimine).

- koormavate faktorite väljaselgitamine ja võrguliikluse analüüs
- võrgu pudelikaelade tuvastamine
- kriitiliste valdkondade tuvastamine

2. Kontseptsioon

- Võrgu kontseptsiooni loomine (vt M 2.141 Võrgukontseptsiooni väljatöötamine , M 2.142 Võrguplaani väljatöötamine ja M 5.60 Sobiva magistraalvõrgutehnika valimine)
- Võrguhalduse kontseptsioon (vt M 2.143 Võrguhalduse kontseptsiooni väljatöötamine ja M 2.144 Sobiva võrguhaldusprotokolli valimine).

3. Võrgu turvaline kasutamine

Võrgu segmentimine (vt M 5.61 Sobiv füüsiline segmenteerimine ja M 5.62 Sobiv loogiline segmenteerimine).

- Võrguhaldustarkvara kasutamine (vt M 2.145 Nõuded võrguhaldusinstrumendile ja M 2.146 Võrguhaldussüsteemi turvaline kasutamine).
- Võrgu audit ja läbivaatus (vt M 2.64 Logifailide kontroll ja M 4.81 Võrgutoimingute audit ja logimine).

4. Valmisolek hädaolukorraks

- Võrgukomponentide liiasuse rakendamine (vt M 6.53 Võrgukomponentide liiasus).
- Konfiguratsiooniandmete säilimise tagamine (vt M 6.52 Võrgu aktiivkomponentide konfiguratsiooniandmete regulaarne varundamine).

Järgnevalt on ära toodud võrku kajastavate meetmete kogum, milles kajastuvad nõuanded on oma sisult pigem üldistavat laadi, pakkudes täiendust eelpool loetletud sammudele.

Planeerimine ja kontseptsioon

- (L) M 2.139 Olemasoleva võrgukeskkonna läbivaatus
- (M) M 2.140z Võrgu hetkeolukorra analüüsimine
- (M) M 2.141 Võrgukontseptsiooni väljatöötamine
- (L) M 4.79 Kohapealse võrguhalduse turvalised pääsumehhanismid
- (L) M 5.2 Võrgu sobiv topograafia
- (L) M 5.13 Võrgu ühendusaparatuuri õige kasutamine
- (L) M 5.60 Sobiva magistraalvõrgutehnika valimine
- (L) M 5.61 Sobiv füüsiline segmenteerimine
- (L) M 5.62z Sobiv loogiline segmenteerimine
- (M) M 5.77z Alamvõrkude rajamine

Rakendamine

- (L) M 4.7 Algparoolide muutmine
- (M) M 4.80 Kaug-võrguhalduse turvalised pääsumehhanismid
- (L) M 4.82 Võrgu aktiivkomponentide turvaline konfigureerimine
- (L) M 5.7 Võrguhaldus

Kasutamine

- (M) M 4.81 Võrgutoimingute audit ja logimine
- (L) M 4.83 Võrgukomponentide riistvara ja tarkvara värskendamine ja täiendamine
- (M) M 5.8 Võrgu regulaarne turvakontroll

Valmisolek hädaolukorraks

- (L) M 6.52 Võrgu aktiivkomponentide konfiguratsiooniandmete regulaarne varundamine
- (M) M 6.53z Võrgukomponentide liiasus
- (M) M 6.54 Protseduurid võrgu tervikluse kao puhuks
- (M) M 6.75z Varu-sidekanalid

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.24 Paroolide regulaarkontroll parooliskänneriga
- HG.30 VPNi kasutamise kohustus, kui raadiovõrku kasutatakse magistraalvõrguna

- HG.31 Traadita kohtvõrgu väline turvaaudit
- HG.38 Turvapaikade paigaldatuse regulaarseire

Teabe käideldavus (K)

- HK.9 Varusidekanali nõue

Teabe terviklus (T)

- HT.51 Lisanõuded teabe hankimisele turvaaukude kohta
- HT.57 Algparoolide muutmise regulaarkontroll

Teabe konfidentsiaalsus (S)
-

B 4.2 Võrgu- ja süsteemihaldus

Tavalise kohtvõrgu (LAN, VLAN) haldussüsteemi ülesandeks on võimalikult paljude kohtvõrku liidetud riist- ja tarkvarakomponentide tsentraalne haldus. Haldussüsteem peab suutma süsteemihaldurit tema igapäevatöös maksimaalselt aidata. Üldjoontes on võimalik teineteisest eristada võrguhaldust ja süsteemihaldust. Erinevused tekivad erinevatest hallatavatest komponentidest.

Võrguhaldus hõlmab kõiki ettevaatusabinõusid ning töid ja tegemisi, mis on vajalikud võrgu efektiivse toimimise tagamiseks. Siia alla kuuluvad näiteks võrgukomponentide korrektse funktsiooni jälgimine, võrgu jõudluse jälgimine ning võrgukomponentide tsentraliseeritud konfigureerimine. Võrguhaldus tegeleb esmajoones organisatoorsete küsimustega, kus probleemide lahendamisel otsitakse abi vaid tehnilistest vahenditest nagu võrguhaldussüsteem.

Süsteemihaldus tegeleb esmajoones laialijaotatud IT-süsteemide haldusega. Siia alla kuuluvad näiteks kasutajate tsentraalne haldamine, tarkvara jagamine, rakenduste haldus jne. Teatud valdkondades seevastu, nt konfiguratsioonide halduse (süsteemi või võrgukomponendi jälgimise ja nende konfiguratsioonide ühtlustamise) puhul ei ole võrgu- ja süsteemihaldus teineteisest selgesti eristatavad.

Edaspidi kasutatakse võrgu ja selle komponentide haldamisel kasutatava (tarkvara-)süsteemi tähistamiseks alati mõistet „haldussüsteem“ ning selle abil hallatavate komponentide tähistamiseks mõistet „hallatav süsteem“. Inglisekeelseteks vasteteks oleks siinkohal „ management system “ ning „ managed system “, eriti kehtib see võrguhalduse kohta.

Võrgu- ja süsteemihalduse raamistik on defineeritud normiga ISO/IEC-7498-4, täpsemalt ITU-T standardiga X.700. Definitsioonidele toetudes kuuluvad haldussüsteemi ülesannete hulka:

1. Konfiguratsiooni haldus,
2. Jõudluse haldus,
3. Vigade haldus,
4. Kuluarvestuse haldus,
5. Turvahaldus.

Samas ei pea üks konkreetne süsteemihalduse toode toetama kõiki äsja loetletud valdkondi. Süsteemitootjad pakuvad reeglina tooteid, mis on oma ülesehituselt jaotatud eri moodulitesse, võimaldades spetsiaalseid vajadusi katta erinevate eraldi saadaolevate üksiktoodete abil.

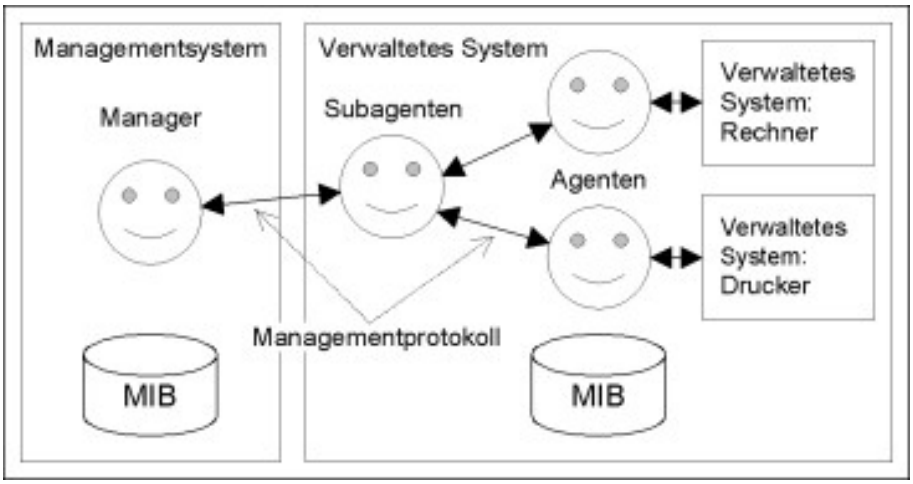
Võrguhaldus on neist kahest vanem ja veidi küpsem haldusvaldkond. Süsteemihaldus on sellega võrreldes veel küllaltki noor teadus, kuid tänu üha suuremale võrgustruktuuride levikule nii firmades kui ametiasutustes ja sellega kaasnevale üha kasvavale heterogeensusele ja keerukusele läheb seda aina rohkem tarvis. Eesmärgiks tuleb seada nende kahe valdkonna integreerimine. Hetkel saadaolevad haldust võimaldavad tooted on loodud selliselt, et nende algne eesmärk on pakkuda kas võrguhalduse või siis süsteemihalduse funktsioone. Tooteid, mis võimaldaksid mõlemaid funktsioone ühendada, alles arendatakse. Reeglina lubavad süsteemihalduse jaoks loodud tooted ka juurdepääsu võrguhalduseks vajaminevatele andmetele.

Tänapäevaste võrkude riist- ja tarkvara heterogeensus teeb süsteemihaldusest vägagi keeruka ülesande. Süsteemihaldust raskendab veel ka asjaolu, et haldus-

tarkvara ja tarkvara, mida hallata tahetakse, peavad suutma teha omavahel väga tihedalt koostööd. Reeglina ei ole aga tänapäeval saadaoleva tarkvara loomisel arvestatud, et see peaks suutma teha koostööd ka haldussüsteemiga. Ühelt poolt on selles süüdi olukord, kus antud valdkonnas puuduvad ühesed standardid, mis garanteeriksid näiteks piisava turvalisuse, teiselt poolt võib põhjuseid otsida sellest, et suuremad tarkvarapaketid on varustatud oma, tootja poolt loodud haldussüsteemiga, kuna tarkvara puudutavaid detaile, mis on haldamiseks vajalikud, ei taheta avalikustada. Näiteks Microsoft Internet Exploreril on olemas oma haldustarkvara, „ Internet Explorer Administration Kit (IEAK)“, mis lubab administraatoril teha turvaseadistusi, mida kasutaja ei saa enam muuta või saab muuta ainult tema jaoks lubatud raamides. Selle vahendi tööfunktsioon on tootja poolt loodud ning see ei allu mitte ühelegi standardile.

Üldjuhul on haldustarkvara arhitektuur tsentraliseeritud ülesehitusega: on olemas tsentraalne halduskeskus või -konsool, mille abil on süsteemi administraatoril võimalik hallata tema hoolde usaldatud võrku ja selles olevaid riist- ja tarkvarakomponente. Eelnimetud ülesehitust kohtab eriti sageli just võrguhaldussüsteemide puhul. Kuna süsteemihalduse valdkonnas ei ole kehtestatud üheseid standardeid, on paljud saadaolevad tooted küll tsentraliseeritud arhitektuuriga, kuid kuna detailides on tegu siiski tootjapoolsete lahendustega, ei ole siinkohal võimalik arhitektuuri kohta täiendavaid üldisi tunnuseid rohkem välja tuua.

Reeglina on võrguhaldussüsteemi aluseks mudel, mis eristab „haldajat“, „agenti“ (ka „haldusagenti“) ja „hallatavaid objekte“ (ka „ managed objects “). Täiendavad koostisosad on haldaja ja agentide vaheliseks kommunikatsiooniks kasutatav protokoll ning andmebaas, nn „MIB“ (Management Information Base). MIB peab olema kättesaadav nii haldajale kui ka kõikidele hallatavatele agentidele. Kontseptsioonist lähtuvalt loetakse hallatavad agendid ja nende MIB hallatava süsteemi
osaks.



Joonis: võrguhaldussüsteem

Joonisel /Managementsystem – haldussüsteem, Manager – haldaja, Verwaltetes System – hallatav süsteem, Subagenten – allagendid, Managementprotokoll – haldusprotokoll, Verwaltetes Süstem: Rechner – hallatav süsteem: arvuti, Verwal-

tetes System: Drucker: hallatav süsteem: printer, MIB – Management Information Base/

Üks agent vastutab kas ühe või mitme hallatava objekti eest. Agente on võimalik organiseerida nende hierarhia alusel: üks agent on sellisel juhul vastutav tema alla koondatud allagentide eest. Iga sellisel moel koostatud käsuliini lõpus asub alati mõni hallatav objekt. Hallatavaks objektiks on kas füüsilisel kujul olemasolev objekt (seade) nagu arvuti, printer või marsruuter, või siis tarkvaraobjekt nagu nt tagaplaani protsess, mille ülesandeks on printimisülesannete haldamine. Seadmetel, mida on võimalik hallata haldussüsteemide abil, on haldusagent reeglina juba tootja poolt „kindlalt“ sisse ehitatud. Kui vastav haldusagent ei suuda aga haldaja poolt kasutatava kommunikatsiooniprotokolliga töötada, läheb tarvis nt tarkvara-haldusagenti, mis oskab protokolli ümber tõlkida. Sarnasel moel võivad ka tarkvaralised komponendid juba algselt sisaldada haldusagente, või siis läheb tarvis haldusagenti, mis on loodud spetsiaalselt vastavate tarkvarakomponentide haldamiseks.

Hallatava süsteemi üksikute komponentidega suhtlemiseks vahetavad haldaja ja vastavad agendid omavahel informatsiooni. Haldussüsteemi jõudluse ja eriti turvalisuse määrab suuresti kommunikatsiooniks kasutatava protokolli liik.

Üldiselt saab haldussüsteeme jaotada neis kasutatava kommunikatsiooniprotokolli alusel kolme kategooriasse(vt lisaks M 2.144 Sobiva võrguhaldusprotokolli valimine):

1. SNMP protokoll (Simple Network Management Protocol), laialt levinud TCP/IP-baasil töötava süsteemihalduse standardprotokoll.
2. CMIP protokoll (Common Management Information Protocol), vähem kasutatav ISO/OSI-baasil töötava süsteemihaldus standardprotokoll.
3. Spetsiaalse, tootja poolt loodud protokolli kasutamine. Enamikel juhtudel on võimalik standardprotokollide kasutamiseks rakendada nn adaptereid, kusjuures reeglina eksisteerib vaid SNMP-ühendusvõimalus.

Kõiges sagedamini kasutatav protokoll on SNMP. SNMP on väga lihtne protokoll, mis tunneb ainult viit erinevat teadete tüüpi ning seetõttu on seda ka väga lihtne juurutada. CMIP protokolli kasutatakse peamiselt telekommunikatsioonivõrkude haldamiseks, ning Interneti- ja Intraneti baasil toimivas halduses ei oma see mingisugust tähendust, kuna see kasutab OSI-protokollipinu, mitte TCP/IP-protokollipinu.

Süsteemihaldussüsteemid on küll reeglina samuti tsentraliseeritud ülesehitusega, et süsteemi oleks võimalik hallata ühest haldusjaamast, kuid konkreetne arhitektuur sõltub siiski sellest, milline on hallatavate süsteemide suurus ning milliseid funktsioone läheb haldamiseks tarvis. Sellekohane tootevalik ulatub väikestest haldusrakenduste valikust, mida on võimalik kasutada väikestes võrkudes üksteise kõrval ilma integreerimata, kuni suurte haldusplatvormideni välja, mis suudavad hallata ülemaailmset mitme tuhande arvutiga firmavõrku.

Teatud osa haldusplatvormidest kasutab komponentidevahelises kommunikatsioonis tootja poolt loodud protokolle. Vastavad süsteemid on reeglina palju suurema jõudlusega ning neid saab kasutada lisaks võrgu- ja süsteemihalduse rakendustele lisas ka terve ettevõtte või ametiasustuse ressursihalduse funktsioonides. Kuna asjakohaseid standardeid on vähe, pole ka standardite turvamehhanismid eriti põhjalikud, mistõttu lubavad tootjapoolsed lahendused kasutada lisaks ka (mittestandardiseeritud) turvalisust mõjutavaid mehhanisme nagu nt krüpteerimist.

Ohud

Infosüsteemide etalonturbe seisukohalt loetakse haldussüsteemidel tüüpilisteks järgmisi ohuallikaid:

Vääramatu jõud:

- G 1.1 Personali väljalangemine
- G 1.2 IT-süsteemi avarii

Organisatsioonilised puudused:

- G 2.27 Ebapiisav või puuduv dokumentatsioon
- G 2.59 Registreerimata komponentide kasutamine
- G 2.60 Võrgu- ja süsteemihalduse puuduv või ebasobiv strateegia
- G 2.61 Isikuandmete volitamatu kogumine

Inimvead:

- G 3.9 IT-süsteemi väär haldus
- G 3.28 Võrgu aktiivkomponentide ebasobiv konfiguratsioon
- G 3.34 Võrguhaldussüsteemi ebasobiv konfiguratsioon
- G 3.35 Töötava serveri elektritoite väljalülitamine
- G 3.36 Sündmuste väär tõlgendamine

Tehnilised rikked:

- G 4.31 Võrgukomponentide rike või tõrge
- G 4.38 Võrgu- või süsteemihaldussüsteemi komponendi rike

Ründed:

- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.9 IT-süsteemide volitamata kasutamine
- G 5.18 Süstemaatiline paroolide mõistatamine
- G 5.28 Teenuse halvamine
- G 5.66 IT-süsteemide volitamatud võrguühendused
- G 5.67 Võrguhaldusfunktsioonide volitamatu käivitamine
- G 5.86 Haldusparameetrite manipulatsioon

Soovitatavad meetmed

Selleks, et tagada kogu loetletud IT-süsteemi turvalisus, tuleb lisaks käesolevale moodulile rakendada veel ka teisi, IT-etalonturbe modelleerimise käigus selguvaid mooduleid.

Hallatav süsteem koosneb eraldiseisvatest arvutitest, võrguühenduselementidest ja füüsilisest võrgust. Iga üksik nimetatud komponent kujutab endast potentsiaalset turvariski terviksüsteemile. Haldustarkvara juurutamisega üksi ei ole üldjuhul võimalik neid riske täielikult kõrvaldada. Seda ainuüksi juba seetõttu, et haldussüsteem ei suuda reeglina kõiki hallatavaid süsteeme ühtmoodi enda alla rakendada. Süsteemi turvalisuse peamiseks eelduseks on ühelt poolt see, et organisatsioon on defineerinud oma turvapoliitika ning teiselt poolt selle ellurakendamine, mis antud juhul väljendub kõige selgemini riist- ja tarkvara konfiguratsioonis. Sellest lähtuvalt tuleks kasutada meetmeid moodulite komplektist nr 3. Lähtemooduliks sobib siinkohal moodul B 4.1 Heterogeensed võrgud .

Kuna haldussüsteemid põhinevad tsentraliseeritud süsteemi ideel, on turvalisuse tagamisel väga oluline roll kesksel haldusjaamal, mida on tarvis spetsiaalselt kaitsta. Haldussüsteemi tsentraalsed komponendid tuleks seetõttu paigutada ruumidesse, mis vastavad serveriruumile esitatud nõudmistele (vt B 2.4 Serveriruum). Serveriruumi puudumisel tuleks alternatiivse lahendusena kasutada serverikappi (vt B 2.7 Kaitsekapid).

Eduka võrgu- ja süsteemihaldussüsteemi ülesehitamiseks tuleb läbida mitmeid etappe, tegeldes kontseptsiooni ja soetamisega kuni lõpliku töötamiseni välja.

Järgnevalt anname ülevaate erinevatest kohustuslikest etappidest ja meetmetest, mida tuleks iga etapi puhul rakendada.

1. Halduse kontseptsiooni väljatöötamine, mis põhineb reeglina juba olemasoleval IT-süsteemil.

- Esitatavate nõudmiste analüüs (vt M 2.168 IT-süsteemi analüüs enne süsteemihaldussüsteemi evitust)
- Kontseptsiooni loomine (vt M 2.169 Süsteemihalduse strateegia väljatöötamine)

2. Haldussüsteemi väljatöötamiseks on vaja esmalt sõnastada halduse kontseptsioonil põhinevad

- haldustootele esitatavad nõudmised (vt M 2.170 Nõuded süsteemihaldussüsteemile) ning nendest lähtuvalt
- langetada valik halduseks sobilike toodete hulgast (vt M 2.171 Sobiva süsteemihaldustoote valimine).

3. Haldussüsteemi turvalisust mõjutavaid meetmeid jaotatakse eri valdkondade vahel järgnevalt:

- halduskontseptsiooni rakendamisel põhinev installeerimine (vt M 4.91 Süsteemihaldussüsteemi turvaline installeerimine) ning
- süsteemihaldussüsteemi kasutamine (vt M 4.92 Süsteemihaldussüsteemi turvalise töö tagamine).

- Selle lisaks tuleb arvestada ka hallatavate süsteemide kasutamist kirjeldavate meetmetega (vt erinevaid mooduleid moodulite komplektis nr 3).

Alljärgnevalt tutvustatakse meetmete kogumit, mida tuleb rakendada valdkonnas „Võrgu- ja süsteemihaldus“:

Planeerimine ja kontseptsioon

- (L) M 2.143 Võrguhalduse kontseptsiooni väljatöötamine
- (L) M 2.144 Sobiva võrguhaldusprotokolli valimine
- (L) M 2.168 IT-süsteemi analüüs enne süsteemihaldussüsteemi evitust
- (L) M 2.169 Süsteemihalduse strateegia väljatöötamine

Soetamine

- (M) M 2.145 Nõuded võrguhaldusinstrumendile
- (L) M 2.170 Nõuded süsteemihaldussüsteemile
- (L) M 2.171 Sobiva süsteemihaldustoote valimine

Rakendamine

- (L) M 4.91 Süsteemihaldussüsteemi turvaline installeerimine

Kasutamine

- (L) M 2.146 Võrguhaldussüsteemi turvaline kasutamine
- (L) M 4.92 Süsteemihaldussüsteemi turvalise töö tagamine
- (L) M 3.11 Hooldus- ja halduspersonali väljaõpe
- (M) M 4.81 Võrgutoimingute audit ja logimine

Valmisolek hädaolukorraks

- (L) M 6.52 Võrgu aktiivkomponentide konfiguratsiooniandmete regulaarne varundamine
- (L) M 6.57 Avariiplaani koostamine haldussüsteemi avarii puhuks

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.4 Võrguhaldussüsteemi turbe regulaarseire
- HG.30 VPNi kasutamise kohustus, kui raadiovõrku kasutatakse magistraalvõrguna
- HG.31 Traadita kohtvõrgu väline turvaaudit
- HG.38 Turvapaikade paigaldatuse regulaarseire

Teabe käideldavus (K)

- HK.9 Varusidekanali nõue

Teabe terviklus (T)

- HT.7 Kasutajate ja nende profiilide perioodiline seire
- HT.71 Lisanõuded võrguhaldusprotokolli valimisele

Teabe konfidentsiaalsus (S)
-

B 4.3 Modem

Modemi abil ühendatakse terminal, nt PC, andmevahetuse eesmärgil läbi avaliku telefonivõrgu teiste terminalidega. Modem muudab terminali digitaalsed signaalid ümber analoog elektrisignaalideks, mis seejärel läbi telefonivõrgu edasi kantakse. Selleks, et kaks IT-süsteemi suudaksid modemi abil teineteisega kommunikeeruda, peab IT-süsteemides olema installeeritud vastav kommunikatsioonitarkvara.

Liigituse poolest eristatakse väliseid, sisemisi ja PCMCIA-modemeid. Välise modemi puhul on tegu iseseisva seadmega, millel on oma voolutoide ning mis on reeglina ühendatud IT-süsteemi külge järjestiksiini abil. Sisemise modemi all peetakse silmas modemi funktsioonidega kaarte, millel puudub iseseisev voolutoide. PCMCIA-modem on krediitkaardi suurune pistikkaart, mida kasutatakse PCMCIA-liidese abil tavaliselt sülearvutites.

Käesolev moodul ISDNi kaudu toimivat andmeedastust ei käsitle, selleks tutvuge eraldi moodulitega B 3.401 Kodukeskjaam (PBX) ja B 4.5 IT-süsteemi kohtvõrguühendus ISDN kaudu .

Ohud

Infosüsteemide etalonturbe seisukohalt loetakse modemi puhul tüüpilisteks järgmisi ohuallikaid:

Inimvead:

- G 3.2 Seadme või andmete hävitamine hooletuse tõttu
- G 3.3 Hooletus turvameetmete suhtes
- G 3.5 Liinide juhuslik kahjustamine

Ründed:

- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.7 Liinide pealtkuulamine
- G 5.8 Liinide manipuleerimine
- G 5.9 IT-süsteemide volitamata kasutamine
- G 5.10 Kaughooldeportide väärkasutus
- G 5.12 Telefonikõnede ja andmesaadetiste pealtkuulamine
- G 5.18 Süstemaatiline paroolide mõistatamine
- G 5.23 Viirused
- G 5.25 Maskeerimine
- G 5.39 Sissetung arvutitesse modemi kaudu

Soovitatavad meetmed

Selleks, et tagada kogu loetletud IT-süsteemi turvalisus, tuleb lisaks käesolevale moodulile rakendada veel ka teisi, IT-etalonturbe modelleerimise käigus selguvaid mooduleid.

Modemi kasutamise puhul tuleb rakendada terve rida erinevaid meetmeid, tegeldes planeerimise ja soetamisega kuni seadme töötamiseni välja. Järgnevalt anname ülevaate erinevatest kohustuslikest etappidest ja meetmetest, mida tuleks iga etapi puhul rakendada.

Planeerimine ja kontseptsioon

Juba enne modemi kasutamist tuleks kohalikud olud üle kontrollida, et selgitada välja, kas täiendava ülepinge kaitse kasutamine on vajalik või mitte. Samuti tuleks kindlaks määrata, mil moel ja millistel töötajatel on õigus modemit kasutamiseks.

Soetamine

Peamised sammud, mida modemi valimisel tuleb järgida, on kirjas meetmes M 2.59z Sobiva modemi valimine .

Rakendamine

Enne modemi kasutuselevõttu tuleb see sobival moel konfigureerida, mille käigus on väga oluline, et võimalikud olemasolevad, tootja poolt ette antud algparoolid saaksid muudetud. Modemi installeerimisel ei tohi tekkida olukorda, kus modemi abil luuakse uus turvamata juurdepääs arvutivõrgule, nt tulemüürist mööda minnes.

Kasutamine

Selleks, et modemi kasutamine ei kujutaks endast uut turvariski, peab olema tagatud modemi turvaline administreerimine ja kasutus. Turvalisust on võimalik saavutada ainult seeläbi, et modemit kasutavad töötajad läbivad piisava asjakohase koolituse. Siia alla kuulub näiteks töötajate teavitamine sellest, et kuna modemiühenduse kasutamisel tekib oht viiruste sissepääsemiseks, tuleb edastatavate andmete puhul olla eriti hoolikas ja andmed võimalike viiruste leidumise suhtes üle kontrollida.

Väljastpoolt tulevate, modemühendust ärakasutavate rünnete raskendamiseks tuleks kaaluda võimalust konfigureerida modem selliselt, et kõik ühendused luuakse ainult seestpoolt väljapoole, ning et sissetulevad ühenduse loomise katsed ühendatakse ainult tagasihelistusfunktsiooniga.

Alljärgnevalt tutvustatakse meetmete kogumit, mida tuleb rakendada valdkonnas „Modem“:

Planeerimine ja kontseptsioon

- (L) M 2.42 Võimalike suhtluspartnerite määramine
- (L) M 2.61 Modemi kasutamise reeglid
- (M) M 4.34z Krüpteerimise, kontrollsummade ja digitaalallkirjade rakendamine
- (L) M 5.32 Sidetarkvara turvaline kasutamine

Soetamine

- (L) M 2.59z Sobiva modemi valimine

Rakendamine

- (L) M 1.38 Modemi õige paigutus

- (M) M 2.46 Krüpteerimise õige korraldus
- (L) M 2.204 Ebaturvalise võrkupääsu tõkestamine
- (L) M 4.7 Algparoolide muutmine
- (M) M 5.30z Olemasoleva tagasihelistusfunktsiooni aktiveerimine
- (L) M 5.31 Modemi sobiv konfigureerimine

Kasutamine

- (L) M 2.60 Modemi turvaline haldus
- (L) M 3.17 Töötajate juhendamine modemi kasutamise alal
- (L) M 4.33 Viirustõrjeprogrammi kasutamine andmekandjate vahetamisel ja andmete edastamisel
- (M) M 5.44z Ühesuunaline ühenduse loomine

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.6 Arvuti paroolkaitse rangemad reeglid
- HG.24 Paroolide regulaarkontroll parooliskänneriga
- HG.38 Turvapaikade paigaldatuse regulaarseire
- HG.74 Modemi kaudu sooritatava kaughoolduse keeld

Teabe käideldavus (K)
-
Teabe terviklus (T)

- HT.51 Lisanõuded teabe hankimisele turvaaukude kohta
- HT.57 Algparoolide muutmise regulaarkontroll
- HT.59 Lisanõuded turvalisele sisselogimisele

Teabe konfidentsiaalsus (S)
-

B 4.4 Virtuaalne privaatvõrk (VPN)

Arvutite ja arvutikoosluste üha suurenev võrgustatus on kutsunud esile muutusi asutuste ja ettevõtete kommunikatsioonikäitumises. Kommunikatsioonivõrke kasutatakse informatsiooni otsimiseks, mis peab kaasa aitama tööülesannete efektiivseks täitmiseks, üha enam aga eelkõige universaalse andmete edastamise keskkonnana. Virtuaalsete privaatvõrkude (VPN-d) abil on võimalik realiseerida turvameetmeid, et edastada tundlikke andmeid mitte usaldusväärsete võrkude, näiteks Interneti kaudu.

Varasemates infosüsteemide etalonturbe kataloogides käsitleti moodulis B 4.4 teemat „Virtuaalne privaatvõrk (VPN)" (Remote Access). Käesolev moodul sisaldab soovitusi site-to-site (kahe võrgu vaheline VPN), end-to-end (otspunktide vaheline VPN) ja end-to-site (sissepääsu VPN) rakenduste kasutamiseks. Kaugpääsuks vajalikud standardsed turvameetmed on integreeritud käesolevasse moodulisse pealkirja all Sissepääsu VPN-d (end-to-site VPNs).

Virtuaalne privaatvõrk (VPN) on võrk, mille käitamine toimub füüsiliselt teises võrgus, näiteks Internetis, kuid on loogiliselt sellest võrgust eraldatud. Virtuaalsed privaatvõrgud võivad krüptograafiliste meetodite abil kaitsta andmete terviklust ja konfidentsiaalsust. Kommunikatsioonipartnerite turvaline autentimine on võimalik ka juhul, kui mitmed võrgud või arvutid on omavahel ühendatud renditud liinide või avalike võrkude kaudu.

Eristatakse järgmisi virtuaalsete privaatvõrkude variante või kombinatsioone:

- Site-to-site VPN : kaks arvutivõrku on virtuaalse privaatvõrgu kaudu ühendatud, näiteks selleks, et siduda turvaliselt asutuse filiaale.
- End-to-end-VPN : selle variandi korral paigaldatakse kahe lõppseadme vahele üks VPN: Kui ühe VPN-iga ühendatakse spetsiaalselt kaks serverit, nimetatakse seda tihti ka host-to-host ühenduseks.
- End-to-end-VPN (või Remote-Access VPN): lõppseadme ja võrgu vahele paigaldatakse VPN. Seda varianti kasutatakse tavaliselt siis, kui mobiilne kasutaja tahab teel olles oma sülearvutilt VPN- juurdepääsusõlme kaudu siseneda oma asutuse LAN-i. Seda liiki juurdepääsu nimetatakse ka kaugpöörduseks.

Kahe võrgu vahelisi VPN-e (site-to-site VPN-s) kasutatakse ühe asutuse või ettevõtte filiaalide detsentraalsete LAN-ide vahelise võrgu loomiseks. Otspunktide vaheliste VPN-de (end-to-end-VPN-s) abil saavad äripartnerid või kliendid juurdepääsu asutuse tsentraalsele IT-süsteemile. Sissepääsu VPN-i (Remote-Access-VPN) abil saavad kaugtöötajad juurdepääsu ettevõtte või asutuse LAN-ile.

Ohud

Käesolev moodul käsitleb ohtusid, mis on virtuaalsete privaatvõrkude kasutamisel olulise tähtsusega. Nende hulka kuuluvad organisatsioonilised puudused, näiteks ebapiisav planeerimine, aga ka inimvead (näiteks puuduliku haldustöö tagajärjel). Lisaks sellele on virtuaalsed privaatvõrgud siseandmete edastamise tõttu mitte usaldusväärsete võrkude kaudu pidevas ohus.
Infosüsteemide etalonturbes peetakse virtuaalse privaatvõrgu kasutamist mõjutavateks ohtudeks järgnevaid ohtusid:
Vääramatu jõud

- G 1.2 IT-süsteemi avarii

Organisatsioonilised puudused:

- G 2.2 Reeglite puudulik tundmine
- G 2.16 Sülearvuti reguleerimata edasiandmine
- G 2.19 Krüpteerimise halb korraldus
- G 2.22 Logiandmete analüüsimata jätmine
- G 2.24 Kaitsetus välisvõrgu vastu
- G 2.37 Sideliinide kontrollimatu kasutamine
- G 2.87 Ebaturvalised protokollid avalikes võrkudes
- G 2.128 VPN-i juurutamise ebapiisav või puuduv planeerimine
- G 2.129 VPN-i kasutamise ebapiisavad või puuduvad reeglid
- G 2.130 VPN-i krüpteerimisprotseduuri ebaõnnestunud valik
- G 2.131 VPN-i puudulik seire

Inimvead:

- G 3.16 Väär pääsuõiguste haldus
- G 3.40 Vead VPN-ide autentimisteenuse kasutamisel
- G 3.41 VPN-teenuste väär kasutamine
- G 3.42 VPN-klientsüsteemide kaugpöörduse ebaturvaline konfiguratsioon
- G 3.43 Puudulik paroolihooldus
- G 3.44 Teabe hooletu kasutamine
- G 3.90 VPN-ide väär haldus
- G 3.91 Väärkasutusest tingitud VPN-ühenduse katkemine

Tehnilised rikked:

- G 4.35 Ebaturvaline krüptoalgoritm
- G 4.57 Häired IP-kõne kasutamisel üle VPNi
- G 4.69 Probleemid IPSec-i konfigureerimisel
- G 4.70 VPN-i komponentide ebaturvaline standardseadistus

Ründed:

- G 5.22 Kaasaskantava IT-süsteemi vargus
- G 5.71 Tundliku informatsiooni konfidentsiaalsuse kadu
- G 5.92 VPN-klientsüsteemi kasutamine VPN-serverina
- G 5.93 VPN-ühenduse kasutamise võimaldamine kõrvalistele isikutele

Soovitatavad meetmed

Vaadeldava IT-koosluse turvalisuse tagamiseks tuleb lisaks käesolevale moodulile rakendada veel teisigi mooduleid vastavalt infosüsteemide etalonturbe rakendusjuhendi modelleerimise tulemustele.

Virtuaalsete privaatvõrkude edukaks ülesehitamiseks on vaja rakendada terve rida meetmeid, alustades nõude analüüsiga, millele järgneb planeerimine, kontseptsiooni koostamine, installeerimine ja käitus. Eriti tähtis on sobiva ootamatuste plaani koostamine, et tagada avarii korral kiire kommunikatsiooniühenduse taastamise.

Järgnevalt on loetletud vajalikud meetmed virtuaalse privaatvõrgu korrakohaseks juurutamiseks ja turvaliseks käitlemiseks:

VPNi kasutamise planeerimine

Kui on vastu võetud otsus kasutada teatud ühendusteks virtuaalset privaatvõrku, tuleb koostada selle ülesehitamiseks plaan ja kontseptsioon. Seejuures võib ühes asutuses kasutada mitmesuguseid VPNi variante. Esimeseks sammuks on alati sellisele süsteemile esitatavate vajaduste kindlaksmääramine (vaata M M 2.415 VPN vajaduste analüüs). Alles siis, kui vajadused on selgelt defineeritud, saab alustada vastava kontseptsiooni koostamisega (M 2.416 VPNi kasutamise planeerimine ja M 2.417 VPNi tehnilise teostuse planeerimine).

Erilist tähelepanu tuleb pöörata asutusesisese VPNi turvapoliitika väljatöötamisele, mis tuleb vastavusse viia üldise IT turvapoliitikaga. Aspektid, millega seejuures tuleb arvestada, on koondatud meetmesse M 2.418 VPNi kasutamise turvapoliitika koostamine .

Soetamine

Otsustava tähtsusega planeeritud vajaduste rakendamiseks on sobiva VPN-toote valimine. VPN-komponentide valikul on tähtis järgida meetmes M 2.419 Sobivate VPN-toodete valimine antud soovitusi. Kui virtuaalse privaatvõrgu ülesehitamine tellitakse väliselt teenusetarnijalt, tuleb arvestada meetmes M 2.420 Trusted VPN teenusepakkuja valimine valimine esitatud aspektidega.

Rakendamine

Pärast organisatoorsete ja planeerimistööde lõpetamist võib alustada VPNi installeerimisega. Seejuures tuleb eriti järgida meedet M 4.319 VPNi lõppseadmete turvaline installeerimine . Kui installeerimine on lõpetatud, tuleb süsteem viia seisundisse, mis võimaldab selle turvalist kasutamist, et seejärel oleks võimalik alustada jooksva tööga (vaata M 4.320 VPNi turvaline konfigureerimine). VPN-lõppseadmete küllaldaseks kaitseks tuleb need integreerida turvainfrastruktuuri vastavalt meetmele M 4.224 Virtuaalsete privaatvõrkude integreerimine turvalüüsidesse .

Kasutamine

Ka jooksva töö käigus tuleb tagada virtuaalsete privaatvõrkude turvalisus (vt M 4.321 VPNi turvaline käitamine).

Likvideerimine

Unustatud VPN-pääsupunktid või partnerite pääsupunktid, kellega koostöö on juba lõpetatud, kujutavad endast turvaaukusid ning need tuleb sulgeda nii kiiresti kui võimalik (vt M 4.322 Mittevajalike VPN-pääsude blokeerimine).

Valmisolek hädaolukorraks

Sõltuvalt käideldavusele esitatavatest nõuetest võib virtuaalse privaatvõrgu seiskumine tekitada väiksemaid või suuremaid probleeme. Nende seljatamiseks tuleb luua sobilik hädaolukorraks valmisoleku kontseptsioon (vt M 6.109 Virtuaalse privaatvõrgu (VPN) hädaolukorraks valmisoleku plaan).

Alljärgnevalt tutvustatakse turvameetmete kogumit mida tuleb rakendada valdkonnas "Virtuaalne privaatvõrk".

Planeerimine ja kontseptsioon

- (L) M 2.415 VPN vajaduste analüüs
- (L) M 2.416 VPNi kasutamise planeerimine
- (M) M 2.417 VPNi tehnilise teostuse planeerimine
- (L) M 2.418 VPNi kasutamise turvapoliitika koostamine
- (L) M 3.65w Sissejuhatus VPNi põhimõistetesse
- (M) M 4.113z Autentimisserveri kasutamine kaugpöördussüsteemis
- (M) M 5.76w Sobivate tunneldusprotokollide kasutamine VPN-süsteemis
- (M) M 5.77z Alamvõrkude rajamine

Soetamine

- (M) M 2.419 Sobivate VPN-toodete valimine
- (M) M 2.420 Trusted VPN teenusepakkuja valimine

Rakendamine

- (M) M 4.224z Virtuaalsete privaatvõrkude integreerimine turvalüüsidesse
- (M) M 4.319 VPNi lõppseadmete turvaline installeerimine
- (L) M 4.320 VPNi turvaline konfigureerimine
- (L) M 5.122 Sülearvuti turvaline ühendamine kohtvõrguga
- (M) M 5.148 Turvaline välisvõrguühendus OpenVPN-i abil
- (M) M 5.149 Turvaline välisvõrguühendus IPSec-i abil

Kasutamine

- (L) M 4.321 VPNi turvaline käitamine

Likvideerimine

- (L) M 4.322 Mittevajalike VPN-pääsude blokeerimine

Valmisolek hädaolukorraks

- (M) M 6.109 Virtuaalse privaatvõrgu (VPN) hädaolukorraks valmisoleku plaan

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.6 Arvuti paroolkaitse rangemad reeglid
- HG.24 Paroolide regulaarkontroll parooliskänneriga
- HG.25 Kaugpöörduste kohustuslik logimine
- HG.30 VPNi kasutamise kohustus, kui raadiovõrku kasutatakse magistraalvõrguna
- HG.31 Traadita kohtvõrgu väline turvaaudit
- HG.38 Turvapaikade paigaldatuse regulaarseire

Teabe käideldavus (K)
-
Teabe terviklus (T)

- HT.51 Lisanõuded teabe hankimisele turvaaukude kohta
- HT.57 Algparoolide muutmise regulaarkontroll
- HT.58 Lisanõuded tarbetute kontode ja terminalide blokeerimisele
- HT.59 Lisanõuded turvalisele sisselogimisele

Teabe konfidentsiaalsus (S)
-

B 4.5 IT-süsteemi kohtvõrguühendus ISDN kaudu

ISDN (Integrated Services Digital Network) on digitaalne sidevõrk, mille vahendusel on võimalik kasutada erinevaid teenuseid nagu telefon ja faks, samuti saab selle kaudu edastada andmeid ja pildimaterjali.

Käesolev peatükk käsitleb eemalasuva IT-süsteemi ühendamist kohtvõrku avaliku ISDN võrgu abil. Eemalasuva IT-süsteemi juures toimub ühendamine ISDN-adapterkaardiga, millel on S0-liides. Ühendamine kohtvõrku toimub marsruuteri abil, mis on ühendatud avalikku ISDN-võrku S2M-liidese abil.

Sellisel kujul ühendatakse eemalasuvaid IT-süsteeme tavaliselt kaugtöö eesmärgil.

Ohud

Infosüsteemide etalonturbe seisukohalt loetakse IT-süsteemi kohtvõrguühendusel ISDNi kaudu tüüpilisteks järgmisi ohuallikaid:

Vääramatu jõud:

- G 1.2 IT-süsteemi avarii

Organisatsioonilised puudused:

- G 2.6 Volitamata pääs ruumidesse
- G 2.7 Õiguste volitamata kasutamine
- G 2.9 Halb kohanemine IT muutustega
- G 2.19 Krüpteerimise halb korraldus
- G 2.24 Kaitsetus välisvõrgu vastu
- G 2.32 Võrgu ebapiisav võimsus
- G 2.37 Sideliinide kontrollimatu kasutamine

Inimvead:

- G 3. 1 Andmete konfidentsiaalsuse või tervikluse kadu kasutaja vea tõttu
- G 3.6 Koristajad jm väljastpoolt tellitud töötajad
- G 3.13 Väära või soovimatu andmekogumi saatmine
- G 3.16 Väär pääsuõiguste haldus

Tehnilised rikked:

- G 4.25 Lahutamata ühendused

Ründed:

- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.7 Liinide pealtkuulamine
- G 5.8 Liinide manipuleerimine
- G 5.9 IT-süsteemide volitamata kasutamine
- G 5.10 Kaughooldeportide väärkasutus
- G 5.14 Telefoniteenuste vargus
- G 5.16 Ohud hoolde- ja haldustööde ajal
- G 5.18 Süstemaatiline paroolide mõistatamine

- G 5.25 Maskeerimine
- G 5.39 Sissetung arvutitesse modemi kaudu
- G 5.48 IP-aadressi võltsimine
- G 5.61 Marsruuterite kaughaldusportide väärkasutus
- G 5.63 ISDN-i D-kanali manipulatsioonid

Soovitatavad meetmed

Selleks, et tagada kogu loetletud IT-süsteemi turvalisus, tuleb lisaks käesolevale moodulile rakendada veel ka teisi, IT-etalonturbe modelleerimise käigus selguvaid mooduleid.

Käesolev peatükk keskendub esmajoones turvalise side tagamisele. Täiendavad, sides osalevate IT-süsteemide turvalisust kajastavad meetmed leiate vastavatest IT-süsteeme käsitlevatest moodulitest.

IT-süsteemi kohtvõrguühenduseks ISDNi kaudu tuleb rakendada terve rida erinevaid meetmeid, tegeldes planeerimise, kontseptsiooni ja soetamisega kuni igapäevase kasutamiseni välja. Järgnevalt anname ülevaate erinevatest kohustuslikest etappidest ja meetmetest, mida tuleks iga etapi puhul rakendada.

Planeerimine ja kontseptsioon

IT-süsteemide kaugpöörduse turvaliseks kasutamiseks tuleb arvestada terve rea sidealast turvalisust tagavate meetmetega (vt M 5.32 Sidetarkvara turvaline kasutamine).

Soetamine

Peamised valikriteeriumid, mida ISDN-liideskaartide valimisel tuleb järgida, on kirjas M 2.59 Sobiva modemi valimine .

Rakendamine

ISDN-juurdepääsu konfigureerimisel tuleb lähtuda põhireeglist, mis ütleb, et kõik mittevajalikud teenused ja funktsioonid tuleb välja lülitada, sest nende töös-hoidmine toob endaga kaasa vaid ebavajalikke riske. Reaalselt kasutatavad funktsioonid tuleb konfiguratsioonidega võimalikult hästi kaitsta, mille alla kuulub ilmtingimata ka viivitamatu tootjapoolsete algparoolide muutmine. Kindlaks määratud konfiguratsioon tuleb kirjalikult talletada ning võimalike muudatuste korral tuleb vastavat dokumentatsiooni täiendada.

Oluliseks aspektiks ISDN-juurdepääsu installeerimisel on lisaks ka asjaolu, et juurdepääsu loomisega ei tohi kahjustada olemasoleva arvutivõrgu turvalisust. Eriti oluline on siinkohal vältida olukorda, kus ühenduste loomisel väliste võrkudega minnakse mööda olemasolevast tulemüüri süsteemist ja muudetakse tulemüüri süsteem seeläbi suures osas kasutuks.

Kasutamine

ISDN-ühenduse võimalikku väärkasutust on võimalik kergemini avastada tekkinud logiandmete regulaarse kontrollimisega. Pisteline programmeeritud sihtkoha aadresside ja logide kontrollimine aitab vältida , et eksikombel ei loodaks ühendusi valede sidepartneritega.

Alljärgnevalt tutvustatakse meetmete kogumit, mida tuleb rakendada valdkonnas „IT-süsteemi kohtvõrguühendus ISDNi kaudu“:

Planeerimine ja kontseptsioon

- (L) M 2.42 Võimalike suhtluspartnerite määramine
- (M) M 4.34z Krüpteerimise, kontrollsummade ja digitaalallkirjade rakendamine
- (L) M 5.32 Sidetarkvara turvaline kasutamine
- (M) M 5.47z Kinnise kasutajagrupi konfigureerimine

Rakendamine

- (L) M 1.43 Võrgu aktiivkomponentide turvaline paigutus
- (M) M 2.46 Krüpteerimise õige korraldus
- (L) M 2.107 ISDN-liideste konfiguratsiooni dokumenteerimine
- (L) M 2.204 Ebaturvalise võrkupääsu tõkestamine
- (L) M 4.7 Algparoolide muutmine

Kasutamine

- (L) M 5.29 Sihtaadresside ja logide perioodiline kontroll

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.6 Arvuti paroolkaitse rangemad reeglid
- HG.24 Paroolide regulaarkontroll parooliskänneriga
- HG.38 Turvapaikade paigaldatuse regulaarseire

Teabe käideldavus (K)

- HK.9 Varusidekanali nõue

Teabe terviklus (T)

- HT.51 Lisanõuded teabe hankimisele turvaaukude kohta
- HT.57 Algparoolide muutmise regulaarkontroll
- HT.59 Lisanõuded turvalisele sisselogimisele

Teabe konfidentsiaalsus (S)
-

B 4.6 Traadita kohtvõrgud

Wireless LANs (WLANs) ehk traadita kohtvõrgu tehnoloogia pakub võimaluse luua väikese kuluga traadita kohtvõrke või laiendada olemasolevaid kaablivõrke. WLAN tähistust kasutatakse traadita kontvõrkude puhul, mis põhinevad IEEE 802.11 standardite grupil, mille on väljastanud Institute of Electrical and Electronics Engineers (IEEE).

Tänu nende lihtsale installeerimisele kasutatakse traadita kohtvõrke ka ajutiste võrgulahenduste jaoks, nt messidel või väiksematel üritusel. Sellele lisaks on avalikes kohtades nagu lennujaamades või rongijaamades võimalik luua netijuurdepääse nn Hotspotide ehk traadita Interneti pääsupunktide abil. Seeläbi võimaldatakse mobiilsetele kasutajatele pääs Internetti või ühendus firmavõrguga. Kommunikatsioon toimib sellistel juhtudel enamasti keskse pääsupunkti, Access Pointi , ja mobiilse lõppseadme WLAN-komponentide vahel (nt WLAN-USB-pulga või vastava WLAN võrgukaardi vahel).

Suurem osa turul saadaolevatest WLAN komponentidest põhinevad aastal 2003 IEEE poolt väljastatud spetsifikatsiooni täiendusel 802.11g, mis lubab andmekiirust kuni 54 Mbit/s. Sellele lisaks on olemas mõningaid süsteeme, mis toetavad ainult 1999. aastal väljatulnud täiendust IEEE 802.11b, mille puhul on andmekiiruseks võimalik saavutada maksimaalselt 11 Mbit/s. Mõlemad täiendused toimivad samas, litsentsivabas 2,4 GHz.

Turvamehhanismid on ära toodud standardis IEEE 802.11 ja selle täienduses IEEE 802.11i. Esialgses standardis 802.11 on Wired Equivalent Privacy (WEP) määratletud kui turvamehhanism, kuid WEPi mitmete kitsaskohtade tõttu ei saa seda praegu enam piisavalt turvaliseks pidada. Seetõttu arendas vastav tootjate liit, WiFi-Alliance , välja turvamehhanismi Wi-Fi Protected Access (WPA). Selle lahenduse puhul rakendatakse lisaks staatiliste võtmete täiendusele, nn Pre-Shared Keys , ka dünaamilist võtmete haldust TKIP andmeturbeprotokolli abil. Nimetatud mehhanismid on suures osas integreeritud 2004. aastal avaldatud ametlikku täiendusse IEEE 802.11i, kusjuures kasutatakse seal krüpteerimiseks, samamoodi nagu WPA2 puhul, standardit AES, (Advanced Encryption Standard), mitte RC4 nagu WEP ja WPA puhul. Lisaks on IEEE 802.11i määratlenud ka AES krüpteerimis- ja tervikluse kontrollimehhanismi juurutamise standardiks CCMP, (Counter Mode with CBC-MAC Protocol). Nimetatud meetod on pikaajaliselt toimiv, kuid nõuab vastupidiselt TKIP-variandile uue riistvara kaasamist. Autentimismeetodiks määrab täiendus 802.11i laiendatava autentimisprotokolli EAP, (Extensible Authentication Protocol), mis vastab standardile IEEE 802.1X.

Käesoleva mooduli eesmärgiks on näidata, kuidas luua kontseptsioon organisatsioonisiseseks traadita kohtvõrkude kasutamiseks ning kuidas tagada selle ellurakendamine.

Ohud

Infosüsteemide etalonturbe seisukohalt loetakse traadita kohtvõrkude kasutamise puhul tüüpilisteks järgmisi ohuallikaid:

Vääramatu jõud:

- G 1.17 Raadiovõrgu väljalangemine

Organisatsioonilised puudused:

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.2 Reeglite puudulik tundmine
- G 2.4 Turvameetmete ebapiisav järelevalve
- G 2.117 Traadita kohtvõrgu ebapiisav või puuduv planeerimine
- G 2.118 Traadita kohtvõrgu kasutamise ebapiisav reguleerimine
- G 2.119 Traadita kohtvõrgu autentimismeetodite ebaõnnestunud valik
- G 2.120 Turvalisust tagavate IT-süsteemide ebasobiv paigutus
- G 2.121 Traadita kohtvõrkude ebapiisav kontrollimine

Inimvead:

- G 3.3 Hooletus turvameetmete suhtes
- G 3.9 IT-süsteemi väär haldus
- G 3.38 Vead konfigureerimisel ja kasutamisel
- G 3.43 Puudulik paroolihooldus
- G 3.84 Traadita kohtvõrgu taristu väär konfiguratsioon

Tehnilised rikked:

- G 4.60 Raadiolainete kontrollimatu levi
- G 4.61 Traadita kohtvõrgu ebausaldusväärsed või puuduvad turbemehhanismid

Ründed:

- G 5.71 Tundliku informatsiooni konfidentsiaalsuse kadu
- G 5.137 Traadita sideühenduse andmete analüüs
- G 5.138 WLAN-i komponentide vastu suunatud ründed
- G 5.139 WLAN-i side pealtkuulamine

Soovitatavad meetmed

Selleks, et tagada kogu loetletud IT varade turvalisus, tuleb lisaks käesolevale moodulile rakendada veel ka teisi, IT-etalonturbe modelleerimise käigus selguvaid mooduleid.

Traadita kohtvõrkude kasutamisel tuleb rakendada erinevaid meetmeid, tegeldes kontseptsiooni ja soetamisega kuni kasutamiseni välja. Järgnevalt anname ülevaate erinevatest kohustuslikest etappidest ja meetmetest, mida tuleks iga etapi puhul rakendada.

Planeerimine ja kontseptsioon

Traadita kohtvõrgu turvalisusele pannakse alus juba planeerimise faasis. Hoolikalt läbimõeldud strateegia (vt M 2.381 Traadita kohtvõrgu kasutamise strateegia väljatöötamine) ja õige WLAN-standardi ja sellega seotud krüpteerimismeetodi valik (vt M 2.383 Sobiva traadita kohtvõrgu standardi valik ja M 2.384 Sobiva traadita kohtvõrgu krüpteerimisviisi valik) on traadita kohtvõrgu turvalisel kasutamisel nurgakiviks. Erinevates traadita kohtvõrgu turvalisust puudutavates mõistetes aitab ülevaadet luua meede M 3.58 Sissejuhatus traadita kohtvõrgu põhimõistetesse .

Kõik vastuvõetud otsused, mis puudutavad turvaseadistusi, väljavalitud WLAN-standardeid, samuti traadita kohtvõrgu kasutamise ja administreerimise alased reeglid tuleb kirjalikult talletada ja koondada ühtsesse traadita kohtvõrgu turvajuhendisse (vt M 2.382 Traadita kohtvõrgu turvajuhendi väljatöötamine).

Soetamine

Traadita kohtvõrgu komponentide valikul tuleb rakendada meedet M 2.385 Sobivate traadita kohtvõrgu komponentide valik . Traadita kohtvõrkude standardid, protokollid ja turvamehhanismid muutuvad väga kiirelt. Seetõttu on traadita kohtvõrgud sagedasti migratsioonifaasis.

Traadita kohtvõrgu komponentide või tervete WLAN-valdkondade migratsioonifaaside korral tuleb arvestada meetmega M 2.386 Traadita kohtvõrgu migratsioonietappide hoolikas planeerimine .

Rakendamine

Pärast komponentide soetamist, kui asutakse traadita kohtvõrgu sisseseadmise juurde, tuleb arvestada, et pääsupunktide (Access Points) paigutus ei tohi olla suvaline (vt M 1.63 Sobiv pääsupunktide paigutus), ning et traadita kohtvõrgu ühendamisel olemasolevasse kaablitest koosnevasse infrastruktuuri on samuti omad nõuded (vt M 5.139 Traadita kohtvõrgu turvaline ühendamine kohtvõrguga). Samuti tuleb jälgida, et erinevate traadita kohtvõrgu komponentide konfigureerimine, nt pääsupunktid, (vt M 4.294 Pääsupunktide turvaline konfigureerimine) või WLAN-kliendid (vt M 4.295 Traadita kohtvõrgu kliendi turvaline konfiguratsioon), toimuks alati kooskõlas turvasuuniste ja väljatöötatud turvastrateegiaga.

Traadita kohtvõrgu kasutajaid ja administraatorid vajavad kõikidel juhtudel asjakohast koolitust ning neid tuleb teavitada traadita kohtvõrgu väärast kasutamisest tingitud ohtudest, selleks, et turvariske võimalikult maandada (vt M 3.59 Traadita kohtvõrgu turvalise kasutamise koolitus).

Kui on otsustatud, et traadita kohtvõrgu teenuse installeerib, konfigureerib, st teenindab, väljastpoolt tulev teenusepakkuja, tuleb tingimata arvestada meetmega M 2.387 Kolmandate osapoolte kasutamine traadita kohtvõrgu paigaldamisel, konfigureerimisel ja nõustamisel .

Kasutamine

Pärast traadita kohtvõrgu kasutuselevõttu ja kõikide selle kasutajate piisavat koolitust tuleb ühelt poolt regulaarsete auditite ga (vt M 4.298 Traadita kohtvõrgu komponentide regulaarne audit) tagada, et ükski turvalisust puudutav seadistus ei oleks aegunud ning teiselt poolt regulaarsete turvakontrollidega (vt M 5.141 Regulaarsed traadita kohtvõrgu turvakontrollid) kindlustada, et vastavad seadistused on piisavalt tõhusad. Eelnevale lisaks tuleb jooksvalt tagada kõikide traadita kohtvõrgu komponentide turvaline kasutamine (vt M 4.297 Traadita kohtvõrgu komponentide turvaline kasutamine).

Side turvaliseks muutmisel ei saa üle ega ümber traadita kohtvõrgus kasutatavate krüptovõtmete haldusest (vt M 2.388 Asjakohane traadita kohtvõrgu võtmehaldus). Võtmete haldust võib kergendada WLAN-halduslahendus, samuti võimaldab see traadita kohtvõrgu tsentraliseeritud haldamist (vt M 4.296 Traadita kohtvõrgu sobiva haldussüsteemi kasutamine).

Väljavahetamine

WLAN-komponentide tööst kõrvaldamisel tuleb vastavad konfiguratsiooniseaded nagu nt võrgunimi või SSID standardväärtuste peale tagasi muuta ning võimalik WLAN-komponentidele salvestatud info WLANi kaudu toimiva võrguliikluse või pääsuandmete kohta kustutada (vt M 2.390 Traadita kohtvõrgu komponentide kasutusest kõrvaldamine).

Valmisolek hädaolukorraks

Kui traadita kohtvõrgu puhul on tuvastatud ründeid, peavad nii traadita kohtvõrgu kasutajad kui ka administraator teadma, kuidas nad peavad käituma (vt M 6.102 Käitumisreeglid traadita kohtvõrkude turvaintsidentide puhul). Selle alusel koostatakse hädaolukorraks valmisoleku plaan, mis sätestab vajalikud sammud ja määrab kindlaks isikud, keda tuleb asetleidnud turvaintsidendi korral teavitada. Sellele lisaks võib olla hädavajalik luua traadita tagavara kohtvõrk, et häda korral oleks võtta kiire lahendus sideserverite ühenduste taastamiseks. Siinjuures tuleb alati veenduda, et ka varuks loodud traadita kohtvõrgusüsteem vastaks samadele turvanõuetele nagu tavakasutuse WLAN. Varuks loodud traadita kohtvõrgu puhul tuleb samuti rakendada kõiki käesoleva mooduli meetmeid, kuna seda tuleb vaadelda kui eraldiseisvat WLANi. Üldised juhised varuga loodavate sideühenduste loomiseks on kokku võetud meetmes M 6.75 Varu-sidekanalid .

Traadita kohtvõrgu turvaliseks kasutamiseks peavad ka sellega seotud kliendid olema turvaliselt konfigureeritud, samuti tuleb neid regulaarselt hooldada ja hallata. Vastavad IT-turvasuunised leiate IT-etalonturbe kataloogide vastavatest moodulitest.

Alljärgnevalt tutvustatakse meetmete kogumit, mida tuleb rakendada valdkonnas „Traadita kohtvõrgu kasutamine“:

Planeerimine ja kontseptsioon

- (L) M 2.381 Traadita kohtvõrgu kasutamise strateegia väljatöötamine
- (L) M 2.382 Traadita kohtvõrgu turvajuhendi väljatöötamine
- (L) M 2.383 Sobiva traadita kohtvõrgu standardi valik
- (L) M 2.384 Sobiva traadita kohtvõrgu krüpteerimisviisi valik
- (L) M 3.58w Sissejuhatus traadita kohtvõrgu põhimõistetesse
- (M) M 5.138z RADIUS serverite kasutamine

Soetamine

- (L) M 2.385 Sobivate traadita kohtvõrgu komponentide valik
- (M) M 2.386z Traadita kohtvõrgu migratsioonietappide hoolikas planeerimine

Rakendamine

- (L) M 1.63 Sobiv pääsupunktide paigutus
- (M) M 2.387z Kolmandate osapoolte kasutamine traadita kohtvõrgu paigaldamisel, konfigureerimisel ja nõustamisel
- (L) M 3.59 Traadita kohtvõrgu turvalise kasutamise koolitus
- (L) M 4.294 Pääsupunktide turvaline konfigureerimine
- (L) M 4.295 Traadita kohtvõrgu kliendi turvaline konfiguratsioon

- (L) M 5.139 Traadita kohtvõrgu turvaline ühendamine kohtvõrguga
- (L) M 5.140 Traadita kohtvõrgu jaotussüsteemi ehitus

Kasutamine

- (L) M 2.388 Asjakohane traadita kohtvõrgu võtmehaldus
- (M) M 2.389z Avalike pääsupunktide turvaline kasutus
- (M) M 4.293z Avalike pääsupunktide turvaline käitamine
- (L) M 4.296 Traadita kohtvõrgu sobiva haldussüsteemi kasutamine
- (L) M 4.297 Traadita kohtvõrgu komponentide turvaline kasutamine
- (L) M 4.298 Traadita kohtvõrgu komponentide regulaarne audit
- (L) M 5.141 Regulaarsed traadita kohtvõrgu turvakontrollid

Väljavahetamine

- (L) M 2.390 Traadita kohtvõrgu komponentide kasutusest kõrvaldamine

Valmisolek hädaolukorraks

- (M) M 6.75z Varu-sidekanalid
- (L) M 6.102 Käitumisreeglid traadita kohtvõrkude turvaintsidentide puhul

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.6 Arvuti paroolkaitse rangemad reeglid
- HG.24 Paroolide regulaarkontroll parooliskänneriga
- HG.38 Turvapaikade paigaldatuse regulaarseire
- HG.42 Nõuded traadita kohtvõrgu migratsioonietappide planeerimisele
- HG.43 Lisanõuded traadita kohtvõrgu tööde väljasttellimisele
- HG.44 Avalike pääsupunktide turvaline opereerimine ja kasutus
- HG.51 Traadita kohtvõrgu IP-adresseerimine
- HG.52 Traadita ründetuvastus- ja -tõkestussüsteemid
- HG.53 Avalike pääsupunktide kasutamise piiramine
- HG.76 Traadita kohtvõrgu nimevalikunõuded

Teabe käideldavus (K)

- HK.9 Varusidekanali nõue

Teabe terviklus (T)

- HT.42 VPNi kasutuskohustus traadita võrgus
- HT.43 Keskse autentimisserveri kasutamine
- HT.51 Lisanõuded teabe hankimisele turvaaukude kohta
- HT.57 Algparoolide muutmise regulaarkontroll
- HT.59 Lisanõuded turvalisele sisselogimisele

Teabe konfidentsiaalsus (S)

- HS.73 Traadita kohtvõrgu kasutuskeeld

B 4.7 IP-kõne (VOIP)

IP-kõne võimaldab edastada informatsiooni signaalide kujul, näiteks telefonikõnet, kasutades spetsiaalseid signaliseerimisprotokolle. Edastatavad andmed nagu kõne ja video suunatakse edasi vastava meediatranspordiprotokolli vahendusel. Mõlemat protokolli läheb tarvis multimeediaühenduse loomiseks ja käigushoidmiseks. Mõningate tehnoloogiate puhul kasutatakse ühte ja sama protokolli nii signaalide kui ka meediate edastamiseks.

Käesolev moodul käsitleb lõppseadmete ja vahevara (Middleware) turvaaspekte. Siin kirjeldatavad komponendid sarnanevad oma funktsioonilt moodulis B 3.401 Kodukeskjaam (PBX) kirjeldatud telekommunikatsiooniseadmetele.

Ohud

IP-kõne kasutamise puhul esineb terve rida ohtusid. Paljud nendest ohtudest taanduvad andmevõrkudele, mida kasutatakse IP-kõne edastamiseks. Siia alla kuuluvad mitmesugused ründed konfidentsiaalsuse vastu nagu nuhutamine (sniffing) ning ründed kättesaadavuse halvamiseks.

Üldjuhul peab paika tõsiasi, et iga üksiku komponendi turvalisus sõltub suuresti tema kasutusalast ehk siinkohal, kas seda kasutatakse lõppseadmena või vahevarana. Samuti mõjutab iga üksik ohuallikas omakorda ka kogu süsteemi turvalisust.

Infosüsteemide etalonturbe seisukohalt loetakse IP-kõne kasutamise puhul tüüpilisteks järgmisi ohuallikaid:

Organisatsioonilised puudused:

- G 2.112 IP-kõne kasutamise ebapiisav planeerimine
- G 2.113 Võrgumahu ebapiisav planeerimine IP-kõne juurutamisel

Inimvead:

- G 3.7 Käsitsemisvea tõttu tekkinud kodukeskjaama (PBX) rike
- G 3.82 IP-kõne vahendustarkvara väär konfiguratsioon
- G 3.83 IP-kõne komponentide väär konfiguratsioon

Tehnilised rikked:

- G 4.56 IP-kõne arhitektuuri rike
- G 4.57 Häired IP-kõne kasutamisel üle VPNi
- G 4.58 IP-kõne lõppseadmete puudused
- G 4.59 IP-kõne kasutuskõlbmatus NAT tõttu

Ründed:

- G 5.11 Kodukeskjaamas (PBX) salvestatud andmete konfidentsiaalsuse kadu
- G 5.12 Telefonikõnede ja andmesaadetiste pealtkuulamine
- G 5.13 Pealtkuulamine kodukeskjaama (PBX) lõppseadmete ruumides
- G 5.14 Telefoniteenuste vargus
- G 5.15 Kodukeskjaama rakenduste väärkasutus
- G 5.134 Telefonikõne osapoolte puudulik identifitseerimine
- G 5.135 SPIT ja Vishing
- G 5.136 Vaba ligipääsuga telefoniliinide kuritarvitamine

Soovitatavad meetmed

Selleks, et tagada kogu loetletud IT-süsteemi turvalisus, tuleb lisaks käesolevale moodulile rakendada veel ka teisi, IT-etalonturbe modelleerimise käigus selguvaid mooduleid.

Kuna IP-kõne toimib üle andmevõrkude, tuleb turvalisuse tagamisel lisaks arvestada ka mooduliga B 4.1 Heterogeensed võrgud . Samuti vajavad tähelepanu andmevõrgus olevad aktiivsed võrgukomponendid (vt B 3.302 Marsruuterid ja kommutaatorid).

IP-kõnet kasutatakse sageli mitte spetsiaalseadmete, vaid just tavaliste IT-süsteemide abil. Vahevarakomponendi kasutamiseks läheb IT-süsteemis tarvis spetsiaalset võrguteenust. Seetõttu tuleb vastaval juhul arvestada mooduliga B 3.101 Server .

Kliendi tarkvara, mis võimaldab mikrofoniga varustatud multimeedia-PCd kasutada kõneedastuse lõppseadmena, nimetatakse tarkvaratelefoniks (Softphone). Tarkvaratelefoni kasutamisel tuleb kliendi juures rakendada moodulit B 3.201 Klient . Lisaks tuleb nii vahevara kui ka tarkvaratelefoni puhul arvestada vastava operatsioonisüsteemiga, mida vastav IT-süsteem parasjagu kasutab, näiteks mooduliga B 3.102 Server Unixi all .

IP-kõne kasutamise puhul tuleks lõppseadmete ja vahevara IT-alase turvalisuse tagamiseks läbi teha järgmised sammud:

IP-kõne kasutuselevõtu planeerimine

IP-kõne kasutus tuleb hoolikalt ette planeerida (vt M 2.372 IP-kõne kasutamise planeerimine). IP-kõne võimalikke kasutusvaldkondi tutvustatakse meetmes M 3.57 IP-kõne kasutamise stsenaariumid . Olulisel kohal on ka signaaliedastusprotokolli valimine, kuna IP-kõnet võimaldavate seadmete tootjad toetavad tihti vaid ühte protokolli. Kuna signaaliedastusprotokollid ei ühildu omavahel, mõjutab signaaliedastusprotokolli valik ka IP-kõnet võimaldavate komponentide valikut. Enimlevinud protokollid on lühidalt kokku võetud meetmes M 5.133 IP-kõne signaliseerimisprotokolli valik .

IP-kõnet kasutades võivad esile kerkida kõik need samad probleemid nagu üks-kõik millise muu IP kaudu toimiva kommunikatsiooni puhul. Paljud teadaolevad konfidentsiaalsuse ja tervikluse vastased ründed, mis kehtivad IP-andmevõrgu kohta, võib IP-kõne puhul otse üle võtta. Kaitset vastavate rünnete vastu pakub muuhulgas signaliseeritavate andmete või meediatransportandmete krüpteering. Millistes võrkudes millist sisu kaitsta tuleb, selgitab meede M 2.374 IP-kõne krüpteerimise ulatus . Signaliseerimise ja meediatranspordi krüpteerimisfunktsioone selgitavad meetmed M 5.134 IP-kõne turvaline signaliseerimine ja M 5.135 Turvaline meediatransport SRTP abil .

Paralleelselt eelnimetatuga tuleb täiendada üldist turvapoliitikat lisades sinna täpsemad suunised IP-kõne kasutuse kohta (vt M 2.373 IP-kõne turvajuhendi

väljatöötamine .

Soetamine

Järgmisena sammuna tuleks ette võtta lõppseadmete ja IP-kõne vahevara soetamine. Kasutada võib nii tarkvaralahendusi kui ka lisaseadmeid. Kasutusvaldkondadest lähtudes tuleks sõnastada toodetele seatavad nõudmised ning vastavalt nendele teha valik sobilike toodete hulgast. Soovitused erinevate valikukriteeriumite kohta on ära toodud meetmes M 2.375 Asjakohane IP-kõne (VOIP) süsteemide valik .

Rakendamine

Valmisolek IP-kõne juurutamiseks või IP-kõnele üleminekuks eeldab, et administraatorid on saanud piisava asjakohase koolituse (vt M 3.56 IP-kõne administraatorite koolitus).

Lisaks spetsiaalselt IP-kõnet puudutavatele muudatustele tuleb tihti teha mugandusi ka olemasolevas IP-andmevõrgus endas. Mõningatel juhtudel võib olla mõistlik lahendus kasutada paralleelselt kahte andmevõrku. IP-kõne võrgu ja ülejäänud andmesidevõrgu teineteisest eraldamine, mida on võimalik lahendada nii loogilise kui ka füüsilise segmentimise teel, ei kulge alati just probleemivabalt. Vastavad juhised leiate meetmest M 2.376 Andmeside ja IP-kõne (VOIP) võrgu eraldamine . Sellele lisaks tuleb kaitsta ka juurdepääsu IP-kõne komponentidele (vt M 4.289 Ligipääsu piiramine IP-kõne komponentidele). Kui füüsilist eraldamist ei toimu, tuleks võrgu ülekoormamise ennetamiseks vastu võtta reeglid, mis sätestavad IP-kõne andmepakettide edastamise prioriteedid. Prioriteete käsitletakse muuhulgas meetmes M 5.136 IP-kõne teenuse kvaliteet ja võrguhaldus .

Avalikust võrgust lähtuva kättesaadavuse jaoks on tarvis teha ettevalmistusi. Muuhulgas kuulub siia alla avaliku võrgu ja privaatvõrgu vahelise ülemineku kokkusobitamine. Näiteks võib NATi (Network Address Translation) kasutamine privaatsete IP-aadresside avalikeks IP-aadressideks ümbernimetamisel osutuda väga keeruliseks (vt M 5.137 NAT kasutamine IP-kõne puhul). Turvalüüsidele kehtivad aga samuti spetsiaalsed nõudmised, mida kirjeldatakse meetmes M 4.290 IP-kõne kasutamisest tulenevad nõuded turvalüüsidele .

Kasutamine

Pärast esmakordset installeerimist ja testimisfaasi läbimist võetakse seadmed üle tavakasutusse, vt meetmed M 4.287 IP-kõne vahetarkvara turvaline administreerimine ja M 4.288 IP-kõne lõppseadmete turvaline administreerimine . Valmisolek probleemidele õigeaegselt reageerida eeldab tähtsamate sündmuste logimist ja logide kontrollimist. Sellekohased soovitused leiate meetmest M 4.292 IP-kõne logimine .

Töötajate koolitamine telefoni kasutuse osas ei ole ei majanduslikus ega ka üldises plaanis tihti eriti mõttekas, seda ka seetõttu, et tüüpilised tänapäeva büroseadmed täidavad niikuinii mitut funktsiooni korraga. Sellele vaatamata tuleks töötajaid siiski teavitada üldlevinud ohuallikatest, rakendades selleks meetmeid M 3.12 Töötajate teavitamine kodukeskjaama (PBX) signaalidest ja teadetest ja M 3.13 Töötajate teavitamine kodukeskjaama (PBX) kasutusega seotud ohtudest .

Väljavahetamine

IP-kõnet võimaldavate komponentide mällu jääb tihtipeale konfidentsiaalset infot. Seadmete väljavahetamisel tuleb arvestada meetmega M 2.377 Turvaline IP-

kõne komponentide kasutusest kõrvaldamine .

Valmisolek hädaolukorraks

Vaid reeglipärane ja ulatuslik andmete varundamine suudab kindlalt tagada, et riistvaraliste rikete, avariide ning tahtlike või tahtmatute kustutamiste korral on kõiki salvestatud andmeid võimalik uuesti kättesaadavaks teha. Vajalikud meetmed leiate moodulist B 1.4 Andmevarunduspoliitika . Sellele lisaks tuleb andmevarunduspoliitikat täiendada IP-kõnet võimaldavate komponentide osas, nagu seda on kirjeldatud meetmes M 6.101 IP-kõne (VOIP) andmevarundus .

Mõningad IP-kõne serveri kohta käivad, spetsiaalselt ootamatuseplaani puudutavad aspektid on ära toodud meetmes M 6.100 IP-kõne (VOIP) hädaolukorraks valmisoleku plaani koostamine .

Alljärgnevalt tutvustatakse meetmete kogumit, mida tuleb rakendada valdkonnas "IP-kõne (VOIP):

Planeerimine ja kontseptsioon

- (M) M 2.28z Väline sidealase konsultatsiooni teenus
- (L) M 2.372 IP-kõne kasutamise planeerimine
- (L) M 2.373 IP-kõne turvajuhendi väljatöötamine
- (L) M 2.374 IP-kõne krüpteerimise ulatus
- (M) M 3.57w IP-kõne kasutamise stsenaariumid
- (L) M 5.133 IP-kõne signaliseerimisprotokolli valik
- (L) M 5.134 IP-kõne turvaline signaliseerimine
- (L) M 5.135 Turvaline meediatransport SRTP abil

Soetamine

- (L) M 2.375 Asjakohane IP-kõne (VOIP) süsteemide valik

Rakendamine

- (L) M 1.30 PBX-arveldusandmetega andmekandjate kaitse
- (M) M 2.29 Kodukeskjaama (PBX) kasutamisjuhendid
- (L) M 2.376 Andmeside ja IP-kõne (VOIP) võrgu eraldamine
- (L) M 3.56 IP-kõne administraatorite koolitus
- (L) M 4.7 Algparoolide muutmine
- (M) M 4.10 Kodukeskjaama (PBX) terminalide paroolikaitse
- (L) M 4.287 IP-kõne vahetarkvara turvaline administreerimine
- (L) M 4.288 IP-kõne lõppseadmete turvaline administreerimine
- (L) M 4.289 Ligipääsu piiramine IP-kõne komponentidele
- (L) M 4.290 IP-kõne kasutamisest tulenevad nõuded turvalüüsidele
- (M) M 5.136 IP-kõne teenuse kvaliteet ja võrguhaldus
- (L) M 5.137 NAT kasutamine IP-kõne puhul

Kasutamine

- (L) M 3.12 Töötajate teavitamine kodukeskjaama (PBX) signaalidest ja teadetest

- (L) M 3.13 Töötajate teavitamine kodukeskjaama (PBX) kasutusega seotud ohtudest
- (L) M 4.5 Kodukeskjaama (PBX) haldustööde logi
- (L) M 4.6 Kodukeskjaama (PBX) konfiguratsiooni läbivaatus.
- (L) M 4.291 IP-kõne vahendustarkvara turvaline konfiguratsioon
- (L) M 4.292 IP-kõne logimine

Väljavahetamine

- (L) M 2.377 Turvaline IP-kõne komponentide kasutusest kõrvaldamine

Valmisolek hädaolukorraks

- (M) M 6.29z Hädaabikõnede avariiliin

- (L) M 6.100 IP-kõne (VOIP) hädaolukorraks valmisoleku plaani koostamine
- (L) M 6.101 IP-kõne (VOIP) andmevarundus

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.38 Turvapaikade paigaldatuse regulaarseire
- HG.48 Võrdõigusteenuse keeld IP-kõne puhul
- HG.49 IP-kõne protokollistiku funktsionaaltestimine

Teabe käideldavus (K)

- HK.25 Puhvertoiteallika kasutamine IP kõne puhul
- HK.26 IP-kõne keskseadmete dubleeritus
- HK.34 IP-kõne võrgu eraldatusnõue

Teabe terviklus (T)

- HT.51 Lisanõuded teabe hankimisele turvaaukude kohta

Teabe konfidentsiaalsus (S)

- HS.65 Tarkvaratelefonide kasutuskeeld
- HS.72 IP-kõne täismahus krüpteerimise nõue

B 4.8 Bluetooth

Bluetooth on avatud tööstusstandard, mis rakendab IT-seadmete vaheliseks suhtlemiseks, st kõne ja andmeside edastamiseks litsentsivaba lähiraadiosidet (kaablite asendamiseks ja ad hoc võrkude loomiseks). Tootearenduse initsiatiiv tekkis 1998. aastal, mil loodi Bluetooth Special Interest Group (Bluetooth SIG), mis koondas suurel hulgal erinevaid tootjaid.

Bluetooth'iga on võimalik IT-seadmeid omavahel kiiresti ja lihtsalt ühendada, kasutades raadioside liidest. Seadmetesse sisse ehitatud erinevad Bluetooth'i profiilid võimaldavad edastada andmeid, kõnesid, juhtimissignaale ning luua juurdepääsu erinevatele teenustele nagu FTP, modemi- ja võrguteenused. Bluetooth töötab sarnaselt WLAN-iga litsentsivabal ISM-ribalaiusel vahemikus 2,402–2,480 GHz, pakkudes siiski vaid 100 m tööraadiust, kuid vastupidiselt infrapunale ei vaja see otsest silmsidet kahe lõppseadme vahel. Bluetooth'i rakendatakse peamiselt kaasaskantavates seadmetes nagu mobiiltelefonid, pihuarvutid ja sülearvutid.

Selles moodulis kirjeldatakse süstemaatilist lähenemist, kuidas kasutada turvaliselt institutsiooni Bluetoothi toega lõppseadmeid.

Ohud

Infosüsteemide etalonturbe seisukohalt loetakse Bluetooth'i puhul tüüpilisteks järgmisi ohuallikaid:

Vääramatu jõud

- G 1.17 Raadiovõrgu väljalangemine

Organisatsioonilised puudused

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.2 Reeglite puudulik tundmine

Inimvead

- G 3.3 Hooletus turvameetmete suhtes
- G 3.38 Vead konfigureerimisel ja kasutamisel
- G 3.43 Puudulik paroolihooldus

Tehnilised rikked

- G 4.60 Raadiolainete kontrollimatu levi
- G 4.79 Bluetooth'i kasutuselevõtul tehtud vead
- G 4.80 Bluetooth'i ebausaldusväärsed või puuduvad turvamehhanismid

Ründed

- G 5.28 Teenuse halvamine
- G 5.143 Man-in-the-Middle tüüpi rünne
- G 5.159 Liikumisprofiilide koostamine Bluetooth'iga
- G 5.160 Bluetooth'i profiilide väärkasutus

Soovitatavad meetmed

Selleks, et tagada kogu vaadeldava IT-koosluse turvalisus, tuleb lisaks käesolevale moodulile rakendada veel ka teisi, IT-etalonturbe modelleerimise käigus selguvaid mooduleid.

Bluetooth 'i turvalise käitamise tagamiseks peavad ka kõik sellega ühendatud klientsüsteemid olema turvaliselt konfigureeritud. Klientsüsteemidele sobivad IT-turvasuunised leiate moodulite kihist nr 3.Bluetooth'i kasutamisel tuleb rakendada erinevaid meetmeid, alates kontseptsioonist ja soetamisest kuni käitamiseni välja. Järgnevalt anname ülevaate erinevatest kohustuslikest etappidest ja meetmetest, mida iga etapi puhul tuleks rakendada.

Planeerimine ja kontseptsioon

Bluetooth'i turvaliseks ja efektiivseks kasutamiseks tuleb välja töötada kontseptsioon, mis arvestab institutsiooni üldkehtiva turvastrateegiaga ja lisaks ka nõuetega, mis tulenevad seadmete jaoks planeeritud kasutusvaldkondadest. Eelnevast lähtudes tuleb Bluetooth'i kasutamise kohta ametiasutuses või ettevõttes välja töötada vastav reeglistik ja turvapoliitika (vt M 2.461 Bluetooth'i turvalise kasutamise planeerimine).

Soetamine

Bluetooth'i komponentide soetamisel tuleb lähtuda eelnevalt välja töötatud kontseptsioonist, mis sõnastab vajaminevate toodete jaoks kehtivad nõuded, millest lähtudes tehakse lõplik valik sobilike toodete hulgast (vt M 2.462 Bluetooth-seadmete soetamise valikukriteeriumid).

Rakendamine

Sõltuvalt kehtivatest turvanõuetest tuleb Bluetoothi komponentidele teha erinev konfiguratsioon (vt M 4.362 Bluetoothi turvaline konfigureerimine). Turvaintsidentide minimeerimiseks tuleb kasutajaid ja administraatoreid piisavalt koolitada, st neid tuleb teavitada Bluetooth'i ebapädeva kasutamise korral tekkivatest ohtudest (vt M 3.80 Bluetooth'i kasutamise teadlikkuse tõstmine).

Kasutamine

Bluetooth-seadmete käitamine peab olema turvaline (vt M 4.363 Bluetooth-seadmete turvaline käitamine).

Väljavahetamine

Olukorras, kus Bluetooth-seadmeid ootab ees kasutusest kõrvaldamine, tuleb nendest kindlasti kustutada kõik konfidentsiaalsed andmed, nt pääsuandmed (vt M 4.364 Bluetooth-seadmete kasutusest kõrvaldamise reeglid).

Alljärgnevalt tutvustatakse meetmete kogumit, mida tuleb rakendada valdkonnas "Bluetooth":

Planeerimine ja kontseptsioon

- (L) M 2.461 Bluetooth'i turvalise kasutamise planeerimine

- (M) M 3.79w Sissejuhatus Bluetooth'i põhimõistetesse ja tööpõhimõtetesse

Soetamine

- (M) M 2.462z Bluetooth-seadmete soetamise valikukriteeriumid

Rakendamine

- (L) M 3.80 Bluetooth'i kasutamise teadlikkuse tõstmine
- (L) M 4.362 Bluetoothi turvaline konfigureerimine

Kasutamine

- (L) M 2.463z Bluetooth-lisaseadmete seadmekogu kasutamine
- (L) M 4.363 Bluetooth-seadmete turvaline käitamine

Väljavahetamine

- (L) M 4.364 Bluetooth-seadmete kasutusest kõrvaldamise reeglid

B5 Rakendused

Moodulite nimekiri

B 5.2 Andmekandjatel toimuv andmevahetus

Käesolev moodul käsitleb andmekandjaid, mida kasutatakse andmete transportimiseks ühest IT-süsteemist teise. Andmekandjad on paljudel juhtudel erinevate kommunikatsioonipartnerite ja IT-süsteemide vahel informatsiooni edastamiseks parimaks lahenduseks ning samas võivad need osutuda ka hädavajalikuks. Üheks põhjuseks võib olla asjaolu, et vastavate IT-süsteemide vahel puudub võrguühendus või ei ole võrguühendus piisavalt turvaline. Andmekandjaid on võimalik eraviisiliselt üksteisele üle anda või ka posti teel kätte toimetada. Tüüpilised kasutatavad andmekakandjad on disketid, vahetatavad plaadid (magnetilised, magnetilis-optilised), CD- ROMid, DVDd, magnetlindid, kassetid ning ka Flash -salvestid nagu USB-mälupulgad ja USB-kõvakettad. Siinkohal ei tohi unustada, et andmekandjate hulka loetakse ka paberdokumendid, mille puhul kehtivad sõltuvalt informatsiooni konfidentsiaalsusastmest täpselt samad turvanõuded.

Muuhulgas käsitletakse käesolevas moodulis ka andmete salvestamist saatja- ja vastuvõtja-süsteemile, kuivõrd see on otseselt seotud andmekandjatevahelise andmevahetusega, samuti andmekandjatega ümberkäimist enne ja pärast andmevahetust.

Ohud

Infosüsteemide etalonturbe seisukohalt loetakse andmekandjatevahelise andmevahetuse kasutamise puhul tüüpilisteks järgmisi ohuallikaid:

Vääramatu jõud:

- G 1.7 Lubamatu temperatuur ja niiskus
- G 1.8 Tolm, saastumine
- G 1.9 Tugevast magnetväljast tingitud andmekadu

Organisatsioonilised puudused:

- G 2.3 Puuduvad, puudulikud või ühildumatud ressursid
- G 2.10 Probleemid andmekandjate kättesaadavusega
- G 2.17 Andmekandjate puudulik märgistus
- G 2.18 Andmekandjate väär saatmine
- G 2.19 Krüpteerimise halb korraldus

Inimvead:

- G 3. 1 Andmete konfidentsiaalsuse või tervikluse kadu kasutaja vea tõttu
- G 3.3 Hooletus turvameetmete suhtes
- G 3.12 Andmekandjate kaotamine saatmisel
- G 3.13 Väära või soovimatu andmekogumi saatmine

Tehnilised rikked:

- G 4.7 Defektsed andmekandjad

Ründed:

- G 5.1 IT-seadmete või -tarvikute manipuleerimine ja hävitamine

- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.4 Vargus
- G 5.9 IT-süsteemide volitamata kasutamine
- G 5.23 Viirused
- G 5.29 Andmekandjate volitamata kopeerimine
- G 5.43 Makroviirused

Soovitatavad meetmed

Selleks, et tagada kogu loetletud IT-süsteemi turvalisus, tuleb lisaks käesolevale moodulile rakendada veel ka teisi, IT-etalonturbe modelleerimise käigus selguvaid mooduleid.

Andmekandjatel toimuva andmevahetuse puhul tuleb rakendada erinevaid meetmeid, tegeldes planeerimise, kontseptsiooni loomise ja igapäevase kasutamisega kuni ootamatuseplaanini välja. Järgnevalt anname ülevaate erinevatest kohustuslikest etappidest ja meetmetest, mida iga etapi puhul tuleks rakendada.

Planeerimine ja kontseptsioon

Enne andmekandjate kasutuselevõttu tuleb välja selgitada ja kindlalt fikseerida, milliste kommunikatsioonipartnerite vahel vastav andmevahetus võib toimuda ning andmekandjate halduses tuleb kindlaks määrata andmekandjate tüübid ja tähistada väliseks andmevahetuseks kasutatavad andmekandjad.

Soetamine

Andmekandjate valik tuleb kommunikatsioonipartnerite vahel kokku leppida. Valiku langetamise kergendamiseks võib abi olla meetmest M 4.169 Sobiva arhiveerimis-andmekandja valimine .

Rakendamine

Vältimaks andmekandjate võimalikke kahjustusi nende transportimise käigus, tuleb kindlaks määrata andmekandjate saatmise liik, mis võib eri liiki andmekandjate puhul (nt paberdokumentide, CD- ROMde või magnetlintide) puhul olla täiesti erinev.

Kasutamine

Võimalike kahjustuste vältimiseks, st tagajärgede pehmendamiseks, tuleb andmekandjatel põhineva andmevahetuse käigus järgida tervet rida meetmeid. Siia alla kuuluvad turvaline hoiulepanek ja pakend, samuti üheselt mõistetav märgistus, mis peab aitama vähendada vahetusseminemise riski. Digitaalsete andmekandjate juures kuulub üldiste turvanõuete alla arvutiviiruste kontroll enne andmeedastust või andmekandja üleandmist, samuti kontroll peale vastuvõtmist.

Väljavahetamine

Magnetlindid, mida on kasutanud erinevad kommunikatsioonipartnerid, tuleb enne uut kasutamist füüsiliselt kustutada, sest vastasel korral on oht jääkinformatsiooni edasikandumiseks ebasoovitud adressaatideni.

Valmisolek hädaolukorraks

Kuna andmekandjate puhul ei saa transpordi käigus kaotsiminekut mitte kunagi lõplikult välistada, tuleks edastatavad andmed vähemalt senikaua lokaalse koo-

piana alles hoida, kuni adressaat on kinnitanud, et ta on saadetud andmekandja probleemideta kätte saanud. Vastavalt andmevahetuseks kasutatavate andmekandjate liigile ja sihtotstarbele võib olla mõttekas salvestatud andmeid koos andmekandjaga hoiule panna, varudes seeläbi tõendusmaterjali hilisemate konfliktide lahendamiseks.

Alljärgnevalt tutvustatakse meetme'te kogumit, mida tuleb rakendada valdkonnas „Andmekandjatel toimuv andmevahetus".

Planeerimine ja kontseptsioon

- (L) M 2.3 Andmekandjate haldus
- (L) M 2.42 Võimalike suhtluspartnerite määramine
- (L) M 2.45 Andmekandjate üleandmine
- (L) M 2.393 Infovahetuse reguleerimine
- (M) M 4.34z Krüpteerimise, kontrollsummade ja digitaalallkirjade rakendamine

Rakendamine

- (M) M 2.46 Krüpteerimise õige korraldus
- (L) M 4.32 Andmekandjate füüsiline kustutamine enne ja pärast nende kasutamist
- (L) M 4.64 Ülekantavate andmete kontrollimine enne edastamist/peidetud info kõrvaldamine
- (L) M 5.22 Saate- ja vastuvõtupoole ühilduvuse kontroll
- (L) M 5.23 Andmekandjate sobivate edastusviiside valimine

Kasutamine

- (L) M 1.36 Andmekandjate transpordieelne ja –järgne turvaline säilitus
- (L) M 2.43 Andmekandjate õige märgistus edasiandmiseks
- (L) M 2.44 Andmekandjate pakkimine edasiandmiseks
- (L) M 3.14 Töötajate juhendamine informatsiooni ja andmekandjate edasiandmise korrektsetest protseduuridest
- (L) M 4.33 Viirustõrjeprogrammi kasutamine andmekandjate vahetamisel ja andmete edastamisel
- (M) M 4.35z Saatmisele eelnev andmete kontroll

Valmisolek hädaolukorraks

- (L) M 6.38 Edastatud andmete varukoopiad

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.26 Andmekandjate vahetuse dokumenteerimine

Teabe käideldavus (K)

- HK.6 Edastmiseks genereeritud andmete kahes eksemplaris varukopeerimine

Teabe terviklus (T)

- HT.65 Lisanõuded teisaldatavate andmekandjate kasutusele

Teabe konfidentsiaalsus (S)

- HS.11 Lisanõuded andmekandjate turvalisele kasutamisele
- HS.75 Lisanõuded infovahetuse reguleerimisele
- HS.76 Mobiilsete andmekandjate võimalik vältimine

B 5.3 Rühmatarkvara

Rühmatarkvara all mõeldakse rakendusi, mis aitavad IT-süsteemide abil töörühmade ülesandeid ja äriprotsesse toetada ja organiseerida. Rühmatarkvara keskmes on tugi, mida osutatakse töörühmadele koostöö, tähtaegade määramise ja koordineerimise ning igapäevase suhtluse käigus. Rühmatarkvara mõiste hõlmab rühmatarkvaraserverit, selle juurde kuuluvaid rühmatarkvarakliente ja vajalikke rühmatarkvarateenuseid .

Rühmatarkvara on muuhulgas mõeldud ka sõnumite (näiteks meilide) vahetamise jaoks – nii asutuse piires kui sellest väljaspool. Rühmatarkvara abil saab sõnumeid hallata, filtreerida ja edastada. Samuti pakutakse ja hallatakse rühmatarkvarasüsteemide abil tüüpilisi suhtlusrakendusi nagu uudisgrupid , kalender ja ülesannete nimekirjad, samuti Unified Messaging liidest .

Rühmatarkvara süsteemi funktsioonid on väga mitmekesised. Üks põhifunktsioone on tavaliselt e-post, nii et käesolevas moodulis käsitletakse ka meilisüsteemile esitatavaid üldisi infoturbenõudeid .

Rühmatarkvara pakuvad paljud firmad. Näitena võib tuua selliseid süsteeme nagu Microsoft Exchange ja Outlook (vt B 5.12 Microsoft Exchange / Outlook) ning Lotus Notes (B 5.5 Lotus Notes/Domino). Peale nende on arvukalt muidki vabavaralisi rühmatarkvarasüsteeme või -komponente.

Käesolevas moodulis vaadeldakse rühmatarkvarasüsteemide üldisi turvaaspekte kasutatavast tootest olenemata. Siia kuuluvad ka meilisüsteemi üldised turvaaspektid, krüpteerimine ja digiallkiri, aktiivsisu käitlemine , viirusetõrjetarkvara kasutamine ja palju muud. Tootespetsiifiliste turvaaspektide puhul on infosüsteemide etalonturbe kataloogides konkreetsete rühmatarkvarasüsteemide puhul täiendavalt kasutatavad lisamoodulid .

Ohud

Infosüsteemide etalonturbes peetakse rühmatarkvarasüsteemi mõjutavateks ohtudeks järgnevaid tüüpilisi ohtusid:

Vääramatu jõud:

- G 1.2 IT-süsteemi avarii

Organisatsioonilised puudused:

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.2 Reeglite puudulik tundmine
- G 2.7 Õiguste volitamata kasutamine
- G 2.54 Konfidentsiaalsuse kadu jääkinfo kaudu
- G 2.55 Rühmatarkvara reguleerimata kasutamine

Inimvead:

- G 3. 1 Andmete konfidentsiaalsuse või tervikluse kadu kasutaja vea tõttu
- G 3.8 IT-süsteemi väär kasutamine
- G 3.9 IT-süsteemi väär haldus

- G 3.13 Väära või soovimatu andmekogumi saatmine

Tehnilised rikked:

- G 4.20 Andmekadu andmekandja täitumise tõttu
- G 4.32 Sõnumi kaotsiminek
- G 4.37 Rühmatarkvara puudulik usaldusväärsus

Ründed:

- G 5.9 IT-süsteemide volitamata kasutamine
- G 5.23 Viirused
- G 5.24 Sõnumite korduv sisestamine
- G 5.25 Maskeerimine
- G 5.26 Sõnumivoo analüüsimine
- G 5.27 Sõnumi salgamine
- G 5.28 Teenuse halvamine
- G 5.71 Tundliku informatsiooni konfidentsiaalsuse kadu
- G 5.72 Rühmatarkvarasüsteemi kuritarvitamine
- G 5.73 Saatja aadressi võltsimine
- G 5.75 Ülekoormus siseneva meili tõttu
- G 5.77 Võõraste meilide lugemine
- G 5.110 Veebilutikad
- G 5.111 Meilide aktiivsisu kuritarvitamine

Soovitatavad meetmed

Vaadeldava IT-süsteemi kindlustamiseks on infosüsteemide etalonturbe modelleerimistulemuste kohaselt lisaks neile moodulitele kasutusel veel teisigi.

Rühmatarkvara turvameetmed puudutavad nii kliente kui ka piirkonnas töötavat serverit. Vastavalt sellele on vaja turvata nii kliente kui serverit. Seda valdkonda aga käesolevas moodulis ei käsitleta. Rühmatarkvara turvaliseks kasutamiseks kasutatakse vastavaid 3. kihi mooduleid. Samuti on väga tähtis, et kasutajad peaksid kinni turvameetmetest ja -juhistest.

Rühmatarkvarasüsteeme kasutatakse tavaliselt muude süsteemide keskkonnas, kus kontrollitakse välist juurdepääsu sisevõrgule. E raldi tuleb mainida koos rühmatarkvaraga töötavaid turvalüüse ja kaughooldussüsteeme . Seetõttu ei tohi rühmatarkvara puhul rakendatavate meetmete elluviimisel unustada ka muid neis moodulites esitatud soovitusi vastavate süsteemide kohta. Nende soovituste hulka kuuluvad muuhulgas järgmised moodulid :

- B 3.301 Turvalüüs (tulemüür) , rühmatarkvarasüsteemide kasutamise puhul tulemüürikeskkonnas,
- B 4.4 Virtuaalne privaatvõrk (VPN) , kui juurdepääs rühmatarkvarasüsteemile toimub VPN-i kaudu.

Rühmatarkvarasüsteemi edukaks ülesehitamiseks tuleb rakendada mitmeid meetmeid, alates strateegilistest otsustest planeerimise, kontseptsiooni väljatöötamise ja installeerimise kohta kuni süsteemi kasutamiseni .

Planeerimine ja kontseptsioon

Kui otsus rühmatarkvarasüsteemi kohta on langetatud, tuleb koostada kasutusplaan ja välja töötada kontseptsioon. Aspektid, mida selle juures silmas pidada, on kokku võetud peatükis M 2.454 Rühmatarkvarasüsteemide turvalise kasutamise planeerimine . Rühmatarkvarasüsteemi turvet saab otsustavalt mõjutada juba planeerimis- ja kontseptsioonifaasis – selleks tuleb turbe mõttes olulistele aspektidele piisavalt tähelepanu pöörata.

Rakendamine

Pärast korralduse ja planeerimisega seotud eeltööde lõppemist võib hakata rühmatarkvarasüsteemi installeerima. Seejuures tuleb silmas pidada meedet M 4.356 Rühmatarkvarasüsteemide turvaline installeerimine .

Konkreetsed kasutajakoolituse meetmed leiate peatükkidest M 3.74 Rühmatarkvarasüsteemide süsteemiarhitektuuri ja turbe koolitus administraatoritele ja M 3.75 Rühmatarkvaraklientide turvamehhanismide koolitus kasutajatele . Need meetmed on olulised, kuna kasutajate ja administraatorite piisavad oskused avaldavad rühmatarkvarasüsteemide turbele märkimisväärset mõju.

Rühmatarkvarasüsteemi installeerimine on ainult tühine osa elluviimisfaasis tehtavatest töödest. Peamine töökoormus tuleneb süsteemi algkonfigureerimisest. Algkonfiguratsioon määrab kindlaks rühmatarkvarasüsteemi kasutuselevõtu alusturbe ja hilisema turbe raamtingimused .

Turvalist haldamist tuleb planeerida (vt M 2.456 Rühmatarkvarasüsteemide turvaline haldamine).

Rühmatarkvarasüsteemid on üles ehitatud osadena, mis kasutavad üksteise või väliste kliendi- või serverisüsteemidega suhtlemiseks mitmesuguseid liideseid. Seetõttu on oluline suhtlemist adekvaatselt turvata. Üldiselt võib rühmatarkvarasüsteem kasutada paljusid erinevaid suhtluskanaleid, mis sõltuvad ka installeeritud rakendustest ja moodulitest. Tavaliselt aga kasutatakse vaid mõnda põhilist suhtlusmehhanismi ja -liidest (vt M 2.456 Rühmatarkvarasüsteemide turvaline haldamine .

Kasutamine

Pärast alginstalleerimist ja testfaasi algab regulaarne kasutamine. Turvaprobleemide õigeaegseks avastamiseks peab rühmatarkvarasüsteem alluma adekvaatsele kontrollile. Vastavad juhised leiab meetmest M 4.358 Rühmatarkvarasüsteemide logid .

Kuna rühmatarkvarasüsteem allub alati enamasti muutuvatest nõuetest või kasutusstsenaariumidest põhjustatud muutustele, tuleb tagada soovitud turvalisustaseme püsimine (vt M 2.221 Muudatuste haldus ja B 1.14 Turvapaikade ja muudatuste haldus).

Valmisolek hädaolukorraks

Süsteemi kasutamisega paralleelselt peab hädaolukorraks valmis olema. Nõnda tagatakse hädaolukorra puhul süsteemi tööshoidmine. Infoturbehaldus ja ülevaatus tagavad ühtlasi eeskirjadest kinnipidamise . Soovitused, kuidas rühmatarkvarasüsteemide hädaolukorra puhuks ette valmistuda, leiate meetmest M 6.140 Hädaolukorra plaani koostamine rühmatarkvarasüsteemide avarii puhuks .

Alljärgnevalt tutvustatakse meetmete kogumit, mida tuleb rtakendada valdkonnas “Rühmatarkvara”:

Planeerimine ja kontseptsioon

- (L) M 2.42 Võimalike suhtluspartnerite määramine
- (L) M 2.274 Asendamise korraldamine meilivahetuse alal
- (L) M 2.454 Rühmatarkvarasüsteemide turvalise kasutamise planeerimine
- (L) M 2.455 Infoturbepoliitika kehtestamine rühmatarkvara jaoks

Soetamine

- (L) M 2.123z Rühmatarkvara või meiliteenuse pakkuja valimine

Rakendamine

- (L) M 2.122z Meiliaadresside standard
- (L) M 2.456 Rühmatarkvarasüsteemide turvaline haldamine
- (L) M 3.74 Rühmatarkvarasüsteemide süsteemiarhitektuuri ja turbe koolitus administraatoritele
- (M) M 3.75 Rühmatarkvaraklientide turvamehhanismide koolitus kasutajatele
- (M) M 4.64 Ülekantavate andmete kontrollimine enne edastamist/peidetud info kõrvaldamine
- (L) M 4.355 Kasutajahaldus rühmatarkvarasüsteemide puhul
- (L) M 4.356 Rühmatarkvarasüsteemide turvaline installeerimine
- (L) M 5.57 Rühmatarkvara/meiliklientide turvaline konfiguratsioon

Kasutamine

- (M) M 3.76 Rühmatarkvara ja meili kasutajate koolitus
- (L) M 4.199 Ohtlike failivormingute vältimine
- (L) M 4.357 Rühmatarkvarasüsteemide turvaline kasutamine
- (L) M 4.358 Rühmatarkvarasüsteemide logid
- (L) M 5.54 Meili ülekoormuse ja spämmi tõrje
- (L) M 5.56 Meiliserveri turvaline kasutamine
- (M) M 5.108z Rühmatarkvara või meilisüsteemi krüptograafiline kaitse
- (M) M 5.109z Meiliskanneri kasutamine meiliserveril

Valmisolek hädaolukorraks

- (L) M 6.90 Andmete varundamine ja arhiveerimine rühmatarkvara ja e-posti puhul
- (M) M 6.140 Hädaolukorra plaani koostamine rühmatarkvarasüsteemide avarii puhuks

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.6 Arvuti paroolkaitse rangemad reeglid

- HG.24 Paroolide regulaarkontroll parooliskänneriga
- HG.28 Kõrge turbetaseme serveri kettatäitumise kaugindikatsioon
- HG.33 Meiliaadresside asenduskorra regulaarseire
- HG.38 Turvapaikade paigaldatuse regulaarseire

Teabe käideldavus (K)

- HK.6 Edastmiseks genereeritud andmete kahes eksemplaris varukopeerimine

Teabe terviklus (T)

- HT.7 Kasutajate ja nende profiilide perioodiline seire
- HT.51 Lisanõuded teabe hankimisele turvaaukude kohta
- HT.57 Algparoolide muutmise regulaarkontroll
- HT.59 Lisanõuded turvalisele sisselogimisele
- HT.72 Turvatunneldamise protokolli kasutuskohustus

Teabe konfidentsiaalsus (S)
-

B 5.4 Veebiserver

Tänapäeva infoühiskonna üks olulisi meediume on internet. Internetis hoitavate andmete kasutusvõimaluse eest hoolitsevad serverid, mis teevad andmed, enamasti HTML-lehekülgedena, klientprogrammidele kättesaadavaks. Tüüplahendustes kasutatakse selleks selliseid protokolle nagu HTTP (Hypertext Transfer Protocol) või HTTPS (HTTP üle SSL-i või TLS-i, st HTTP-d kaitstakse krüpteeritud ühendusega). Peale interneti kasutatakse veebiservereid aina enam ka andmete ja rakenduste jaoks firmade sisevõrkudes (intranetis). Üks põhjus on asjaolu, et veebiserverid kujutavad endast lihtsat ja standardiseeritud liidest serveripõhiste rakenduste ja kasutajate vahel ning nende kasutamiseks vajalikku klientsüsteemide tarkvara (veebilehitsejaid) pakutakse tasuta peaaegu kõikide operatsioonisüsteemide jaoks.

Nimetusega „veebiserver" (või „WWW-server") tähistatakse enamasti nii programmi, mis vastab HTTP-päringutele, kui ka arvutit, milles see programm töötab. Veebiserverite puhul tuleb arvestada erinevate turvaaspektidega.

Kuna veebiserver on avalik ligipääsetav süsteem, on väga oluline, et selle tööle rakendamisele eelneksid nii süsteemi kui ka võrgukeskkonna hoolikas planeerimine, turvaline installimine ja konfigureerimine. Turvalisuse valdkond on veebiserverite puhul suhteliselt lai ka veel seepärast, et sageli on nendes peale puhtakujuliste veebiserverirakenduste ka veel teisi serverirakendusi, mis on vajalikud veebiserveri tööshoidmiseks ning mille turvaline kasutamine peab samuti olema tagatud. Näiteks transporditakse andmeid serveritesse tihti läbi võrgu (nt läbi ftp või scp) või on tarvis pääsuõiguseid, et kasutada mõnd andmebaasi.
Dünaamilist sisu ja suuresti HTML-i piiridest väljuvaid funktsioone, mida täidavad veebirakendused, selles moodulis ei käsitleta.

Ohud

Veebiserveri ja internetikasutusega seonduva IT-etalonturbe puhul loetakse tüüpilisteks järgmisi ohtusid:

Organisatsioonilised puudused

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.4 Turvameetmete ebapiisav järelevalve
- G 2.7 Õiguste volitamata kasutamine
- G 2.9 Halb kohanemine IT muutustega
- G 2.28 Autoriõiguste rikkumine
- G 2.32 Võrgu ebapiisav võimsus
- G 2.37 Sideliinide kontrollimatu kasutamine
- G 2.96 Aegunud või väär teave veebisaidil
- G 2.100 Interneti domeeninimede taotlemise või haldamise vead

Inimvead

- G 3. 1 Andmete konfidentsiaalsuse või tervikluse kadu kasutaja vea tõttu
- G 3.37 Tulemusteta otsingud
- G 3.38 Vead konfigureerimisel ja kasutamisel

Tehnilised rikked

- G 4.10 Keerukad ligipääsuvõimalused võrgustatud IT-süsteemides
- G 4.22 Tüüptarkvara turvaaugud või vead
- G 4.39 Tarkvarakontseptsiooni viga

Ründed

- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.19 Kasutajaõiguste väärkasutus
- G 5.20 Administraatori õiguste väärkasutus
- G 5.21 Trooja hobused
- G 5.23 Viirused
- G 5.28 Teenuse halvamine
- G 5.48 IP-aadressi võltsimine
- G 5.71 Tundliku informatsiooni konfidentsiaalsuse kadu
- G 5.78 DNS-i võltsimine
- G 5.85 Tundliku informatsiooni tervikluse kadu
- G 5.87 Veebilehe võltsimine
- G 5.88 Aktiivsisu väärkasutus

Soovitatavad meetmed

Vaadeldava IT-koosluse turvalisuse tagamiseks tuleb peale käesoleva mooduli rakendada veel teisigi mooduleid, mis selguvad IT-etalonturbe rakendusjuhendi põhjal tehtava modelleerimise tulemusel.

Selles moodulis kirjeldatakse veebiserveritele iseäralikke ohtusid ja nende vastumeetmeid. Kasutatava serveri turbeks tuleb lisaks rakendada moodulit B 3.101 Server ning olenevalt operatsioonisüsteemist teisi mooduleid, nt B 3.102 Server Unixi all või B 3.108 Windows Server 2003 . Juhtudel, kus veebilehel on sisu, mille on koostanud veebirakendused dünaamiliselt, toetudes mõnele andmebaasile, tuleks arvestada ka mooduliga B 5.7 Andmebaasid . Lahenduste puhul, kus veebiserverile on võimalik interneti kaudu ligi pääseda, tuleks rakendada ka moodulit B 1.8 Turvaintsidentide käsitlus .

Veebiserveri turvaliseks ühendamiseks avalike võrkudega (nt internetiga) ning mitme intraneti ühendamiseks kasutage moodulit B 3.301 Turvalüüs (tulemüür) . Väliste ühenduspunktide (nt läbi ISDN-i toimivate kaugtöökohtade) kontrollitud ühendusvõimalusi käsitleb moodul B 5.8 Kaugtöö .

Veebiserver tuleks paigaldada eraldiseisvasse serveriruumi. Vajalikke meetmeid kirjeldab moodul B 2.4 Serveriruum . Serveriruumi puudumisel võib veebiserveri paigaldada ka serverikappi (vt B 2.7 Kaitsekapid). Juhtudel, kus veebiserverit ei käitata organisatsioonis kohapeal, vaid sellega tegeleb mõni väline teenusepakkuja, tuleb rakendada moodulit B 1.11 Väljasttellimine (Outsourcing) .

Veebiserveri edukaks ja turvaliseks ülesseadmiseks tuleb võtta mitmesuguseid meetmeid. Järgnevalt anname ülevaate erinevatest kohustuslikest etappidest ja meetmetest, mida iga etapi puhul tuleks võtta.

Planeerimine ja kontseptsioon

Enne veebiserveri sisseseadmist tuleks koostada veebiserveri turbestrateegia, mis kirjeldab kasutatavaid turvameetmeid ja nende ulatust (vt M 2.173 Veebiserveri turbestrateegia väljatöötamine).

Veebiserveri turvalisuse üks oluline aspekt kerkib esile juba enne serveri ülesseadmist: veebilehe planeerimine ja korraldus. Turvaprobleeme saab asjakohaste meetmete abil võimalikult hästi vältida vaid juhul, kui aegsasti on selge, milliseid eesmärke soovitakse veebilehega saavutada ning millist sisu ja rakendusi selleks otstarbeks pakutakse. Seetõttu tuleb turbeteemaga arvestada juba väga varajases planeerimisfaasis, et loodav arhitektuur saaks võimalikult turvaline (vt M 2.172 Veebilehe kasutamise kontseptsiooni väljatöötamine).

Lisaks tuleb veebilehel olevaid andmeid regulaarselt hooldada ja värskendada. Veebilehe hooldamisse on sageli korraga kaasatud organisatsiooni eri osakonnad ning tehnilise poole ja sisu hooldamise eest vastutavad tihti eri allüksused. Veebilehe võimalikult tõrkevabaks funktsioneerimiseks tuleb luua asjakohased organisatsioonilised raamtingimused. Ideaaljuhul võiksid veebilehe jaoks olemas olla toimetajad (vt M 2.272 Veebitoimetajate meeskonna loomine).

Planeerimise ja kontseptsiooni käigus, mil otsustatakse, mis moel infot veebilehel pakkuda, tuleks vältida aktiivsisu (vt M 4.360 Veebiserveri turvaline konfiguratsioon .

Soetamine

Veebiserverit saab kasutusele võtta ka teenusepakkuja vahendusel. Sobiva teenusepakkuja valimisel tuleb lähtuda veebiserveri turvastrateegiast (vt M 2.176 Sobiva internetiteenuse pakkuja valimine).

Rakendamine

Kui planeerimistööd on tehtud ja serveri operatsioonisüsteemile on veebiserveri rakendused installitud, tuleb veebiserver turvaliselt tööle seada (vt M 2.175 Veebiserveri ülesseadmine) ja konfigureerida (vt M 4.360 Veebiserveri turvaline konfiguratsioon). Juhtudel, kus veebiserver peab võimaldama ka veebirakendusi, tuleb ka neid sobival moel kaitsta. Veebiserveril hoitavaid faile ja katalooge tuleb kaitsta volitamata muutmise eest, kuid võib-olla ka volitamata lugemisõigusega juurdepääsu eest (vt M 4.94 Veebiserveri failide turve).

Kasutamine

Pärast veebiserveri installimist ja konfigureerimist võetakse see tavakasutusse. Meetme M 2.174 Veebiserveri turvaline kasutamine rakendamisega tuleb tagada, et oluliste infosüsteemide turvalisust hoitaks pidevalt kõige ajakohasemal tasemel. Selleks tuleb veebiserverit regulaarselt ajakohastada (vt M 2.273 Turvalisust mõjutavate paikade ja värskenduste kiire paigaldamine) ning värskendusi manipulatsioonide suhtes kontrollida (vt M 4.177 Tarkvarapakettide tervikluse ja autentsuse tagamine).

Valmisolek hädaolukorraks

Riistvaraliste rikete, avariide ning (tahtliku või tahtmatu) kustutamise korral on kõiki salvestatud andmeid võimalik uuesti kättesaadavaks teha vaid juhul, kui sellele on eelnenud regulaarne ja ulatuslik andmevarundus. Vajalikke meetmeid käsitleb moodul B 1.4 Andmevarunduspoliitika .

Hädaolukorraennetuse raames tuleb luua kontseptsioon, mis aitaks hoida hädaolukordade tagajärjed võimalikult minimaalsed ja määraks, millised tegevused on hädaolukorra puhul kohustuslikud. Selleks tuleb veebiserverile koostada hädaolukorraks valmisleku plaan (vt M 6.88 Veebiserveri hädaolukorraks valmisoleku

plaani koostamine). Lisaks tuleks arvestada ka mooduli B 1.3 Hädaplaanimine meetmetega.

Alljärgnevalt tutvustatakse meetmeid, mida tuleb rakendada valdkonnas „Veebiserver". Korduvatest viidetest teiste moodulite meetmetele on ruumi kokkuhoiu eesmärgil loobutud.

Planeerimine ja kontseptsioon

- (L) M 2.172 Veebilehe kasutamise kontseptsiooni väljatöötamine
- (L) M 2.173 Veebiserveri turbestrateegia väljatöötamine
- (L) M 2.272z Veebitoimetajate meeskonna loomine
- (L) M 2.298z Interneti domeeninimede haldus
- (M) M 4.34z Krüpteerimise, kontrollsummade ja digitaalallkirjade rakendamine
- (L) M 4.176 Autentimismeetodite valimine veebilehtede jaoks
- (L) M 4.359w Veebiserveri koostisosade ülevaade
- (M) M 5.64z Secure Shell (SSH)
- (M) M 5.66z SSL-i/TLS-i kasutamine kliendis
- (L) M 5.159w Veebiserveri protokollide ja kommunikatsioonistandardite ülevaade
- (L) M 5.160w Autentimine veebiserveril
- (M) M 5.177 SSL-i/TLS-i kasutamine serveris

Soetamine

- (M) M 2.176z Sobiva internetiteenuse pakkuja valimine

Rakendamine

- (L) M 2.175 Veebiserveri ülesseadmine
- (L) M 4.64 Ülekantavate andmete kontrollimine enne edastamist/peidetud info kõrvaldamine
- (M) M 4.94 Veebiserveri failide turve
- (L) M 4.95 Minimaalne operatsioonisüsteem
- (L) M 4.96z DNSi desaktiveerimine
- (L) M 4.98 Side piiramine miinimumini paketifiltritega
- (M) M 4.360 Veebiserveri turvaline konfiguratsioon
- (L) M 5.161w Dünaamiliste veebilehtede koostamine

Kasutamine

- (L) M 2.174 Veebiserveri turvaline kasutamine
- (L) M 2.273 Turvalisust mõjutavate paikade ja värskenduste kiire paigaldamine
- (M) M 4.33 Viirustõrjeprogrammi kasutamine andmekandjate vahetamisel ja andmete edastamisel
- (L) M 4.78 Konfiguratsioonimuudatuste hoolikas teostamine

- (L) M 4.177 Tarkvarapakettide tervikluse ja autentsuse tagamine
- (L) M 5.59 DNS võltsimise tõrje

Valmisolek hädaolukorraks

- (L) M 6.88 Veebiserveri hädaolukorraks valmisoleku plaani koostamine

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.6 Arvuti paroolkaitse rangemad reeglid
- HG.24 Paroolide regulaarkontroll parooliskänneriga
- HG.25 Kaugpöörduste kohustuslik logimine
- HG.38 Turvapaikade paigaldatuse regulaarseire

Teabe käideldavus (K)

- HK.16 Veebipääsu dokumenteerimine

Teabe terviklus (T)

- HT.7 Kasutajate ja nende profiilide perioodiline seire
- HT.14 Süsteemi tegevuslogide krüptoaheldamine
- HT.51 Lisanõuded teabe hankimisele turvaaukude kohta
- HT.72 Turvatunneldamise protokolli kasutuskohustus
- HT.73 Välise sertifikaadi kasutuskohustus

Teabe konfidentsiaalsus (S)
-

B 5.5 Lotus Notes/Domino

Lotus Notesi kirjeldatakse kui rühmatarkvara (groupware) ja ka koostöö (collaboration) platvormi. Nende terminitega tähistatakse aina komplekssemaks muutuvat tarkvara, mis keskendub kommunikatsiooni, koostöö ja andmehalduse tagamisele. Kasutusvõimalused algavad lihtsatest töörühmadest ja projektidest ning lõpevad institutsiooniüleste lahendustega.

Selles moodulis käsitletakse Lotuse olulisimaid tooteid: Lotus Domino Serverit ja erinevaid Lotus Notesi Cliente. Peamiselt vaadeldakse siin küll redaktsioone 8.0.x ja 8.5.x, kuid paljusid käsitlusi saab kasutada ka vanemate redaktsioonide puhul.

Lotus Notesi/Domino platvormi turbe tagamisel tuleb peale taristupõhiste turbemeetmete (ruumid, spetsiaalsed serveritaristud, riistvara, võrgukomponendid) võtta ka selliseid meetmeid, mis kaitsevad Domino ja Notesi komponentide tööks vajalikke operatsioonisüsteeme.

Kui Lotus Notesi/Domino platvormi käitamiseks kasutatakse ka lisakomponente, nt DB2 andmebaase, tuleb nendega infokoosluse modelleerimisel kindlasti arvestada ning nende jaoks asjakohaseid IT-etalonturbe meetmeid võtta (selle näite puhul moodul B 5.7 Andmebaasid).

Ohud

IT-etalonturbe seisukohalt loetakse Lotus Notesi/Domino kasutamisel tüüpilisteks järgmisi ohte.

Organisatsioonilised puudused:

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.2 Reeglite puudulik tundmine
- G 2.4 Turvameetmete ebapiisav järelevalve
- G 2.7 Õiguste volitamata kasutamine
- G 2.19 Krüpteerimise halb korraldus
- G 2.26 Ebapiisavad või puuduvad tarkvara katsetamis- ja evitusprotseduurid
- G 2.28 Autoriõiguste rikkumine
- G 2.37 Sideliinide kontrollimatu kasutamine
- G 2.38 Installimata või piisavalt aktiveerimata andmebaasi turvamehhanismid
- G 2.40 Andmebaasipöörduse keerukus
- G 2.103 Töötajate ebapiisav koolitamine
- G 2.105 Õigusaktide ja lepingute sätete rikkumine

Inimvead:

- G 3. 1 Andmete konfidentsiaalsuse või tervikluse kadu kasutaja vea tõttu
- G 3.9 IT-süsteemi väär haldus
- G 3.43 Puudulik paroolihooldus
- G 3.45 Sidepartnerite puudulik autentimine
- G 3.46 Lotus Notes Serveri väär konfiguratsioon

- G 3.80 Andmebaaside sünkroniseerimisvead
- G 3.113 Lotus Notesi kliendi või võõra, Lotus Dominole juurdepääsu omava kliendi väär konfiguratsioon

Tehnilised rikked:

- G 4.22 Tüüptarkvara turvaaugud või vead
- G 4.26 Andmebaasi rike
- G 4.28 Andmebaasi andmekadu
- G 4.30 Andmebaasi tervikluse ja vastavuse kadu
- G 4.32 Sõnumi kaotsiminek
- G 4.35 Ebaturvaline krüptoalgoritm
- G 4.47 Vananenud krüptomeetodid
- G 4.52 Kaasaskantava seadme andmekadu

Ründed:

- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.7 Liinide pealtkuulamine
- G 5.8 Liinide manipuleerimine
- G 5.10 Kaughooldeportide väärkasutus
- G 5.19 Kasutajaõiguste väärkasutus
- G 5.20 Administraatori õiguste väärkasutus
- G 5.22 Kaasaskantava IT-süsteemi vargus
- G 5.27 Sõnumi salgamine
- G 5.71 Tundliku informatsiooni konfidentsiaalsuse kadu
- G 5.83 Krüptograafiliste võtmete paljastamine
- G 5.84 Võltsitud sertifikaadid
- G 5.85 Tundliku informatsiooni tervikluse kadu
- G 5.90 Aadressi- ja levitusloendite manipuleerimine
- G 5.100 Aktiivsisu väärkasutus Lotus Notesi poole pöördumisel
- G 5.101 Lotus Notesi häkkimine

Soovitatavad meetmed

Vaadeldava IT-koosluse turvalisuse tagamiseks tuleb peale selle mooduli rakendada veel ka teisi, IT-etalonturbe modelleerimise käigus selguvaid mooduleid.

Lotus Notesi/Domino turvaliseks käitamiseks tuleb esmalt rakendada taristu turvet käsitlevaid mooduleid, k.a operatsioonisüsteemid, ning kasutatud turvakomponente käsitlevaid mooduleid, nt B 3.301 Turvalüüs (tulemüür) ja B 1.6 Viirusetõrje kontseptsioon . Lisamoodulina tuleks rakendada eelkõige moodulit B 5.3 Rühmatarkvara , milles käsitletakse rühmatarkvara turbe üldaspekte.

Selles moodulis ei vaadelda Lotus Notesi/Domino platvormi tehnilisi üksikasju, sest see väljuks IT-etalonturbe põhimõtete kirjeldamise piirest. Näiteks ei käsitleta siin rakenduse tasandi klasterdamist (clustering), mida on tarvis rakendada juhul, kui käideldavuse turbenõuded on kas suured või väga suured.

Eduka Notesi süsteemi ülesehitamiseks tuleb võtta erinevaid meetmeid, alustades kontseptsiooni koostamisest ja süsteemi installimisest ning lõpetades süsteemi kasutusest kõrvaldamisega. Järgnevalt on esitatud ülevaade erinevatest kohustuslikest etappidest ja meetmetest, mida tuleks iga etapi puhul võtta.

Planeerimine ja kontseptsioon

Alustuseks on soovitatav tegeleda meetmega M 3.87 Sissejuhatus Lotus Notesi/Dominosse , mis annab ülevaate Notesi süsteemi struktuurist ja terminitest.

Pärast seda, kui Notesi süsteemi kasutuselevõtt on otsusega heaks kiidetud, tuleb alustada planeerimisega ja koostada kontseptsioon. Selleks on vaja arvesse võtta erinevaid aspekte, mida on kirjeldatud meetmes M 2.206 Lotus Notesi/Domino kasutuselevõtu planeerimine . Sellega paralleelselt tuleb välja töötada uus turvapoliitika (vt M 2.207 Lotus Notesi/Domino turvakontseptsioon), milles tuleb võimalikud olemasolevad turvapoliitikad Lotus Notesi konteksti ümber tõsta ning defineerida ka Notesi eripära arvestavad täiendused.

Kontseptsiooni koostamisel tuleb arvestada institutsiooni IT-süsteemides rakendatavate turvakomponentidega. Lisateavet selle kohta, kuidas Lotus Notesi/Domino keskkond ja institutsiooni turvakomponendid üksteist vastastikku mõjutavad, leiate meetmest M 2.492 Lotus Notesi/Domino keskkonna integreerimine olemasoleva turvataristuga .

Soetamine

Pärast kontseptsiooni koostamist ja Notesi süsteemi soetamisel järgitavate valikukriteeriumite kindlaksmääramist tuleks väljavalitud komponentide arvu järgi (vt M 2.494 Lotus Notesi/Domino keskkonna taristu jaoks komponentide valimine) valida ka sobiv litsentsimudel. Selleks leiate lisateavet meetmest M 2.493 Litsentsihaldus ja litsentsiaspektid Lotus Notesi/Domino soetamisel .

Rakendamine

Pärast töökorralduslike meetmete võtmist ja planeerimise eeltööde tegemist saab edasi liikuda Notesi süsteemi installimise juurde. Installimistööd võib lugeda lõpetatuks alles pärast seda, kui Notesi süsteemid on õnnestunud viia turvalisse seisundisse (vt M 4.116 Lotus Notesi/Domino turvaline installimine). Konfigureerimistöödel tuleks arvestada meetmega M 4.429 Lotus Notesi/Domino turvaline konfiguratsioon .

Kasutamine

Notesi süsteem ei ole staatiline, vaid muutub pidevalt. Seetõttu tuleb pidevalt kohandada ka turbega seotud parameetreid. Lisaks tuleb arvestada, et klient-server-süsteemide turve sõltub suurel määral ka teiste osasüsteemide turvalisusest.

Üldisi soovitusi käituse kohta (k.a rakenduste arendamine ja nende integreerimine Lotus Notesi/Dominoga) leiate meetmest M 4.128 Lotus Notesi/Domino turvaline käitus . Võimalike probleemide kiireks lahendamiseks tuleks võtta meede M 4.427 Lotus Notesi/Domino turbe seisukohalt oluline logimine ja analüüs .

Kasutusest kõrvaldamine

Kui Lotus Notesi/Domino keskkond otsustatakse kasutusest kõrvaldada, tuleb kogu oluline teave üle kanda asendussüsteemi ning tagada, et vanast süsteemist kustutataks andmed turvaliselt ära. Samas on tähtis meeles pidada, et meetme M 2.495 Lotus Notesi/Domino komponentide kasutusest kõrvaldamine teatud punkte tuleks järgida ka siis, kui kasutusest kõrvaldatakse vaid mõni üksik Lotus Notesi/Domino keskkonda kuuluv komponent.

Valmisolek hädaolukorraks

Lotus Notesi/Domino keskkonna käitamisel on vaja arvestada ka hädaolukordadega, milleks tuleb kindlaks määrata töötajate vastutusalad ja koostada hädaolukorra plaan (vt M 6.73 Hädaolukorraplaani koostamine Lotus Notes süsteemi tõrgete puhuks).

Alljärgnevalt tutvustatakse meetmete kogumit, mida tuleb rakendada valdkonnas „Lotus Notes/Domino”:

Planeerimine ja kontseptsioon

- (L) M 2.206 Lotus Notesi/Domino kasutuselevõtu planeerimine
- (L) M 2.207 Lotus Notesi/Domino turvakontseptsioon
- (L) 2.492 Lotus Notesi/Domino keskkonna integreerimine olemasoleva turvataristuga
- (L) M 3.87w Sissejuhatus Lotus Notesi/Dominosse

Soetamine

- (L) M 2.493w Litsentsihaldus ja litsentsiaspektid Lotus Notesi/Domino soetamisel
- (L) M 2.494 Lotus Notesi/Domino keskkonna taristu jaoks komponentide valimine

Rakendamine

- (L) M 3.88 Lotus Notesi/Domino sihtrühmade koolitused
- (L) M 4.116 Lotus Notesi/Domino turvaline installimine
- (L) M 4.429 Lotus Notesi/Domino turvaline konfiguratsioon

Kasutamine

- (L) M 4.128 Lotus Notesi/Domino turvaline käitus
- (L) M 4.132 Lotus Notes’i süsteemi seire
- (M) M 4.426 Lotus Notesi/Domino keskkonna arhiveerimine
- (L) M 4.427 Lotus Notesi/Domino turbe seisukohalt oluline logimine ja analüüs
- (M) M 4.428 Lotus Notesi/Domino keskkonna audit

Kasutusest kõrvaldamine

- (M) M 2.495 Lotus Notesi/Domino komponentide kasutusest kõrvaldamine

Valmisolek hädaolukorraks

- (L) M 6.73 Hädaolukorraplaani koostamine Lotus Notes süsteemi tõrgete puhuks

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.25 Kaugpöörduste kohustuslik logimine
- HG.38 Turvapaikade paigaldatuse regulaarseire

Teabe käideldavus (K)

- HK.6 Edastmiseks genereeritud andmete kahes eksemplaris varukopeerimine
- HK.8 Andmebaasi tervikliku varundamise nõue

Teabe terviklus (T)

- HT.7 Kasutajate ja nende profiilide perioodiline seire
- HT.17 Krüptoaheldatud saate- ja vastuvõtulogid
- HT.51 Lisanõuded teabe hankimisele turvaaukude kohta

Teabe konfidentsiaalsus (S)
-

B 5.6 Faksiserver

Vaatluse alla tuleb informatsiooni edastamine faksi teel. Meetmete valikul infosüsteemide etalonturbes ei ole tähtis, millist ülekandestandardit kasutatakse (nt CCITT grupp 3). Käesolevas moodulis vaadeldakse faksisaadetiste tehnilise baasina eranditult vaid faksiservereid. Faksiserver selles mõttes on rakendus, mis on installeeritud IT-süsteemile ning mis osutab ühes võrgus teistele IT-süsteemidele faksi saatmise ja/või vastuvõtmise teenuseid.

Faksiserverid integreeritakse reeglina juba olemasolevatesse e-posti süsteemidesse. Nii on muu seas võimalik, et sisse tulevad faksidokumendid edastatakse kasutajatele läbi faksiserveri e-posti kaudu. Saadetavad dokumendid edastatakse faksiserverile printeri ootejärjekorra või e-posti teel. Faksiserveri integreerimisel e-posti süsteemi on võimalik saata ka “seeriakirju” valikuliselt kas faksi või e-posti teel. Kui adressaadiga on võimalik e-posti ühendus, saab ta sõnumi e-posti teel, mis maksumuselt soodsam, vastasel korral faksi teel. Faksiserveri kaudu saadetud või vastu võetud dokument on graafikafail, mida ei saa tingimata tekstitöötlussüsteemides edasi töödelda. Igal juhul on aga võimalik arhiveerimine. See võib toimuda nii faksiserveri tarkvara abil kui ka dokumendihaldussüsteemides.

Faksiserverid on olemas tervele reale operatsioonisüsteemidele, nagu nt erinevatele Unixi distributsioonidele, Microsoft Windows’ile ja Novell Netware’le . Võimalikud ohud ja meetmed, mis on tingitud kasutatavast operatsioonisüsteemist, ei leia käesolevas moodulis käsitlemist. Pigem käsitletakse siinkohal moodulit B 3.101 Server ning vastavale operatsioonisüsteemile vastavat moodulit.

Faksiserveritel on tihti lisaks binaaredastusrežiim (binary transfer mode). Selle abil edastatakse suvalisi faile, mis ei ole faksiformaadis olemas. Sel juhul ei ole tegemist faksiedastustega. Seepärast ei vaadelda käesolevas moodulis nimetatud teenusega kaasnevaid ohtusid ja meetmeid nende vältimiseks. Kui binaaredastusrežiimi kasutamine on lubatud, tuleb rakendada ka moodulit B 4.3 Modem .

Ohud

Informatsiooni edastamisel faksi teel faksiserveri vahendusel peetakse infosüsteemide turvalisust mõjutavaks järgmisi tüüpilisi ohtusid:

Organisatsioonilised puudused:

- G 2.7 Õiguste volitamata kasutamine
- G 2.9 Halb kohanemine IT muutustega
- G 2.22 Logiandmete analüüsimata jätmine
- G 2.63 Fakside kontrollimatu kasutamine

Inimvead:

- G 3.3 Hooletus turvameetmete suhtes
- G 3.14 Faksi juriidilise siduvuse ülehindamine

Tehnilised rikked:

- G 4.15 Faksi saatmine vääral aadressil
- G 4.20 Andmekadu andmekandja täitumise tõttu

Ründed:

- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.7 Liinide pealtkuulamine
- G 5.9 IT-süsteemide volitamata kasutamine
- G 5.24 Sõnumite korduv sisestamine
- G 5.25 Maskeerimine
- G 5.27 Sõnumi salgamine
- G 5.30 Faksiaparaadi või -serveri volitamata kasutamine
- G 5.31 Saabuvate fakside volitamata lugemine
- G 5.32 Faksiaparaadi ja -serveri jääkinfo lugemine
- G 5.33 Väära identiteedi kasutamine faksi saatmisel
- G 5.35 Faksisaadetistest tulenev ülekoormus
- G 5.39 Sissetung arvutitesse modemi kaudu
- G 5.90 Aadressi- ja levitusloendite manipuleerimine

Soovitatavad meetmed

Vaadeldava IT varade turvalisuse tagamiseks tuleb lisaks käesolevale moodulile rakendada veel teisigi mooduleid vastavalt infosüsteemide etalonturbe rakendusjuhendi modelleerimise tulemustele.

Kõigepealt tuleks välja töötada faksiserveri üldised turvaeeskirjad ja soetada sobiv faksiserver. Nendest tulenevad omakorda korraldamise protseduurid. Lõpuks tuleb kindlaks määrata faksiserveri töösserakendamise eest vastutajad (vt M 3.10 Usaldusväärse administraatori ja tema asetäitja valimine). Nii turvaeeskirjade kui ka nendest tulenevate korraldusprotseduuride ja vastutajate määramine peab toimuma kirjalikult. Koostatud eeskirjade järgi tuleks seejärel välja töötada konkreetsed turvameetmed. Lisaks faksiserveri turvalisele käitusele on erilise tähtsusega ka asjaolu, et kasutajad peaksid kinni vastavatest turvaeeskirjadest ja –juhistest.

Alljärgnevalt tutvustatakse turvameetmete kogumit rakendamiseks valdkonnas “ Faksiserver ”.

Rakendamine

- (L) M 3.10 Usaldusväärse administraatori ja tema asetäitja valimine
- (L) M 3.15 Kõigi töötajate juhendamine faksi kasutamise alal
- (M) M 4.36z Faksi adressaatnumbrite blokeerimine
- (M) M 4.37z Faksi saatjanumbrite blokeerimine

Kasutamine

- (L) M 5.24z Sobiva faksiblanketi kasutamine
- (L) M 5.25 Saate- ja vastuvõtulogide kasutamine

Valmisolek hädaolukorraks

- (L) M 6.69 Faksiserverite avariiplaan ja rikkekindluse tagamine

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele

Kohustuslikud üldmeetmed

- HG.6 Arvuti paroolkaitse rangemad reeglid
- HG.24 Paroolide regulaarkontroll parooliskänneriga
- HG.25 Kaugpöörduste kohustuslik logimine
- HG.38 Turvapaikade paigaldatuse regulaarseire

Teabe käideldavus (K)

-

Teabe terviklus (T)

- HT.7 Kasutajate ja nende profiilide perioodiline seire
- HT.35 Tavalise faksiteenuse kasutuskeeld
- HT.51 Lisanõuded teabe hankimisele turvaaukude kohta

Teabe konfidentsiaalsus (S)

-

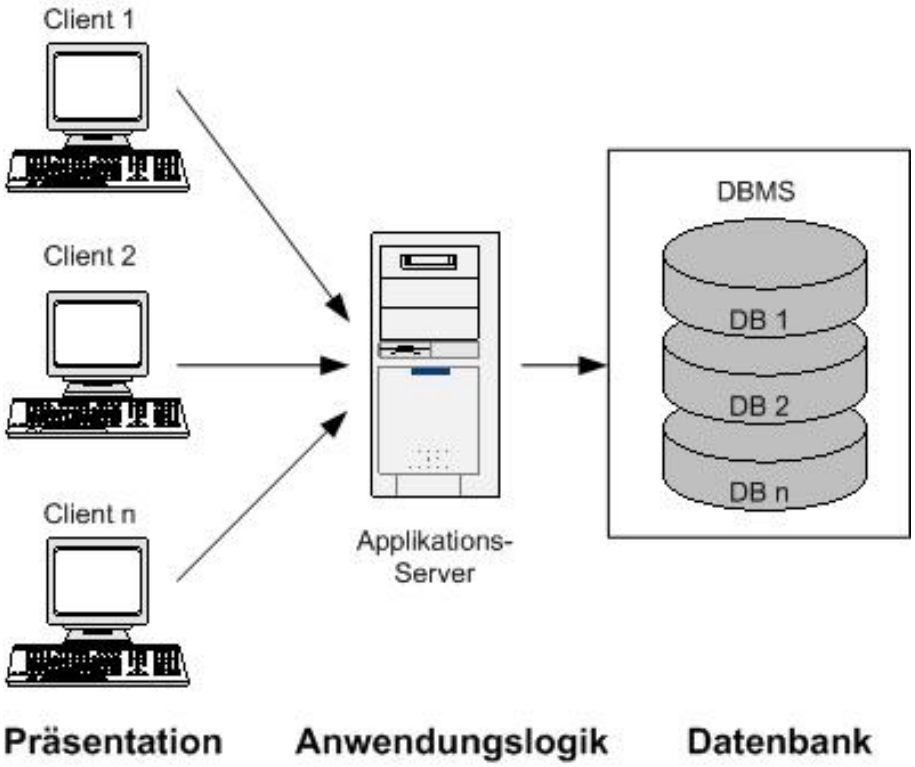
B 5.7 Andmebaasid

Andmebaasisüsteemid (DBS) on laialdaselt kasutatav abivahend suurte andmekoguste arvuti abil organiseerimiseks, tootmiseks, muutmiseks ja haldamiseks, mis loovad paljudes ettevõtetes ja organisatsioonides keskse infobaasi ülesannete täitmiseks. Andmebaasisüsteem (DBS) koosneb nn andmebaasihaldurist (DBMS) ning ühest või mitmest andmebaasist.

Andmebaas on kombinatsioon andmetest ja nende kirjeldusest (metaandmed), mis salvestatakse püsivalt andmebaasisüsteemi.

Andmebaasihaldur (DBMS) on liideseks andmebaaside vahel ning abiks kasutajatele andmete haldamisel ja muutmisel. Andmebaasihalduri kesksteks ülesanneteks on eelkõige erinevate vaadete valmisoleku kindlustamine andmetele (views), andmete konsistentsuse kontroll (tervikluse tagamine), autoriseerimise kontroll, erinevate kasutajate samaaegse pöörduse käsitlus (sünkroniseerimine) ning andmekaitse tagamine, et süsteemi tõrke korral oleks võimalik andmeid kiiresti taastada.

Moodsad andmebaasisüsteemid on enamasti kolmekihilise arhitektuuri koostisoasaks. Kahekihilise arhitektuuri laiendusena (klient-server arhitektuur) rakendatakse siinkohal kliendi ja serveri vahel kolmanda kihina rakendusserverit andmebaasi rakenduste valmisolekuks. Nimetatud arhitektuuri kaudu on vähenenud kliendi varustuse ja lihtsama andmebaaside haldamise tõttu eriti tarkvara levitamisel võimalik kulusid vähendada. Kasutajate käsutusse saab sel moel väikeste kulutustega anda tarkvara versioonid, mis on neile andmebaasisüsteemilt rakendusserveri kaudu automaatselt kättesaadavad.



Joonis: Andebaasihalduri kolmekihiline arhitektuur

Joonis :/ klient 1, klient 2, klient n, Applikationsserver – rakendusserver, DBMS – andmebaasihaldur, DB 1 – andmebaas 1, DB 2 – andmebaas 2, DB n – andmebaas n, Präsentation – esitlus, Anwendungslogik – rakendusloogika, Datenbank – andmebaas./

Andmebaasisüsteem peab võimaldama erinevate kasutajategevuste (nn transaktsioonide) paralleelset töötlemist. Oluline on kinni pidada neljast alljärgnevast põhikarakteristikust, mis on tuntud ACID-printsiibina:

- Atomaarsus (Atomicity)

Transaktsioon on väikseim, tehingu etappide mitte enam killustatav ühik, mis viiakse läbi täielikult või üldse mitte. Kui tehingu sooritamisel peaks tekkima viga või katkestus, tühistatakse kõik transaktsiooni käigus andmebaasi juures juba sisse viidud muutused.

- Konsistentsus (Consistency)

Transaktsioon annab andmebaasi alati konsistentsest seisundist üle teise konsistentsesse seisundisse, s.t et täidetakse kõiki andmebaasi terviklusnõudeid.

- Isoleeritus (Isolation)

Iga transaktsioon toimub isoleeritult ja igas mõttes sõltumatult teistest transaktsioonidest. Lisaks sellele tähendab isoleeritus ka, et iga transaktsiooni käsutusse antakse andmebaasist ainult need andmed, mis on konsistentse seisundi osaks. Kui paralleelsed transaktsioonid konkureerivad ressursside pärast, tuleb transaktsioonid jagada seeriateks.

- Püsivus (Durability)

Edukalt lõpetatud transaktsiooni tulemused jäävad püsivalt andmebaasi.

Andmebaasisüsteemid on standardtarkvara ning neid pakutakse turul erinevate tootjate poolt. Kui andmebaasi kasutatakse andmete töötlemiseks, tuleb kõigepealt valida sobiv andmebaasisüsteem (DBS). Seepärast tuleb arvestada vastavate ohtude ja meetmetega moodulist B 1.10 Tüüptarkvara .

Andmebaase ei saa vaadelda eraldiseisvana keskkonnast, milles neid kasutatakse. Üksikarvuti on samuti mõeldav nagu suurarvutite keskkond või võrgustatud Unixi või Windowsi süsteemid. Seetõttu tuleb sõltuvalt kasutuskeskkonnast rakendada mooduleid kihtidest 3 kuni 5.

Ohud

Lisaks IT-süsteemi mõjutavatele põhiohtudele, eksisteerivad ohud, mis mõjutavad eriti andmebaaside käideldavust ning salvestatud andmete konfidentsiaalsust või terviklust.

Üldiselt sõltub ohtude olemus kasutusmudelist ja volitatud kasutajate ringist. Näiteks võib rääkida kõrgenenud ohuolukorrast, kui lisaks identifitseeritavale asutuse- või ettevõttesisesele kasutajate ringile lubatakse anonüümsete kasutajate juurdepääsu (nt Interneti kaudu).

Edasine aspekt tuleneb andmebaasihalduri üha suurenevast keerukusest, mille põhjuseks on muu seas ka andmete säilitamine üksteisest kaugel asuvates kohtades ning sellega kaasnevatest nõuetest turvalistele sideliinidele ja konsistentsele andmete sünkroniseerimisele.

Infosüsteemide etalonturbes peetakse andmebaase mõjutavateks ohtudeks alljärgnevaid ohtusid:

Organisatsioonilised puudused:

- G 2.22 Logiandmete analüüsimata jätmine
- G 2.26 Ebapiisavad või puuduvad tarkvara katsetamis- ja teavitusprotseduurid
- G 2.38 Installimata või piisavalt aktiveerimata andmebaasi turvamehhanismid
- G 2.39 Andmebaasi haldussüsteemi keerukus
- G 2.40 Andmebaasipöörduse keerukus
- G 2.41 Andmebaasi kasutajate vahetumise halb korraldus
- G 2.57 Andmekandjate puudulik talletus hädajuhtumi korral
- G 2.110 Andmebaasi versiooniuuenduste ja üleviimise puudulik organiseerimine

Inimvead:

- G 3.6 Koristajad jm väljastpoolt tellitud töötajad

- G 3.16 Väär pääsuõiguste haldus
- G 3.23 Andmebaasisüsteemi hooletu haldus
- G 3.24 Andmete juhuslik manipuleerimine
- G 3.80 Andmebaaside sünkroniseerimisvead

Tehnilised rikked:

- G 4.26 Andmebaasi rike
- G 4.27 Pääsukontrollist kõrvalehoidumine ODBC kaudu
- G 4.28 Andmebaasi andmekadu
- G 4.30 Andmebaasi tervikluse ja vastavuse kadu
- G 4.39 Tarkvarakontseptsiooni viga

Ründed:

- G 5.9 IT-süsteemide volitamata kasutamine
- G 5.10 Kaughooldeportide väärkasutus
- G 5.18 Süstemaatiline paroolide mõistatamine
- G 5.64 Andmete või tarkvara manipuleerimine andmebaasisüsteemides
- G 5.65 Teenusetõkestus andmebaasisüsteemis
- G 5.131 SQL-injektsioon

Soovitatavad meetmed

Vaadeldavate IT-varade turvalisuse tagamiseks tuleb lisaks käesolevale moodulile rakendada veel teisigi mooduleid vastavalt infosüsteemide etalonturbe rakendusjuhendi modelleerimise tulemustele.

Andmebaasiserver kui asutuse või ettevõtte keskne informatsioonisalvesti on soovitav paigaldada eraldi serveriruumi või tsentraalsesse arvutuskeskusesse. Rakendatavad meetmed on kirjeldatud moodulites B 2.4 Serveriruum ja B 2.9 Arvutuskeskus .

Kui andmebaasiserver paigaldatakse kaitsekappi, tuleb meetmete rakendamisel juhinduda moodulist B 2.7 Kaitsekapid .

Kui juurdepääsuks andmebaasile kasutatakse mobiilseid lõppseadmeid nagu nt vastavalt varustatud mobiiltelefone või pihuarvuteid (PDA), tuleb juhinduda moodulitest B 3.404 Mobiiltelefon või B 3.405 Pihuarvuti (PDA) .

Nimetatud andmebaasi turvameetmete grupeerimine toimub olenevalt andmebaasi elutsüklist. Andmebaasisüsteemide turvaliseks käitamiseks tuleb muu hulgas läbida alljärgnevad etapid:

1. Planeerimine

Andmebaasisüsteemid on komplekssed tooted, mille töösserakendamiseks ja käituseks on vajalik süstemaatiline planeerimine. Selle aluseks on muu hulgas soetatavale tarkvarale esitatavate nõuete kataloog (vt M 2.80 Tüüptarkvara nõuete kataloogi koostamine) ning andmebaasi turvakontseptsioon (vt M 2.126 Andmebaasi turvakontseptsioon).

2. Administraatorite koolitus ja tarkvara soetamine

Et oleks võimalik andmebaasi tarkvara produktiivne töösserakendamine, peavad vastutavad administraatorid läbima andmebaasisüsteemi turvalise käitamise alase koolituse (vt M 3.11 Hooldus- ja halduspersonali väljaõpe). Väljaõpe peaks toimuma võimaluse korral juba enne andmebaasisüsteemi soetamist (vt M 2.124

Sobiva andmebaasitarkvara valimine), et vastutavaid administraatoreid oleks võimalik varakult ja efektiivselt kontseptsiooni ja ülesseadmisse kaasata.

3. Andmebaasi kontseptsiooni/andmebaasi mudeli koostamine

Enne andmebaasi kasutusele võtmist tuleb koostada andmebaasi kontseptsioon, mis kirjeldab nii andmebaasi komponentide installeerimist ja konfigureerimist, kui ka kasutusotstarbest olenevat andmebaasi struktuuri. Lisaks sellele on vaja koostada praktilist laadi kasutaja kontseptsioon. Olenevalt andmebaasi mahust ja kasutusvaldkonnast ning valitud andmebaaside tüüptarkvarast võib nimetatud kontseptsioon osutuda väga ulatuslikuks (M 2.125 Andmebaasi installeerimine ja konfigureerimine , M 2.126 Andmebaasi turvakontseptsioon , M 2.128 Andmebaasisüsteemi pääsu reguleerimine ja M 2.129 Andmebaasiinfo pääsu reguleerimine).

4. Andmebaasisüsteemi käitus

Andmebaasisüsteemi töösserakendamine ja käitus nõuab lisaks kontseptsiooni realiseerimisele ka pideva seire teostamist, et garanteerida andmete käideldavus, terviklus ja konfidentsiaalsus. Sellekohased tähtsamad meetmed puudutavad dokumenteerimist (M 2.31 Volitatud kasutajate ja õiguste profiilide dokumenteerimine ja M 2.34 IT-süsteemi muutuste dokumenteerimine), haldust (M 2.130 Andmebaasi tervikluse tagamine ja M 2.133 Andmebaasisüsteemi logifailide kontroll) ning andmebaasi kasutamist (M 2.65 IT-süsteemi kasutajate eraldatuse kontroll ja M 3.18 PC kasutajate väljalogimiskohustus).

5. Valmisolek hädaolukorraks

Lisaks andmebaasi töösserakendamist ja tõrgeteta käitust tagavate meetmete rakendamisele tuleb ennetada igat liiki väljalangemisi ning nende mõju minimeerida. Selleks tuleb tähelepanu pöörata spetsiaalselt andmebaasi puudutavatele asjaoludele, et süsteemi või andmebaasi väljalangemise järgselt oleks võimalik täita nõudeid andmebaasisüsteemi kiireks taaskäivitamiseks ning viia andmekao oht miinimumini (M 6.49 Andmebaasi varundamine ja M 6.50 Andmehulkade arhiveerimine).

Alljärgnevalt tutvustatakse turvameetmete kogumit mida tuleb rakendada valdkonnas “Andmebaasid”:

Planeerimine ja kontseptsioon

- (M) M 2.80 Tüüptarkvara nõuete kataloogi koostamine
- (L) M 2.126 Andmebaasi turvakontseptsioon
- (L) M 2.132 Andmebaasi kasutajate ja kasutajagruppide konfigureerimise reeglid
- (L) M 2.134 Andmebaasipäringute suunised
- (L) M 2.336 Koguvastutus infoturbe eest juhtkonna tasemel
- (L) M 2.363 SQL-injektsiooni kaitse
- (M) M 2.E22 Kruäptograafiliste algoritmide vahetatavuse noõue
- (M) M 5.58 Andmebaasiliidese draiverite valik ja installeerimine

Soetamine

- (M) M 2.124 Sobiva andmebaasitarkvara valimine

Rakendamine

- (L) M 2.125 Andmebaasi installeerimine ja konfigureerimine

- (L) M 2.135 Andmete turvaline teisaldus andmebaasi
- (L) M 4.7 Algparoolide muutmine
- (L) M 4.71 Andmebaasi linkide kasutamise kitsendamine
- (M) M 4.73 Valitavate andmehulkade ülempiiride määramine

Kasutamine

- (L) M 2.31 Volitatud kasutajate ja õiguste profiilide dokumenteerimine
- (L) M 2.34 IT-süsteemi muutuste dokumenteerimine
- (L) M 2.65 IT-süsteemi kasutajate eraldatuse kontroll
- (M) M 2.127 Tuletamise vältimine andmebaasis
- (L) M 2.128 Andmebaasisüsteemi pääsu reguleerimine
- (L) M 2.129 Andmebaasiinfo pääsu reguleerimine
- (L) M 2.130 Andmebaasi tervikluse tagamine
- (L) M 2.131 Haldusülesannete lahusus andmebaasisüsteemides
- (L) M 2.133 Andmebaasisüsteemi logifailide kontroll
- (L) M 3.18 PC kasutajate väljalogimiskohustus
- (L) M 4.67 Tarbetute andmebaasikontode sulgemine ja kustutamine
- (L) M 4.68 Järjekindla andmebaasi halduse tagamine
- (M) M 4.69 Andmebaasi regulaarne turvakontroll
- (L) M 4.70 Andmebaasiseire teostamine
- (L) M 4.72z Andmebaasi krüpteerimine
- (M) M 4.134 Sobivate andmevormingute valimine
- (M) M 5.117z Andmebaasiserveri integreerimine turvalüüsi koostisse

Valmisolek hädaolukorraks

- (L) M 6.48 Protseduurid andmebaasi tervikluse kao puhuks
- (L) M 6.49 Andmebaasi varundamine
- (L) M 6.50z Andmehulkade arhiveerimine
- (L) M 6.51 Andmebaasi taastamine

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.6 Arvuti paroolkaitse rangemad reeglid
- HG.24 Paroolide regulaarkontroll parooliskänneriga
- HG.25 Kaugpöörduste kohustuslik logimine
- HG.38 Turvapaikade paigaldatuse regulaarseire
- M 2.E22 Krüptograafiliste algoritmide vahetatavuse nõue

Teabe käideldavus (K)

- HK.6 Edastmiseks genereeritud andmete kahes eksemplaris varukopeerimine
- HK.8 Andmebaasi tervikliku varundamise nõue

Teabe terviklus (T)

- HT.7 Kasutajate ja nende profiilide perioodiline seire

- HT.9 Andmebaasi pääsuõiguste perioodiline seire
- HT.10 Andmebaasi kannete krüptoaheldamine
- HT.17 Krüptoaheldatud saate- ja vastuvõtulogid
- HT.34 Digiallkirja kasutamine
- HT.49 Lisanõuded arhiveeritud andmete krüptoatribuutide regenereerimisele
- HT.51 Lisanõuded teabe hankimisele turvaaukude kohta
- HT.68 OWASP rünnete vastased lisakaitsemeetodid

Teabe konfidentsiaalsus (S)

- HS.39 Lisanõuded andmebaaside krüpteerimisele

B 5.8 Kaugtöö

Kaugtöö all mõistetakse iga informatsiooni- ja kommunikatsioonitehnikale toetuvat tegevust, mida tehakse eranditult või ajutiselt väljaspool tööandja või tellija hoonet. Tegevuste sooritamise hõlbustamiseks on kaugtöötajal ühendus tööandja või töö tellija IT-süsteemiga.

On olemas erinevaid kaugtöö vorme. Kaugtöötaja võib töötada kodus või siis ringi reisides. Võimalik on ka, et töötajad rakendatakse tööle kliendi või tarnija juures ning nad töötavad seal oma tööandja sidevahenditega. Järgmiseks võimaluseks on kaugtöö niinimetatud kaugtöökeskustes või satelliit- või naabrusbüroodes.

Koduse kaugtöö puhul tehakse vahet eranditult kodus tehtaval tööl ja alternatiivsel kaugtööl. Alternatiivse kaugtöö korral töötatakse vaheldumisi oma töökohal tööandja juures ja kodus.

Käesolev moodul keskendub kaugtöö vormidele, mille sooritamine toimub osaliselt või täielikult koduses keskkonnas. Seejuures lähtutakse asjaolust, et koduse töökoha ja asutuse vahel on telekommunikatsiooniühendus, mis teeb võimalikuks andmevahetuse või ka juurdepääsu asutuse andmebaasile.

Käesolevas moodulis kirjeldatud soovitatavad meetmed hõlmavad nelja valdkonda:

- Kaugtöö organiseerimist,
- kaugtöötaja tööarvutit,
- ühendust kaugtööarvuti ja asutuse vahel,
- kodutöötajaga sidet pidava arvuti ühendamist kaugtööarvutiga.

Käesolevas moodulis kirjeldatud soovitatavad meetmed keskenduvad kaugtööks kasutatavale IT-süsteemile esitatavatele täiendavatele turvanõuetele ning kaugtöö käigus töödeldavale informatsioonile. Eriti kaugtöö tehniliste komponentide osas (kaugtööarvuti, sideliinid ja kaugtöötajaga sidet pidav arvuti) formuleeritakse turvanõuded, mis tuleb vastavalt konkreetsele kujundusele sobivate IT-süsteemide abil realiseerida.

Ohud

Infosüsteemide etalonturbes peetakse kaugtööd mõjutavateks ohtudeks järgnevaid tüüpilisi ohtusid:

Vääramatu jõud:

- G 1.1 Personali väljalangemine

Organisatsioonilised puudused:

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.4 Turvameetmete ebapiisav järelevalve
- G 2.7 Õiguste volitamata kasutamine
- G 2.22 Logiandmete analüüsimata jätmine
- G 2.24 Kaitsetus välisvõrgu vastu
- G 2.49 Kaugtöötajate ebapiisav või puuduv koolitamine
- G 2.50 Hilistused kaugtöötajate ajutise piiratud kättesaadavuse tõttu
- G 2.51 Kaugtöötajate halb integratsioon infovoogu
- G 2.53 Kaugtöötajate asendamise puudulikud eeskirjad

Inimvead:

- G 3. 1 Andmete konfidentsiaalsuse või tervikluse kadu kasutaja vea tõttu
- G 3.3 Hooletus turvameetmete suhtes
- G 3.9 IT-süsteemi väär haldus
- G 3.13 Väära või soovimatu andmekogumi saatmine
- G 3.16 Väär pääsuõiguste haldus
- G 3.30 Kaugtööjaamade volitamatu kasutamine eraotstarbel

Tehnilised rikked:

- G 4.13 Salvestatud andmete hävimine

Ründed:

- G 5.1 IT-seadmete või -tarvikute manipuleerimine ja hävitamine
- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.9 IT-süsteemide volitamata kasutamine
- G 5.10 Kaughooldeportide väärkasutus
- G 5.18 Süstemaatiline paroolide mõistatamine
- G 5.19 Kasutajaõiguste väärkasutus
- G 5.20 Administraatori õiguste väärkasutus
- G 5.21 Trooja hobused
- G 5.71 Tundliku informatsiooni konfidentsiaalsuse kadu

Soovitatavad meetmed

Vaadeldava IT-koosluse turvalisuse tagamiseks tuleb lisaks käesolevale moodulile rakendada veel teisigi mooduleid vastavalt infosüsteemide etalonturbe rakendusjuhendi modelleerimise tulemustele.

Kaugtöö turvalise toimimise tagamiseks on vaja rakendada terve rida meetmeid, alates planeerimisest ja kontseptsiooni koostamisest, millele järgneb seadmete soetamine ja valmisolek hädaolukorraks. Järgnevalt on ära toodud etapid, mis seejuures tuleb läbida, ning meetmed, mida vastavatel etappidel on vaja rakendada. Kaugtöökoha infrastruktuurse turvalisuse tagamiseks rakendatavaid meetmeid kirjeldatakse moodulis B 2.8 Kaugtöökoht kodus . Kaugtööarvutina kasutava IT-süsteemi turvalisuse tagamiseks tuleb rakendada lisaks sellele sobivat kliendi moodulit.

Planeerimine ja kontseptsioon

Kaugtöö jaoks tuleb luua kontseptsioon, milles on välja toodud turvasuunised, kaugtöö käigus töödeldava informatsiooni kaitsevajadus ning riskid ja soovitatavad turvameetmed (vaata M 2.117 Kaugtöötajate pääsu reguleerimine).

Turvanõuetele vastava kaugtöö eeldusteks on organisatsioonilised eeskirjad ja personaliga seotud meetmed. Erilist tähelepanu tuleb pöörata kaugtöötajate spetsiaalsetele kohustustele ning nende instrueerimisele kommunikatsioonitehnika kasutusreeglite alal. Need on kirjeldatud meetmetes M 2.113 Kaugtöö reeglid , M 2.116 Sidevahendite kasutamise reguleerimine , M 2.117 Kaugtöötajate pääsu reguleerimine ja M 3.21 Kaugtöötajate turbealane koolitus .

Rakendamine

Pärast organisatsiooniliste ja planeerimisalaste eeltööde korraldamist võib installeerida kaugtööarvutid, kommunikatsiooniarvutid ja teised IT-süsteemid. Seejuures tuleb rakendada alljärgnevaid meetmeid:

- Kaugtööarvuti turvalisus: kaugtööarvuti tuleb kujundada selliselt, et selle turvaline kasutamine on võimalik ebaturvalises kasutuskeskkonnas. Erilist tähelepanu tuleb pöörata asjaolule, et kaugtööarvutit saaks offline - ja online -töörežiimil kasutada vaid volitatud isikud. Seejuures tuleb kõrgendatud tähelepanu pöörata meetmes M 4.63 Kaugtöökohaarvutite turvanõuded kirjeldatud turvanõuetele.
- Turvaline side kaugtööarvuti ja asutuse vahel: kuna side toimub avalike võrkude kaudu (näiteks ISDN- või DSL-ühenduse kaudu), tuleb erilise hoolikusega täita nõudeid turvalise side tagamiseks kaugtööarvuti ja asutuse vahel. Need on kirjeldatud meetmes M 5.51 Turvanõuded kaugtööarvuti ja organisatsiooni vahelisele sideühendusele . Kaugtööarvuti ühendamiseks avalike võrkude kaudu tuleb rakendada moodulit B 4.5 IT-süsteemi kohtvõrguühendus ISDN kaudu . Kaugtööarvuti ühendamiseks virtuaalse privaatvõrgu (VPN) kaudu tuleb järgida moodulit B 4.4 Virtuaalne privaatvõrk (VPN)
- Asutuse sidearvuti turvalisus: see arvuti kujutab endast nii-öelda avalikult juurdepääsetavat liidest, mille kaudu kaugtöötaja saab kasutada asutuse infotehnoloogiat ja andmeid. Kuna siin on vajalik ära hoida väärkasutust kolmandate isikute poolt, tuleb täita meetmes M 5.52 Sidearvutite turvanõuded .

Kasutamine

Kaugtöö turvalisus sõltub olulisel määral kasutajatest. Seetõttu peavad kaugtöötajad saama turvasuuniste ja IT-süsteemi kasutamise alast koolitust (vaata M 3.21 Kaugtöötajate turbealane koolitus).

Valmisolek hädaolukorraks

Kõigist kaugtöö käigus loodud ja muudetud olulise tähtsusega andmetest tuleb teha varukoopiad (vaata M 6.47 Kaugtöö andmevarundus).

Alljärgnevalt tutvustatakse turvameetmete kogumit, mida tuleb rakendada valdkonnas “ Kaugtöö ”.

Planeerimine ja kontseptsioon

- (L) M 2.113 Kaugtöö reeglid
- (L) M 2.114 Infovool kaugtöötaja ja asutuse vahel
- (L) M 2.115 Kodutööjaama hooldus
- (L) M 2.116 Sidevahendite kasutamise reguleerimine
- (L) M 2.117 Kaugtöötajate pääsu reguleerimine
- (M) M 2.217 Teabe, rakenduste ja süsteemide hoolikas liigitamine ja käitlus
- (M) M 2.241 Kaugtöökoha nõuete analüüsi sooritamine

Rakendamine

- (L) M 4.63 Kaugtöökohaarvutite turvanõuded

- (L) M 5.51 Turvanõuded kaugtööarvuti ja organisatsiooni vahelisele sidehendusele
- (L) M 5.52 Sidearvutite turvanõuded

Kasutamine

- (L) M 3.21 Kaugtöötajate turbealane koolitus

Valmisolek hädaolukorraks

- (L) M 6.47 Kaugtöö andmevarundus

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.25 Kaugpöörduste kohustuslik logimine
- HG.61 Nõuded kodutööarvutile

Teabe käideldavus (K)

- HK.6 Edastmiseks genereeritud andmete kahes eksemplaris varukopeerimine
- HK.7 Kahes eksemplaris varukopeerimine kodutööl

Teabe terviklus (T)

- HT.7 Kasutajate ja nende profiilide perioodiline seire
- HT.50 Andmete turvaline haldamine kodu- ja kaugtööl
- HT.56 Lisanõuded mobiilsele kaugtööarvutile
- HT.63 Sülearvutite krüpteerimine
- HT.67 Pihuarvutite krüpteerimine
- HT.72 Turvatunneldamise protokolli kasutuskohustus

Teabe konfidentsiaalsus (S)
-

B 5.9 Novell eDirectory

Novell eDirectory on kompleksne ja mitmekülgne toode, mis

- ühelt poolt asutuse või ettevõtte võrgu siseselt võib üle võtta ühendatud ressursside ja nende kasutajate halduse kogu platvormi ulatuses
- teiselt poolt on see kasutatav ka turvatud ja standardiseeritud pääsuvõimalustega Interneti informatsioonibaasina sobivate klientide kaudu.

Mõlemad kasutusmudelid kätkevad endas täiesti erinevaid ohtusid nimetatud süsteemi installeerimisel ja käitamisel. Eelkõige nimetatud kasutusmudelite kombineerimine suurendab infoturbealaseid ohtusid.

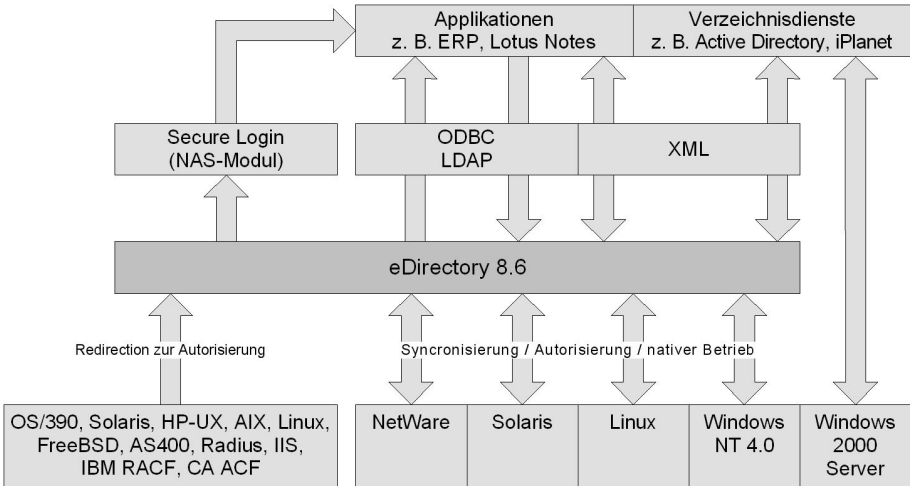
eDirectory kataloogi salvestatud andmete turvalisuse tagamiseks tuleb tähelepanu pöörata ka selle aluseks olevale operatsioonisüsteemi turvalisusele. Viimane ei ole küll käesoleva mooduli komponent ning seepärast viidatakse vastavatele kirjeldustele kasutatava operatsioonisüsteemi turvalisuse tagamiseks 3. kihi moodulites.

eDirectory on välja kasvanud Novell Directory Services (NDS) kataloogiteenusest, mis oli operatsioonisüsteemi Netware 4 komponent. See oli omal ajal väljapaistev uuendus võrreldes operatsioonisüsteemiga Netware 3 . Praeguseks ajaks pakub Novell nimetatud kataloogiteenuseid iseseisva toote eDirectory näol täiesti sõltumatult Netware operatsioonisüsteemist. eDirectory't on võimalik installeerida ja käitada paljude operatsioonisüsteemidel. Kirjanduses ja muudes allikates kasutatakse siiski tihti endiselt mõistet Novell Directory Services ning käsitletakse mõisteid NDS ja eDirectory sünonüümidena.

Käesolevas moodulis käsitletakse spetsiaalselt versiooni eDirectory 8.6, ja nimelt inglise versiooni. Tarkvara toetab platvorme Netware, Windows NT/2000, Linux ja Sun Solaris.

eDirectory't saab kasutada spetsiaalse klienditarkvaraga, nii nagu Novell Client on sobiv kasutamiseks Windows operatsioonisüsteemides. Nimetatud kliendid on integreeritud vastava arvuti buutimisprotseduuri ning need võtavad üle kasutajate autentimise eDirectory kataloogiteenuste suhtes. Ka Unix 'i operatsioonisüsteemide jaoks (Linux, Solaris) on olemas taoline võimalus, mis kasutab programmiliidest Pluggable Authentication Modules (PAM). Seejuures kasutatakse tarkvaramooduleid Novell Account Management Modules . Ka seejuures toimub sisselogimisel kasutajate autentimine eDirectory kataloogiteenuse suhtes.

Teist juurdepääsuvõimalust kataloogidele pakub LDAP-liides. Nimetatud standardiseeritud liidese kasutamise abil on eDirectory kasutamine võimalik ka teiste rakenduste ja süsteemidega. Internetis kasutamiseks sobivaks pöördusmeetodiks on üldjuhul LDAP-protokoll.



Joonis: ülevaade arhitektuurist

Joonis: /Applikationen – rakendused, Verzeichnisdienste – kataloogiteenused, z. B – nt, NAS-Modul – NAS-moodul, Redirection zur Autorisierung – ümbersuunamine autoriseerimisele, Syncronisierung – sünkroniseerimine, Autorisierung – autoriseerimine, nativer Betrieb – esialgne kasutamine./

Lisaks eelnimetatule pakub eDirectory tarkvara suurel hulgal vahendeid, muuhulgas iMonitori , mis loob veebilehitsejalt kataloogiteenuse serveri kaudu võimaluse monitooringuks ja diagnoosiks.

Ohud

Tarkvara keerukuse ja paljude funktsioonide tõttu on eDirectory kataloogiteenuse kasutamine seotud terve rea ohtudega. Nendele lisanduvad ohud, mis puudutavad kasutatavat operatsioonisüsteemi, eriti aga üldist juurdepääsu serverile ja failisüsteemile.

Infosüsteemide etalonturbes peetakse Novell eDirectory süsteemi kasutamisel tüüpilisteks järgmisi ohtusid:

Vääramatu jõud:

- G 1.2 IT-süsteemi avarii

Organisatsioonilised puudused:

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.2 Reeglite puudulik tundmine
- G 2.7 Õiguste volitamata kasutamine
- G 2.69 Novell eDirectory kasutamise ebapiisav või puuduv planeerimine
- G 2.70 Novell eDirectory partitsioonide ja replikatsioonide ebapiisav või puuduv planeerimine
- G 2.71 Novell eDirectory LDAB-pöörduse ebapiisav või puuduv planeerimine

Inimvead:

- G 3.9 IT-süsteemi väär haldus

- G 3.13 Väära või soovimatu andmekogumi saatmine
- G 3.16 Väär pääsuõiguste haldus
- G 3.34 Võrguhaldussüsteemi ebasobiv konfiguratsioon
- G 3.35 Töötava serveri elektritoite väljalülitamine
- G 3.36 Sündmuste väär tõlgendamine
- G 3.38 Vead konfigureerimisel ja kasutamisel
- G 3.43 Puudulik paroolihooldus
- G 3.50 Novell eDirectory väär konfiguratsioon
- G 3.51 Novell eDirectory pääsuõiguste väär andmine
- G 3.52 Novell eDirectoryt kasutava intranet-klientsüsteemi pöörduse väär konfiguratsioon
- G 3.53 Novell eDirectoryt kasutava LDAP-pöörduse väär konfiguratsioon

Tehnilised rikked:

- G 4.10 Keerukad ligipääsuvõimalused võrgustatud IT-süsteemides
- G 4.13 Salvestatud andmete hävimine
- G 4.33 Autentimise puudumine või puudulikkus
- G 4.34 Krüptomooduli rike
- G 4.44 Novell eDirectory rike

Ründed:

- G 5.16 Ohud hoolde- ja haldustööde ajal
- G 5.18 Süstemaatiline paroolide mõistatamine
- G 5.19 Kasutajaõiguste väärkasutus
- G 5.20 Administraatori õiguste väärkasutus
- G 5.65 Teenusetõkestus andmebaasisüsteemis
- G 5.78 DNS-i võltsimine
- G 5.81 Krüptomooduli volitamata kasutamine

Soovitatavad meetmed

Vaadeldavate IT varade turvalisuse tagamiseks tuleb lisaks käesolevale moodulile rakendada veel teisigi mooduleid vastavalt infosüsteemide etalonturbe rakendusjuhendi modelleerimise tulemustele.

eDirectory komponentide kasutamiseks tuleks juba planeerimisel luua vastavasisuline IT-alane turvakontseptsioon, mida on võimalik konsistentselt integreerida olemasolevasse üleorganisatsioonilisse infoturbe kontseptsiooni. eDirectory süsteem tuleb selliselt konfigureerida, et rakendataks juba olemasolevaid turvameetmeid ning nendele lisaks ka eDirectory puudutavaid spetsiifilisi nõudeid.

eDirectory süsteemi kasutatakse reeglina koos teiste süsteemidega, mille ülesandeks on kontrollida sisevõrgu poole pöördumist väljast. Siinkohal tuleb eriti tähtsaks pidada tulemüüri ja kaughoolduse süsteeme, millega eDirectory peab koos töötama. Seepärast tuleb eDirectory spetsiifiliste meetmete rakendamisel rakendada alati lisaks ka vastavate süsteemide mooduleid. Lisaks 3. kihi moodulitele tuleb muu hulgas rakendada mooduleid B 3.101 Server , B 4.4 Virtuaalne

privaatvõrk (VPN) ja B 5.7 Andmebaasid .

eDirectory süsteemi edukaks juurutamiseks on vaja rakendada terve rida meetmeid, alustades kontseptsiooni koostamisega, millele järgneb installatsioon ja käitus. Alljärgnevalt käsitletakse kokkuvõtlikult üksikud etappe ning meetmeid, mida vastavate etappide läbimisel on vaja rakendada.

1. Pärast eDirector y kataloogisüsteemina juurutamise otsust tuleb soetada vastav tarkvara ning lisaks vajaminev riistvara. Kuna eDirectory'l on mitmeid rakendusvõimalusi (vt eestpoolt), sõltub soetatav tarkvara planeeritavatest kasutusmudelitest. Seepärast tuleb rakendada alljärgnevaid meetmeid:

- Kõigepealt tuleb planeerida eDirectory süsteemi installeerimine.
- Paralleelselt sellega tuleb välja töötada turvasuunised, mis ühelt poolt realiseerib juba olemasolevad turvasuunised eDirectory kontekstis ning teiselt poolt määratleb konsistentselt eDirectory spetsiifilised täiendused.
- Enne eDirectory süsteemi tegelikku kasutamist normaalkäituses peavad kasutajad ja administraatorid läbima koolituse toote kasutamise alal. Eriti administraatoritel on soovitav intensiivselt tegelda teemaga, mis peaks baseeruma ulatuslikel teadmistel kasutatavate operatsioonisüsteemide turvalisuse alal (vt M 3.29 Novell eDirectory haldamise koolitus). Kasutajatele tuleb info installeeritud klientide kättesaadavate turvamehhanismide kohta detailselt edastada (vt M 3.30 Novell eDirectory klienttarkvara kasutamise koolitus).

2. Pärast organisatoorsete ja planeerimisalaste eeltööde läbiviimist võib järgneda eDirectory süsteemi installeerimine. Seejuures tuleb rakendada alljärgnevaid meetmeid:

- Installeerimist võib lugeda lõpetatuks alles siis, kui eDirectory süsteemid on viidud turvalisse seisundisse. Sellega tagatakse, et järgnevas konfiguratsioonifaasis omavad eDirectory süsteemile juurdepääsu vaid volitatud administraatorid.
- "Toorinstallatsioonile" järgneb eDirectory süsteemi esmane konfigureerimine.

3. Pärast konfigureerimist ja testimisfaasi alustatakse normaalkäitusega. Seejuures tuleb tähelepanu pöörata alljärgnevatele turvaaspektidele:

- eDirectory süsteem on reeglina allutatud pidevatele muutustele. Seetõttu on vajalik ohutuse seisukohalt tähtsate turvaparameetrite pidev kohandamine vajadustele. Lisaks sellele sõltub jaotatud tarkvaraarhitektuuri turvalisus kõigi osasüsteemide turvalisusest. See kehtib eriti eDirectory klienditarkvara kohta.
- Lisaks turvalise kasutamise tagamise meetmetele on olulise tähtsusega ka meetmed, mis tagavad valmisoleku hädaolukorraks. Nõuandeid nimetatud teema kohta leiate meetmest M 6.81 Novell eDirectory andmete varundamine .

Alljärgnevalt tutvustatakse turvameetmete kogumit, mida tuleb rakendada moodulis "Novell eDirectory ":

Planeerimine ja kontseptsioon

-

Rakendamine

- (L) M 3.29 Novell eDirectory haldamise koolitus
- (L) M 3.30 Novell eDirectory klienttarkvara kasutamise koolitus

Kasutamine

-

Valmisolek hädaolukorraks

- (L) M 6.81 Novell eDirectory andmete varundamine

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele

Kohustuslikud üldmeetmed

- HG.6 Arvuti paroolkaitse rangemad reeglid
- HG.24 Paroolide regulaarkontroll parooliskänneriga
- HG.25 Kaugpöörduste kohustuslik logimine
- HG.38 Turvapaikade paigaldatuse regulaarseire

Teabe käideldavus (K)

-

Teabe terviklus (T)

- HT.7 Kasutajate ja nende profiilide perioodiline seire
- HT.17 Krüptoaheldatud saate- ja vastuvõtulogid

Teabe konfidentsiaalsus (S)

-

B 5.12 Microsoft Exchange / Outlook

Microsoft Exchange on elektrooniliste teadete haldussüsteem, mis toetab ka Workflow' funktsioone. See on muu hulgas mõeldud keskmise suurusega ja suurtele ametiasutustele ja ettevõtetele teadete, nt meilide vahetamiseks nii institutsiooni sees kui ka väljaspool. Exchange'iga saab teateid hallata, kätte toimetada, filtreerida ja välja saata. Samuti võimaldab Exchange kasutada ja hallata selliseid tüüpilisi siderakendusi nagu uudistegrupid, kalender, tööülesannete loetelud ja Unified Messaging (sissetulevate ja väljasaadetavate meilide kokkukoondamine).

Microsoft Outlook on Microsoft Office'i paketti kuuluv e-mail client . Tavalise meilifunktsiooni kõrval on selles ka terve hulk lisafunktsioone, nt kommunikatsioon ja kiirsõnumivahetus, mis peaksid lihtsustama ametiasutuste ja ettevõtete tööprotsesse.

Selles moodulis kirjeldatakse turbesoovitusi, mida saab rakendada peamiselt versioonides Microsoft Exchange 2010 ja Microsoft Outlook 2010. Samu põhimõtteid saab siiski järgida ka vanemate ja tulevikus ilmuvate versioonide puhul.

Ohud

IT-etalonturbe seisukohalt peetakse Microsoft Exchange'i serveril ja Microsoft Outlooki klientidel põhinevate sidesüsteemide puhul tüüpilisteks järgmisi ohuallikaid.

Vääramatu jõud:

- G 1.1 Personali väljalangemine
- G 1.2 IT-süsteemi avarii

Organisatsioonilised puudused:

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.2 Reeglite puudulik tundmine
- G 2.7 Õiguste volitamata kasutamine
- G 2.37 Sideliinide kontrollimatu kasutamine
- G 2.55 Rühmatarkvara reguleerimata kasutamine

Inimvead:

- G 3. 1 Andmete konfidentsiaalsuse või tervikluse kadu kasutaja vea tõttu
- G 3.8 IT-süsteemi väär kasutamine
- G 3.9 IT-süsteemi väär haldus
- G 3.16 Väär pääsuõiguste haldus
- G 3.38 Vead konfigureerimisel ja kasutamisel
- G 3.61 Outlook 2000 klientsüsteemide väär konfiguratsioon

Tehnilised rikked:

- G 4.20 Andmekadu andmekandja täitumise tõttu
- G 4.22 Tüüptarkvara turvaaugud või vead
- G 4.26 Andmebaasi rike
- G 4.28 Andmebaasi andmekadu
- G 4.32 Sõnumi kaotsiminek

- G 4.35 Ebaturvaline krüptoalgoritm
- G 4.83 Enda arendatud makrode väärfunktsioonid Outlookis

Ründed:

- G 5.9 IT-süsteemide volitamata kasutamine
- G 5.19 Kasutajaõiguste väärkasutus
- G 5.22 Kaasaskantava IT-süsteemi vargus
- G 5.23 Viirused
- G 5.77 Võõraste meilide lugemine
- G 5.83 Krüptograafiliste võtmete paljastamine
- G 5.84 Võltsitud sertifikaadid
- G 5.135 SPIT ja Vishing
- G 5.163 Exchange'i süsteemide vastu suunatud ründed
- G 5.164 Programmeerimisliideste väärkasutus Outlookis

Soovitatavad meetmed

Vaadeldava IT-koosluse turvalisuse tagamiseks tuleb peale selle mooduli rakendada veel teisigi mooduleid, mis selguvad IT-etalonturbe rakendusjuhendi kohase modelleerimise tulemusel.

Microsoft Exchange'i süsteemi turvaliseks käitamiseks tuleb muu hulgas tegeleda ka meilisüsteemide üldiste infoturbeaspektidega, mis puudutavad näiteks internetiühendust, võimalikke krüpteerimismeetodeid, aktiivsisu, viirusetõrjetarkvara. Selleks on soovitatav rakendada moodulit B 5.3 Rühmatarkvara . Selles moodulis kirjeldatud ohud ja meetmed kehtivad Microsoft Exchange'i/Outlooki kontekstis ilma piiranguteta.

Rühmatarkvara moodulile lisaks on IT-etalonturvet kajastavatel veebilehtedel nimetatud abivahendeid, milles on Microsoft Exchange Server 2010 ja Microsoft Outlook 2010 kohta käivad juhised ning turvanõuded sõnastatud konkreetsemalt. Neid abivahendeid tuleks käsitleda siin toodud meetmete detailsemate kirjeldustena. Iga olulise meetme jaoks on sõnastatud soovitused ja turbemeetmed, mis lähtuvad käsitletud komponendi konkreetsest versioonist.

Järgnevalt kirjeldatud meetmete võtmisega seotud aspekte seoses Microsoft Exchange Server 2010 ja Microsoft Outlook 2010 turbesuunistega käsitletakse ka IT-etalonturbe kataloogide abivahendites.

Microsoft Exchange'i süsteemide turbes mängib keskset rolli Windowsi operatsioonisüsteemide turbe tagamine. See kehtib nii serveri kui ka vaadeldava võrgu klientide kohta. Seetõttu tuleb pöörata piisavalt tähelepanu ka Exchange'i süsteemi aluseks olevale operatsioonisüsteemile. Viimast siin moodulis siiski ei käsitleta. Asjakohased kirjeldused operatsioonisüsteemide turbe tagamise kohta leiate IT-etalonturbe kataloogide moodulite kolmandast kihist. Eriti olulised on siinkohal ka töötajatele mõeldud ja kohustuslikuks tehtud turbemeetmete järgimine ning töötajate sellekohane koolitus.

Exchange'i süsteem pannakse enamasti tööle teiste süsteemide keskkonnas, mille ülesanne on kaitsta sisevõrgu juurdepääsu väljastpoolt. Siinkohal tuleb eraldi mainida turvalüüse ja kaughoolduseks kasutatavaid süsteeme, millega Microsoft

Exchange peab suutma koostööd teha. Sellest tingituna tuleb spetsiaalsete, Microsoft Exchange'i ja Outlooki puudutavate meetmete võtmisel arvestada ka teiste asjasse puutuvate süsteemide kohaste moodulitega. Moodulite kolmandasse kihti kuuluvate moodulite kõrval tuleb arvesse võtta ka mooduleid B 3.301 Turvalüüs (tulemüür) , juhul kui Exchange'i süsteeme kasutatakse demilitariseeritud tsoonides (DMZ) ja B 4.4 Virtuaalne privaatvõrk (VPN) , juhul kui Exchange'i süsteemide juurdepääsuks kasutatakse VPN-i.

Planeerimine ja kontseptsiooni koostamine

Pärast seda, kui Exchange'i süsteemi kasutuselevõtt on otsusega heaks kiidetud, tuleb alustada turvalise käituse planeerimisega ja koostada kontseptsioon. Selleks tuleb võtta arvesse erinevaid aspekte, mida on kirjeldatud meetmes M 2.247 Exchange/Outlook 2000 kasutamise planeerimine . Exchange'i süsteemi turvet saab ka juba planeerimise ja kontseptsiooni koostamise etapis oluliselt mõjutada, eeldusel et turbeaspektidele pööratakse piisavalt tähelepanu.

Eriti hoolikas tuleks turbe planeerimisega olla nende kasutusvaldkondade puhul, kus Microsoft Exchange'i süsteeme rakendatakse tüüpilistes internetikeskkondades. Selleks tuleb võtta meedet M 2.481 Exchange'i kasutuse planeerimine Outlook Anywhere'i jaoks .

Rakendamine

Pärast töökorralduslike eeltööde tegemist saab edasi liikuda Microsoft Exchange'i süsteemi installimise juurde. Siin tuleb arvestada meetmega M 4.161 Exchange / Outlook turvaline installeerimine . Exchange'i süsteemide administraatoreid ja kasutajaid tuleb ka piisavalt koolitada.

Microsoft Exchange'i süsteemi installimine moodustab kõikidest rakendamise etapis võetavatest meetmetest vaid ühe väikse osa. Töömaht suureneb märkimisväärselt pärast installimist, kui hakatakse tegelema Microsoft Exchange'i süsteemi aluskonfiguratsiooniga. Aluskonfiguratsiooni loomisega määratakse kindlaks raamtingimused, mis hakkavad toimima Microsoft Exchange'i süsteemi kasutuselevõtul ning mis mõjutavad selle turvet.

Iga Microsoft Exchange'i süsteemi tuuma moodustavad andmebaas ja selles hoitavad andmetabelid. Andmebaasi võimalikud turbeprobleemid mõjutavad alati tervet süsteemi. Exchange'i serverite ja andmebaaside turvet puudutavad soovitused on koondatud meetmesse M 4.162 Exchange 2000 serverite turvaline konfiguratsioon .

Microsoft Exchange'i süsteemid on laiali jaotatud ülesehitusega ning need suhtlevad omavahel läbi erinevate liideste, lisaks suhtlevad nad väliste serveri- ja klientsüsteemidega. Seetõttu tuleb pöörata piisavalt tähelepanu andmeside turbe tagamisele (vt M 5.100 Exchange'i süsteemi siseneva ja väljuva kommunikatsiooni kaitse).

Microsoft Exchange'i süsteemi tööd tuleb ametiasutuse või ettevõtte lokaalsete funktsioonivajaduste (nt tööprotsesside vajaduste) järgi muuta. Muutmiseks tuleb seda kohandada institutsiooni vajadustega (customizing) (vt M 2.483 Exchange'i süsteemide turvaline kohandamine).

Kasutamine

Pärast esmast installimist ja katsetusetapi läbimist minnakse üle tavakasutusele. Turvaintsidentide avastamiseks tuleb tagada, et Microsoft Exchange'i süsteemid oleksid allutatud asjakohasele seirele (vt M 2.482 Exchange'i süsteemide

regulaarsed turvakontrollid ja M 4.166 Exchange/Outlook 2000 turvaline käitamine).

Kuna Microsoft Exchange'i süsteemid on pidevas muutuses, mis on sageli tingitud muutuvatest kasutusnõuetest ja -valdkondadest, tuleb hoolitseda ka piisava turbeastme säilimise eest (vt B 1.14 Turvapaikade ja muudatuste haldus). See puudutab eriti just enda tehtud tarkvaraarendusi (vt M 2.379 Tarkvaraarendus lõppkasutaja poolt).

Valmisolek hädaolukorraks

Microsoft Exchange'i süsteemide soovitused hädaolukorraks ettevalmistuse kohta leiate meetmest M 4.166 Exchange/Outlook 2000 turvaline käitamine .

Alljärgnevalt tutvustatakse meetmete kogumit, mida tuleb rakendada valdkonnas "Microsoft Exchange/ Outlook":

Planeerimine ja kontseptsioon

- (L) M 2.480w Exchange'i ja Outlooki dokumentatsiooni kasutamine
- (L) M 2.481 Exchange'i kasutuse planeerimine Outlook Anywhere'i jaoks
- (L) M 3.84w Sissejuhatus Exchange'i süsteemidesse
- (M) M 4.381z Exchange'i System-andmebaaside krüpteerimine

Rakendamine

- (M) M 2.483 Exchange'i süsteemide turvaline kohandamine
- (L) M 4.165 Outlook 2000 turvaline konfigureerimine
- (M) M 5.100 Exchange'i süsteemi siseneva ja väljuva kommunikatsiooni kaitse

Kasutamine

- (L) M 2.482 Exchange'i süsteemide regulaarsed turvakontrollid

Valmisolek hädaolukorraks

- (L) M 6.149 Andmevarundus Exchange'is

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele

Kohustuslikud üldmeetmed

- HG.6 Arvuti paroolkaitse rangemad reeglid
- HG.24 Paroolide regulaarkontroll parooliskänneriga
- HG.25 Kaugpöörduste kohustuslik logimine
- HG.38 Turvapaikade paigaldatuse regulaarseire

Teabe käideldavus (K)

-

Teabe terviklus (T)

- HT.7 Kasutajate ja nende profiilide perioodiline seire
- HT.51 Lisanõuded teabe hankimisele turvaaukude kohta
- HT.73 Välise sertifikaadi kasutuskohustus

Teabe konfidentsiaalsus (S)

-

B 5.13 SAP süsteem

SAP süsteeme kasutatakse ettevõtetes nii siseste kui ka väliste äriprotsesside automatiseerimiseks ning nende tehniliseks toetamiseks (Enterprise Resource Planning , ERP) SAP süsteem töötleb seega tavaliselt konfidentsiaalseid andmeid, mistõttu tuleb tagada kõikide süsteemikomponentide ja andmete kaitse ning turvalisuse tase tuleb viia vastavusse ohtudega. Lisaks sellele on otsustava tähtsusega ka andmete tervikluse ja käideldavuse tagamine.

SAP pakub hulgaliselt süsteeme, komponente ja funktsioone, seega ei saa mõiste “SAP süsteem” ühemõtteliselt tähistada ühte kindlat installatsiooni või komponentide gruppi. Käesoleva moodulis ei ole võimalik käsitleda kõiki olemasolevaid SAP tooteid, seepärast piirdutakse tüüpilise ja praktikas sagedasti kasutatava baasinstallatsiooniga.

Tüüpiline näide SAP süsteemist on mySAP ERP süsteem, varem tuntud nimetuse all SAP R/3, mis sisaldab ettevõtte põhimooduleid – personalijuhtimine (HCM), finantsjuhtimine (FI/CO), materjali haldus (MM), müük ja turustus (SD), logistika (PP), projektijuhtimine (PS) ja kvaliteedijuhtimine (QM). Baaskomponendina on kasutusel niinimetatud SAP NetWeaver Application Server (varem tuntud nimetuse all SAP Web Application Server). Lisaks sellele sisaldab aktuaalne NetWeaver platvorm (hetkel Netweaver 04) SAP XI komponenti, mis on andmete integratsiooniplatvormiks erinevate SAP süsteemide vahel ning ka SAP süsteemide ja mitte-SAP süsteemide vahel, ning SAP Enterprise portaali, mis on integratsiooniplatvormiks rakendustele ja kasutajatele. Ka need mõlemad komponendid töötavad SAP NetWeaver Application Server ’il.

Lühikese ülevaate SAP süsteemist ja tähtsamatest SAP alastest mõistetest leiab turvameetmes M 3.53 Sissejuhatus SAP süsteemidesse .

Käesoleva mooduli ohud ja turvameetmed põhinevad peamiselt SAP NetWeaver ApplicationServer ’il, NetWeaver platvormi tähtsaimal tehnilisel baaskomponendil. Kuna aga ka juba nimetatud baaskomponent on saadaval mitmes versioonis, mis on ka funktsionaalselt erinevad, ei käsitleta käesolevas moodulis teadlikult versioonide erinevusi. Sellega saavutatakse mooduli pikem kasutusiga ning luuakse võimalus mooduli rakendamiseks ka olemasolevatele SAP R/3 süsteemidele. Turvameetmed ja ohud on fokuseeritud SAP süsteemi baaskaitsele niinimetatud baasadministratsiooni tasemel. Rakenduste ja moodulite kaitse (nt HCM, FI) iseenesest ei ole käesoleva mooduli eesmärk. Kuna aga paljud rakendused ja moodulid kasutavad baaskomponendi turvamehhanisme, võib kirjeldatud turvameetmeid teatavate kohandustega kasutada ka SAP rakenduste ja moodulite kaitseks.

Käesoleva mooduli eesmärgiks ei ole olemasoleva mahuka SAP dokumentatsiooni ümber kirjutada, vaid käsitleda infoturbe soovitatavaid protseduure ja tähelepanu väärivaid eripärasid. Samas võib olemasolevat SAP detailseid tehnili-

si üksikasju sisaldavat dokumentatsiooni kasutada lisamaterjalina. Olulisest SAP dokumentatsioonist annab ülevaate M 2.346 SAP dokumentatsiooni kasutamine . Infoturbe ametnikke ja administraatoreid aitab moodul mitte ainult SAP kasutamise planeerimisel, vaid see annab ülevaate ka tähtsamatest infoturbe alastest tehnilistest aspektidest.

Ohud

Käesolev moodul käsitleb SAP NetWeaver baaskomponendi SAP NetWeaver Application Server' ile mõjuvaid ohtusid, mis on olulise tähtsusega seoses selle komponendi niinimetatud baasadministratsiooniga sise- või välisvõrgus.

Üldiselt sõltuvad SAP süsteemide ohud kasutusmudelist. SAP süsteem asutuse või ettevõtte isoleeritud sisevõrgus on reeglina vähem ohustatud kui süsteem, mis on ühenduses Internetiga. Aga ka sisevõrkudes võib võrgu- või SAP süsteemi ebapiisav kaitse luua olukorra, et tekivad võimalused volitamatuks juurdepääsuks. Siinkohal mängib suurt rolli asjaolu, kas andmetele pääseb juurde vaid lugemiseks või on võimalik ka andmete muutmine. See on kriitiline peamiselt asutuste ja ettevõtete jaoks ning sellealast Sarbanes Oxley Act 'il põhinevat juurdlust teostatakse ka kontrollimisel. Nimetatud kontekstis on erilise tähtsusega ebapiisava volituste planeerimise ja puuduva funktsioonide eraldamisega seotud probleemid.

Just veebitehnoloogiate, nagu HTTP-l põhinevate pääsuvõimaluste ja internetiühendusega veebirakenduste kasutamine on oluliselt suurendanud SAP süsteemidele mõjuvate potentsiaalsete ohtude hulka. Avaliku võrguühendusega SAP süsteemid on ebakompetentse või väära konfigureerimise tagajärjel oluliselt tugevamini ohustatud. See kehtib ka kindlaks määramata või mitte täielikult kindlaks määratud protsesside kohta, eriti väljasttellimise (Outsourcing) korral.

Vääramatu jõud:

- G 1.1 Personali väljalangemine

Organisatsioonilised puudused:

- G 2.7 Õiguste volitamata kasutamine
- G 2.37 Sideliinide kontrollimatu kasutamine
- G 2.87 Ebaturvalised protokollid avalikes võrkudes
- G 2.108 SAP süsteemi ebapiisav või puuduv planeerimine

Inimvead:

- G 3.8 IT-süsteemi väär kasutamine
- G 3.9 IT-süsteemi väär haldus
- G 3.16 Väär pääsuõiguste haldus

Ründed:

- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.7 Liinide pealtkuulamine
- G 5.9 IT-süsteemide volitamata kasutamine
- G 5.21 Trooja hobused
- G 5.23 Viirused
- G 5.128 Volitamatu juurdepääs andmetele seoses võõra koodi lisamisega SAP tarkvarasse

Soovitatavad meetmed

Vaadeldavate IT varade turvalisuse tagamiseks tuleb lisaks käesolevale moodulile rakendada veel teisigi mooduleid vastavalt infosüsteemide etalonturbe rakendusjuhendi modelleerimise tulemustele.

SAP süsteemi edukaks ülesseadmiseks on vaja rakendada terve rida meetmeid, alustades strateegilise otsuse vastuvõtmisega, millele järgneb planeerimine, kontseptsiooni koostamine, installatsioon ja käitus. Seejuures ei tohi unustada nõuetele vastavat süsteemi likvideerimist, kui lõpetatakse selle käitus.

Paralleelselt käitusfaasiga peab ootamatuseplaan garanteerima süsteemi funktsioneerimise ka hädaolukorras. IT-alane turve ja audit peavad tagama normaalkäitusest kinnipidamise.

Järgnevalt on ära toodud etapid, mis seejuures tuleb läbida, ning meetmed, mida vastavatel etappidel tuleks rakendada.

Planeerimine ja kontseptsioon

Kui otsus SAP süsteemi kasuks on langetatud, peab järgnema SAP süsteemi kasutamise planeerimine ja vastavasisulise kontseptsiooni koostamine. Seejuures tähelepanu alla võetavad aspektid on koondatud turvameetmesse M 2.341 SAP kasutuselevõtu planeerimine . Seejuures on tähtis, kuidas planeeritakse SAP süsteemi kasutajate volitused. Sellekohased olulised teemad on kirjeldatud turvameetmes M 2.342 SAP pääsuõiguste planeerimine . Tähtis on teada, et SAP süsteemi turvalisust saab juba planeerimis- ja kontseptsiooni koostamise faasis otsustavalt mõjutada, kui täidetakse turvalisuse seisukohalt olulisi nõudeid. Ülevaate meetmetest SAP süsteemi kasutajate koolituseks annab M 3.52 SAP süsteemide koolitus , kuna süsteemi turvalisuse tagamiseks on vajalikud kasutajate ja administraatorite küllaldased teadmised SAP süsteemidest.

Erilist tähelepanu tuleb pöörata turvalisuse planeerimisele selliste lahenduste korral, mil SAP süsteemid on eriliselt ohustatud. Seejuures võib tegu olla tüüpiliste internetilahendustega, ning rakendada tuleb soovitusi meetmest M 2.344 Interneti SAP süsteemide turvaline kasutamine . Tegemist võib aga olla ka sisevõrgulahendusega, nt kui SAP süsteemiga on võimalik ühendust võtta asutuse või ettevõtte portaalilt. Sel juhul on määrava tähtsusega meetmes M 2.343 SAP süsteemi portaalilahenduse kaitse antud soovitused. Sage kasutusmudel, mis on seotud spetsiifiliste ohtudega, on SAP süsteemi väljasttellimine (Outsourcing), sest sel juhul teostatakse konfiguratsioon ja haldus asutusele või ettevõttele võõraste isikute poolt. Nõuanded ja soovitused nimetatud juhuks on kirjeldatud meetmes M 2.345 SAP süsteemi väljasttellimine .

Rakendusfaas

Pärast organisatoorsete ja planeerimisalaste eeltööde läbiviimist võib järgneda SAP süsteemi installeerimine. Seejuures tuleb rakendada meedet M 4.256 SAP süsteemi turvaline installeerimine .

SAP süsteemi installeerimine moodustab ainult väikese osa rakendusfaasis läbiviidavatest töödest. Valdava osa tööst moodustab installeerimisele järgnev SAP süsteemi esmane konfigureerimine. Esmase konfigureerimise käigus määratakse kindlaks ja defineeritakse SAP süsteemi baasturvalisus kasutuselevõtul ning raamtingimused süsteemi turvalisuse tagamiseks tulevikus. Seepärast tuleb rakendusfaasis arvestada järgmiste turvaaspektidega:

Esmane konfigureerimine on vajalik nii ABAP kui ka Java protokollistiku jaoks. Eriti tuleb vältida olukordi, mil üks mõlemast protokollistikust jääb konfigureerimata, kuna seda ei kasutata. Vastavasisulisi soovitusi sisaldavad meetmed M 4.258 SAPi ABAP-pinu turvaline konfiguratsioon ja M 4.266 SAP Java protokollistiku turvaline konfigureerimine.

Iga SAP süsteemi keskmeks on andmebaas ning selles hoitavad tabelid andmetega. Andmebaas ei salvesta mitte ainult asutuse või ettevõtte äriandmeid, vaid ka SAP süsteemi sisemisi funktsioone ja haldusinfot. Andmebaasi turvaprobleemid puudutavad seepärast kohe kogu SAP süsteemi turvalisust. Andmebaasi puudutavad turvameetmed on koondatud meetmesse M 4.269 SAP süsteemi andmebaasi turvaline konfiguratsioon .

SAP süsteemid on jaotatult üles ehitatud ja on seetõttu erinevate liideste kaudu üksteisega või teiste väliste kliendi- või serverisüsteemidega ühenduses. Sellepärast on tähtsaks ülesandeks kommunikatsiooni kaitse. Üldiselt saab SAP süsteem kasutada palju erinevaid kommunikatsioonikanaleid, mis sõltuvad ka installeeritud rakendustest ja moodulitest. Reeglina kasutatakse aga siiski vaid mõningaid baaskommunikatsioonimehhanisme ja liideseid. Tähtsaks süsteemi juurutamisalaseks meetmeks on M 5.125 SAP-süsteemi siseneva ja väljuva kommunikatsiooni kaitse .

SAP süsteem tuleb kohandada asutuse või ettevõtte kohalike funktsionaalsete nõuetega. See toimub niinimetatud tarbija vajadustele orienteerumise (Customizing) teel. Nimetatud kontekstis tähtsust omavateks turvameetmeks on M 2.348 Turvaline SAP-süsteemide kohandamine .

Kasutamine

Pärast esmast installeerimist ja testimisfaasi alustatakse normaalkäitusega. Seejuures tuleb arvesse võtta alljärgnevaid turvaaspekte:

Turvanõuete eiramise avastamiseks peab toimuma vastav SAP süsteemi monitooring. Nõuandeid selleks sisaldavad meetmed M 2.347 SAP süsteemi regulaarsed turvakontrollid ja M 4.270 SAP logimine .

SAP tarkvara uuemad versioonid võimaldavad kasutada viirusetõrje programmi, nii et näiteks SAP süsteemi saadetud dokumente ja andmeid on võimalik viiruste suhtes kontrollida. Vastavasisulisi nõuandeid sisaldab meede M 4.271 SAP süsteemi viirusetõrje .

Kuna SAP süsteem on allutatud pidevatele muutustele, mis on enamasti tingitud muutunud nõuetest või kasutusmudelitest, tuleb tagada soovitud turvataseme säilimine. Eelkõige puudutab see omaarendusi. Nimetatud kontekstis on tähtsamad meetmed M 2.221 Muudatuste haldus ja M 2.349 Turvaline SAP süsteemi tarkvara arendamine .

Uus kood või teised muudetavad komponendid tuleb süsteemi sisse viia. Selleks on ABAP muudatuste jaoks olemas transportsüsteem. Tarkvara levitamiseks Java protokollistiku alal kasutatakse seevastu teist mehhanismi. Mõlematel juhtudel tuleb tagada, et nimetatud mehhanisme ei oleks võimalik kuritarvitada. Vastavasisulised tähtsad meetmed on M 4.272 SAP transportsüsteemi turvaline kasutamine ja M 4.273 SAP Java protokollistiku tarkvara levitamise turvaline kasutamine .

Kasutusest kõrvaldamine

Soovitusi SAP süsteemide deinstalleerimiseks, näiteks pärast normaalkäituse lõppemist, leiab meetmes M 2.350 SAP süsteemi likvideerimine .

Valmisolek hädaolukorraks

Soovitusi SAP süsteemide ootamatuseplaani koostamiseks leiab meetmest M 6.97 SAP süsteemi valmisolek hädaolukorraks .

Alljärgnevalt tutvustatakse meetmete kogumit, mida tuleb rakendada valdkonnas "SAP süsteem":

Planeerimine ja kontseptsioon

- (L) M 2.341 SAP kasutuselevõtu planeerimine
- (L) M 2.342 SAP pääsuõiguste planeerimine
- (M) M 2.343 SAP süsteemi portaalilahenduse kaitse
- (M) M 2.344 Interneti SAP süsteemide turvaline kasutamine
- (M) M 2.345 SAP süsteemi väljasttellimine
- (L) M 2.346 SAP dokumentatsiooni kasutamine
- (L) M 3.52 SAP süsteemide koolitus
- (M) M 3.53w Sissejuhatus SAP süsteemidesse

Rakendamine

- (L) M 4.256 SAP süsteemi turvaline installeerimine
- (L) M 4.257 SAP-installatsioonikaustade turvamine operatsioonisüsteemi tasandil
- (L) M 4.258 SAPi ABAP-pinu turvaline konfiguratsioon
- (L) M 4.259 ABAP-pinu turvaline kasutajate haldus
- (L) M 4.260 SAP-volituste haldus
- (M) M 4.261 Kriitiliste SAP volituste turvaline rakendamine.
- (M) M 4.262 SAP-volituste lisakontrollide konfigureerimine
- (L) M 4.263 SAP sihtpunkti kaitse
- (L) M 4.264 SAP süsteemide tabelite otsemuudatuste piiramine
- (M) M 4.265 SAP süsteemi pakktöötluse turvaline konfigureerimine
- (L) M 4.266 SAP Java protokollistiku turvaline konfigureerimine
- (L) M 4.267 SAP Java pinu turvaline kasutajate haldus
- (L) M 4.268 SAPi Java pinu pääsuõiguste turvaline konfiguratsioon
- (L) M 4.269 SAP süsteemi andmebaasi turvaline konfiguratsioon
- (M) M 5.125 SAP-süsteemi siseneva ja väljuva kommunikatsiooni kaitse
- (L) M 5.126 SAP RFC liidese kaitse
- (M) M 5.127 SAP Internet Connection Framework (ICF) kaitse

- (M) M 5.128 SAP ALE (IDoc/BAPI) liidese kaitse
- (M) M 5.129 SAP süsteemide HTTP teenuste turvaline konfiguratsioon

Kasutamine

- (M) M 2.347 SAP süsteemi regulaarsed turvakontrollid
- (L) M 2.348 Turvaline SAP-süsteemide kohandamine
- (M) M 2.349 Turvaline SAP süsteemi tarkvara arendamine
- (L) M 4.270 SAP logimine
- (M) M 4.271 SAP süsteemi viirusetõrje
- (L) M 4.272 SAP transportsüsteemi turvaline kasutamine
- (L) M 4.273 SAP Java protokollistiku tarkvara levitamise turvaline kasutamine

Kasutuselt kõrvaldamine

- (L) M 2.350 SAP süsteemi likvideerimine

Valmisolek hädaolukorraks

- (L) M 6.97 SAP süsteemi valmisolek hädaolukorraks

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.6 Arvuti paroolkaitse rangemad reeglid
- HG.24 Paroolide regulaarkontroll parooliskänneriga
- HG.38 Turvapaikade paigaldatuse regulaarseire
- HG.46 SAP rakenduslüüside kasutamine
- HG.75 Lisanõuded SAP-süsteemi väljasttellimisele

Teabe käideldavus (K)

- HK.20 SAP'i klasterlahenduse kasutamine
- HK.27 Puhvertoiteallikas serveri sulgemise tagamiseks

Teabe terviklus (T)

- HT.7 Kasutajate ja nende profiilide perioodiline seire
- HT.39 SAP'i parooli tugevdamine
- HT.51 Lisanõuded teabe hankimisele turvaaukude kohta
- HT.74 SAP'i konfiguratsiooni regulaarseire

Teabe konfidentsiaalsus (S)
-

B 5.14 Mobiilsed andmekandjad

Käesolevas moodulis käsitletakse mobiilsete andmekandjate põhimõttelist laadi turvaaspekte. Mobiilseid andmekandjaid võib kasutada

- andmevahetuseks (vt B 5.2 Andmekandjatel toimuv andmevahetus),
- andmete transportimiseks IT-süsteemide vahel, mis ei ole omavahel võrgustatud või erinevate asukohtade vahel (vt B 5.8 Kaugtöö),
- turvakoopiate (backup) arhiveerimiseks või salvestamiseks, kui teised automatiseeritud meetodid ei ole otstarbekad (vt B 1.4 Andmevarunduspoliitika ja B 1.12 Arhiveerimine),
- selliste andmete salvestamiseks, mis on liiga tundlikud salvestamiseks töökohaarvutitele või serveritele,
- andmete mobiilseks kasutamiseks või täiendamiseks (nt MP3-mängija, digitaalkaamera jne).

Olemas on terve hulk erinevaid mobiilseid andmekandjaid, mille hulka kuuluvad muu seas disketid, eemaldatavad kettad (magnetilised, magnetilis-optilised), CD-ROMid, DVDd, magnetlindid, kassetid, USB-kõvakettad ning ka välksalvestid (flash-memory) nagu USB-mälupulgad. Kuna mobiilseid andmekandjaid on palju ning nende kasutamisvaldkonnad mitmekesised, ei käsitleta alati kõiki vajalikke turvaaspekte.

Andmekandjaid võib klassifitseerida selle järgi, kas need on ainult loetavad, kas need on ette nähtud ühekordseks või mitmekordseks salvestamiseks.

Andmekandjaid võib klassifitseerida ka teiste kriteeriumite järgi, näiteks

- andmete salvestamise viisi järgi: analoog- või digitaalandmekandjad
- kuidas on võimalik andmeid salvestada: ilma tehniliste abivahenditeta, nagu nt paber, või ainult tehniliste abivahenditega, nagu nt mikrofilmid või helilindid
- ehituse järgi: väljavahetatavad andmekandjad, välised andmesalvestid või –kandjad, mis on integreeritud teistesse seadmetesse.

Väljavahetatavad andmekandjad, mida osaliselt nimetatakse ka eemaldatavateks andmekandjateks, sisestatakse draivi. Sellekohasteks näideteks on disketid, CD-ROMd, DVDd, magnetlindid ja kassetid. Väliseid andmekandjaid, nagu näiteks USB mälupulki ja väliseid kõvakettaid seevastu saab otse IT-süsteemiga ühendada. Näited andmekandjatest, mis on integreeritud teistesse seadmetesse, on salvestuskomponendid mobiiltelefonides, MP3 mängijates ja digitaalkaamerates.

Lisaks digitaalsetele andmekandjatele tuleb turvakontseptsooni koostamisel arvesse võtta ka paberil, mikrofilmidel või teistel analoogandmekandjatel olevat informatsiooni. See puudutab eelkõige dokumentide väljatrükkimist, paljundamist ja sisseskaneerimist, samuti faksiteenuste kasutamist. Vastavasisulised nõuanded on kirjas ka moodulites B 3.402 Faks ja B 3.406 Printerid, koopiamasinad ja multifunktsionaalsed seadmed .

Käesolevas moodulis tuuakse ühelt poolt välja, kuidas peab toimuma mobiilsetele andmekandjatele salvestatud andmete turvaline kasutamine, ning teiselt poolt, kuidas saaks vältida informatsiooni mittekompetentset edastamist mobiilsete andmekandjate kaudu.

Ohud

Infosüsteemide etalonturbes peetakse mobiilsete andmekandjate kasutamisega kaasnevateks tüüpilisteks ohtudeks alljärgnevaid ohtusid:

Vääramatu jõud:

- G 1.9 Tugevast magnetväljast tingitud andmekadu
- G 1.15 Muutuvast rakenduskeskkonnast tingitud kahjustused

Organisatsioonilised puudused:

- G 2.2 Reeglite puudulik tundmine
- G 2.10 Probleemid andmekandjate kättesaadavusega

Inimvead:

- G 3. 1 Andmete konfidentsiaalsuse või tervikluse kadu kasutaja vea tõttu
- G 3.3 Hooletus turvameetmete suhtes
- G 3.44 Teabe hooletu kasutamine

Tehnilised rikked:

- G 4.7 Defektsed andmekandjad
- G 4.52 Kaasaskantava seadme andmekadu

Ründed:

- G 5.1 IT-seadmete või -tarvikute manipuleerimine ja hävitamine
- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.4 Vargus
- G 5.9 IT-süsteemide volitamata kasutamine
- G 5.23 Viirused
- G 5.141 Andmevargus kaasaskantavate andmekandjatega
- G 5.142 Pahavara levimine kaasaskantavate andmekandjate kaudu

Soovitatavad meetmed

Vaadeldavate IT varade turvalisuse tagamiseks tuleb lisaks käesolevale moodulile rakendada veel teisigi mooduleid vastavalt infosüsteemide etalonturbe rakendusjuhendi modelleerimise tulemustele.

Mobiilsete andmekandjate turvalise kasutamise tagamiseks on vaja rakendada terve rida meetmeid, alates planeerimisest ja kontseptsiooni koostamisest, millele järgneb soetamine ja ootamatuste planeerimine. Järgnevalt on ära toodud etapid, mis seejuures tuleb läbida, ning meetmed, mida vastavatel etappidel tuleb rakendada.

Planeerimine ja kontseptsioon

Mobiilsete andmekandjate turvalise kasutamise tagamiseks tuleb koostada kontseptsioon, milles oleks ära toodud erinevat liiki mobiilsete andmekandjate kasutamisega seotud ohud ja turvameetmed nende vältimiseks (vt M 2.401 Mobiilsete andmekandjate ja seadmete kasutamine).

Soetamine

Sobivate andmekandjate valik tuleb kooskõlastada. Otsustamaks, millist liiki andmekandjaid kasutusse võtta, tuleks rakendada meedet M 4.169 Sobiva arhiveerimis-andmekandja valimine .

Kasutamine

Turvanõuete alusel tuleks kasutusmudelitest lähtuvalt koostada kõigi töötajate jaoks turvasuunised (vt M 3.60 Töötajate teadlikkuse tõstmine mobiilsete andmekandjate ja seadmete turvalise kasutamise kohta).

IT-süsteemide draivipilud ja liited peaks olema vastavalt turvasuunistele kaitstud (vt M 4.4 Eemaldatavate andmekandjate draivipilude ja väliste andmekandjate nõuetele vastav kasutamine).

Kasutusest kõrvaldamine

Kui andmekandjaid edasi antakse, peaks need enne uuesti kasutuselevõttu või likvideerimist füüsiliselt kustutama, et tundlik informatsioon ei satuks valedesse kätesse (vt M 4.32 Andmekandjate füüsiline kustutamine enne ja pärast nende kasutamist).

Valmisolek hädaolukorraks

Mobiilsetele andmekandjatele salvestatud tähtis info peaks olema kaotsimineku vältimiseks ka veel teise kohta salvestatud.

Alljärgnevalt tutvustatakse turvameetmete kogumit mida tuleb rakendada valdkonnas “Mobiilsed andmekandjad ”.

Planeerimine ja kontseptsioon

- (L) M 2.3 Andmekandjate haldus
- (L) M 2.218 Andmekandjate ja IT-komponentide kaasavõtmise protseduurid
- (L) M 2.401 Mobiilsete andmekandjate ja seadmete kasutamine
- (M) M 4.34z Krüpteerimise, kontrollsummade ja digitaalallkirjade rakendamine

Rakendamine

- (L) M 4.32 Andmekandjate füüsiline kustutamine enne ja pärast nende kasutamist

Kasutamine

- (L) M 3.60 Töötajate teadlikkuse tõstmine mobiilsete andmekandjate ja seadmete turvalise kasutamise kohta
- (L) M 4.4 Eemaldatavate andmekandjate draivipilude ja väliste andmekandjate nõuetele vastav kasutamine
- (L) M 4.200z USB-salvestuskandjatega ümberkäimine

- (L) M 4.232z Mälulaienduskaartide turvaline kasutamine

Kasutusest kõrvaldamine

- (L) M 2.306 Kahjudest teatamine

Valmisolek hädaolukorraks

- (L) M 6.38 Edastatud andmete varukoopiad

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed
-
Teabe käideldavus (K)

- HK.33 Kõrgkäideldavuse lisanõuded mobiilsetele andmetekandjatele

Teabe terviklus (T)
-
Teabe konfidentsiaalsus (S)

- HS.51 Lisanõuded tundlike ressursside hävitamisele
- HS.54 Lisanõuded turvalisele kustutamisele
- HS.76 Mobiilsete andmekandjate võimalik vältimine

B 5.15 Üldine kataloogiteenus

Kataloogiteenuse abil saab arvutivõrgus defineeritud viisil informatsiooni suvaliste objektide kohta. Ühe objektiga koos on võimalik salvestada selle juurde kuuluvad täiendusi, nt kasutajatunnuse juurde kasutaja ees- ja perekonnanime, personaalset numbrit, arvuti nime. Neid andmeid võivad seejärel ühtmoodi kasutada erinevad rakendused. Kataloogiteenus ja selle andmed vajavad vaid ühekordset tsentraalset haldamist.

Kataloogiteenuste tüüpilisteks rakendusvaldkondadeks on näiteks:

- Telefoninumbreid, meiliaadresse, elektrooniliste signatuuride sertifikaate ja muud sarnast sisaldavate aadressiraamatute haldamine
- Arvutite, skännerite ja teiste väliste seadmete ressursside haldamine
- Kasutajate haldamine, nt kasutajakontode ja kasutajavolituste haldamiseks
- Autentimine, nt sisselogimiseks operatsioonisüsteemidesse või rakendustesse

Kataloogiteenused on optimeeritud lugemispääsudele, kuna andmete saamiseks esitatakse kataloogiteenusele tavaliselt päring, samal ajal kui kirjutuspääsud, nagu sissekannete tegemine, muutmine või kustutamine on harvem vajalikud.

Andmed kataloogiteenuses on reeglina objektile baseeruvalt puustruktuurina loogiliselt paigutatud. Struktuur võib seejuures kujutada andmete poliitilist, geograafilist või organisatoorset seisukorda. Objektid salvestatakse kataloogidesse või andmepankadesse hierarhiliselt. Lähtudes juurobjektist (root) hargnevad objektid sugupuuna kuni lehtedeni. Samas kui objekte, mis ise sisaldavad objekte, nimetatakse konteinerobjektideks (containerobjects), nimetatakse objekte puu tipus lehtobjektideks (leafobjects).

Kataloogiteenuste tarkvara pakuvad paljud tootjad. Sellekohased näited on Microsoft Active Directory (vt B 5.16 Active Directory) ja Novell eDirektory (vt B 5.9 Novell eDirectory). Teised kataloogiteenused baseeruvad vabalt kättesaadaval tarkvaral nimega OpenLDAP , mida kasutatakse paljudes Unixil baseeruvates süsteemides, aga mida kasutab ka operatsioonisüsteem Mac OS.

Käesolevas moodulis käsitletakse kataloogiteenuste üldisi turvaaspekte sõltumata sellest, millist toodet kasutatakse. Tootespetsiifiliste turvaaspektide jaoks on IT-etalonturbe kataloogides veel mooduleid, mida tuleb rakendada lisaks vastavale kataloogiteenusele.

Ohud

Kataloogiteenuseid mõjutab terve rida otseseid ohte. Nendele lisanduvad kaudsed ohud, mis on seotud selle all asuva operatsioonisüsteemiga.

Infosüsteemide etalonturbes peetakse kataloogiteenuseid mõjutavateks ohtudeks alljärgnevaid ohte:

Vääramatu jõud:

- G 1.2 IT-süsteemi avarii

Organisatsioonilised puudused:

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.2 Reeglite puudulik tundmine
- G 2.7 Õiguste volitamata kasutamine
- G 2.123 Kataloogiteenuste ebapiisav või puuduv planeerimine
- G 2.124 Kataloogiteenuse partitsioonide ja replikatsioonide väär või puudulik planeerimine
- G 2.125 Kataloogiteenuse juurdepääsu väär ja ebapiisav planeerimine

Inimvead:

- G 3.9 IT-süsteemi väär haldus
- G 3.13 Väära või soovimatu andmekogumi saatmine
- G 3.16 Väär pääsuõiguste haldus
- G 3.43 Puudulik paroolihooldus
- G 3.87 Kataloogiteenuste väär konfiguratsioon
- G 3.88 Väär pääsuõiguste andmine
- G 3.89 Kataloogiteenuse LDAP-juurdepääsu väär konfiguratsioon

Tehnilised rikked:

- G 4.10 Keerukad ligipääsuvõimalused võrgustatud IT-süsteemides
- G 4.13 Salvestatud andmete hävimine
- G 4.33 Autentimise puudumine või puudulikkus
- G 4.67 Kataloogiteenuste rike

Ründed:

- G 5.16 Ohud hoolde- ja haldustööde ajal
- G 5.18 Süstemaatiline paroolide mõistatamine
- G 5.19 Kasutajaõiguste väärkasutus
- G 5.20 Administraatori õiguste väärkasutus
- G 5.65 Teenusetõkestus andmebaasisüsteemis
- G 5.71 Tundliku informatsiooni konfidentsiaalsuse kadu
- G 5.78 DNS-i võltsimine
- G 5.85 Tundliku informatsiooni tervikluse kadu
- G 5.144 Kataloogiteenuste kompromiteerimine volitamata juurdepääsu kaudu

Soovitatavad meetmed

Vaadeldava IT-koosluse turvalisuse tagamiseks tuleb lisaks käesolevale moodulile rakendada veel teisigi mooduleid vastavalt infosüsteemide etalonturbe rakendusjuhendi modelleerimise tulemustele.

Kataloogiteenused võivad olla juba operatsioonisüsteemi integreeritud, nt Active Directory Windows Serverisse alates Windows 2000-st, kuid neid võib olla saadaval ka iseseisvate tarkvarakomponentidena, nt vabalt kättesaadava tarkvarana

nimetusega OpenLDAP. Kataloogi salvestatud andmete turvalisuse tagamiseks tuleb tähelepanu pöörata ka selle aluseks olevale operatsioonisüsteemi turvalisusele. Viimati nimetatu ei ole siiski käesoleva mooduli komponent. Seepärast viidatakse vastavatele kirjeldustele kasutatava operatsioonisüsteemi turvalisuse tagamiseks kolmanda kihi moodulites.

Samuti eeldatakse kataloogiteenuste installeerimisel, et käsitlemist leiavad ka üldised aspektid, mis on toodud esimese kihi olulistes moodulites. Seetõttu tuleks kataloogiteenuse turvanõudeid arvestada üldkontseptsiooni koostamisel (vt B 1.6 Viirusetõrje kontseptsioon).

Kataloogiteenuse turvaliseks juurutamiseks on vaja rakendada terve rida meetmeid, alustades kontseptsiooni koostamisega, millele järgneb soetamine ja käitus. Järgnevalt on ära toodud etapid, mis tuleb seejuures läbida, ning meetmed, mida on vastavatel etappidel vaja rakendada.

Planeerimine ja kontseptsioon

Alustuseks on soovitatav võtta vaatluse alla meede M 3.61 Sissejuhatus kataloogiteenuste põhialustesse , mis annab ülevaate kataloogiteenuse ülesehitusest ja mõistetest.

Et võtta vastu otsus, millist liiki kataloogiteenust institutsioonis oleks võimalik kasutada, tuleb kõigepealt läbi viia nõuete analüüs. Selle alusel peab toimuma kataloogiteenuse kasutamise planeerimine (vt M 2.403 Kataloogiteenuste kasutuselevõtu planeerimine ja M 2.409 Kataloogiteenuse partitsioonide loomise ja replikeerimise planeerimine). Seejuures on suure tähtsusega administratiivsete ülesannete jaotamine (vt M 2.407 Kataloogiteenuste administreerimise planeerimine).

Sellega seoses on vaja välja töötada turvakontseptsioon ja turvasuunised (vt M 2.404 Kataloogiteenuse turvakontseptsiooni koostamine ja M 2.405 Kataloogiteenuse turvapoliitika koostamine). Need tuleb lisada olemasolevatesse turvakontseptsioonidesse ja turvasuunistesse ning samaaegselt tuleb defineerida spetsiifilised täiendused kataloogiteenuste kasutamiseks.

Kui ümberstruktureerimise või aktualiseerimise tõttu IT-koosluses tuleb üks kataloogiteenus üle viia, on samuti vajalikud ulatuslikud planeerimis- ja kontseptuaalsed tööd (vt M 2.408 Kataloogiteenuste üleviimise planeerimine).

Soetamine

Kui on võetud vastu otsus kataloogiteenuse kasutamiseks, tuleb soetada selleks vajaminev tarkvara ning vajadusel ka puuduv riistvara. Kuna kataloogiteenus võimaldab erinevaid kasutusvõimalusi, sõltub nende valik ja soetamine (vt M 2.406 Kataloogiteenuste kasutamiseks sobivate komponentide valik) plaanitud kasutusmudelitest.

Rakendamine

Pärast seda kui organisatsioonilised ettevalmistused ja planeerimistööd on teostatud ning otsus kataloogiteenuse soetamise kohta vastu võetud, võib kataloogiteenuse installeerida. Seejuures tuleb rakendada alljärgnevaid meetmeid:

Installeerimise eesmärgiks on kataloogiteenuse esmane ülesseadmine (vt M 4.308 Kataloogiteenuste turvaline installeerimine) ning seda võib lugeda lõppenuks alles siis, kui kataloogiteenus on viidud turvalisse seisundisse. Sellega tagatakse, et järgnevas konfiguratsioonifaasis omavad kataloogiteenusele juurdepääsu vaid volitatud administraatorid.

Pärast installeerimist toimub kataloogiteenuse esmane konfigureerimine (vt M 4.307 Kataloogiteenuste turvaline konfigureerimine , M 4.309 Kataloogiteenuste pääsuõiguste seadmine ja M 4.310 Kataloogiteenuste LDAP-pöörduste seadmine).

Kataloogiteenuse kasutajad ja administraatorid peavad saama piisava koolituse, et hoida ära turvaintsidente ning tõsta nende teadlikkust ebakompetentse kasutamise tagajärjel tekkivatest ohtudest (vt M 3.62 Kataloogiteenuste administreerimise koolitus ja M 3.63 Kasutajate koolitus autentimiseks kataloogiteenuste abil).

Kasutamine

Pärast konfigureerimist ja testimisfaasi alustatakse tavakäitamist. Seejuures tuleb tähelepanu pöörata alljärgnevatele turvaaspektidele:

Kataloogiteenused on oma loomu poolest allutatud pidevatele muutustele. Seetõttu tuleb turvalisuse seisukohalt tähtsaid konfiguratsiooniparameetreid pidevalt muutustele vastavalt kohandada (vt M 4.78 Konfiguratsioonimuudatuste hoolikas teostamine). Turvalise käituse seisukohalt tähtsad aspektid on koondatud meetmesse M 4.311 Kataloogiteenuste turvaline käitamine ning eriaspektid turvalise kommunikatsiooni tagamiseks meetmesse M 5.147 Turvalise kommunikatsiooni tagamine kataloogiteenuste abil .

Et kataloogiteenuse turvalisuse tase oleks tõestatav, on soovitatav teostada selle pidevat järelevalvet (vt M 4.312 Kataloogiteenuste monitooring).

Kasutusest kõrvaldamine

Kui võetakse vastu otsus, et kataloogiteenust enam edasi kasutata, tuleb allesjäänud andmed ja õigused turvaliselt kustutada. Kuid kui ka vaid mõned osad kataloogiteenustest kuuluvad kasutusest kõrvaldamisele, tuleb pöörata tähelepanu mõningatele aspektidele, mida on lähemalt kirjeldatud meetmes M 2.410 Kataloogiteenuse korrakohane kasutuselt kõrvaldamine .

Valmisolek hädaolukorraks

Lisaks meetmetele, mis tagavad kataloogiteenuse turvalisuse tööprotsessis, on olulise tähtsusega ka meetmed, mis tagavad valmisoleku hädaolukorraks. Nõuandeid nimetatud teema kohta leiate meetmetest M 6.106 Kataloogiteenuse hädaolukorraks valmisoleku plaani koostamine ja M 6.107 Kataloogiteenuste andmevarundus .

Alljärgnevalt tutvustatakse turvameetmete kogumit mida tuleb rakendada valdkonnas “Kataloogiteenus ” .

Planeerimine ja kontseptsioon

- (L) M 2.403 Kataloogiteenuste kasutuselevõtu planeerimine
- (L) M 2.404 Kataloogiteenuse turvakontseptsiooni koostamine
- (L) M 2.405 Kataloogiteenuse turvapoliitika koostamine
- (L) M 2.407 Kataloogiteenuste administreerimise planeerimine
- (M) M 2.408z Kataloogiteenuste üleviimise planeerimine
- (M) M 2.409 Kataloogiteenuse partitsioonide loomise ja replikeerimise planeerimine
- (L) M 3.61w Sissejuhatus kataloogiteenuste põhialustesse

Soetamine

- (L) M 2.406 Kataloogiteenuste kasutamiseks sobivate komponentide valik

Rakendamine

- (L) M 3.62 Kataloogiteenuste administreerimise koolitus
- (L) M 3.63 Kasutajate koolitus autentimiseks kataloogiteenuste abil
- (L) M 4.307 Kataloogiteenuste turvaline konfigureerimine
- (L) M 4.308 Kataloogiteenuste turvaline installeerimine
- (L) M 4.309 Kataloogiteenuste pääsuõiguste seadmine
- (M) M 4.310 Kataloogiteenuste LDAP-pöörduste seadmine

Kasutamine

- (L) M 4.78 Konfiguratsioonimuudatuste hoolikas teostamine
- (L) M 4.311 Kataloogiteenuste turvaline käitamine
- (M) M 4.312 Kataloogiteenuste monitooring
- (M) M 5.147 Turvalise kommunikatsiooni tagamine kataloogiteenuste abil

Kasutusest kõrvaldamine

- (M) M 2.410 Kataloogiteenuse korrakohane kasutuselt kõrvaldamine

Valmisolek hädaolukorraks

- (M) M 6.106z Kataloogiteenuse hädaolukorraks valmisoleku plaani koostamine
- (M) M 6.107 Kataloogiteenuste andmevarundus

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.38 Turvapaikade paigaldatuse regulaarseire

Teabe käideldavus (K)
-
Teabe terviklus (T)

- HT.7 Kasutajate ja nende profiilide perioodiline seire
- HT.61 Kataloogiteenuse sidumine rahvusliku PKIga
- HT.72 Turvatunneldamise protokolli kasutuskohustus

Teabe konfidentsiaalsus (S)
-

B 5.16 Active Directory

Active Directory on Microsofti poolt välja töötatud kataloogiteenus, mis võeti esmakordselt kasutusele operatsioonisüsteemiga Windows 2000 Server. Lähtudes operatsioonisüsteemi Microsoft Windows 2000 Active Directory funktsioonidest, lisati Windows Server 2003 Active Directory teenusele uusi võtmefunktsioone.

Active Direktory 't kasutatakse peamiselt IT-võrkudes ja enamasti koos Microsofti komponentidega. Active Directory salvestab IT-võrgusiseselt informatsiooni objektide, nt kasutajate või arvutite kohta, ning kergendab kasutajatel ja administraatoritel nimetatud informatsiooni kasutusse andmist, organiseerimist, kasutamist ja seiret. Objektile baseeruva kataloogiteenusena võimaldab Active Directory objektide ja nende omavaheliste seoste haldamist, mis moodustavad tegeliku võrgukeskkonna. Active Directory loob võimalused vastava võrgu tsentraalseks juhtimiseks ja kontrollimiseks. Taolise kataloogiteenuse kasutamine on võimalik eelkõige just seal, kus näiteks võrgu klientide arv raskendab detsentraliseeritud haldamist. Ilma kataloogiteenuseta ei saaks enam suurte personalikulude tõttu tagada kohapeal tehtavate seadistuste usaldusväärsust, nt turvasuunistest lähtuvate nõuete realiseerimist. Võrgusiseseid haldusülesandeid, nt paroolide muutmist, kontode loomist ja pääsuõigusi on kataloogiteenuste rakendamise abil võimalik efektiivsemalt teostada.

Käesolevas moodulis võetakse vaatluse alla Active Directory 't mõjutavad spetsiifilised ohud ja meetmed nende vältimiseks. Üldised kataloogiteenuste turvaalased soovitused leiate moodulist B 5.15 Üldine kataloogiteenus . Selles kirjeldatud üldisi meetmeid täpsustatakse ja täiendatakse käesolevas moodulis.

Ohud

Infosüsteemide etalonturbes peetakse Active Directory kasutamisel tüüpilisteks alltoodud ohte. Nendele lisanduvad ohud, mis on seotud üldiste kataloogiteenustega ning nende all asuva Windows Server operatsioonisüsteemiga.

Vääramatu jõud

- G 1.2 IT-süsteemi avarii

Organisatsioonilised puudused:

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.2 Reeglite puudulik tundmine
- G 2.7 Õiguste volitamata kasutamine
- G 2.22 Logiandmete analüüsimata jätmine
- G 2.68 Activa Directory kasutamise ebapiisav või puuduv planeerimine
- G 2.126 Active Directory muudatuste ebapiisav logimine
- G 2.127 Domeenikontrolleri andmevarundusmeetodite ebapiisav planeerimine

Inimvead:

- G 3.9 IT-süsteemi väär haldus
- G 3.13 Väära või soovimatu andmekogumi saatmine
- G 3.16 Väär pääsuõiguste haldus
- G 3.49 Activa Directory väär konfiguratsioon
- G 3.88 Väär pääsuõiguste andmine
- G 3.89 Kataloogiteenuse LDAP-juurdepääsu väär konfiguratsioon

Tehnilised rikked:

- G 4.10 Keerukad ligipääsuvõimalused võrgustatud IT-süsteemides
- G 4.13 Salvestatud andmete hävimine
- G 4.33 Autentimise puudumine või puudulikkus
- G 4.67 Kataloogiteenuste rike
- G 4.68 Ebavajalikust replikeerimisest tingitud tõrked Active Directory töös

Ründed:

- G 5.16 Ohud hoolde- ja haldustööde ajal
- G 5.18 Süstemaatiline paroolide mõistatamine
- G 5.19 Kasutajaõiguste väärkasutus
- G 5.20 Administraatori õiguste väärkasutus
- G 5.65 Teenusetõkestus andmebaasisüsteemis
- G 5.71 Tundliku informatsiooni konfidentsiaalsuse kadu
- G 5.78 DNS-i võltsimine
- G 5.85 Tundliku informatsiooni tervikluse kadu
- G 5.144 Kataloogiteenuste kompromiteerimine volitamata juurdepääsu kaudu

Soovitatavad meetmed

Vaadeldava IT-koosluse turvalisuse tagamiseks tuleb lisaks käesolevale moodulile rakendada veel teisigi mooduleid vastavalt infosüsteemide etalonturbe rakendusjuhendi modelleerimise tulemustele. Eelkõige tuleb aga lisaks rakendada moodulit B 5.15 Üldine kataloogiteenus , mis sisaldab soovitusi kataloogiteenuste üldise turvalisuse tagamiseks.

Active Directory 's töödeldud andmete nõuetele vastava turvalisuse tagamise eeltingimuseks on selle all oleva serveri operatsioonisüsteemi vajaliku turvalisuse tagamine. Microsoft Windows Serveri operatsioonisüsteemide turvalisuse tagamine ei ole käesoleva mooduli osa, vaid seda käsitletakse kolmanda kihi vastavates moodulites. Seetõttu tuleb sõltuvalt valitud operatsioonisüsteemist Active Directory turvaliseks kasutamiseks järgida ka moodulit B 3.108 Windows Server 2003 .

Active Directory edukaks ülesseadmiseks on vaja rakendada terve rida meetmeid, alustades kontseptsiooni koostamisega, millele järgneb installatsioon ja käitus.

Järgnevalt on toodud etapid, mis seejuures tuleb läbida, ning meetmed, mida vastavatel etappidel on vaja rakendada.

Planeerimine ja kontseptsioon

Alustuseks on soovitatav rakendada meedet M 3.64 Sissejuhatus Active Directory'sse , mis annab ülevaate Active Directory ülesehitusest ja mõistetest.

Enne Active Directory tegelikku seadistamist tuleb luua institutsiooni organisatsiooniline struktuur, et sellest oleks võimalik Active Direstory jaoks tuletada võimalikult optimaalne konfiguratsioon. M 2.229 Active Directory planeerimine jagab selgitusi planeerimisfaasi protseduuride ja Active Directory domeenikontseptsiooni kohta. M 2.230 Active Directory halduse planeerimine tegeleb domeeni haldamise baasstruktuuriga ning kirjeldab administratiivsete rollide ülesandeid ja rakendusi.

M 2.231 Windowsi grupipoliitika planeerimine tegeleb Windowsi operatsioonisüsteemide grupeerimissuunistega, mida on võimalik hallata ka Active Directory abil. Lisaks sellele selgitatakse meetmes M 2.411 Active Directory teenuse- ja andmehalduse lahutamine administratiivsete kontode organisatsioonilist ülesehitust ja volituste kooskõlastamist. Sellest tulenevad ka soovitused meetmest M 2.412 Autentimise kaitse Active Directory kasutamisel , milles tutvustatakse kohandusi kataloogiteenuste turvalisuse tagamiseks.

Aktiivses kasutuses oleva Active Directory keskkonna terviklikkuse tagamiseks DNS komponentide kaitse kaudu, tuleb rakendada meedet M 2.413 DNSi turvaline kasutamine Active Directory 's . Lisaks sellele tuleb rakendada meedet M 2.414 Domeenikontrollerite kaitse arvutiviiruste eest , mis annab ülevaate spetsiifilistest eripäradest viirusetõrjeprogrammide kasutamisest domeenikontrolleritel.

Soetamine

Pärast kontseptuaalsete planeerimistööde lõpetamist ning serveri soetamiskriteeriumide defineerimist tuleks olenevalt soetatavate serverite arvust ning valitud operatsioonisüsteemist välja valida sobiv litsentsimudel. Kui valik langeb Windows Server 2003-le, pakuvad toetust IT etalonturbe abivahendid.

Rakendamine

Ühtse turvastandardi saavutamiseks tuleb rakendada meedet M 4.318 Active Directory turvaliste haldusmeetodite rakendamine . Lisaks sellele tuleb kataloogiteenuse haldamise eest vastutavatele isikutele meetme M 3.27 Koolitus Active Directory haldamiseks baasil tutvustada neile nende ülesandeid.

Nende alusel, mis on kogu võrgukeskkonna jaoks keskset tähtsust omav, tuleb ettevõtte domeenikontrolleri jaoks tagada piisav füüsiline kaitse (vt M 4.313 Turvaliste domeenikontrollerite kasutuse võimaldamine). Et sellele lisaks oleks võimalik säilitada võrgus turvastandardit ning takistada domeenistruktuuride ja nende domeenikontrolleritega manipuleerimist, tuleb rakendada vastavalt meetmes M 4.314 Domeenide ja domeenikontrollerite turvaliste poliitikaseadistuste loomine kirjeldatud suuniseid.

Teatud juhtudel toimub üheaegselt rakendamisega juba olemasolevate Windowsi kataloogiteenuste migratsioon. Meetme M 4.317 Windowsi kataloogiteenuste turvaline migratsioon sisuks on seejuures eriti olemasolevate Windows NT serverisüsteemide kataloogiteenuste migratsiooni puudutatavad küsimused.

Kasutamine

Meetmete M 4.315 Active Directory töökindluse tagamine ja M 4.316 Active Directory infrastruktuuri monitooring abil peab olema võimalik tagada IT-koosluse oluliste süsteemide aktuaalse turvaseisundi säilitamine. Lisaks sellele tulenevad domeenikontrollerite olulisusest erinõuded süsteemisätetele, mida kirjeldatakse meetmes M 4.138 Windows Serveri konfigureerimine domeenikontrollerina .

Lisaks aluseks olevale operatsioonisüsteemile on vajalik ka Active Directory hoolikas haldamine (vt M 4.315 Active Directory töökindluse tagamine). Et suuta esile kerkivate probleemide korral õigeaegselt reageerida, tuleb rakendada meedet M 4.316 Active Directory infrastruktuuri monitooring . Selle sisuks ei ole mitte ainult tagasiside defineeritud piirväärtuste ületamisel vaid ka läbi viidud süsteemimuudatuste logimine.

Kasutusest kõrvaldamine

Domeenikontrolleri plaanipärase likvideerimise korral arvestatavad aspektid on kirjeldatud meetmes M 2.410 Kataloogiteenuse korrakohane kasutuselt kõrvaldamine .

Valmisolek hädaolukorraks

Active Directory keskkonda puudutavad hädaolukorraks valmisoleku planeerimise aspektid on keskseks teemaks meetmes M 6.108 Domeenikontrollerite andmevarundus .

Alljärgnevalt tutvustatakse turvameetmete kogumit mida tuleb rakendada valdkonnas “ Active Directory”

Planeerimine ja kontseptsioon

- (L) M 2.229 Active Directory planeerimine
- (L) M 2.230 Active Directory halduse planeerimine
- (L) M 2.231 Windowsi grupipoliitika planeerimine
- (L) M 2.411 Active Directory teenuse- ja andmehalduse lahutamine
- (M) M 2.412 Autentimise kaitse Active Directory kasutamisel
- (M) M 2.413 DNSi turvaline kasutamine Active Directory ’s
- (M) M 2.414 Domeenikontrollerite kaitse arvutiviiruste eest
- (L) M 3.64w Sissejuhatus Active Directory’sse

Rakendamine

- (L) M 3.27 Koolitus Active Directory haldamiseks
- (L) M 4.313 Turvaliste domeenikontrollerite kasutuse võimaldamine
- (L) M 4.314 Domeenide ja domeenikontrollerite turvaliste poliitikaseadistuste loomine
- (M) M 4.317z Windowsi kataloogiteenuste turvaline migratsioon
- (L) M 4.318 Active Directory turvaliste haldusmeetodite rakendamine
- (L) M 5.89 Turvalise kanali konfigureerimine Windowsis

Kasutamine

- (L) M 4.138 Windows Serveri konfigureerimine domeenikontrollerina
- (L) M 4.315 Active Directory töökindluse tagamine
- (M) M 4.316 Active Directory infrastruktuuri monitooring

Kasutusest eemaldamine

- (M) M 2.410 Kataloogiteenuse korrakohane kasutuselt kõrvaldamine

Valmisolek hädaolukorraks

- (M) M 6.108 Domeenikontrollerite andmevarundus

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed

- HG.38 Turvapaikade paigaldatuse regulaarseire

Teabe käideldavus (K)
-
Teabe terviklus (T)

- HT.7 Kasutajate ja nende profiilide perioodiline seire
- HT.72 Turvatunneldamise protokolli kasutuskohustus

Teabe konfidentsiaalsus (S)
-

B 5.17 Samba

Käesolevas moodulis käsitletakse Samba tarkvara põhimõttelisi turvaaspekte. Samba on vabalt kättesaadav autentimis-, faili- ja trükkimisteenus ning võimaldab interoperatiivsust Microsoft Windowsi ja Unixi maailma vahel. Samba ühendab terve hulga erinevaid protokolle ja tehnikaid. Nende hulka kuulub näiteks serverisõnumiploki protokoll (Server Message Block Protokoll – SMB), tuntud ka uuema nimetuse all üldine interneti-failisüsteem (Common Internet File System – CIFS). Samba serveriteks nimetatakse servereid, millel Sambat kasutatakse autentimis-, faili- ja trükkimisteenusena. Need on reeglina Unixi serverid.

Samba koosneb paljudest komponentidest, mis võimaldavad kasutada erinevaid funktsioone, millest tähtsamad on järgnevalt lühidalt nimetatud. Kõige tähtsam Samba rakendus on „smbd". Selle kaudu on teistel SMB klientidel võimalik kasutada sisselogimis-, faili- ja trükkimisteenust. Lisaks sellele on olulise tähtsusega ka rakendus „nmbd", mis pakub erinevaid NetBIOS nimeteenuseid, ning rakendus „winbindd".

Käesolev moodul vaatleb Samba versiooni 3. Erinevustele versioon 3-s ja eelnevate ja alaversioonide versioonide vahel juhitakse vajadusel eraldi tähelepanu. Käesolevat moodulit on võimalik rakendada iga vaadeldava IT-koosluse serverile, millel kasutatakse serveriteenusena Sambat.

Ohud

Infosüsteemide etalonturbes peetakse Samba serveri kasutamisel tüüpilisteks järgmisi ohtusid:

Organisatsioonilised puudused:

- G 2.9 Halb kohanemine IT muutustega
- G 2.22 Logiandmete analüüsimata jätmine
- G 2.87 Ebaturvalised protokollid avalikes võrkudes
- G 2.143 Informatsioonikadu andmete kopeerimisel ja teiseldamisel Samba ühiskasutuses
- G 2.144 Samba serveri ebapiisav valmisolek hädaolukorraks
- G 2.145 Triviaalse andmebaasi failide ebapiisav varundamine Sambas

Inimvead:

- G 3.9 IT-süsteemi väär haldus
- G 3.38 Vead konfigureerimisel ja kasutamisel
- G 3.94 Samba kommunikatsiooniprotokollide väär konfiguratsioon
- G 3.95 Samba serveri operatsioonisüsteemi väär konfiguratsioon
- G 3.96 Samba serveri väär konfiguratsioon

Tehnilised rikked:

- G 4.13 Salvestatud andmete hävimine
- G 4.22 Tüüptarkvara turvaaugud või vead
- G 4.54 Turbe kadu krüptofailisüsteemi (EFS) kasutamisel
- G 4.72 Triviaalse andmebaasi vormingus andmebaaside ebakõlad Samba keskkonnas

Ründed:

- G 5.7 Liinide pealtkuulamine
- G 5.21 Trooja hobused
- G 5.28 Teenuse halvamine
- G 5.71 Tundliku informatsiooni konfidentsiaalsuse kadu
- G 5.85 Tundliku informatsiooni tervikluse kadu
- G 5.133 Veebipõhiste administreerimisvahendite volitamata kasutamine

Soovitatavad meetmed

Vaadeldava IT-koosluse turvalisuse tagamiseks tuleb lisaks käesolevale moodulile rakendada veel teisigi mooduleid vastavalt infosüsteemide etalonturbe rakendusjuhendi modelleerimise tulemustele.

Samba serveri kõikide turvakaalutluste aluseks tuleb võtta moodulis B 3.101 Server sisalduvad meetmed. Kuna Sambat kasutatakse reeglina Unixi operatsioonisüsteemil, tuleb arvestada ka moodulis B 3.102 Server Unixi all loetletud meetmetega. Nimetatud moodulites kirjeldatud üldiseid meetmeid konkretiseeritakse ja täiendatakse käesolevas moodulis.

Planeerimine ja kontseptsioon

Kui serveri kasutamise üldine planeerimine on lõpetatud, tuleb luua alamkontseptsioonid Samba kasutamiseks, arvestades seejuures kõiki kehtivaid kõrgemal seisvaid kontseptsioone ja direktiive. Põhilised planeerimise protseduurid on lahti seletatud meetmes M 2.315 Serveri kasutuselevõtu planeerimine . Planeerimise käigus tuleb muu hulgas vastu võtta ka tähtsad otsused põhiliste võrguteenuste (näiteks WINS) kohta. Võrguteenuste kontseptsiooni loomisel tuleks arvestada ka meetmes M 2.437 Samba-serveri kasutuselevõtu plaanimine kirjeldatud meetmeid.

Soetamine

Pärast kontseptuaalsete planeerimistööde lõpetamist tuleb kontrollida installeerimiseks kasutatud tarkvarapakettide (lähteteksti- või binaarpaketid) terviklust ja autentsust (vaata M 4.327 Samba tarkvarapakettide ja lähtetekstide tervikluse ja autentsuse kontroll).

Rakendamine

Enne Samba installeerimist serverarvutile peab toimuma operatsioonisüsteemi sobiv konfigureerimine ja turvaliseks muutmine (vt M 4.331 Samba serveri operatsioonisüsteemi turvaline konfiguratsioon). Tegeliku installeerimise ja sellele järgneva aluskonfigureerimise käigus tuleb arvestada terve rea aspektidega, mis on kirjeldatud meetmetes M 4.326 NTFS funktsioonide tagamine Samba failiserveril , M 4.330 Samba serveri turvaline installeerimine , M 4.332 Samba serveri pääsuõiguste turvaline konfiguratsioon ja M 5.151 Samba veebiadministreerimistööriista turvaline konfigureerimine . Lisaks tuleb tähelepanu pöörata asjaolule, et Samba ei seo ebaturvalisi väliseid programme (vaata M 2.438 Väliste programmide turvaline kasutus Samba-serveril). Nagu meetmes M 2.437 Samba-serveri

kasutuselevõtu plaanimine mainitud, võivad teatud tingimustel olulise tähtsusega olla ka meetmes M 4.333 Winbindi turvaline konfigureerimine Samba keskkonnas loetletud abinõud. Lisaks sellele on vaja tähelepanu pöörata meetmes M 4.329 Sideprotokollide turvaline kasutamine Samba serveri kasutamisel nimetatud turvaabinõudele.

Administraatorid peavad läbima Samba serveri turvalise installeerimise ja käitamise alase koolituse. Olulise tähtsusega aspektid, millele sellisel koolitusel tuleb tähelepanu pöörata, on kirjeldatud meetmes M 3.68 Samba-serveri administraatorite koolitus .

Kasutamine

Regulaarsel kasutamisel peab olema tagatud ajakohane dokumentatsioon. Lisaks sellele tuleb tähelepanu pöörata meetmes M 4.333 Winbindi turvaline konfigureerimine Samba keskkonnas kirjeldatud aspektidele.

Valmisolek hädaolukorraks

Spetsiaalsed aspektid, millele Samba serveri kasutamisel tuleb lisaks meetmele M 6.96 Serveri avariiplaan tähelepanu pöörata, on kokku võetud meetmetes M 6.135 Samba serveri tähtsate süsteemikomponentide regulaarne varundamine ja M 6.136 Hädaolukorraks valmisoleku plaani koostamine Samba serveri avarii puhuks .

Järgnevalt tutvustatakse Samba serveri käitamiseks vajalikku turvameetmete kogumit. Teistes tähtsates moodulites kirjeldatud meetmed (näiteks M 6.96 Serveri avariiplaan ja B 3.101 Server) ülevaatlikkuse tõttu siin uuesti kajastamist ei leia.

Planeerimine ja kontseptsioon

- (L) M 2.437 Samba-serveri kasutuselevõtu plaanimine
- (L) M 4.147z EFS-i turvaline kasutamine Windows 'i keskkonnas
- (M) M 4.326 NTFS funktsioonide tagamine Samba failiserveril

Soetamine

- (M) M 4.327 Samba tarkvarapakettide ja lähtetekstide tervikluse ja autentsuse kontroll

Rakendamine

- (M) M 2.438z Väliste programmide turvaline kasutus Samba-serveril
- (M) M 3.68 Samba-serveri administraatorite koolitus
- (L) M 4.328 Samba serveri turvaline aluskonfiguratsioon
- (M) M 4.329 Sideprotokollide turvaline kasutamine Samba serveri kasutamisel
- (L) M 4.330 Samba serveri turvaline installeerimine
- (M) M 4.331 Samba serveri operatsioonisüsteemi turvaline konfiguratsioon
- (M) M 4.332 Samba serveri pääsuõiguste turvaline konfiguratsioon
- (M) M 4.333 Winbindi turvaline konfigureerimine Samba keskkonnas
- (M) M 4.334 SMB Message Signing ja Samba

- (M) M 5.151 Samba veebiadministreerimistööriista turvaline konfigureerimine

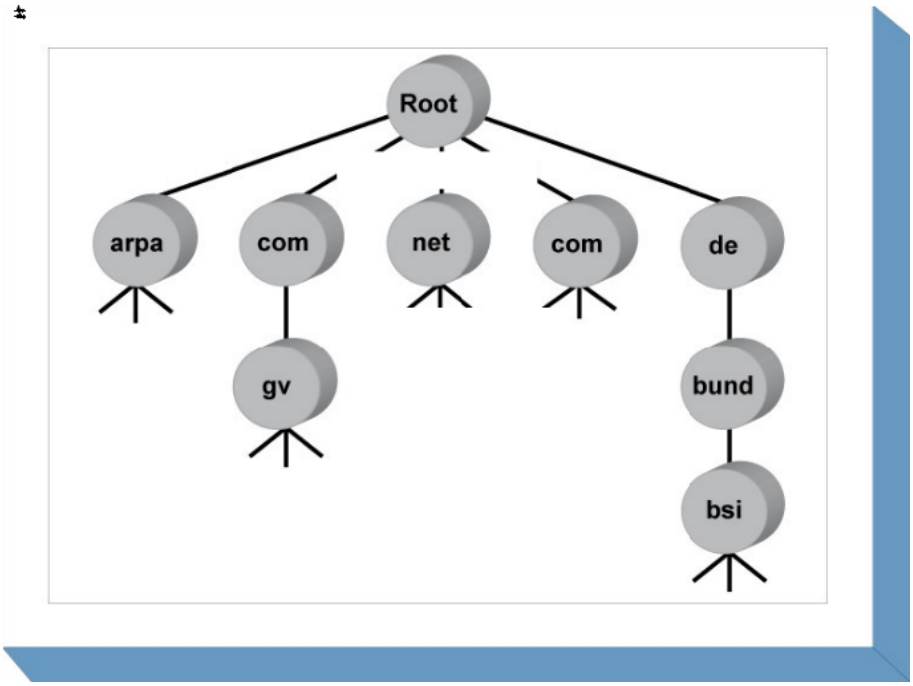
Kasutamine

- (M) M 4.335 Samba serveri turvaline kasutamine

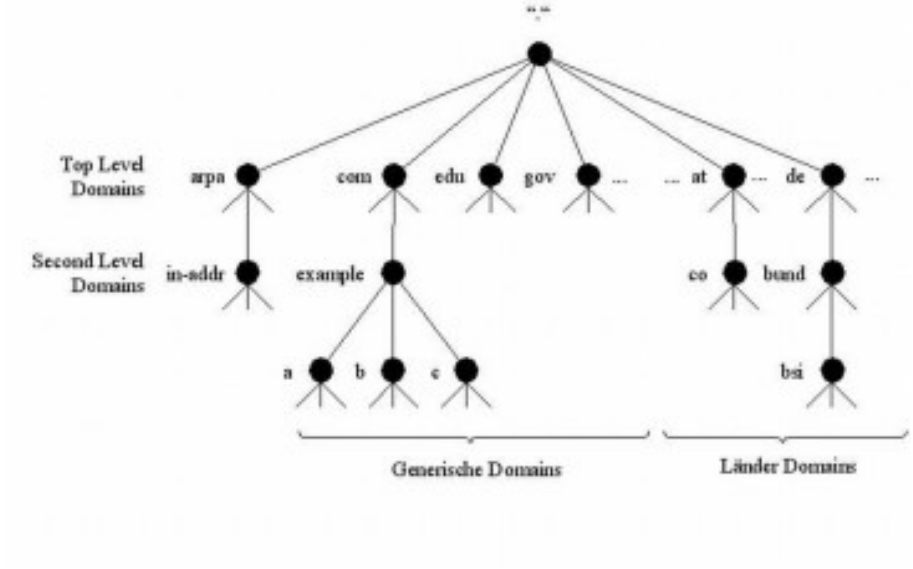
Valmisolek hädaolukorraks

- (L) M 6.135 Samba serveri tähtsate süsteemikomponentide regulaarne varundamine
- (L) M 6.136 Hädaolukorraks valmisoleku plaani koostamine Samba serveri avarii puhuks

B 5.18 DNS-server



Selles moodulis vaadeldakse domeeninimesüsteemi (Domain Name System, DNS) ja selle tööks vajalike serverite turbeomadusi. DNS on võrguteenus, mis teisendab IT-süsteemide hostinimed IP-aadressideks. Tavaolukorras otsitakse hostinimega kokkusobivat IP-aadressi (teisendus). Kui aga IP-aadress on teada ja otsitakse hostinime, on tegemist nn tagurpidise teisendusega. DNS-i on paslik võrrelda telefoniraamatuga, kuid erinevus on selles, et nimede taga pole loetletud mitte telefoninumbrid, vaid nimedega kokkukuuluvad IP-aadressid. Sellega muudetakse kasutajate elu lihtsamaks. Raskesti meeldejäävate IP-aadresside asemel peavad kasutajad ühenduse loomiseks teadma ainult arvuti nime. IP-aadresside ja nimede haldus toimub domeeni nimeruumis. Nimeruum on hierarhilise ülesehitusega ning seda haldavad DNS-serverid. DNS-serverid haldavad enamasti küll internetidomeenide nimeruumi, kuid neid kasutatakse sageli ka institutsioonide sisevõrkudes. Kasutaja arvutil töötab nn Resolver (koordinaadinumbri arvutaja), mille kaudu esitatakse DNS-serverile päringuid ning mis tagastab vastusena info domeeni nimeruumi kohta. Terminiga „DNS-server” tähistatakse tegelikult kasutatavat programmi, kuid seda terminit kasutatakse ka sünonüümina arvuti kohta, kus see programm töötab.



Joonis. Domeeni nimeruum

Top Level Domains – tipptaseme domeenid; Second Level Domains – teise astme domeenid; Generische Domains – üldised domeenid; Länder Domains – riigidomeenid.

Internet on avalik keskkond ja IT-kooslused käitavad IT-süsteeme, mis peavad olema interneti kaudu kättesaadavad, nt veebi- ja meiliserverid. Internetiühenduse loomiseks on vaja DNS-i. Selleks saadab kommunikatsioonipartner DNS-serverile DNS-päringu. DNS-server peab olema sellisel juhul avalikus võrgus kättesaadav, mis tähendab, et see on avalikult ligipääsetav IT-süsteem. Nimeteisenduse hoolikas planeerimine ja professionaalne teostus on vigadeta töö eeltingimusteks, sest nimeteisenduse funktsioon on paljude rakenduste puhul hädavajalik. Seetõttu on mooduli põhirõhk DNS-serveri käideldavusel, terviklusel ning lisaks DNS-serveri käitamisega seotud probleemidel.

Selles moodulis kirjeldatakse DNS-serveritele iseäralikke ohtusid ja nende vastumeetmeid. Moodulit tuleb kasutada juhtudel, kus IT-koosluses hoitakse töös DNS-serverit. DNS-serveri turbe tagamiseks tuleb rakendada veel teisigi mooduleid.

Ohud

DNS-serveri kasutusega seonduva IT-etalonturbe puhul loetakse tüüpilisteks järgmisi ohtusid:

Vääramatu jõud

- G 1.2 IT-süsteemi avarii

Organisatsioonilised puudused

- G 2.1 Reeglite puudumine või puudulikkus

- G 2.32 Võrgu ebapiisav võimsus
- G 2.100 Interneti domeeninimede taotlemise või haldamise vead
- G 2.152 DNS-i kasutamise ebapiisav või puudulik planeerimine

Inimvead

- G 3.3 Hooletus turvameetmete suhtes
- G 3.9 IT-süsteemi väär haldus
- G 3.38 Vead konfigureerimisel ja kasutamisel
- G 3.103 Vale domeeniinfo
- G 3.104 DNS-serveri väär konfiguratsioon

Tehnilised rikked

- G 4.22 Tüüptarkvara turvaaugud või vead

Ründed

- G 5.78 DNS-i võltsimine
- G 5.151 DNS-i üleujutamine ja teenusetõkestamine
- G 5.152 DNS-i kaaperdamine
- G 5.153 DNS-i ülevõimendamine
- G 5.154 DNS-i info lekkimine
- G 5.155 DNS-i dünaamiliste värskenduste ärakasutamine

Soovitatavad meetmed

Vaadeldava IT-koosluse turvalisuse tagamiseks tuleb tavaliselt peale käesoleva mooduli rakendada veel teisigi mooduleid, mis selguvad IT-etalonturbe rakendusjuhendi põhjal tehtava modelleerimise tulemusel.

Nendeks on eelkõige moodul B 3.101 Server ning olenevalt kasutatavast operatsioonisüsteemist kas moodul B 3.102 Server Unixi all , B 3.108 Windows Server 2003 või B 3.109 Windows Server 2008 .

Kuna vähemalt üks osa IT-koosluses kasutatavast DNS-serverist suhtleb internetiga, tuleb turvalise ühenduse tagamiseks järgida ka mooduleid B 1.8 Turvaintsidentide käsitlus ja B 3.301 Turvalüüs (tulemüür) .

DNS-serverid haldavad kogu IT-koosluse nimeinfot ja sisaldavad seega võrgutaristut kajastavat infot. Seetõttu tuleks DNS-server üles seada kas serveriruumi või lukustatud serverikappi, vt moodulid B 2.4 Serveriruum ja B 2.7 Kaitsekapid . Väliste teenusepakkujate korral tuleb arvestada mooduliga B 1.11 Väljasttellimine (Outsourcing) .

Selles moodulis kirjeldatakse DNS-serveritele iseäralikke ohtusid ja nende vastumeetmeid.

Planeerimine ja kontseptsioon

Enne tarkvara väljavalimist ja taristu planeerimist tuleks kontrollida, kas soovitud domeeninimi on veel vaba. Kuna registreerimisel tuleb esitada vastutavate DNS-serverite andmed, tuleks arvestada meetmega M 2.298 Interneti domeeninimede

haldus . Kui planeeritakse DNSSEC kasutamist, on oluline luua krüptograafiliste võtmete haldamise kontsept, nagu on kirjeldatud meetmes M 2.46 Krüpteerimise õige korraldus . Planeerimisel määratakse kindlaks, milline domeeniinfo vajab kõrgemat turbeastet. Lisaks tuleb otsustada, kui suur peab olema DNS-serveri jõudlus. See hõlmab nii IT-süsteemi ennast (eelkõige peamälu) kui ka võrguühenduse ribalaiust. Seetõttu tuleks ka planeerida, kuidas DNS-serverid IT-koosluse võrgutaristuga ühendatakse (vt M 2.451 DNS-i kasutamise planeerimine) ja milliste põhimõtete alusel väljastatakse pääsuõigused (M 2.8 IT-rakendustele ja andmetele pääsuõiguste andmine) . Planeerimistegevuse tulemus tuleb dokumenteerida.

Soetamine

DNS-serverite tarkvara valik on lai. Sobiva toote valimiseks tuleb potentsiaalseid tooteid analüüsida ja vaadelda, kas need vastavad planeerimisdokumendis toodud funktsioonide ja turvalisusega seotud nõuetele (M 2.452 Sobiva DNS-serveritoote valimine).

Rakendamine

Valitud DNS-serverist olenevalt tuleb koolitada ka administraatoreid (vt M 3.73 DNS-serveri administraatorite koolitamine). Koolitusega tagatakse, et vastutavad administraatorid oskavad kasutada serveri konfiguratsioonivõimalusi. Koolituse ja korraliku planeerimise baasil tuleks välja töötada turvaline konfiguratsioon, mis tagab DNS-i käideldavuse ning edastatava info tervikluse (vt M 4.198 Rakenduse installeerimine chroot -puuri , M 4.350 DNS-serveri turvaline aluskonfiguratsioon , M 4.351 Tsooniedastuse turve ja M 4.352 DNS-i dünaamiliste värskenduste turve).

Kasutamine

Igapäevase kasutuse ajal tuleb olla teadlik teadaolevatest turvaaukudest ja installida vajalikud tarkvarauuendused või võtta mõned teist laadi turvameetmed, vt moodul B 1.14 Turvapaikade ja muudatuste haldus . Lisaks tuleks DNS-serveri kommunikatsioon teiste DNS-serverite ja klientidega piirata paketifiltrite abil miinimumini (vt M 4.98 Side piiramine miinimumini paketifiltritega). Tõrkevaba käitamise tagamiseks ja võimalike rikete või anomaaliate kindlakstegemiseks peaks DNS-server olema pideva järelevalve all (vt M 4.354 DNS-serveri seire).

Konfiguratsiooni või DNS-i infot tohiks hakata käsitsi muutma alles pärast seda, kui domeeniinfo on varundatud, et tagada info taastamine võimalike vigade korral, vt M 4.78 Konfiguratsioonimuudatuste hoolikas teostamine .

Väljavahetamine

Kui DNS-server kõrvaldatakse kasutusest, tuleks see kõrvaldada nõuetekohasel viisil (vt M 2.453 DNS-serverite kasutusest kõrvaldamine).

Valmisolek hädaolukorraks

Hädaolukorraks valmisoleku raames tuleks oluliste ohtude jaoks koostada avariiplaanid (vt M 6.139 DNS-serveri avariiplaani koostamine). Kuna DNS on võrguside üks baasfunktsioone, tuleks mõelda sobivate liiasusega süsteemide kasutamisele.

Planeerimine ja kontseptsioon

- (L) M 2.298z Interneti domeeninimede haldus
- (L) M 2.450w Sissejuhatus DNS-i põhimõistetesse
- (L) M 2.451 DNS-i kasutamise planeerimine

Soetamine

- (L) M 2.176z Sobiva internetiteenuse pakkuja valimine
- (L) M 2.452 Sobiva DNS-serveritoote valimine

Rakendamine

- (L) M 2.32z Piiratud kasutajakeskkonna loomine
- (L) M 2.46 Krüpteerimise õige korraldus
- (L) M 3.73 DNS-serveri administraatorite koolitamine
- (L) M 4.95 Minimaalne operatsioonisüsteem
- (M) M 4.97z Ainult üks teenus serveri kohta
- (L) M 4.98 Side piiramine miinimumini paketifiltritega
- (L) M 4.198z Rakenduse installeerimine chroot -puuri
- (L) M 4.350 DNS-serveri turvaline aluskonfiguratsioon
- (M) M 4.351 Tsooniedastuse turve
- (M) M 4.352 DNS-i dünaamiliste värskenduste turve
- (L) M 4.353z DNSSEC kasutamine

Kasutamine

- (L) M 2.8 IT-rakendustele ja andmetele pääsuõiguste andmine
- (M) M 2.35 Teabe hankimine turvaaukude kohta
- (L) M 2.273 Turvalisust mõjutavate paikade ja värskenduste kiire paigaldamine
- (L) M 4.78 Konfiguratsioonimuudatuste hoolikas teostamine
- (M) M 4.354 DNS-serveri seire
- (M) M 5.118z DNS-serveri integreerimine turvalüüsi koostisse

Väljavahetamine

- (M) M 2.453 DNS-serverite kasutusest kõrvaldamine

Valmisolek hädaolukorraks

- (L) M 6.139 DNS-serveri avariiplaani koostamine

B 5.19 Interneti kasutamine

Paljudel tänapäeva töökohtadel on internetiteenuste kasutamine muutunud iseenesest mõistetavaks ja hädavajalikuks. Selliste teenuste hulka kuuluvad näiteks meiliteenus, info- ja internetiteenused, internetipangandus, samuti netikaubandust ja e-riiki puudutavad teenused. Olenevalt töökoha ja -ülesannete eripärast kasutatakse lisaks veel kiirsõnumiteenust (instant messaging), suhtlusvõrgustikke, veebikonverentse jms teenuseid.

Suurt osa internetiteenustest saab kasutada kas veebilehitsejate või teiste rakendustega, mis on integreeritud standardsete operatsioonisüsteemidega. Mõningate valdkondade puhul (nt kiirsõnumiteenus, uudiste lugemine ja internetipangandus) läheb internetiteenuste kasutamiseks tarvis ka spetsiaalset tarkvara.

Seda moodulit tuleb rakendada kõikidel neil juhtudel, kus internetti sisenetakse kas veebilehitseja või mõne spetsiaalse tarkvara abil (v.a meiliteenus). See moodul ei käsitle võrke ega teisi ühendusi. Selleks tuleb kasutada eraldi mooduleid. Turvalise meiliühenduse loomist kirjeldab moodul B 5.3 Rühmatarkvara .

Selles moodulis kirjeldatakse interneti kasutamisega seotud eriohtusid ja nende vastumeetmeid. Interneti turvaliseks ühendamiseks tuleb rakendada lisamooduleid, nt vastavaid võrke käsitlevaid mooduleid ning mooduleid B 1.6 Viirusetõrje kontseptsioon ja B 3.301 Turvalüüs (tulemüür) . Klientsüsteemide turbeks tuleb kasutada moodulit B 3.201 Klient ja võib-olla ka vastavat operatsioonisüsteemi käsitlevat lisamoodulit. Selles moodulis ei käsitleta interneti kasutamise erijuhtu interneti-PC-d (vt ka B 3.208 Interneti-PC).

Ohud

Infosüsteemide etalonturbe seisukohast loetakse interneti kasutamise puhul tüüpilisteks järgmisi ohtusid.

Vääramatu jõud

- G 1.10 Laivõrgu tõrge

Organisatsioonilised puudused

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.2 Reeglite puudulik tundmine
- G 2.4 Turvameetmete ebapiisav järelevalve

Inimvead

- G 3.3 Hooletus turvameetmete suhtes
- G 3.38 Vead konfigureerimisel ja kasutamisel
- G 3.44 Teabe hooletu kasutamine
- G 3.45 Sidepartnerite puudulik autentimine
- G 3.105 Väliste teenuste volitamata kasutamine
- G 3.106 Väär käitumine interneti kasutamisel
- G 3.107 Mainekahjud

Tehnilised rikked

- G 4.22 Tüüptarkvara turvaaugud või vead

Ründed

- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.28 Teenuse halvamine
- G 5.42 Inimestega manipuleerimine (Social Engineering)
- G 5.48 IP-aadressi võltsimine
- G 5.78 DNS-i võltsimine
- G 5.87 Veebilehe võltsimine
- G 5.88 Aktiivsisu väärkasutus
- G 5.156 Robotvõrgud
- G 5.157 Andmepetturlus ja Pharming
- G 5.158 Sotsiaalvõrgustike väärkasutus
- G 5.177 Lühi-URL-ide või QR-koodide kuritarvitamine

Soovitatavad meetmed

Vaadeldava IT-koosluse turvalisuse tagamiseks tuleb peale käesoleva mooduli rakendada veel teisigi mooduleid, mis selguvad IT-etalonturbe rakendusjuhendi põhjal tehtava modelleerimise tulemusel.

Interneti turvaliseks kasutamiseks tuleks ettevõttes või asutuses läbi töötada järgmised infoturvet käsitlevad sammud.

Planeerimine ja kontseptsioon

Alustuseks tuleks kindlaks määrata interneti kasutamise pidepunktid, nt milliseid internetiteenuseid hakatakse institutsioonis kasutama, kes milliseid teenuseid kasutada tohib, millised on kasutusreeglid ning kuidas tuleks turvata sisemisi IT-süsteeme, mis tohivad internetti kasutada (vt M 2.457 Interneti turvalise kasutamise kontseptsioon).

Interneti turvaliseks kasutamiseks tuleb koostada kohustuslik reeglistik, mis määrab kindlaks muu hulgas näiteks selle, kes milliseid internetiteenuseid millal ja mille jaoks kasutada tohib (vt M 2.458 Interneti kasutamise reeglistik). Meiliteenuse kohta on olemas eraldi moodul, mis sisaldab ka meiliteenuse kasutamise reeglistikku.

Rakendamine

Interneti turvalist kasutamist mõjutavad märkimisväärselt nii kasutajad kui ka administraatorid. Seetõttu tuleb kasutajatele ja administraatoritele õpetada, kuidas rakendatavaid IT-komponente ja internetiteenuseid kasutada (vt M 3.77 Interneti kasutamisega seotud teadlikkuse suurendamine).

Kasutamine

Olenevalt erinevatest turvanõuetest tuleb IT-komponendid ka erinevalt konfigureerida. See puudutab turvalüüse ja võrguühenduselemente, aga ka servereid ja

klientsüsteeme. Klientsüsteemide puhul tuleb ilmtingimata kaitsta veebibrauserit (vt M 5.45 Veebibrauserite turvaline kasutamine ja M 5.155 Interneti kasutamise andmekaitseaspektid), E-Mail-Client-süsteeme (vt B 5.3 Rühmatarkvara) ja tarkvara, millega kasutatakse veebirakendusi.

Valmisolek hädaolukorraks

Kuna interneti kasutamine võib tööülesannete täitmisel olla määrava tähtsusega, tuleb rikkeid ennetada. Selleks peavad olema välja töötatud ka internetirakenduste asendusprotseduurid (vt M 6.141 Interneti kasutamise asendusprotseduurid). Lisaks tuleb kindlaks määrata, kuidas tegutseda interneti kasutamisest tingitud turvaintsidentide korral (vt B 1.8 Turvaintsidentide käsitlus).

Alljärgnevalt tutvustatakse meetmete kogumit, mida tuleb rakendada valdkonnas „Interneti kasutamine”:

Planeerimine ja kontseptsioon

- (L) M 2.457 Interneti turvalise kasutamise kontseptsioon
- (L) M 2.458 Interneti kasutamise reeglistik
- (L) M 2.459w Internetiteenuste ülevaade
- (L) M 5.66z SSL-i/TLS-i kasutamine kliendis
- (L) M 5.69 Aktiivsisu tõrje

Rakendamine

- (M) M 2.460 Väliste teenuste reguleeritud kasutamine
- (L) M 3.77 Interneti kasutamisega seotud teadlikkuse suurendamine

Kasutamine

- (L) M 2.313 Turvaline sisselogimine internetiteenustesse
- (L) M 3.78w Korrektne käitumine internetis
- (L) M 5.45 Veebibrauserite turvaline kasutamine
- (L) M 5.155z Interneti kasutamise andmekaitseaspektid
- (L) M 5.156z Twitteri turvaline kasutamine
- (L) M 5.157z Sotsiaalvõrgustike turvaline kasutamine
- (L) M 5.158z Veebimälu turvaline kasutamine
- (L) M 5.173z Lühi-URL-ide või QR-koodide kasutamine

Valmisolek hädaolukorraks

- (M) M 6.141 Interneti kasutamise asendusprotseduurid

B 5.20 OpenLDAP

Selles moodulis kirjeldatakse OpenLDAP olulisimaid turbeomadusi. OpenLDAP on vabavaraline kataloogiteenus, millega saab andmevõrgus teatud defineeritaval viisil ligi pääseda mis tahes objektide, nt kasutajate või arvutite andmetele. Andmed võivad olla lihtsustatud atribuudid, nagu objektide nimed ja numbrid, kuid need võivad esineda ka keerulisemas andmevormingus, nt fotode ja digisignatuurideks vajaminevate sertifikaatide kujul. Tüüpiline kasutusvaldkond on nt aadressiraamatute ja kasutajate haldus.

OpenLDAP-d saab rakendada ka serverites ning vastav tootelahendus on Lightweight Directory Access Protocol (LDAP). OpenLDAP-d pakutakse vabavarana väga paljudele operatsioonisüsteemidele.

Mooduli piiritlemine

Selles moodulis kirjeldatakse OpenLDAP-le iseäralikke ohte ja nende vastumeetmeid. Kirjeldamisel lähtutakse versioonist OpenLDAP 2.4. Kataloogiteenuste üldkehtivad turbesoovitused leiate moodulist B 5.15 Üldine kataloogiteenus . Käesoleva mooduliga püütakse eelnimetatud üldisi meetmeid täpsustada ja täiendada. Seda moodulit tuleb rakendada kõikides infokoosluse serverites, kus käitatakse OpenLDAP slapd-deemonit.

Ohud

IT-etalonturbe seisukohalt loetakse OpenLDAP puhul tüüpilisteks järgmisi ohuallikaid.

Vääramatu jõud

- G 1.2 IT-süsteemi avarii

Organisatsioonilised puudused

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.2 Reeglite puudulik tundmine
- G 2.7 Õiguste volitamata kasutamine
- G 2.28 Autoriõiguste rikkumine
- G 2.155 OpenLDAP ebapiisav või puuduv planeerimine

Inimvead

- G 3.8 IT-süsteemi väär kasutamine
- G 3.9 IT-süsteemi väär haldus
- G 3.13 Väära või soovimatu andmekogumi saatmine
- G 3.88 Väär pääsuõiguste andmine
- G 3.110 OpenLDAP väär konfiguratsioon
- G 3.111 OpenLDAP offline- ja online-pöörduste ebapiisav lahutamine

Tehnilised rikked

- G 4.10 Keerukad ligipääsuvõimalused võrgustatud IT-süsteemides
- G 4.13 Salvestatud andmete hävimine
- G 4.22 Tüüptarkvara turvaaugud või vead

- G 4.33 Autentimise puudumine või puudulikkus
- G 4.67 Kataloogiteenuste rike

Ründed

- G 5.16 Ohud hoolde- ja haldustööde ajal
- G 5.18 Süstemaatiline paroolide mõistatamine
- G 5.19 Kasutajaõiguste väärkasutus
- G 5.20 Administraatori õiguste väärkasutus
- G 5.21 Trooja hobused
- G 5.65 Teenusetõkestus andmebaasisüsteemis
- G 5.71 Tundliku informatsiooni konfidentsiaalsuse kadu
- G 5.78 DNS-i võltsimine
- G 5.85 Tundliku informatsiooni tervikluse kadu
- G 5.144 Kataloogiteenuste kompromiteerimine volitamata juurdepääsu kaudu

Soovitatavad meetmed

Vaadeldava IT-koosluse turvalisuse tagamiseks tuleb tavaliselt peale käesoleva mooduli rakendada veel teisigi mooduleid, mis selguvad IT-etalonturbe rakendusjuhendi põhjal tehtava modelleerimise tulemusel.

OpenLDAP-ga töödeldavate andmete kaitsmiseks tuleb keskenduda eeskätt serveri operatsioonisüsteemi turbele. Seda teemat käesolev moodul ei puuduta. Asjakohased käsitlused leiate 3. kihi moodulite hulgast. Kui platvormina kasutatakse näiteks Unixit, tuleb arvestada mooduliga B 3.102 Server Unixi all .

OpenLDAP edukaks rakendamiseks tuleb läbida mitmeid etappe, mis puudutavad kontseptsiooni koostamist, installimist ja käitamist. Järgnevalt on esitatud ülevaade erinevatest kohustuslikest etappidest ja meetmetest, mida iga etapi puhul tuleks võtta.

Planeerimine ja kontseptsioon

Pärast seda, kui kataloogiteenuse kasutuselevõtu üldised planeerimistööd on tehtud, tuleb välja töötada OpenLDAP kasutamise osakontseptsioonid, lähtudes kõikidest üldkehtivatest kontseptsioonidest ja ettekirjutustest. Alustuseks on soovitatav tegelda meetmega M 3.85 Sissejuhatus OpenLDAP-sse , mis annab ülevaate OpenLDAP struktuurist ja terminitest. Üldiseid tööetappe kirjeldatakse meetmes M 2.484 OpenLDAP planeerimine . Planeerimisetapis tuleb muu hulgas langetada vajalikud otsused tagaprogrammide kasutamise kohta, vt M 2.485 Back-end 'ide valimine OpenLDAP jaoks . Enne OpenLDAP juurutamist tuleb eeltööna koostada ka spetsiaalne OpenLDAP turvapoliitika (vt M 2.405 Kataloogiteenuse turvapoliitika koostamine).

Soetamine

Kui kontseptsioonide planeerimist puudutavad tööd on tehtud, tuleb kontrollida installimiseks kasutatavate pakettide (lähteteksti- või binaarpakettide) terviklust ja autentsust (vt M 4.382 OpenLDAP installatsioonipakettide valik ja kontrollimine).

Rakendamine

Enne OpenLDAP installimist mis tahes IT-süsteemi tuleb esmalt selle operatsioonisüsteem sobival moel konfigureerida ja turvaliseks muuta. Samuti tuleb IT-süsteemi installida kõik planeerimise raames kokku lepitud funktsiooni toetavad programmid. Toote enda installimisel ja aluskonfiguratsiooni tegemisel tuleb arvestada meetmetega M 4.383 OpenLDAP turvaline installimine , M 4.384 OpenLDAP turvaline konfiguratsioon , M 4.385 OpenLDAP kasutatava andmebaasi konfiguratsioon , M 4.386 Atribuutide piiramine OpenLDAP puhul , M 4.387 OpenLDAP pääsuõiguste turvaline andmine , M 4.388 OpenLDAP turvaline autentimine ja M 4.389 OpenLDAP partitsioonid ja replikatsioonid .

OpenLDAP turvaline installimine ei ole ühekordne tegevus. Ka seda tarkvara tuleb pidevalt ajakohastada, nagu on kirjeldatud meetmes M 4.390 OpenLDAP turvaline ajakohastamine .

Turvaliseks installimiseks ja käitamiseks peavad administraatorid läbima asjakohased koolitused. Koolituste jaoks olulisi aspekte kirjeldatakse meetmes M 3.86 OpenLDAP administraatorite koolitus .

Kasutamine

Tavakasutuse jaoks peab kogu aeg olemas olema värskete andmetega dokumentatsioon. Oluline pole muidugi mitte üksnes operatsioonisüsteemi, vaid ka OpenLDAP enda hoolikas haldamine (vt M 4.391 OpenLDAP turvaline käitamine). Et probleeme võimalikult vara tuvastada, tuleks võtta arvesse meetmes M 4.407 OpenLDAP kasutamise logimine esitatud soovitusi. Edastatavate andmete konfidentsiaalsuse ja tervikluse kaitsmiseks tuleb muu hulgas tagada, et OpenLDAP serveri ja klientsüsteemide vaheline andmeside oleks turvaline (vt M 5.170 OpenLDAP-d kasutavate sideühenduste turve).

Kasutusest kõrvaldamine

Juhised OpenLDAP installatsiooni nõuetekohaseks kasutusest kõrvaldamiseks leiate meetmest M 2.410 Kataloogiteenuse korrakohane kasutuselt kõrvaldamine .

Valmisolek hädaolukorraks

OpenLDAP-ga seotud hädaolukordadeks valmisoleku planeerimist selgitatakse meetmes M 6.106 Kataloogiteenuse hädaolukorraks valmisoleku plaani koostamine . OpenLDAP andmevarunduse teemat käsitletakse meetmes M 6.150 OpenLDAP andmevarundus .

Alljärgnevalt tutvustatakse meetmete kogumit, mida tuleb rakendada valdkonnas „OpenLDAP”:

Planeerimine ja kontseptsioon

- (L) M 2.405 Kataloogiteenuse turvapoliitika koostamine
- (L) M 2.484 OpenLDAP planeerimine
- (L) M 2.485 Back-end ’ide valimine OpenLDAP jaoks
- (L) M 3.85w Sissejuhatus OpenLDAP-sse

Soetamine

- (M) M 4.382 OpenLDAP installatsioonipakettide valik ja kontrollimine

Rakendamine

- (L) M 3.86 OpenLDAP administraatorite koolitus
- (L) M 4.383 OpenLDAP turvaline installimine
- (L) M 4.384 OpenLDAP turvaline konfiguratsioon
- (L) M 4.385 OpenLDAP kasutatava andmebaasi konfiguratsioon
- (L) M 4.386 Atribuutide piiramine OpenLDAP puhul
- (L) M 4.387 OpenLDAP pääsuõiguste turvaline andmine
- (L) M 4.388 OpenLDAP turvaline autentimine
- (L) M 4.389 OpenLDAP partitsioonid ja replikatsioonid

Kasutamine

- (M) M 4.390 OpenLDAP turvaline ajakohastamine
- (L) M 4.391 OpenLDAP turvaline käitamine
- (L) M 4.407 OpenLDAP kasutamise logimine
- (M) M 5.170 OpenLDAP-d kasutavate sideühenduste turve

Kasutusest kõrvaldamine

- (L) M 2.410 Kataloogiteenuse korrakohane kasutuselt kõrvaldamine

Valmisolek hädaolukorraks

- (L) M 6.150 OpenLDAP andmevarundus

B 5.21 Veebirakendused

Veebirakendused võimaldavad kasutada erinevaid funktsioone ja dünaamilist sisu, rakendades selliseid protokolle nagu HTTP (Hypertext Transfer Protocol) või HTTPS (HTTP üle SSL-i või TLS-i, s.t HTTP-d kaitstakse krüpteeritud ühendusega). Selleks koostatakse serveris kõigepealt dokumendid ja kasutajaliidesed (nt juhtelemendid ja sisestusblanketid), seejärel edastatakse need klientprogrammidele (veebilehitsejatele).

Veebirakendusi arendatakse enamasti raamistike (frameworks) baasil. Raamistikud on lahendused, mida saab kasutada sageli korduvateks ülesanneteks (nt turvakomponentide jaoks). Ühe veebirakenduse jaoks kasutatakse sageli korraga mitut raamistikku, mis toetavad erinevaid valdkondi (nt juurdepääs andmebaasidele, väljundite vormindamine), ja mitut komponenti (nt autentimine, seansihaldus). Seetõttu tuleb juba planeerimisetapis võtta arvesse nii raamistike väljavalimise kui ka tarkvara arhitektuuriga seonduvaid turvaaspekte.

Veebirakenduse käitamiseks läheb sageli tarvis mitut IT-süsteemi komponenti. Nende hulka kuuluvad enamasti veebiserver, mis väljastab andmeid, rakendusserver, mis võimaldab rakendust kasutada, ning täiendavad taustsüsteemid, mis on omavahel ühendatud erinevate liidestega üheks andmeallikaks (nt andmebaas või kataloogiteenus).

Veebirakendusi käitatakse andmete ja rakenduse kasutamiseks nii avalikes IT-võrkudes (nt internetis) kui ka firmavõrkudes (intranetis). Veebirakenduses peavad olema ka turvamehhanismid, mis tagavad piisava andmekaitse ja hoiavad ära andmete väärkasutuse.

Allpool on nimetatud veebirakenduse tüüpilised turvakomponendid ja -mehhanismid.

- Autentimine - juurdepääsuks veebirakenduse kaitstud ressurssidele peavad kasutajad end süsteemi autentimiskomponendis autentima (nt pääsuandmetega).
- Volitused - enne kaitstud ressurssidele ja funktsioonidele ligipääsu võimaldamist tuleb kontrollida, kas kasutajatel on olemas ligipääsuks vajalikud volitused.
- Sisestuse ja väljastuse valideerimine - sisestatavaid ja väljastatavaid andmeid tuleb kontrollida ja filtreerida, et vältida kahjulike andmete (nt pahavara käitatava koodi) töötlemist.
- Seansihaldus - kuna internetiprotokoll HTTP ei võimalda kokkukuuluvaid päringuid siduda ühe konkreetse kasutajaga, tuleb seostamiseks kasutada veebirakenduse seansihaldust.
- Tõrkekäsitlus - tekkivaid tõrkeid tuleb käsitleda selliselt, et veebirakenduse andmete turve säiliks ka tõrke korral.
- Logimine - veebirakenduste logi peab võimaldama tagantjärele selgitada nii aset leidnud tegevuste kui ka võimalike turvaintsidentide tagamaid.

Mooduli piiritlemine

Selles moodulis kirjeldatakse veebirakendustele iseäralikke ohte ja nende vastumeetmeid. Kui veebiserverid väljastavad veebilehti (vt B 5.4 Veebiserver), siis

veebirakendused võimaldavad kasutada funktsioone ja valmistavad ette veebiserveri väljastatavat dünaamilist sisu. B 5.4 Veebiserver kirjeldatakse muu hulgas veebilehe redaktsioonide planeerimist ja hädaolukorraks valmisolekut, mida siin moodulis üle ei korrata. Nii nagu veebirakendused, on ka veebiteenused seotud protsessiloogikaga, mistõttu kehtib suur osa veebirakendustega seotud ohtudest ja meetmetest ka veebiteenuste loogikakomponentide kohta.

Tavaliste veebirakenduste puhul võimaldatakse selle funktsioone kasutada üksnes rakenduse piirides. Seevastu SOAP-il (Simple Object Access Protocol) põhinevate veebiteenuste puhul töötavad veebirakendused üksteisest eraldi, sõltumatute ja üksteisega asendatavate teenustena, mida teenusepakkujad osutavad standardsete liideste kaudu. Erinevalt veebirakendustest ei valmista veebiteenused veebilehitseja tarbeks enamasti oma tulemusi ette, vaid teevad oma tulemuse kättesaadavaks struktureeritud masinloetavas vormis (nt SOAP-teadetena), mida on võimalik automaatselt edasi töödelda. Selle protsessi käigus töödeldakse andmeid veebiteenuse erinevates komponentides (nt parseris või krüpteerimis- ja dekrüpteerimiskomponendis). Teenusele orienteeritud arhitektuuri (SOA) ülesehitamist puudutavaid turvaaspekte selles moodulis ei käsitleta.

Ohud

Veebirakenduste kasutusega seonduva IT-etalonturbe puhul loetakse tüüpilisteks järgmisi ohte:

Organisatsioonilised puudused

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.4 Turvameetmete ebapiisav järelevalve
- G 2.7 Õiguste volitamata kasutamine
- G 2.22 Logiandmete analüüsimata jätmine
- G 2.27 Ebapiisav või puuduv dokumentatsioon
- G 2.67 Pääsuõiguste puudulik haldus
- G 2.87 Ebaturvalised protokollid avalikes võrkudes
- G 2.103 Töötajate ebapiisav koolitamine
- G 2.157 Veebirakenduste halb valik või kontseptsioon
- G 2.158 Veebirakenduste arendamise ja laiendamisega seotud puudused
- G 2.159 Isikuandmete ebapiisav turve veebirakendustes

Inimvead

- G 3.16 Väär pääsuõiguste haldus
- G 3.38 Vead konfigureerimisel ja kasutamisel
- G 3.43 Puudulik paroolihooldus

Tehnilised rikked

- G 4.22 Tüüptarkvara turvaaugud või vead
- G 4.33 Autentimise puudumine või puudulikkus
- G 4.35 Ebaturvaline krüptoalgoritm
- G 4.84 Enda arendatud makrode väärfunktsioonid Outlookis
- G 4.85 Veebirakenduste ebapiisav või puuduv tõrkekäsitlus

- G 4.86 Turbe jaoks oluliste sündmuste ebapiisav kontrollitavus veebirakendustes
- G 4.87 Konfidentsiaalse info ilmsikstulek veebirakendustes

Ründed

- G 5.18 Süstemaatiline paroolide mõistatamine
- G 5.19 Kasutajaõiguste väärkasutus
- G 5.20 Administraatori õiguste väärkasutus
- G 5.28 Teenuse halvamine
- G 5.88 Aktiivsisu väärkasutus
- G 5.131 SQL-injektsioon
- G 5.165 Volitamata juurdepääs veebirakenduse andmetele või andmete manipuleerimine
- G 5.166 Automatiseeritud kasutusest tingitud veebirakenduste väärkasutus
- G 5.167 Veebirakenduste loogikavead
- G 5.168 Veebirakenduste turbefunktsioonide kasutamise eiramine klientprogrammides
- G 5.169 Veebirakenduste puudulik seansihaldus
- G 5.170 Murdskriptimisründed (XSS)
- G 5.171 Cross-Site Request Forgery (CSRF, XSRF, Session Riding)
- G 5.172 Veebirakenduste autentimise eiramine
- G 5.173 Võõraste andmete ja pahavarakoodi smugeldamine veebirakendustesse
- G 5.174 Injektsiooniründed
- G 5.175 Klõpsurööv (clickjacking)

Soovitatavad meetmed

Veebirakenduste turvalisuse tagamiseks tuleb peale käesoleva mooduli rakendada veel teisigi mooduleid, mis selguvad IT-etalonturbe rakendusjuhendi põhjal tehtava modelleerimise tulemusel.

Veebirakenduse käitamiseks tuleb käitada ka lisakomponente. Seetõttu on vaja alati rakendada ka moodulit B 3.101 Server ja olenevalt operatsioonisüsteemist nt moodulit B 3.102 Server Unixi all , B 3.108 Windows Server 2003 või B 3.109 Windows Server 2008 . Veebirakenduse käitamiseks läheb tarvis ka veebiserverit (vt B 5.4 Veebiserver).

Funktsioonide tagamine ja andmetöötlus suunatakse veebirakenduste puhul tavaliselt taustsüsteemidesse (nt andmebaasi ja identiteedi mällu). Seetõttu tuleb vastavalt taustsüsteemidele arvestada ka selliste lisamoodulitega nagu B 5.7 Andmebaasid ja B 5.15 Üldine kataloogiteenus (või ka B 5.16 Active Directory).

Kui veebirakendus töötleb muu hulgas isikuandmeid või analüüsib kasutajaandmeid (nt külastatavuse statistika, kasutajaprofiilid), tuleb rakendada ka moodulit B 1.5 Andmekaitse .

Kui veebiteenust osutab või arendab mõni väline teenusepakkuja, tuleb pöörata tähelepanu ka moodulile B 1.11 Väljasttellimine (Outsourcing) .

Veebirakenduse turvalisuse tagamiseks tuleb võtta mitmeid meetmeid. Järgnevalt on esitatud ülevaade erinevatest kohustuslikest etappidest ja meetmetest, mida iga etapi puhul tuleks võtta.

Planeerimine ja kontseptsioon

Veebirakendust planeerides tuleb enamasti langetada otsus, kas sellele esitatavaid nõudmisi on võimalik täita standardtoodetega või tuleb tootelahendus ise välja töötada. Kui veebirakendus pannakse tööle standardtarkvaraga, tuleb tarkvara sageli ka kohandada ning see võib eeldada juba enamat kui tavalist konfiguratsiooni muutmist, s.t vajalikud on ka arendustööd. Standardtarkvaraga töötavad veebirakendused peavad sageli täitma veebirakenduste arendamisele ja laiendamisele esitatavaid nõudeid (vt M M 2.487 Veebirakenduste arendamine ja laiendamine).

Töödeldavate andmete kaitse tagamiseks tuleb turbeaspektidele pöörata tähelepanu juba veebirakenduse kavandamise etapis (vt M 5.169 Veebirakenduse süsteemiarhitektuur). Siinkohal tuleb arvestada ka taustsüsteemide (nt andmebaasi) integreerimise ja nende turvalise ühendamisega (vt M 5.168 Taustsüsteemide turvaline sidumine veebirakendustega).

Kui veebirakendus töötleb, salvestab või analüüsib isikuandmeid (nt kasutajate harjumusi), tuleb tehniliste lahenduste planeerimisel võtta arvesse ka seadustest tulenevaid ettekirjutusi (vt M 2.110 Andmeprivaatsuse suunised logimisprotseduurides ja M 2.488 Web tracking).

Soetamine

Standardtarkvara kasuks otsustamisel tuleb veebirakenduse jaoks välja valida sobiv toode (vt M 2.80 Tüüptarkvara nõuete kataloogi koostamine).

Rakendamine

Enne veebirakenduse kasutuselevõttu igapäevatöös tuleb kas konfigureerida või välja arendada selle turvafunktsioonid. Sel otstarbel rakendatavad komponendid peavad veebirakendust kaitsma teadaolevate ohtude ja ründetehnikate eest (näiteks M 2.363 SQL-injektsiooni kaitse).

Lisaks kuuluvad veebirakenduse oluliste turvakomponentide hulka andmete kontekstipõhine valideerimine ja filtreerimine (vt M 4.392 Autentimine veebirakendustes) ning kasutajaseansside kaitse seansihaldusega (vt M 4.394 Seansihaldus veebirakendustes).

Kasutamine

Pärast seda, kui veebirakendus on edukalt läbinud vastuvõtu ja kasutusse lubamise protseduurid ning kui sellele on tehtud toimiv konfiguratsioon, võib veebirakenduse üle võtta tavakasutusse.

Ilmsiks tulnud turvaaukude ärakasutamise oht on veebirakenduste puhul kõige suurem siis, kui neid kasutatakse avalikes võrkudes (nt internetis). Seetõttu tuleb defineerida protsessid, mis tagaksid püsivalt veebirakenduse vajaliku turbeastme (vt M 2.35 Teabe hankimine turvaaukude kohta ja M 2.273 Turvalisust mõjutavate paikade ja värskenduste kiire paigaldamine).

Veebirakenduse kasutamisel peab olema tagatud, et selles edastatavad andmed ei sisaldaks turbeteavet, mida ründaja saaks ära kasutada turvamehhanismi-

dest möödahiilimiseks (vt M 4.400 Turbe seisukohalt oluliste andmete väljastamine veebirakendustes).Suure kaitsevajaduse korral tuleb veebirakenduse turbeastet kontrollida penetratsioonitestidega, et võimalikud kitsaskohad kiiresti kõrvaldada (vt M 5.150 Penetratsioonitestide läbiviimine).

Alljärgnevalt tutvustatakse meetmete kogumit, mida tuleb rakendada valdkonnas "Veebirakendused". Korduvatest viidetest teiste moodulite meetmetele on ruumi kokkuhoiu eesmärgil loobutud.

Planeerimine ja kontseptsioon

- (L) M 2.1 IT kasutajate vastutuse ja reeglite kehtestamine
- (L) M 2.11 Paroolide kasutamise reeglid
- (L) M 2.63 Pääsuvolituste kehtestamine
- (L) M 2.80 Tüüptarkvara nõuete kataloogi koostamine
- (L) M 2.363 SQL-injektsiooni kaitse
- (L) M 2.486 Veebirakenduste arhitektuuri dokumenteerimine
- (L) M 2.487 Veebirakenduste arendamine ja laiendamine
- (L) M 2.488w Web tracking
- (M) M 4.176 Autentimismeetodite valimine veebilehtede jaoks
- (L) M 4.404 Veebirakenduste turvalise loogika kavandamine
- (L) M 5.66z SSL-i/TLS-i kasutamine kliendis
- (L) M 5.168 Taustsüsteemide turvaline sidumine veebirakendustega
- (L) M 5.169 Veebirakenduse süsteemiarhitektuur
- (M) M 5.177 SSL-i/TLS-i kasutamine serveris
- (L) M 5.178 Infosüsteemis autentimislahendustele kehtivad nõuded ehk autentimisnormatiiv

Soetamine

- (L) M 2.62 Tarkvara vastuvõtuprotseduurid
- (L) M 4.400 Turbe seisukohalt oluliste andmete väljastamine veebirakendustes

Rakendamine

- (L) M 4.392 Autentimine veebirakendustes
- (L) M 4.393 Sisestuste- ja väljastuste põhjalik valideerimine veebirakendustes
- (L) M 4.394 Seansihaldus veebirakendustes
- (L) M 4.395 Tõrkekäsitlus veebirakendustes
- (L) M 4.396 Veebirakenduste kaitsmine keelatud automaatkasutuse eest
- (L) M 4.398 Veebirakenduste turvaline konfiguratsioon
- (L) M 4.399 Andmete ja sisu kontrollitud lisamine veebirakendustesse
- (L) M 4.401 Konfidentsiaalsete andmete kaitse veebirakendustes
- (L) M 4.402 Juurdepääsukontroll veebirakendustes
- (M) M 4.403 Cross-Site Request Forgery (CSRF, XSRF, Session Riding) tõkestamine
- (M) M 4.405 Ressursside blokeerimise (DoS-rünnete) tõkestamine veebirakendustes

- (L) M 4.406z Clickjacking-rünnete tõkestamine

Kasutamine

- (L) M 2.8 IT-rakendustele ja andmetele pääsuõiguste andmine
- (L) M 2.31 Volitatud kasutajate ja õiguste profiilide dokumenteerimine
- (L) M 2.34 IT-süsteemi muutuste dokumenteerimine
- (L) M 2.35 Teabe hankimine turvaaukude kohta
- (M) M 2.64 Logifailide kontroll
- (M) M 2.110 Andmeprivaatsuse suunised logimisprotseduurides
- (L) M 2.273 Turvalisust mõjutavate paikade ja värskenduste kiire paigaldamine
- (L) M 3.5 Turvameetmete koolitus
- (L) M 4.78 Konfiguratsioonimuudatuste hoolikas teostamine
- (M) M 4.397 Veebirakenduste turvet puudutavate sündmuste logimine
- (M) M 4.400 Turbe seisukohalt oluliste andmete väljastamine veebirakendustes
- (M) M 5.150 Penetratsioonitestide läbiviimine

B 5.22 Logimine

IT-süsteemide käitamise puhul mõistetakse logimise all andmete käsitsi või automaatset salvestamist sellisel kujul, mis aitab leida vastuseid järgmistele küsimustele: mida keegi põhjustas (st kasutas), millal ta seda tegi ning milliseid vahendeid ta rakendas? Samuti peaks logimine aitama vastata küsimustele süsteemi seisundi kohta: kellel olid pääsuõigused, millised need olid ja millises ajavahemikus need kehtisid? IT-süsteemide usaldusväärse töö tagamiseks on vajalik, et infokoosluses saaksid logitud kõik turbe seisukohalt kriitilised sündmused. Logimise eesmärk on aidata mõista, miks ja kuidas leidsid IT-süsteemides ja rakendustes aset olulised muudatused, et hinnata süsteemide ja rakenduste turvet. Logimisfunktsioone rakendatakse väga paljudes infokooslustes peamiselt selleks, et avastada riist- ja tarkvaraprobleeme ning tuvastada kiiresti ressursside võimalikku ammendumist. Logiandmetest on siiski ka suur kasu turbeprobleemide puhul ning nende põhjal saab tuvastada teenuste osutamise vastu suunatud ründeid.

Logimist võib rakendada nii lokaalselt kui ka tsentraalselt. Infokooslusest tervikliku ülevaate saamiseks võib kasutada tsentraalselt töötavat logimisserverit, mis koondab erinevad logiandmed kokku, analüüsib ja valvab neid. Sellisel juhul saab andmete analüüsimise ja võrdluse baasil tuvastada ründeid, mis pannakse toime korraga mitme IT-süsteemi vastu.

Tsentraalselt töötava logimise tüüpilised kasutusvaldkonnad on järgmised:

- turvalüüsidest saabuvate teadete kokkukogumine blokeeritud ühendustest tulnud ühenduse loomise katsete kohta;
- hoiatavate teadete tsentraalne kogumispunkt juhtudeks, kus massmälu kvoodid saavad täis;
- arhiiv kohtulike uuringute tarbeks (pärast IT-süsteemi vastu toime pandud ründe tuvastamist).

Selles moodulis vaadeldakse kõiki infokoosluse eriohte seoses logimise ja seirega, olenemata sellest, mis operatsioonisüsteeme parasjagu kasutatakse. Sobiliku protsessi ülesehitamine ja realiseerimine on väga töö- ja ajamahukas. Seetõttu tuleks seda moodulit kasutada alati suuremate infokoosluste puhul ning juhtudel, kus infokoosluses soovitakse juurutada tsentraalselt töötavat logimist. Väiksemate ja vähem keeruliste infokoosluste puhul võib olenevalt olukorrast piisata ka meetmest M 2.500 IT-süsteemide logimine .

Ohud

IT-etalonturbe seisukohalt loetakse logimisfunktsiooni puhul tüüpilisteks allnimetatud ohuallikaid.

Vääramatu jõud

- G 1.2 IT-süsteemi avarii

Organisatsioonilised puudused

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.4 Turvameetmete ebapiisav järelevalve
- G 2.7 Õiguste volitamata kasutamine
- G 2.22 Logiandmete analüüsimata jätmine
- G 2.61 Isikuandmete volitamatu kogumine
- G 2.67 Pääsuõiguste puudulik haldus
- G 2.160 Ebapiisav või puuduv logimine
- G 2.161 Logiandmete konfidentsiaalsuse ja tervikluse kadu

Inimvead

- G 3.3 Hooletus turvameetmete suhtes
- G 3.9 IT-süsteemi väär haldus
- G 3.38 Vead konfigureerimisel ja kasutamisel
- G 3.114 Logimisprotseduuride väär haldus
- G 3.115 Oluliste logiandmete väär valik
- G 3.116 Aja sünkroniseerimata jätmine logiandmete analüüsimisel

Tehnilised rikked

- G 4.89 Logimise puuduv või ebapiisav hoiatamiskontseptsioon

Ründed

- G 5.20 Administraatori õiguste väärkasutus
- G 5.71 Tundliku informatsiooni konfidentsiaalsuse kadu
- G 5.85 Tundliku informatsiooni tervikluse kadu
- G 5.143 Man-in-the-Middle tüüpi rünne
- G 5.176 Logiandmete edastuse kompromiteerimine tsentraalses logimises

Soovitatavad meetmed

Et tagada kogu vaadeldava IT-koosluse turvalisus, tuleb peale käesoleva mooduli rakendada veel ka teisi IT-etalonturbe modelleerimise käigus selguvaid mooduleid.

Logimisteenused võivad olla integreeritud operatsioonisüsteemi või eraldi toimivate tarkvarakomponentide kujul. Logimisteenuse ja salvestatud logiandmete turbe tagamiseks tuleb kaitsta operatsioonisüsteemi. Seda valdkonda siin moodulis ei käsitleta. Selleks tuleb rakendada operatsioonisüsteeme käsitlevaid 3. kihi mooduleid, eelkõige mooduleid B 3.101 Server ja B 3.201 Klient .

Logimisfunktsiooni edu tagamiseks tuleb võtta mitmeid meetmeid, mis puudutavad näiteks kontseptsiooni loomist, soetamist ja turvalist käitamist. Järgnevalt on esitatud ülevaade erinevatest kohustuslikest etappidest ja meetmetest, mida iga etapi puhul tuleks võtta.

Planeerimine ja kontseptsioon

Logimisfunktsiooni kasutuselevõtt infokoosluses eeldab tehniliste lahenduste ja töökorralduse planeerimist (vt M 2.499 Logimise planeerimine ja M 2.500 IT-süsteemide logimine). Samuti kuuluvad planeerimistööde hulka asjakohase turbekontseptsiooni väljatöötamine (vt M 2.497 Logimise turbekontseptsiooni koostamine) ning logimisteenuste ja logiandmete pääsuõiguste andmine (vt M 2.8 IT-rakendustele ja andmetele pääsuõiguste andmine).

Tsentraalse logimise rakendamisel tuleb otsustada, kuidas integreerida tsentraalne logimisserver infokoosluse võrgu infrastruktuuriga (vt M 2.499 Logimise planeerimine ja M 3.90 Tsentraalse logimise põhitõed).

Rakendamine

Vastutavad administraatorid peavad läbima asjakohase koolituse, eriti puudutab see tsentraalse logimisserveri turvalist käitamist. Rohkem teavet leiate meetmest M 3.89 Logimisprotsessi haldamise koolitus . Tõhusa käitamise jaoks on oluline ka võimalikult varane hoiatus, s.t et turvaintsidentide tuvastamisele järgneksid viivitamatult ka hoiatamisprotseduurid. Siinkohal on tarvis kindlaks määrata, keda, kuidas ja mil moel juhtunust teavitatakse ning milliseid teavituskanaleid info edastamisel kasutatakse (vt M 6.151 Logimise häirepoliitika).

Kasutamine

Logimise käigus kogutud andmeid võidakse analüüsida lokaalselt või tsentraalses logimisserveris (vt M 4.430 Logiandmete analüüs). Tsentraalse analüüsi korral tuleb logimisega seotud andmed edastada tsentraalsesse serverisse läbi võrgu.

Siinkohal on oluline, et IT-süsteemide vaheline andmeedastus oleks piisavalt turvaline (vt M 5.171 Turvaline andmeside keskse logiserveriga). Enne kui logiandmeid saab hakata tõhusalt analüüsima, tuleb need analüüsiks ette valmistada (vt M 4.431 Logimise jaoks oluliste andmete valik ja töötlemine).

Kasutusest kõrvaldamine

Logimisserverite kõvaketaste kasutusest kõrvaldamisel, aga ka nendel olevate andmete kustutamisel tuleb arvestada, et konfidentsiaalsed andmed ja isikuandmed tuleb täielikult kustutada (vt M 2.496 Logiserveri korrakohane kasutusest kõrvaldamine).

Valmisolek hädaolukorraks

Hädaolukorraks valmisoleku raames tuleks oluliste ohtude jaoks koostada avariiplaanid (M 6.96 Serveri avariiplaan).

Alljärgnevalt tutvustatakse meetmete kogumit, mida tuleb rakendada valdkonnas „Logimine”:

Planeerimine ja kontseptsioon

- (L) M 2.1 IT kasutajate vastutuse ja reeglite kehtestamine
- (L) M 2.497 Logimise turbekontseptsiooni koostamine
- (L) M 2.499 Logimise planeerimine
- (L) M 2.500 IT-süsteemide logimine
- (L) M 3.90w Tsentraalse logimise põhitõed
- (L) M 5.66z SSL-i/TLS-i kasutamine kliendis
- (M) M 5.68z Krüpteerimisprotseduuride kasutamine võrgusuhtluses

- (M) M 5.177 SSL-i/TLS-i kasutamine serveris

Rakendamine

- (M) M 2.498 Reageerimine hoiatus- ja veateadetele
- (L) M 3.10 Usaldusväärse administraatori ja tema asetäitja valimine
- (L) M 3.89 Logimisprotsessi haldamise koolitus
- (L) M 6.151 Logimise häirepoliitika

Kasutamine

- (L) M 2.8 IT-rakendustele ja andmetele pääsuõiguste andmine
- (L) M 2.64 Logifailide kontroll
- (L) M 2.110 Andmeprivaatsuse suunised logimisprotseduurides
- (M) M 4.225z Logiserveri kasutamine turvalüüsis
- (M) M 4.277 Windows Serverite SMB, LDAP ja RPC kommunikatsiooni kaitse
- (L) M 4.430 Logiandmete analüüs
- (L) M 4.431 Logimise jaoks oluliste andmete valik ja töötlemine
- (L) M 5.9 Serveri logi
- (L) M 5.171 Turvaline andmeside keskse logiserveriga
- (L) M 5.172 Turvaline aja sünkroniseerimine keskse logimise korral

Kasutusest kõrvaldamine

- (L) M 2.167 Andmete kustutamiseks või hävitamiseks sobivate lahenduste valik
- (L) M 2.496 Logiserveri korrakohane kasutusest kõrvaldamine

Valmisolek hädaolukorraks

- (M) M 6.96 Serveri avariiplaan

B 5.24 Veebiteenused

Kirjeldus

Selles moodulis peetakse veebiteenuste all silmas kõiki IT-teenuseid, mida teenusepakkuja osutab korraga ühele või ka mitmele teenusetarbijale (ingl consumer) ning millele tarbija pääseb juurde võrgupõhiste liidestega, st enamasti HTTP-protokolliga.

Erinevalt veebirakendustest (vt moodul B 5.21 Veebirakendused) puudub veebiteenustel kas klient-komponent või visuaalne veebiliides ning selle asemel saab veebiteenuse funktsioone kasutada kindlalt defineeritud liidese vahendusel, mille käivitab veebiteenuse tarbija (enamasti automaatselt). Veebiteenuseid võivad omakorda käivitada ka teised veebiteenused, et võimaldada omavahelises koostöös keerukamate funktsioonide kasutamist. Erinevate veebiteenuste ühendamist teatud funktsioonide osutamise eesmärgil nimetatakse ka orkestreerimisteks ning see võib standardsete liidesekirjelduste baasil toimuda ka dünaamiliselt. Selliseid kompleksse ülesehitusega arhitektuure nimetakse ka SOA-ks ning need võivad ka organisatsiooni piiridest väljapoole ulatuda.

Liidestena on sageli kasutusel kas XML-i põhine SOAP või objektipõhine REST-kontseptsioon. Veebiteenuste ja nende liideste kohta on avaldatud palju standardeid, mis on koondatud W-tüüpi meetmesse M 4.451 Veebiteenuste värsked standardid .

Selles moodulis käsitletakse veebiteenuseid nende käitaja vaatevinklist. Institutsioonid, kelle puhul on tegemist üksnes veebiteenuste tarbijatega, ei saa seda moodulit IT-etalonturbe modelleerimiseks kasutada, vaid peavad tuginema moodulitele B 1.11 Väljasttellimine (Outsourcing) .

Vaatamata tõsiasjale, et veebirakendused ja veebiteenused on teatud valdkondades üpris sarnased ja eeldavad kohati ka sarnaste turbemeetmete võtmist, on IT-etalonturbe kataloogides lahutatud need teemad kasutamise lihtsustamise eesmärgil siiski kaheks eraldi mooduliks. Kui tegemist on kasutajaliidest omava rakendusega, tuleks lähtuda veebirakenduste moodulist ning kui rakendus käivitatakse mõne standardse liidese kaudu, tuleks lähtuda veebiteenuste moodulist. Keerulisema struktuuriga rakenduste puhul, mis on ühelt poolt veebirakendused, kuid mis omakorda osutavad teistele IT-süsteemidele ka veebiteenuseid, tuleks IT-etalonturbe modelleerimisel rakendada mõlemat moodulit.

Ohud

Veebiteenuste kasutamisel peetakse oluliseks järgmisi ohuallikaid.

Organisatsioonilised puudused

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.7 Õiguste volitamata kasutamine
- G 2.22 Logiandmete analüüsimata jätmine
- G 2.27 Ebapiisav või puuduv dokumentatsioon
- G 2.61 Isikuandmete volitamatu kogumine
- G 2.67 Pääsuõiguste puudulik haldus
- G 2.87 Ebaturvalised protokollid avalikes võrkudes
- G 2.103 Töötajate ebapiisav koolitamine
- G 2.158 Veebirakenduste arendamise ja laiendamisega seotud puudused
- G 2.159 Isikuandmete ebapiisav turve veebirakendustes
- G 2.160 Ebapiisav või puuduv logimine
- G 2.181 Veebiteenuste rakendamise puudulik planeerimine ja kontseptsioon

Inimvead

- G 3.3 Hooletus turvameetmete suhtes
- G 3.16 Väär pääsuõiguste haldus
- G 3.38 Vead konfigureerimisel ja kasutamisel
- G 3.119 Standardite väär kasutamine
- G 3.120 Orkestreerimise vead
- G 3.121 Veebiteenuste konfigureerimise ja haldamise vead

Tehnilised rikked

- G 4.13 Salvestatud andmete hävimine
- G 4.22 Tüüptarkvara turvaaugud või vead
- G 4.33 Autentimise puudumine või puudulikkus
- G 4.35 Ebaturvaline krüptoalgoritm
- G 4.84 Veebirakenduste sisendi- ja välundiandmete ebapiisav valideerimine
- G 4.85 Veebirakenduste ebapiisav või puuduv tõrkekäsitlus
- G 4.87 Konfidentsiaalse info ilmsikstulek veebirakendustes
- G 4.94 Volitamata juurdepääs teise teenusetarbija andmetele veebirakendustes ja veebiteenustes

Ründed

- G 5.18 Süstemaatiline paroolide mõistatamine
- G 5.19 Kasutajaõiguste väärkasutus
- G 5.20 Administraatori õiguste väärkasutus
- G 5.28 Teenuse halvamine
- G 5.87 Veebilehe võltsimine
- G 5.131 SQL-injektsioon
- G 5.165 Volitamata juurdepääs veebirakenduse andmetele või andmete manipuleerimine
- G 5.167 Veebirakenduste loogikavead
- G 5.168 Veebirakenduste turbefunktsioonide kasutamise eiramine klientprogrammides

- G 5.169 Veebirakenduste ja veebiteenuste puudulik seansihaldus
- G 5.172 Veebirakenduste ja veebiteenuste autentimise eiramine
- G 5.173 Võõraste andmete ja pahavara koodi smugeldamine veebirakendustesse
- G 5.174 Injektsiooniründed
- G 5.179 Logide vastu suunatud ründed
- G 5.180 Registrite ja hoidlate vastu suunatud ründed
- G 5.181 Veebiteenuste isikutuvastuse ja pääsuõiguste halduse vastu suunatud ründed
- G 5.182 Marsruutide manipuleerimine (Routing Detours)
- G 5.183 XML-i vastu suunatud ründed
- G 5.184 Andmete hankimine veebiteenuste kaudu

Soovitatavad meetmed

Vaadeldava IT-koosluse turvalisuse tagamiseks tuleb lisaks käesolevale moodulile rakendada veel teisigi mooduleid vastavalt IT-etalonturbe rakendusjuhendi modelleerimise tulemustele.

Veebiteenuste kasutamisel tuleb võtta erinevaid meetmeid, tegeldes nt kontseptsiooni koostamise, soetamise ja käitamisega. Järgnevalt esitatakse ülevaade erinevatest kohustuslikest etappidest ja meetmetest, mida iga etapi puhul tuleks võtta. Alljärgnevalt kirjeldatud meetmed sobivad tavapäraste turbenõuete rahuldamiseks.

Planeerimine ja kontseptsioon

Nagu kõikide rakenduste puhul, luuakse ka veebiteenuste turvalise kasutamise eeldused juba selle planeerimise etapis. Ennekõike tähendab see kindlate vastutusalade kindlaksmääramist vastavalt meetmele M 2.1 IT kasutajate vastutuse ja reeglite kehtestamine .

Veebiteenuste arhitektuur ja nende teostus tuleb täpselt planeerida (M 4.458 Üleviimiste planeerimine ja ettevalmistamine) ja dokumenteerida (M 2.486 Veebirakenduste arhitektuuri dokumenteerimine). Olenevalt sellest, kas veebiteenustena hakatakse kasutama kolmandate isikute pakutavaid teenuseid või institutsiooni enda rakendusi, tuleb arvestada kas meetmega M 2.80 Tüüptarkvara nõuete kataloogi koostamine või M 2.487 Veebirakenduste arendamine ja laiendamine . Juhul kui veebiteenus hakkab asendama kas mõnda juba töötavat süsteemi või hakkab kasutama selle süsteemi andmeid, tuleb planeerimisetapis tegeleda ka migratsiooniga (M 2.530 Üleviimiste planeerimine ja ettevalmistus).

Planeerimisetapi oluliste teemade hulka kuulub ka veebiteenuse turve. Turbemeetmete kohta langetatavad otsused tuleks fikseerida kirjalikult (M 2.531 Veebiteenuste turvapoliitika väljatöötamine) ning turbemeetmed peaksid muu hulgas kajastama nt SQL-injektsioon-tüüpi ründeid (M 2.363 SQL-injektsiooni kaitse), erinevate teenusetarbijate ja kasutajate turvalist lahutamist (M 4.457 Teenusetarbijate turvaline lahutamine veebirakendustes ja veebiteenustes) ning liideste turvet (M 5.168 Taustsüsteemide turvaline sidumine veebirakendustega).

Soetamine

Veebiteenuste jaoks vajaminevate komponentide ja tootelahenduste soetamine peab olema arusaadav, toimima süsteemselt ja sisaldama ka IT-komponentide vastuvõtu ja kasutusloa väljastamise protsesse (M 2.62 Tarkvara vastuvõtuprotseduurid). Kui veebiteenuse käitaja soovib enda teenust pakkuda ka kolmandatele isikutele, tuleb mõelda ka veebiteenuse tarbijatega sõlmitavate lepingutingimuste sõnastamisele M 2.533 Veebiteenuste osutamise lepingutingimuste koostamine .

Rakendamine

Eriti siis, kui veebiteenust hakatakse osutama ka kolmandatele isikutele, on väga oluline, et teenuse pakkuja ja selle tarbijate vahel saaksid kõik turbeaspektid täpselt lahendatud ja reguleeritud (vt meede M 2.532 Veebiteenuste osutamine kolmandatele isikutele).

Veebiteenuste kasutuselevõtul on ühest küljest oluline tagada kõikide veebirakendustega sarnaste aspektide toimimine: sisestatavate ja väljastatavate andmete valideerimine (M 4.393 Sisestuste- ja väljastuste põhjalik valideerimine veebirakendustes), tugeva seansihalduse tagamine (M 4.394 Seansihaldus veebirakendustes), liigse teabe avalikustamise vältimine liidesekirjeldustes (M 4.395 Tõrkekäsitlus veebirakendustes ja M 4.400 Turbe seisukohalt oluliste andmete väljastamine veebirakendustes).

Teisalt aga tuleb pöörata ka piisavalt tähelepanu veebiteenuste spetsiifilistele turbeprobleemidele: see hõlmab ühelt poolt veebiteenuste kasutajate turvalist volitamist ja autentimist (M 4.456 Autentimine veebiteenustes) ja teisalt ka meetmeid, mis peavad tõkestama veebiteenuste volitamata kasutamist (M 4.454 Veebiteenuste kaitsmine keelatud kasutuse eest). Juhul kui veebiteenuste arhitektuuris nähakse ette ka pääsmikuteenuste kasutamist, tuleb arvestada ka meetmega M 4.453 Pääsmikuteenuse (Security Token Service) kasutamine .

Iga kord, kui veebiteenus käivitatakse, peab olema tagatud, et kasutajal on vastava funktsiooni käivitamiseks ka piisavad õigused (M 4.454 Veebiteenuste kaitsmine keelatud kasutuse eest). Veebiteenuse ja selle käivitaja vaheline andmeside peab olema sobivalt turvatud (M 4.350 DNS-serveri turvaline aluskonfiguratsioon) ja seda eelkõige juhtudel, kus andmeside kulgeb läbi ebaturvaliste võrkude.

Veebiteenuste puhul, mille liidestele on juurdepääs suurel hulgal inimestel või millele on tagatud juurdepääs ka avalikes võrkudes, tuleks võtta sobivaid meetmeid, mis ennetaksid veebiteenuste käideldavuse vastu suunatud ründeid (M 4.405 Ressursside blokeerimise (DoS-rünnete) tõkestamine veebirakendustes). Veebirakenduse ründekindluse suurendamiseks võib kaaluda ka XML-lüüsi kasutuselevõtmist (M 5.175 XML-lüüsi kasutamine).

Kasutamine

Veebiteenuste turvaline kasutamine eeldab asjakohase dokumentatsiooni haldamist ja teenusetarbijate õiguste juurutamist (seda ka juhul, kui veebiteenuse käivitab mõni rakendus või mõni teine veebiteenus, vt M 2.7 Süsteemi ja võrgu pääsuõiguste andmine ja M 2.31 Volitatud kasutajate ja õiguste profiilide dokumenteerimine).

Nii kasutajad kui ka administraatorid peavad olema turbemeetmetega piisavalt kursis (M 3.5 Turvameetmete koolitus).

Veebiteenuste kasutamine peab olema sobivate logimismehhanismide abil ka

tagantjärele analüüsitav (M 4.397 Veebirakenduste turvet puudutavate sündmuste logimine). Kuna logimine hõlmab sageli ka isikuandmeid, tuleb vastavate andmete käitlemisel arvestada ka andmekaitsenõuetega (M 2.110 Andmeprivaatsuse suunised logimisprotseduurides). Võimalike turvaintsidentide kiireks tuvastamiseks peab olema tagatud, et logifaile mitte ainult ei koostataks, vaid ka analüüsitaks (M 2.64 Logifailide kontroll), vajaduse korral automaatsüsteemidega.

Igapäevatöö käigus tehtavad muudatused tuleb teha hoolikalt (M 4.78 Konfiguratsioonimuudatuste hoolikas teostamine) ja muudatused tuleb ka dokumenteerida (M 2.34 IT-süsteemi muutuste dokumenteerimine). Eriti oluline on pöörata tähelepanu asjaolule, et teave ilmsiks tulnud turvaaukude kohta veebiteenustes või selle poolt kasutatavates komponentides, karkassides või teekides jõuaks ka veebiteenuse käitajani (M 2.35 Teabe hankimine turvaaukude kohta hta) ja et need turvaaugud saaksid ka likvideeritud või muul moel kõrvaldatud (M 2.273 Turvalisust mõjutavate paikade ja värskenduste kiire paigaldamine).

Veebiteenuste nõuetekohast ja tõrkevaba kasutamist tuleb toetada sobivate seiremeetmetega (M 4.452 Veebiteenuse seire). Regulaarne testimine, mis aitab välja selgitada võimalikke kitsaskohti, aitab muu hulgas ennetada ka ründeid (M 5.150 Penetratsioonitestide läbiviimine).

Valmisolek hädaolukorraks
Veebiteenuste hädaolukorraks ettevalmistuses on olulisel kohal sobiva andmevarunduskontseptsiooni juurutamine (M 6.32 Regulaarne andmevarundus).
Lisateavet veebiteenustega seotud hädaolukordade ennetamise ja likvideerimise kohta leiate meetmest M 6.154 Veebiteenuste hädaolukordade haldamine .

Planeerimine ja kontseptsioon

- (L) M 2.1 IT kasutajate vastutuse ja reeglite kehtestamine
- (L) M 2.80 Tüüptarkvara nõuete kataloogi koostamine
- (M) M 2.363 SQL-injektsiooni kaitse
- (L) M 2.486 Veebirakenduste arhitektuuri dokumenteerimine
- (M) M 2.487 Veebirakenduste arendamine ja laiendamine
- (M) M 2.530 Üleviimiste planeerimine ja ettevalmistus
- (L) M 2.531 Veebiteenuste turvapoliitika väljatöötamine
- (L) M 4.451w Veebiteenuste värsked standardid
- (M) M 4.457 Teenusetarbijate turvaline lahutamine veebirakendustes ja veebiteenustes
- (L) M 4.458 Veebiteenuste kasutuselevõtu planeerimine
- (L) M 5.168 Taustsüsteemide turvaline sidumine veebirakendustega

Soetamine

- (M) M 2.62 Tarkvara vastuvõtuprotseduurid
- (L) M 2.533 Veebiteenuste osutamise lepingutingimuste koostamine

Rakendamine

- (M) M 2.532 Veebiteenuste osutamine kolmandatele isikutele

- (M) M 4.393 Sisestuste- ja väljastuste põhjalik valideerimine veebirakendustes
- (L) M 4.394 Seansihaldus veebirakendustes
- (M) M 4.395 Tõrkekäsitlus veebirakendustes
- (L) M 4.405 Ressursside blokeerimise (DoS-rünnete) tõkestamine veebirakendustes
- (L) M 4.450 Veebiteenuste andmeside turve
- (M) M 4.453z Pääsmikuteenuse (Security Token Service) kasutamine
- (L) M 4.454 Veebiteenuste kaitsmine keelatud kasutuse eest
- (L) M 4.455 Volitamine veebiteenustes
- (L) M 4.456 Autentimine veebiteenustes
- (M) M 5.175z XML-lüüsi kasutamine

Kasutamine

- (L) M 2.8 IT-rakendustele ja andmetele pääsuõiguste andmine
- (L) M 2.31 Volitatud kasutajate ja õiguste profiilide dokumenteerimine
- (L) M 2.34 IT-süsteemi muutuste dokumenteerimine
- (M) M 2.35 Teabe hankimine turvaaukude kohta
- (L) M 2.64 Logifailide kontroll
- (L) M 2.110 Andmeprivaatsuse suunised logimisprotseduurides
- (L) M 2.273 Turvalisust mõjutavate paikade ja värskenduste kiire paigaldamine
- (L) M 3.5 Turvameetmete koolitus
- (L) M 4.78 Konfiguratsioonimuudatuste hoolikas teostamine
- (L) M 4.397 Veebirakenduste turvet puudutavate sündmuste logimine
- (M) M 4.400 Turbe seisukohalt oluliste andmete väljastamine veebirakendustes
- (L) M 4.452 Veebiteenuse seire
- (M) M 5.150 Penetratsioonitestide läbiviimine

Valmisolek hädaolukorraks

- (L) M 6.32 Regulaarne andmevarundus
- (M) M 6.154 Veebiteenuste hädaolukordade haldamine

B 5.25 Rakendused

Kirjeldus

Ametiasutuste ja ettevõtete toiminguid ja tööprotsesse toetab enamasti spetsiifiline rakendustarkvara (edaspidi lühidalt rakendused). Selleks otstarbeks ei ole IT-etalonturbe kataloogides ühtki spetsiaalset moodulit, st teemakohased ohukirjeldused ja meetmed puuduvad. Seevastu leidub aga kataloogide kihis nr 1 erinevaid mooduleid, milles käsitletakse vastavat haldusraamistikku, st rakendus-te kasutustsükli erinevate etappidega seotud protsesse ja tegutsemisjuhiseid.

Olulisemad neist on järgmised:

Üldkasutatavad

- B 1.3 Hädaplaanimine
- B 1.4 Andmevarunduspoliitika
- B 1.9 Riist- ja tarkvara haldus
- B 1.10 Tüüptarkvara
- B 1.14 Turvapaikade ja muudatuste haldus
- B 1.16 Nõuete haldus

Vajadusepõhised

- B 1.7 Krüptokontseptsioon
- B 1.11 Väljasttellimine (Outsourcing)
- B 1.12 Arhiveerimine

Nimetatud moodulites keskendutakse, kui mõned üksikud erandid kõrvale jätta, peamiselt infoturbe haldamisele ja IT-süsteemide kasutamise juhtimisele. Seevastu töötajate vastutusalasid seoses tootelahenduste valiku, kasutuselevõtu, käitamise ja ressursside väljavahetamisega puudutatakse loetletud moodulites vähe.

Selles moodulis käsitletakse rakenduste käitamise eest vastutavatele töötajatele kehtivaid peamisi infoturbe nõudeid. Järgnevas tekstiosas käsitletakse kokkuvõtlikult eelpool loetletud mooduleid ja viidatakse nendes moodulites kajastatud protsessidele. Kui nimetatud protsessid peaksid ITHS-i raamkontseptsioonides esile kutsuma muudatusi, nt seoses krüpteerimise kasutamise, andmevarunduse või hädaolukorraks ettevalmistusega, oleks mõistlik täiendada neid kontseptsioone vastava rakenduse eripäradest lähtudes.

Selles moodulis käsitletakse järgmist tüüpi rakendusi:

- institutsiooni enda või sellest väljaspool arendatud individuaaltarkvara;
- individuaalsete kohandustega tüüptarkvara, nt programmide muutmine või nende täiendamine spetsiifiliste moodulitega (customizing);

- tootja tarnitud tüüptarkvara, mis on kasutusse võetud üksnes spetsiifiliseks otstarbeks ja mis on konfigureeritud turbenõuete järgi.

Selles moodulis keskendutakse spetsiifiliseks otstarbeks välja töötatud kompleksetele rakendustele, nt personalihalduse tarkvara või sotsiaalvaldkonna andmete ja elukoharegistri andmete haldus. Valdkonna- ja funktsioonideülest tüüptarkvara, mille kasutusotstarve ei ole täpsemalt piiritletud, nt kontoritarkvara rakendusi, käsitletakse lähemalt moodulis B 1.10 Tüüptarkvara .

Olenevalt tarkvara tüübist ei pruugi kõiki selles moodulis soovitatud meetmeid olla võimalik järgida.

Käesolevas moodulis käsitletakse üldisi ohte ja standardseid turbemeetmeid, mille võtmine ei sõltu ühestki konkreetsest töö- ega halduprotsessist, mille raames vastavat rakendust kasutatakse. Seevastu võib teatud tüüpi rakenduste puhul selle mooduli kõrval lisamaterjalina appi võtta ka teisi täiendavaid mooduleid, nt B 5.13 SAP süsteem ja B 5.21 Veebirakendused .

Ohud

IT-etalonturbe seisukohalt loetakse rakenduste puhul tüüpilisteks järgmisi ohuallikaid:
Organisatsioonilised puudused

- G 2.3 Puuduvad, puudulikud või ühildumatud ressursid
- G 2.5 Hoolduse puudumine või puudulikkus
- G 2.7 Õiguste volitamata kasutamine
- G 2.9 Halb kohanemine IT muutustega
- G 2.22 Logiandmete analüüsimata jätmine
- G 2.26 Ebapiisavad või puuduvad tarkvara katsetamis- ja teavitusprotseduurid
- G 2.27 Ebapiisav või puuduv dokumentatsioon
- G 2.61 Isikuandmete volitamatu kogumine
- G 2.67 Pääsuõiguste puudulik haldus
- G 2.84 Puudused välisteenusepakkujaga sõlmitud lepingu tingimustes
- G 2.105 Õigusaktide ja lepinguliste kokkulepete rikkumine
- G 2. 151 Virtuaalsetel IT-süsteemidel kasutatavate rakenduste ebapiisav tootjatugi
- G 2.154 Ebasobivad rakendused terminaliserveritel kasutamiseks

Inimvead

- G 3. 1 Andmete konfidentsiaalsuse või tervikluse kadu kasutaja vea tõttu
- G 3.2 Seadme või andmete hävitamine hooletuse tõttu

Tehnilised rikked

- G 4.2 Sisevõrkude katkestus
- G 4.13 Salvestatud andmete hävimine
- G 4.22 Tüüptarkvara turvaaugud või vead
- G 4.39 Tarkvarakontseptsiooni viga
- G 4.43 Dokumenteerimata funktsioonid
- G 4.99 Rakenduste ebapiisavad või puuduvad turbemehhanismid

Ründed

- G 5.2 Andmete või tarkvara manipuleerimine

Soovitatavad meetmed

Vaadeldava IT-koosluse turvalisuse tagamiseks tuleb tavaliselt peale käesoleva mooduli rakendada veel teisigi mooduleid, mis selguvad IT-etalonturbe rakendusjuhendi põhjal tehtava modelleerimise tulemusel.

Rakenduste puhul tuleb võtta erinevaid meetmeid alates planeerimisest ja soetamisest ning lõpetades hädaolukorraks valmisoleku tagamise ja ressursside kasutusest kõrvaldamisega. Järgnevalt on esitatud ülevaade erinevatest kohustuslikest etappidest ja meetmetest, mida iga etapi puhul tuleks võtta.

Planeerimine ja kontseptsioon

Enne uue rakenduse soetamist või programmeerimist tuleb kindlaks määrata selle programmi kasutamise raamtingimused (vt M 2.546 Uute rakenduste nõuete analüüs). Selle hulka kuulub ka M 2.547 Rakendustele kehtivate õigusnormide väljaselgitamine ja dokumenteerimine .

Olenevalt rakenduse kasutusotstarbest võib juhtuda, et vastava tarkvara saab soetada juba valmis kujul ning seejärel tuleb seda hakata kohandama, kuid pole välistatud, et spetsiaalne tarkvara tuleb esmalt välja arendada. Selleks tuleks koostada nõuete kataloog (vt M 2.80 Tüüptarkvara nõuete kataloogi koostamine) või nõuetekogumik (vt M 2.458 Interneti kasutamise reeglistik).

Soetamine

Nõuete kataloogi konkreetsete ettekirjutuste põhjal saab kontrollida, kas saadaolev toode vastab planeeritud kasutusotstarbele. Sobivate toodete puudumisel võib kaaluda nt varianti, et tellida sobiva rakendustarkvara arendamise teenus mõnelt välisteenusepakkujalt (vt ka M 2.551 Nõuetekohase ja seadustele vastava hankemenetluse korraldamine).

Olukorras, kus institutsioon otsustab teenuse soetamisel, arendamisel või selle käitamisel kasutada välisteenusepakkujaid, tuleb selleks luua sobivad lepingulised raamtingimused (vt M 2.554 Rakenduste ostu-, arendamis- ja

käitamislepingute koostamine).

Rakendamine

Rakendusega arendustööde jaoks tuleb nõuetekogumiku põhjal välja töötada kohustuslike tööde loetelu (vt M 2.552 Kohustuslike tööde loetelu koostamine). Kohustuslike tööde loetelu koostamisel tuleb arvestada erinevate alamvaldkondadega. Alamvaldkondadena tuleks käsitleda nt rakenduse hooldamist (vt M 2.553 Rakenduste hoolduskontseptsiooni koostamine), kasutajate autentimist (vt M 2.555 Rakenduste autentimiskontseptsiooni koostamine) ja logimisfunktsiooni (vt M 2.500 IT-süsteemide logimine).

Rakenduse kasutuselevõtmisele peaksid eelnema katsetamine ja kasutusloa väljastamine (vt M 2.556 Rakenduste katsetamine ja kasutusloa väljastamine), turvaline installeerimine (vt M 4.463 Rakenduse turvaline installeerimine) ning administraatorite ja kasutajate koolitamine (vt M 3.4 Väljaõpe enne programmi tegelikku kasutamist).

Kasutamine

Rakenduse kasutamise etapis tuleb kanda hoolt selle eest, et turve oleks alati tagatud (vt M 4.464 Turbe tagamine rakenduste igapäevatöös).

Ressursside väljavahetamine

Rakenduse üleviimisel mõnda uude taristusse või rakenduse lõplikul kasutusest kõrvaldamisel tuleb vanas taristus hoolitseda desinstalleerimise eest (vt M 2.89 Tüüptarkvara deinstalleerimine), kustutada või hävitada mittevajalikud andmed (vt M 2.167 Andmete kustutamine või hävitamine) ja tagada, et vanas taristus toimuks ressursside nõuetekohane kasutusest kõrvaldamine (vt M 4.234 IT-süsteemide ja andmekandjate väljavahetamise kord).

Valmisolek hädaolukorraks

Lisateavet hädaolukordadeks ettevalmistamise kohta leiate meetmest M 6.158 Ettevalmistumine rakenduste hädaolukorraks . Juhul kui rakenduse välja arendanud teenusepakkuja puhul esineb oht, et teenusepakkuja ei suuda osutada piisavas mahus tugiteenuseid, nt maksejõuetuse tõttu, on soovitav lähtekood kolmandale poolele hoiule anda (vt HK.37 Usaldusele toetuv deponeerimine (Escrow)). Suurte käideldavusnõuete korral on soovitav koostada käideldavuse kontseptsioon (vt M 6.157 Rakenduste liiasuse kontseptsiooni koostamine).

Planeerimine ja kontseptsioon

- (L) M 2.40z Töötajate esinduse õigeaegne kaasamine
- (L) M 2.546 Uute rakenduste nõuete analüüs
- (L) M 2.547 Rakendustele kehtivate õigusnormide väljaselgitamine ja dokumenteerimine
- (L) M 2.548 Nõuetekogumiku koostamine
- (L) M 2.549 Simultaanteeninduse kontseptsiooni koostamine
- (L) M 2.550 Rakenduse arendamistööde nõuetekohane juhtimine

Soetamine

- (L) M 2.551z Nõuetekohase ja seadustele vastava hankemenetluse korraldamine
- (L) M 2.554z Rakenduste ostu-, arendamis- ja käitamislepingute koostamine

Rakendamine

- (L) M 2.552 Kohustuslike tööde loetelu koostamine
- (L) M 2.553 Rakenduste hoolduskontseptsiooni koostamine
- (L) M 2.555 Rakenduste autentimiskontseptsiooni koostamine
- (L) M 2.556 Rakenduste katsetamine ja kasutusloa väljastamine
- (L) M 4.463 Rakenduse turvaline installeerimine

Kasutamine

- (L) M 3.4 Väljaõpe enne programmi tegelikku kasutamist
- (M) M 4.464 Turbe tagamine rakenduste igapäevatöös

Ressursside väljavahetamine

- (L) M 2.89 Tüüptarkvara deinstalleerimine
- (M) M 2.167 Andmete kustutamine või hävitamine
- (M) M 4.234 IT-süsteemide ja andmekandjate väljavahetamise kord

Valmisolek hädaolukorraks

- (M) M 6.157z Rakenduste liiasuse kontseptsiooni koostamine
- (M) M 6.158 Ettevalmistumine rakenduste hädaolukorraks

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed
-
Teabe käideldavus (K)

- HK.37 Usaldusele toetuv deponeerimine (Escrow)

Teabe terviklus (T)
-
Teabe konfidentsiaalsus (S)
-

B 5.26 Teenustele suunatud struktuur

Kirjeldus

Teenustele suunatud struktuurid (SOA) kirjeldavad üldist lähenemist jagatud süsteemide rakendamiseks, et toetada asutusi IT abil tõhusalt nende äriprotsessides. Seejuures võtavad äriprotsessi üksikud tegevused üle teenused, mida võib uuesti kasutada ka muude äriprotsesside muude tegevuste jaoks. Teenuste koosmõju (orkestreerimise) kaudu saab rakendada näiteks uusi äriprotsesse. SOA kontseptsioon võimaldab lahendada erinevate osasüsteemide integreerimisel ja koostoimel tekkivaid probleeme.

Esitluse lähtepunkt on selles moodulis OASIS-i (Organization for the Advancement of Structured Information Standards) etalonmudel SOA-RM (Reference Model for Service Oriented Architecture, versioon 1.0), mis toetub muu hulgas ka taristul põhinevale teenuste keskkonnale, mis on esindatud Enterprise Service Bus'is (ESB) ja rakendusest sõltuvas transpordiprotokollis, nagu Simple Object Access Protocol (SOAP). Rakendusturvalisuse valdkonnas on SOAP turvastruktuuri jaoks olulise tähtsusega. SOAP on W3C protokolli standard, mis pakub ka vajalikke turvaprotokolli elemente, nagu WS-Security. Peale selle võimaldab SOAP standardiseeritud suhtlust jaotatud rakenduste ja objektide vahel, eriti SOA/ESB-keskkonnas. Kasutada võib ka muid XML-transpordikonteinereid, nagu REST (Representational State Transfer). Tänu SOAP paindlikkusele eelistatakse siin seda standardit.

SOA etalonmudel OASIS väljub moodulites B 5.21 Veebirakendused ja B 5.24 Veebiteenused kirjeldatud puhaste veebirakenduste piiridest ja iseloomustab üldist mudelit, kuidas teenuseid ja teenuseprofiile on just kasutaja kaudu jaotamisel võimalik kasutada ning uute omadustega siduda. Erinevate teenusepakkujate sellise teenuste kasutamise võimaldamiseks kasutatakse standardiseeritud teenuste juurdepääsupunkte.

Enamikus teenustele suunatud struktuurides kasutatakse sõnumivahetuseks SOAP-d ja transpordivahendina HTTP-d. SOAP kui suhtlusprotokoll ja HTTP kui transpordiprotokoll ei toeta oma põhivormis mingeid turbenõudeid. Andmeid vahendatakse pigem loetava teksti kujul. SOAP-sõnumeid vahetatakse enamasti HTTP abil SSL 3.0 või TLS 1.0 või 1.2 (HTTPS) kaudu.

SOAP-l põhinevatele platvormidele viiakse SOAP abil ülekantavate teabeobjektide jaoks täiendavalt sisse „objektikaitse" ja vahendamine toimub koos algse SOAP-teatega. Selline objektikaitse võib põhimõtteliselt koosneda järgmistest elementidest:

- teabeobjektide liigitamise andmed
- koostaja ja/või volitatud kasutaja andmed
- tervikluse kaitse andmed ja
- konfidentsiaalsuse kaitse andmed.

Esmase tehnoloogiana on selle jaoks välja kujunenud OASIS-standard WS-Security. WS-Security põhineb juba olemasolevatel standarditel, nagu XML-krüpteerimine, XML-allkirjad ja X.509-sertifikaadid. WS-Security on SOAP-standardi peamine laiendus, et see vastaks sõnumite terviklust, konfidentsiaalsust ja autentsust puudutavatele nõudmistele ja osalevatele üksustele. Seejuures kasutatakse SAML-il (Security Assertion Markup Language) põhinevat autentimist

ja volitamist.

Juurdepääs SOAP-l põhinevatele teabeobjektidele IT-süsteemides allub erinevatele pääsupiirangutele, kui nendele objektidele ei ole määratud vaba juurdepääsu õigust. Olulised kriteeriumid on siinjuures klassifikatsioon, nagu liigitamise aste ja täiendavad märgistused, plaanitav vastuvõtjate ring ning vajaduse korral teabe või selle osade aegumistähtaeg teabeobjektis.

Teabeobjektide pääsuandmed on märgitud sildile. Selleks, et muuta need lisaandmed (metaandmed) võltsimiskindlaks teabeobjekti kogu kasutusaja jooksul, tuleb need siduda kindlalt teabeobjektiga, nagu ka kõik muud SOAP-sõnumi koostisosad. See toimub tavaliselt lisa-allkirja abil.

Moodul esitab teenustele suunatud struktuuride ohud ja kirjeldab meetmeid, et IT-koosluse kaitse oleks piisav.

Ohud

Teenustele suunatud struktuuridega seonduva IT-etalonturbe puhul loetakse tüüpilisteks järgmisi ohte:

Töökorralduslikud puudused

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.19 Krüpteerimise halb korraldus
- G 2.27 Ebapiisav või puuduv dokumentatsioon
- G 2.66 Puudulik infoturbehaldus
- G 2.205 Puuduv hädaolukorra ennetamise kava teenusele suunatud arhitektuuride jaoks

Inimvead

- G 3.77 Infoturbe vähene aktsepteerimine

Tehnilised rikked

- G 4.22 Tüüptarkvara turvaaugud või vead
- G 4.33 Autentimise puudumine või puudulikkus
- G 4.35 Ebaturvaline krüptoalgoritm
- G 4.48 Välisteenusepakkuja süsteemide rike
- G 4.74 IT-komponentide tõrge virtualiseeritud keskkonnas
- G 4.87 Konfidentsiaalse info ilmsikstulek veebirakendustes

Ründed

- G 5.7 Liinide pealtkuulamine
- G 5.18 Süstemaatiline paroolide mõistatamine
- G 5.23 Pahavara
- G 5.28 Teenuse halvamine
- G 5.83 Krüptograafiliste võtmete paljastamine
- G 5.87 Veebilehe võltsimine

- G 5.143 Man-in-the-Middle tüüpi rünne
- G 5.170 Murdskriptimisründed (XSS)
- G 5.174 Injektsiooniründed
- G 5.179 Logide vastu suunatud ründed
- G 5.180 Registrite ja hoidlate vastu suunatud ründed
- G 5.181 Veebiteenuste isikutuvastuse ja pääsuõiguste halduse vastu suunatud ründed
- G 5.183 XML-i vastu suunatud ründed
- G 5.184 Andmete hankimine veebiteenuste kaudu

Soovitatavad meetmed

IT-koosluse turvalisuse tagamiseks tuleb tavaliselt lisaks sellele moodulile rakendada ka teisi, mis selguvad IT-etalonturbe rakendusjuhendi põhjal tehtava modelleerimise tulemusel. Üldistes moodulites ja vastavates süsteemi-, võrgu- ja rakenduste moodulites juba esitatud meetmeid siinkohal uuesti ei nimetata. Neid mooduleid ja meetmeid tuleb üksikjuhul rakendada nii, et need on ka SOA jaoks eesmärgipärased.

Teenustele suunatud struktuuride jaoks tuleks rakendada järgmisi kasutusaja etappide järgi struktureeritud meetmeid.

Planeerimine ja kontseptsioon

Teenustele suunatud keskkonna planeerimisel tuleb arvestada rea raamtingimustega. Esimeses etapis tuleb luua turvastruktuur SOA-l põhinevate süsteemide jaoks, mis võimaldab turvalist, jaotatud teenuse kasutamist ka väljaspool domeeni piire (vt nt M 2.1 IT kasutajate vastutuse ja reeglite kehtestamine , M 2.378z Süsteemiarendus ja M 2.561 Standardikohaste SOA-rakenduste ja konfiguratsioonide loomine). SOA-l põhinevate süsteemide omavahelisel suhtlemisel tuleks alaliste homogeensete XML-transpordikonteinerite korral kasutada integreeritud turvamehhanisme. Esmase tehnoloogiana on selle jaoks välja kujunenud OASIS-standard WS-Security. Seejuures tuleks kasutada SAML-il (Security Assertion Markup Language) põhinevat autentimist ja volitamist.

Teostus

SOA-l põhineva lähenemise kasutamisel tuleks tähelepanu pöörata sellele, et osalejate (nt klient, server) vaheline suhtlemine on kaitstud (M 4.450 Veebiteenuste andmeside turve) ja et ressursid on kaitstud blokeerimise eest (vt M 4.405 Ressursside blokeerimise (DoS-rünnete) tõkestamine veebirakendustesja veebiteenustes). Peale selle tuleb kasutada asjakohast sisestuste ja väljastuste valideerimist (vt M 4.393 Sisestuste- ja väljastuste põhjalik valideerimine veebirakendustes ja veebiteenustes). Kui SOA-s kantakse üle konfidentsiaalseid andmeid, tuleb täiendavalt kaitsta ka XML-transpordikonteinerit (vt M 4.473 XML-transpordikonteinerite pealtkuulamise kaitse SOA-s). Lisaks peaksid ründevõimalused Backend-rakendustele olema piiratud vahelelülitatud autentimis- ja autoriseerimisvahenditega (vt M 4.474 Turvaaukude kaitse SOA Backend-rakendustes).

Kasutamine

Tuleb takistada seda, et kasutajad muudavad jaotatud SOA-keskkonna kasutajakeskkonda. Samuti tuleb tagada, et nad pääsevad ligi ainult nendele ressurssidele, millele nad ligi pääsema peavad (vt M 4.453z Pääsmikuteenuse (Security Token Service) kasutamine ja M 4.480 WS-Resource'i kaitse SOA-keskkondades). Kui teenusetarbija ja teenuseosutaja vaheline ühendus toimub ebaturvalise võrgu kaudu, tuleb kasutusele võtta abinõud, et suhtlust ei oleks võimalik pealt kuulata, muuta ega segada (vt M 5.68z Krüpteerimisprotseduuride kasutamine võrgusuhtluses).

Valmisolek hädaolukorraks

Üksikute teenuste tõrge SOA-keskkonnas tuleks niipea kui võimalik kompenseerida liiasusega teenuseosutajate kasutamise kaudu (vt M 6.161 Liiasusega riistvarakomponendid teenustele suunatud arhitektuurides). Et üksikute teenuseosutajate tõrke korral võib see puudutada suuremat osa kasutajatest, tuleb võtta meetmeid, et sellest tulenevad kahjustused oleksid võimalikult väikesed. Seetõttu tuleb Business Continuity Plan'is kirjeldada kõiki meetmeid, mis on vajalikud, kui üksikute teenuseosutajate tõrke korral on töö SOA-keskkonnas piiratud (vt M 6.160 Hädaolukorra ennetamise kava SOA-keskkondade jaoks).

Järgneb ülevaade mooduli „SOA" meetmete paketist.

Planeerimine ja kontseptsioon

- (L) M 2.1 IT kasutajate vastutuse ja reeglite kehtestamine
- (L) M 2.378z Süsteemiarendus
- (L) M 2.560 SOA-l põhineva need-to-share-kontseptsiooni integreerimine turbehaldusesse
- (L) M 2.561 Standardikohaste SOA-rakenduste ja konfiguratsioonide loomine
- (L) M 5.68z Krüpteerimisprotseduuride kasutamine võrgusuhtluses

Teostus

- (L) M 2.447 Virtuaalsete IT-süsteemide turvaline kasutamine
- (M) M 4.393 Sisestuste- ja väljastuste põhjalik valideerimine veebirakendustes ja veebiteenustes
- (M) M 4.400 Turbe seisukohalt oluliste andmete väljastamine veebirakendustes
- (L) M 4.405 Ressursside blokeerimise (DoS-rünnete) tõkestamine veebirakendustesja veebiteenustes
- (L) M 4.450 Veebiteenuste andmeside turve
- (L) M 4.453z Pääsmikuteenuse (Security Token Service) kasutamine
- (L) M 4.454 Veebiteenuste kaitsmine keelatud kasutuse eest
- (M) M 4.473 XML-transpordikonteinerite pealtkuulamise kaitse SOA-s
- (M) M 4.474 Turvaaukude kaitse SOA Backend-rakendustes
- (M) M 4.475 Kaitse identiteeditеenuste teesklusrünnete vastu
- (L) M 5.175z XML-lüüsi kasutamine

Kasutamine

- (L) M 3.5 Turvameetmete koolitus
- (M) M 4.476 WS-Notification-Subscription'i kaitse Broker'is
- (M) M 4.477 WS-Notification-Subscription'i kaitse
- (M) M 4.479 Poliitikate kaitse SOA-s
- (L) M 4.480 WS-Resource'i kaitse SOA-keskkondades
- (L) M 4.481 Ühendusevaba SOAP-suhtluse turvaline kasutamine
- (L) M 5.147 Turvalise side tagamine kataloogiteenuste abil
- (L) M 5.150 Penetratsioonitestide läbiviimine

Valmisolek hädaolukorraks

- (L) M 6.160 Hädaolukorra ennetamise kava SOA-keskkondade jaoks
- (L) M 6.161 Liiasusega riistvarakomponendid teenustele suunatud arhitektuurides
- (L) M 6.162z Reageerimine krüpteerimismeetodi praktilise nõrgenemise korral

B 5.27 Tarkvaraarendus

Kirjeldus

Sageli ei ole kasutada oleva tüüptarkvara funktsioonidel oodatud ulatust või ei vasta see soovitud nõudmistele. Samuti on paljudes asutustes kasutusel individuaalselt väljatöötatud tarkvaratooted, mis on vananenud või mida tuleb laiendada lisafunktsioonidega, et neid oleks võimalik kohandada uutele või muutunud äriprotsessidele. Neile nõudmistele suudab sageli vastata üksnes organisatsioonisisene tarkvara.

Tarkvaraarenduse moodul käsitleb kõiki asjakohaseid aspekte, millega asutused peavad firmasisese tarkvara kasutamise korral arvestama. Selleks vaadeldakse asutusepoolset ettevalmistust, realiseerimist ja kasutuselevõtmist ning tehakse kindlaks sellele vastavad ohud ja meetmed.

Moodul ei kujuta endast üldiste protseduuride täielikku juhendit tarkvaraarendusel, vaid keskendub tarkvaraarenduse infoturbe asjakohastele aspektidele. Selle mooduliga täiendatakse mooduleid B 5.25 Rakendused ja B 1.10 Tüüptarkvara konkreetsete firmasisese arenduse rakendusjuhistega.

Ohud

IT-etalonturbe seisukohalt loetakse tarkvaraarenduse puhul tüüpilisteks järgmisi ohuallikaid.

Vääramatu jõud

- G 1.2 IT-süsteemi avarii

Töökorralduslikud puudused

- G 2.1 Reeglite puudumine või puudulikkus
- G 2.2 Reeglite puudulik tundmine
- G 2.4 Turvameetmete ebapiisav järelevalve
- G 2.7 Õiguste volitamata kasutamine
- G 2.26 Ebapiisavad või puuduvad tarkvara katsetamis- ja teavitusprotseduurid
- G 2.27 Ebapiisav või puuduv dokumentatsioon
- G 2.28 Autoriõiguste rikkumine
- G 2.29 Tarkvara testimine tootmisandmetega
- G 2.66 Puudulik infoturbehaldus
- G 2.67 Pääsuõiguste puudulik haldus
- G 2.87 Ebaturvalised protokollid avalikes võrkudes
- G 2.209 Tarkvara jaoks väära arenduskeskkonna valimine
- G 2.210 Arenduskeskkondade ebapiisavalt turvatud kasutamine
- G 2.211 Väära protsessimudeli valik tarkvaraarenduseks
- G 2.212 Ebapiisav arvestamine konfiguratsioonivalikutega tarkvaraarenduses

- G 2.213 Tarkvaraarenduse protsessi puuduv või puudulik kvaliteedi tagamine

Inimvead

- G 3. 1 Andmete konfidentsiaalsuse või tervikluse kadu kasutaja vea tõttu
- G 3.3 Hooletus turvameetmete suhtes
- G 3.9 IT-süsteemi väär haldus
- G 3.16 Väär pääsuõiguste haldus
- G 3.32 Seaduste rikkumine krüptoprotseduuride kasutamisel

Tehnilised rikked

- G 4.33 Autentimise puudumine või puudulikkus
- G 4.35 Ebaturvaline krüptoalgoritm
- G 4.39 Tarkvarakontseptsiooni viga

Ründed

- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.9 IT-süsteemide volitamata kasutamine
- G 5.21 Trooja hobused
- G 5.23 Pahavara
- G 5.28 Teenuse halvamine
- G 5.71 Tundliku informatsiooni konfidentsiaalsuse kadu
- G 5.84 Võltsitud sertifikaadid
- G 5.85 Tundliku informatsiooni tervikluse kadu

Soovitatavad meetmed

IT-koosluse turvalisuse tagamiseks tuleb tavaliselt lisaks sellele moodulile rakendada ka teisi, mis selguvad IT-etalonturbe rakendusjuhendi põhjal tehtava modelleerimise tulemusel.

Kui väljatöötatud tarkvara rakendatakse tootmisprotsessi, tuleb lisaks järgida ka üldise mooduli B 1.10 Tüüptarkvara töökorralduslikke aspekte. Lisaks kirjeldatakse moodulis B 5.25 Rakendused tarkvara rakendamise protseduure ja neid tuleb alati koos kõnealuse mooduliga arvesse võtta. Eriti kehtivad individuaalselt väljatöötatud tarkvara korral ühtviisi nii kasutamise, kasutusest kõrvaldamise kui ka hädaolukorra ennetamise etapid. Veebirakenduste arendamisel tuleb järgida moodulit B 5.21 Veebirakendused .

Planeerimine ja kontseptsioon

Tarkvara arendamisel on oluline hoolikas planeerimine ja kontseptsioon. Kindlaks tuleb määrata vastutusalad (vt M 2.569 Rollide ja vastutuse määratlemine tarkvaraarenduses) ja valida välja protsessimudel (vt M 2.570 Protsessimudeli valik tarkvaraarenduse jaoks). Kogu tarkvaraarenduse korral tuleb arvesse võtta

ka seadusi ja ettekirjutusi (vt M 2.571 Vastavusnõuete järgimine tarkvaraarenduse jaoks).

Soetamine

Valida tuleb asjakohane arenduskeskkond (vt M 4.493 Arenduskeskkonna valimine tarkvaraarenduse jaoks ja M 2.567 Usaldusväärsete arendustööriistade valik).Tarkvaraarenduse tööriistad tuleks soetada standardsete ja dokumenteeritud protseduuride järgi (vt M 2.572 Tööriistade soetamine tarkvaraarenduse jaoks).

Teostus

Tarkvaraarenduse ajal tuleb arenduskeskkonda kasutada turvaliselt (vt M 4.494 Arenduskeskkonna turvaline kasutamine).Tarkvarakujundus peab olema võimalikult turvaline (vt M 4.495 Tarkvaraarenduse turvaline süsteemikujundus) ning selle rakendamine peab olema samuti võimalikult turvaline (vt M 2.573 Kinnipidamine turvalisest protseduurist tarkvaraarenduses ja M 4.42z Turvafunktsioonide rakendamine IT-rakenduses).Tarkvaraarenduse tulemusi tuleb enne produktiivset kasutuselevõtmist piisavalt katsetada (vt M 2.468z Tarkvaralitsentsid terminaliserveri keskkonnas). Kogu arendusprotsess tuleb täielikult dokumenteerida (vt M 2.574 Tarkvaraarenduse põhjalik dokumenteerimine) ja selles osalevaid töötajaid vastavalt koolitada (vt M 3.97 Projektimeeskonna koolitamine tarkvaraarenduse jaoks).

Kasutamine

Kasutuselevõtmise jaoks tuleb tarkvara turvaliselt installeerida (vt M 4.496 Väljatöötatud tarkvara turvaline installeerimine). Viivitamata tuleb paigaldada asjakohased paigad ja värskendused (vt M 2.273 Turvalisust mõjutavate paikade ja värskenduste kiire paigaldamine). Hoolikalt tuleb teostada muudatused ja konfiguratsioon (vt M 4.78 Konfiguratsioonimuudatuste hoolikas teostamine).Tarkvara terviklust tuleb korrapäraselt kontrollida (vt M 4.93z Regulaarne tervikluse kontroll).

Kasutusest kõrvaldamine

Individuaalselt väljatöötatud tarkvara kasutusest kõrvaldamine toimub analoogselt tüüptarkvarale (vt B 1.10 Tüüptarkvara ja B 5.25 Rakendused).

Valmisolek hädaolukorraks

Võimalike tõrgete ennetamiseks tuleb võtta meetmeid hädaolukorraks valmisoleku jaoks (vt M 6.164 Valmisolek hädaolukorraks tarkvaraarenduses). Selleks, et tarkvaraarendust ei takistaks ootamatud andmekaod arendussüsteemides, tuleb arendusandmeid korrapäraselt varundada (vt M 6.32 Regulaarne andmevarundus).

Planeerimine ja kontseptsioon

- (L) M 2.164 Sobiva krüptoprotseduuri valimine
- (L) M 2.569 Rollide ja vastutuse määratlemine tarkvaraarenduses
- (L) M 2.570 Protsessimudeli valik tarkvaraarenduse jaoks
- (L) M 2.571 Vastavusnõuete järgimine tarkvaraarenduse jaoks

- (L) M 4.34z Krüpteerimise, kontrollsummade ja digitaalallkirjade rakendamine

Soetamine

- (L) M 2.567 Usaldusväärsete arendustööriistade valik
- (L) M 2.572z Tööriistade soetamine tarkvaraarenduse jaoks
- (L) M 4.493z Arenduskeskkonna valimine tarkvaraarenduse jaoks

Teostus

- (L) M 2.568 Tarkvara testimisprotseduurid
- (L) M 2.573 Kinnipidamine turvalisest protseduurist tarkvaraarenduses
- (L) M 2.574 Tarkvaraarenduse põhjalik dokumenteerimine
- (L) M 3.97 Projektimeeskonna koolitamine tarkvaraarenduse jaoks
- (L) M 4.42z Turvafunktsioonide rakendamine IT-rakenduses
- (L) M 4.95 Minimaalne operatsioonisüsteem
- (M) M 4.494 Arenduskeskkonna turvaline kasutamine
- (L) M 4.495 Tarkvaraarenduse turvaline süsteemikujundus

Kasutamine

- (L) M 2.273 Turvalisust mõjutavate paikade ja värskenduste kiire paigaldamine
- (L) M 2.575 Tarkvara arenduskeskkonna korrapärane turvaaudit
- (L) M 4.33 Viirustõrjeprogrammi kasutamine andmekandjate vahetamisel ja andmete edastamisel
- (L) M 4.78 Konfiguratsioonimuudatuste hoolikas teostamine
- (L) M 4.93z Regulaarne tervikluse kontroll
- (L) M 4.496 Väljatöötatud tarkvara turvaline installeerimine

Valmisolek hädaolukorraks

- (L) M 6.32 Regulaarne andmevarundus
- (L) M 6.41 Andmete taastamise harjutamine
- (L) M 6.164 Valmisolek hädaolukorraks tarkvaraarenduses

B 5.E2 ID-kaart/PKI

ID kaart, mobiil-ID ja PKI on Eesti-põhine ja Eestis laialt kasutusel olev üksteisega seotud IT taristuvahendite kogum, mis täidab peamiselt nelja eesmärki:

- turvaline digiallkirjastamine ehk digisigneerimine
- turvaline digitembeldamine
- turvaline autentimine nii veebipõhistesse kui ka lokaalkeskkondadesse
- transpordikrüpto realiseerimine – failide krüpteerimine transpordifaasis nende konfidentsiaalsuse tagamise (semantilise sisu peitmise) eesmärgil

PKI all tuleb käesolevas dokumendis mõista pigem kogu ID-kaardi ökosüsteemi, mitte kitsast tehnoloogilist (avaliku võtmega krüptosüsteemidel põhinevat) lahendust. Ökosüsteemi hõlmab ID-kaarti, mobiil-ID-d, nende baastarkvara, sertifitseerimisteenuseid, vastavat õigusruumi jne.

Kõikide nimetatud vahendite kasutamine põhineb avaliku võtmega krüptograafial, kus krüptovõtmed esinevad (genereeritakse) võtmepaaridena ning ühe võtmega krüpteeritud (šifreeritud) teavet saab dešifreerida paarilis-võtmega. Tavaliselt nimetatakse neid võtmeid kasutusotstarbe järgi avalikuks võtmeks ja privaatvõtmeks - esimene neist on kõigile avalik, teine aga kasutaja ainuvalduses.

Turvaliseks vahendiks teeb avaliku võtmega krüptograafia võimalus realiseerida see tarkvara kõrval vajadusel ka pöördkonstrueerimatu (non-reverse-engineerable) riistvaraseadmena. Sel korral genereeritakse võtmepaar mikrokiibina realiseeritud riistvaraseadmes, kust avaliku võtme saab välja lugeda, kuid privaatvõtit pole ID kaardi lahenduste konstruktiivsete eripärade tõttu kiibist välja lugeda võimalik ning see säilib vaid ainueksemplarina kiibi sees. Privaatvõti jääb sel korral kiibi sisse kogu oma kasutuse (elutsükli) vältel, kus seda saab teatud parooli ehk PIN-koodi teades krüpteerimiseks ehk signeerimiseks kasutada. Nii võtmepaari ülekirjutamisel kui ka seadme rikkiminekul või hävimisel kaob privaatvõtme ainueksemplar seega jäädavalt ja lõplikult.

Krüpteerimiseks/signeerimiseks ilma seadme/võtmepaari omaniku nõusoleku ja/või teadmiseta peab potentsiaalne ründaja tegema lihtründe asemel kompleksründe, mis koosneb kahest ründest. Esmalt peab ta saama oma valdusse seadme (kiibi), millele lisaks ta peab teada saama seadet käivitava parooli ehk PIN-koodi. Ainuüksi seadme (kiibi) hõivamine, niisamuti nagu ka vaid PIN-koodi hõivamine, ei võimalda rünnet teostada. Kui seadme valdaja nii seadet kui ka seda aktiveerivat PIN-koodi piisavalt korralikult hoiab, on kahest ründest koosneva kompleksründe eduka sooritamise tõenäosus vägagi väike. Seetõttu saab rääkida paljude teiste lahendustega võrreldes oluliselt turvalisemast signeerimisest, autentimisest või krüpteerimisest. Samal põhjusel saab teatud erijuhtumeil rääkida digiallkirjast ehk digitaalallkirjast – selleks on teatud täiendavate omaduste ja lisa-atribuutidega digi(taal)signatuur, mille andmine toob kaasa samasuguseid õiguslikke tagajärgi kui paberdokumendile omakäelise allkirja andmine.

Et siduda niisugune võtmepaar (täpsemalt – võtmepaari genereerinud ja privaatvõtit sisaldav seade) püsivalt selle omaniku kui kindla subjektiga, on ellu kutsutud PKI ehk avaliku võtme taristu (public key infrastructure). PKI põhineb sertifitseerimisel, mille käigus seotakse avalik võti võtmepaari omanikku identifitseerivate andmetega. Füüsilise isiku korral seotakse avalik võti nime ja isikukoodiga, juriidilise isiku korral Äriregistri registrikoodiga, serveri korral IP- või DNS-aadressiga (FQDN-aadressiga) või nimega.

Sertifitseerimise all tuleb käesolevas mõista genereeritud dokumenti, milles puudub igasugune kvalitatiivne hinnang, selle tulemusena seotakse vaid olemi identiteet ta võtmepaari avaliku võtmega. Sertifitseerimise tulemuseks on tavaliselt digikujul sertifikaat, kus seesugune sidumine on tehtud privaatvõtmega krüpteerimise ehk signeerimise abil. Tavaliselt teostavad sertifitseerimist – st annavad välja sertifikaate – sertifitseerimisteenuse osutajad kui usaldusväärsed kolmandad osapooled. Riikliku taristu korral on sertifitseerimisteenuse osutajatele pandud tavaliselt õigusaktidega jm normdokumentidega hulk lisatingimusi.

Füüsiliste isikute tarbeks on Eestis on hetkel levinud kolm eelmainitud põhimõtetele vastavat turvalist pöördkonstrueerimatut seadet:

- ISO 7816-standardi kiipkaardina kujundatud ID-kaart (õiguslikus keeles isikutunnistus)
- ISO 7816-standardi kiipkaardina kujundatud digi-ID ehk õiguslikus keeles digitaalne isikutunnistus
- Mobiil-ID, mis on realiseeritud GSM-standardi mobiiltelefoni SIM-kaardi lisafunktsionaalsusena.

Kõik nimetatud kolm seadet võimaldavad anda Eesti seaduste kohast, õiguslikku tähendust omavat digiallkirja. Samuti lubavad kõik kolm seadet kasutajal end turvaliselt autentida nii veebipõhistes keskkondades kui ka lokaalsüsteemides.

Digiallkirjastamine on vajalik juhtumeil, kui digikujul failile on vaja anda dokumendi staatus ehk tõestusväärtuse omadus, sidudes faili püsivalt ta looja või allkirjastajaga. Kuna peaaegu kogu kaasaja IT maailm põhineb korduvkirjutatavatel andmekandjatel, siis pole tavalise, ilma digiallkirjastamata faili korral üldjuhul võimalik tuvastada selle muutjaid ja muutmisi, sh ka seda, kas fail on loodud väidetava looja poolt ning seda pole hiljem kuritahtlikult muudetud.

Vastavalt digitaalallkirja seadusele on digiallkirjaga varustatud digidokumendil omakäelise allkirjaga varustatud paberdokumendiga võrdne õiguslik staatus. Seda aspekti tuleb asjaajamise üleviimisel paberdokumentidelt digimaailma läbivalt arvestada. Need dokumendid, mis paberkandjal on varustatud omakäelise allkirjaga, peaksid digikujul olema üldjuhul varustatud digiallkirjaga.

Digiallkirjastamine ei ole seotud konkreetse tehnoloogiaga (DDOC, BDOC jms).

Täna salvestatakse digiallkirjastatud failid BDOC-vormingus ning neid saab luua ning lugeda nii DigiDOCi klientprogrammiga, mitmete veebipõhiste portaalidega kui ka muude tarkvaraliste vahenditega. Viimaste loomiseks on tarkvaraarendajate jaoks koostatud vastavad teegid (täpsemalt vt http://www.id.ee/).

Vanim ja kasutatavaim on neist vahenditest ID-kaart, mida hakati välja andma juba 2002. aastal ning mille omamine siseriikliku (ja Euroopa Liidus aktsepteeritava) isikutunnistusena on vastavalt kehtivatele õigusaktidele Eesti kodanikele kohustuslik. Et ID-kaart toimiks tavalise isikut tõendava dokumendina, on sellele lisatud ka visuaalne pool. Samuti on ID-kaardis olemas ka visuaalset poolt suuresti dubleeriv avalik andmefail, mille saab sealt välja lugeda ilma PIN-koodideta.

Digi-ID ehk digitaalne isikutunnistus erineb ID-kaardist selle poolest, et tal puudub visuaalne pool ning seda ei saa kasutada isikut tõendava dokumendina, vaid ainult digiteenuste juures. Digi-ID on mõeldud esmajoones kasutamiseks ID-kaardi varuseadmena digimaailmas juhtumeil, kui ID-kaardiga peaks midagi juhtuma. Digi-ID-d saab taotleda kehtiva ID-kaardi olemasolul või koos sellega; vt lähemalt http://www.politsei.ee/et/teenused/isikut-toendavad-dokumendid/digi-id/ .

Kõik nimetatud kolm seadet sisaldavad endas kahte avaliku võtmega krüptoalgoritmi võtmepaari – üht turvaliseks autentimiseks, teist digiallkirja andmiseks ehk signeerimiseks. Autoriseerimise võtmepaari pääseb kasutama PIN1 -koodi sisestades, allkirjastamise võtmepaari aga PIN2 -koodi sisestades. PUK-kood on mõeldud vahendi PIN-koodide vahetamiseks.

ID-kaardi ja digi-ID korral saab autentimiseks ehk autoriseerimiseks kasutatavat võtmepaari lisaks kasutada veel failide krüpteerimiseks nende transpordi tarbeks ehk transpordikrüpto realiseerimiseks. Sel korral krüpteeritakse fail adressaadi avaliku võtmega (sertifikaadiga), dešifreerida saab seda adressaadi või adressaatide ID-kaardiga autoriseerimise võtmepaari ja PIN1-koodi kasutades. Krüpteeritud fail salvestatakse tihtipeale CDOC-vormingus.

Mobiil-ID ei ole iseseisev PKI-seade, isik ei saa seda kasutusele võtta ilma eelnevalt ID-kaardi abil aktiveerimata. Mobiil-ID kaardi poolt genereeritud võtmepaari avalik võti seotakse ID-kaardi võtmepaariga signeeritud sertifikaadiga.

Mobiil-ID-d saab taotleda kehtiva ID-kaardi olemasolul, vt lähemalt http://www.politsei.ee/et/teenused/isikut-toendavad-dokumendid/mobiil-id/. Mobiil-ID korral toimub side turvalise seadme ja arvuti vahel üle mobiiltelefoni ja mobiilioperaatori, PIN-koodid sisestatakse sel juhul mobiiltelefonilt. Mobiil-ID-d (ja selle võimalusega SIM-kaarte) pakuvad Eestis kõik kolm peamist

mobiilsideoperaatorit – EMT, Elisa ja TELE2.

ID-kaardi roll nii digi-ID kui ka mobiil-ID juures seisneb seadme aktiveerimisel – kui need seadmed on ID-kaardi abil aktiveeritud, siis ID-kaardi või sellele kantud sertifikaatide kehtetuks tunnistamine ei muuda kord aktiveeritud digi-ID ega mobiil-ID aktiveeritusi.

Oluline roll turvalisel digiallkirjastamisel ja autentimisel on sertifitseerimisteenusel ja sellega kaasnevatel teenustel. Eesti PKI-taristus on hetkel ainukeseks teenusepakkujaks Sertifitseerimiskeskuse AS , kelle välja antud on nii ID-kaardile, digi-ID-le kui ka mobiil-ID võimaluse SIM kaardile kantud sertifikaadid. Kõik väljaantud sertifikaadid on lisaks saadavad ka Sertifitseerimiskeskuse ASi poolt peetavas avalikus LDAP-kataloogiteenuses (aadressil ldap://ldap.sk .ee), kust neid saab igaüks sertifikaadi omaniku isikukoodi teades otsida ja alla laadida. Viimane tegevus on vajalik näiteks CDOC-krüpteerimiseks.

Juhuks kui privaatvõtme kandja väljub kasutaja ainuvaldusest, on ellu kutsutud sertifikaatide peatamine ja tühistamine, mida saab teha sertifitseerimisteenuse osutaja juures mitmetel mugavatel onlain -viisidel. Peatatud sertifikaadiga seotud võtmepaariga turvaliselt autentida ega digiallkirja anda ei saa. Peatatud sertifikaadi saab edaspidi kas lõplikult tühistada või peatatuse lõpetada; viimasel juhul taastub kõikide peatamise eelsete teenuste tegemise võimalus.

Et sertifikaadi peatamine oleks tehniliselt võimalik, on digiallkirjastamise juures ellu kutsutud kehtivuskinnitusteenus. Digiallkirjastamise käigus võetakse ühe viimase tegevusena ühendust Sertifitseerimiskeskuse ASi OCSP-teenusega, mille tulemusena varustatakse digiallkiri automaatselt kehtivuskinnitusega. Kehtivuskinnitus sisaldab digiallkirja andmise aega (millel on muuhulgas ka tõestusväärtus) ning krüptograafilist tõestust selle kohta, et allkirja andmise hetkel oli sertifikaat kehtiv, st ei olnud peatatud ega tühistatud. Kehtivuskinnitus on kõikide digiallkirjade kohustuslik element – ilma selleta ei ole digiallkirjade autentsuses hiljem võimalik veenduda.

Kehtivuskinnituse saamine eeldab juurdepääsu vastavale teenusele, mida tavaliselt realiseeritakse spetsiaalse juurdepääsutõendi näol allkirja andvas tarkvaras. Juurdepääsutõend tuleb tellida Sertifitseerimiskeskuse ASilt. Ilma juurdepääsutõendita ei ole võimalik digiallkirjale kehtivuskinnitust saada, seega digiallkirja anda. Juurdepääsutõendi hankimine on üldjuhul tasuline protsess, kusjuures tasuda tuleb allkirjade arvu pealt. Eraisiku jaoks ühes kuus võimalik anda tasuta kuni kümme digiallkirja. Täpsemaid juurdepääsutõendi hankimise

tingimusi näebSertifiteerimiskeskuse ASi veebilehelt http://www.sk.ee.

Digitempel on digiallkirja analoog juriidiliste isikute (asutuste) jaoks. Kui digiallkiri seob faili (või failid) püsivalt füüsilise isikuga, siis digitempel seob faili (või failid) juriidilise isikuga. Digitempli krüptotehnilised põhimõtted on digiallkirjaga identsed, kuid digitempli praktilisel realiseerimisel on mõningaid eripärasid:

- erinevalt digiallkrija andmise vahendist (ID-kaart, mobiil-ID) on digitempel hetkel realiseeritud krüptopulgal;
- erinevalt digiallkirjast on digitempli korral realiseeritud mitmete dokumentide automaatse tembeldamise võimalus, kus PIN2-kood tuleb sisestada vaid korra - vt http://www.sk.ee/teenused/digitempli-teenus/tempelplus/ ;
- digitempel on Sertifitseerimisekeskuse ASi ärilahendus, millel on digitaalallkirja seaduse tugi

Digitempel tõendab, et dokument on pärit sellest asutusest, kelle digitempel dokumendil on. Seega on digitempel pitsati jäljend ja/või turvablanketi analoog digimaailmas.

ID-kaardi ja teiste ülalkirjeldatud vahendite täpsemad kirjeldused leiab aadressidelt http://www.id.ee/ , http://www.sk.ee/ ja http://www.politsei.ee/et/nouanded/id-kaart-ja-pass/index.dot .

Ohud

Alljärgnevas käsitletakse ohtusid, mis puudutavad ID-kaardi/PKI lahenduste kasutamist erinevates infosüsteemides. Vaatluse alt jäävad välja ohud, mis puudutavad ID-kaardi/PKI lahenduste loojaid ja pakkujaid, sertifitseerimisteenuse osutajaid, OSCP-teenust, digiallkirja tarkvara väljatöötamist jms.

Kuna ID-kaardi/PKI lahendused sisaldavad paljusid alamsüsteeme ja -teenuseid, mis tihti olulisel määral üksteisega kattuvad (ID-kaart, mobiil-ID, digiallkiri, turvaline autentimine, signeerimine, digitembeldamine, krüptopulk jms), pole ohtusid alamliikide järgi võimalik grupeerida. Spetsiaalselt ID-kaardi/PKI teenuste jaoks koostatud ohtude korral selgub ohtude kirjeldusest, milliseid konkreetseid alamkomponente nad puudutavad.

Varasemast ISKE versioonist ülevõetud ohtudel selgub tavaliselt kontekstist, milliste ID-kaardi/PKI komponentide korral nad rakenduvad – nt mobiiltelefoni puudutavad ohud mobiil-ID kasutamise korral, vargust puudutavad ohud kõikide teisaldatavate seadmete osas jms.

ID-kaardi/PKI lahenduste kasutamise peamiste ohtude hulka kuuluvad nii organisatsioonilised puudused, inimvead, samuti aga ka tehnilised rikked ja ründed. Olulisimal kohal on seejuures mitmesuguste lahenduste ja komponentide väärkasutamised või väärkasutamise võimalused, mis suuresti tekivad nende puudulikust konfigureerimisest või taustateabe puudumisest kasutajate seas. Halvematel juhtudel võivad need viia tõsiste identiteedi või tõestusväärtuse rikkumise

intsidentideni – digiallkirja või -templi volitamata andmine, kellegi nimel turvaline väärautentimine teenusesse või seadmesse vms. Olulisel kohal on ka võimalikud käideldavusohud – kuna paljud IT-süsteemid eeldavad turvalisel kasutamisel ID-kaardi või sarnase seadme (mobiil-ID) olemasolu, siis on selle seadme kaotamisel ja/või rikkiminekul tihti tõsised tagajärjed infosüsteemi jaoks.

Ohutähises sisalduv E-täht näitab, et see oht on spetsiaalselt kirja pandud ID-kaardi/PKI lahenduste jaoks. Ülejäänud, oma koodis E-tähte mittesisaldavad ohud, pärinevad BSI standardsetest ohtude nimekirjadest ning on omased lisaks ID-kaardi/PKI lahendustele ka teistele, BSIst tuntud infovaradele.

Selleks, et fokuseerida standardsest BSIst ülevõetud ohtude mõju ID-kaardi/PKI lahendustele, on mitmeid neist paari lausega kommenteeritud. Kommentaarid asuvad ohu nimetuse järel ja on toodud kandiliste sulgude sees ning kursiivis.

Vääramatu jõud:

- G 1.2 IT-süsteemi avarii
- G 1.19 Teenuspakkuja või tarnija väljalangemine

[Eelkõige mõeldakse siin sertifitseerimisteenust ja sellega kaasnevaid teenuseid (OCSP, LDAP jt)]

Organisatsioonilised puudused:

- G 2.1 Reeglite puudumine või puudulikkus

[Asutusesiseste reeglite puudulikkus, valmislahenduste seadistus- ja kasutusreeglid on enamjaolt teatud tasemel olemas]

- G 2.2 Reeglite puudulik tundmine

[Eelkõige ID-kaardi ja/või mobiil-ID lõppkasutajaid]

- G 2.3 Puuduvad, puudulikud või ühildumatud ressursid

[Eelkõige ID-kaardi ja PKI lahendused Windows-operatsioonisüsteemides erinevates süsteemides, mis on kohati väga kaootiliselt lahendustega kaetud]

- G 2.4 Turvameetmete ebapiisav järelevalve
- G 2.8 Ressursside kontrollimatu kasutamine

[Digiallkirjastamise lahenduse korral on peamine oht asutuse poolt ostetud juurdepääsutõendi ressursside võimalikul väärkasutamisel asustusevälistel eesmärkidel]

- G 2.19 Krüpteerimise halb korraldus
- G 2.27 Ebapiisav või puuduv dokumentatsioon

[Eelkõige CDOC-krüpteerimise vaates]

- G 2.47 Failide ja andmekandjate ebaturvaline transport

[Eelkõige konfidentsiaalsete failide edastus CDOC-krüpteerimata]

- G 2.77 Paberdokumentide elektroonilise arhiveerimise puudused
- G 2.90 Välisteenusepakkujaga seotud nõrgad kohad
- G 2.102 Inimeste infoturbeteadlikkuse ebapiisav suurendamine
- G 2.E5 ID-kaardi või sarnase seadme kehtivusaja lõppemine
- G 2.E6 Digiallkirja andmine või autentimine ilma võtmepaari omaniku teadmata
- G 2.E7 Asutusega mitteseotud digiallkirjade andmine asutuse juurdepääsutõendi ressursside arvelt
- G 2.E8 Digiallkirjastatud dokumendi vormingureeglite mitmetimõistetavus
- G 2.E9 Digitempli andmise seadme kasutuseõiguse väljumine asutuse poolt määratud subjektide ringist
- G 2.E10 Juurdepääsutõendiga määratud digiallkirjade mahu ammendumine
- G 2.E11 Signeerimistarkvara puudus, mis võimaldab anda digiallkirja autentimisvõtmepaari ja PIN1-koodi kasutades
- G 2.E12 Pin-pad'i mittekasutamine

Inimvead:

- G 3. 1 Andmete konfidentsiaalsuse või tervikluse kadu kasutaja vea tõttu

[Eelkõige CDOC-krüpteerimata jätmine või digiallkirjaga/-templiga varustamata jätmine]

- G 3.2 Seadme või andmete hävitamine hooletuse tõttu

[Andmete pikaajaline väärsäilitamine CDOC-vormingus ja ID-kaardi ja/või mobiil-ID kasutuskõlbmatuks muutumine korduva vale PIN-koodi sisestamise tulemusena]

- G 3.3 Hooletus turvameetmete suhtes
- G 3.33 Krüptomoodulite väär kasutamine
- G 3.44 Teabe hooletu kasutamine
- G 3.77 Infoturbe vähene aktsepteerimine
- G 3.105 Väliste teenuste volitamata kasutamine

[Eelkõige asutuste ostetud juurdepääsutõendi ressursside volitamata kasutamist asutusevälistel eesmärkidel]

- G 3.E1 E1 ID-kaadi, digi-ID või mobiil-ID hooletu üleandmine teisele isikule

Tehnilised rikked:

- G 4.2 Sisevõrkude katkestus
- G 4.33 Autentimise puudumine või puudulikkus
- G 4.34 Krüptomooduli rike
- G 4.35 Ebaturvaline krüptoalgoritm
- G 4.36 Vead krüpteeritud andmetes

[Eelkõige CDOC ja/või DDOC failide volitamata muutumine (nii juhuslik muutmine kui ka tahtlik võltsimine)]

- G 4.41 Mobiilsidevõrgu rike
- G 4.42 Mobiiltelefoni või PDA tõrge
- G 4.47 Vananenud krüptomeetodid

[Eelkõige DDOCi varasemates versioonides kasutatud lühemad võtmepikkused ja nende pikaajaline mõju]

- G 4.48 Välisteenusepakkuja süsteemide rike

[Eelkõige sertifitseerimisteenus ja sellega kaasnevad teenuseid (OCSP, LDAP jt)]

- G 4.E1 Teenusekatkestuste oht SSOga ühismöllimisel

Ründed:

- G 5.1 IT-seadmete või -tarvikute manipuleerimine ja hävitamine
- G 5.2 Andmete või tarkvara manipuleerimine
- G 5.4 Vargus
- G 5.5 Vandalism
- G 5.6 Füüsiline rünne

[Eelkõige ID-kaardi ja/või mobiil ID röövimine ja selle füüsiline rikkumine/hävitamine. Samuti seadmeteja/või PIN-koodide rööv koos ähvardamisega]

- G 5.9 IT-süsteemide volitamata kasutamine
- G 5.16 Ohud hoolde- ja haldustööde ajal
- G 5.22 Kaasaskantava IT-süsteemi vargus
- G 5.28 Teenuse halvamine

[Eelkõige eesmärgiga halvata digiallkirjastamine ja/või -tembeldamine]

- G 5.40 Pealtkuulamine ruumis arvuti mikrofoni kaudu

[Eelkõige PIN-koodide varguse eesmärgil]

- G 5.42 Inimestega manipuleerimine (Social Engineering)
- G 5.69 Varguseoht kodutöökohas

[ID-kaart ja/või mobiil-ID, iseäranis aga PIN-koodid ning neid sisaldav turvaümbrik]

- G 5.70 Pereliikmete või külaliste manipulatsioonid kodutöökohas

[ID-kaardi/PKI tarkvara kuritahtlik modifitseerimine, PIN-koodide kuritahtlik muutmine, seadmete blokeerimine korduva vale PIN-koodi sisestamise teel]

- G 5.71 Tundliku informatsiooni konfidentsiaalsuse kadu

[Eelkõige tingitud CDOC-vormingus krüpteerimata jätmisest olukordades kus krüpteering vajalik on]

- G 5.81 Krüptomooduli volitamata kasutamine
- G 5.82 Krüptomooduli manipulatsioon
- G 5.83 Krüptograafiliste võtmete paljastamine
- G 5.84 Võltsitud sertifikaadid
- G 5.94 SIM-kaardi kuritarvitamine
- G 5.95 Pealtkuulamine ruumis mobiiltelefonidega

[Eelkõige PIN-koodide varguse eesmärgil (iga klaviatuuri klahv tekitab teistest erineva heli, mis võimaldab valitud klahvide järjestuse heli põhjal taastada)]

- G 5.96 Mobiiltelefoni ehituse muutmine

[Eelkõige PIN-koodide varguse eesmärgil või kasutaja teadmata toimuva mobiil-ID osa kasutamise eesmärgil]

- G 5.E4 PIN-koodide vargus ja/või volitamata kasutamine
- G 5.E5 ID-kaardi või sarnase seadme vargus või röövimine
- G 5.E6 PIN koodi ja ID-kaardi (või sarnase seadme) üheaegne vargus või röövimine
- G 5.E7 Pahavara rünne signeerimis- või autentimissüsteemile

Soovitatavad meetmed

ID-kaardi/PKI lahenduste korral rakendatavad turvameetmed puudutavad eelkõige mitmesuguseid protseduurilisi reegleid ja juhiseid ID-kaardi/PKI komponentide kasutamisel. Nende reeglite järgimine peaks viima eelkirjeldatud ohtudest põhjustatud riskid vastava turvaklassi korral nõutud jääkriskini.

Oma päritolult saab rakendatavad turvameetmed jagada kahte liiki. Esimest liiki turvameetmed pärinevad BSIst ja/või varasemast ISKEst ning on mõeldud lisaks ID-kaardi/PKI lahendustele rakendamiseks ka muude infovarade moodulite juures. Mitmete niisuguste turvameetmete hõlpsamaks fokuseerimiseks ID-kaardi/PKI lahenduste jaoks on meetme nimetuse järel toodud lühikommentaar, mis asub kandiliste sulgude sees ja kursiivis.

Teist liiki turvameetmed on välja töötatud spetsiaalselt ID-kaardi/PKI lahenduste jaoks. Nende meetmete tähises sisaldub täht “E”, mis näitab nende Eesti-kesksust ja unikaalsust.

Plaanimine ja kontseptsioon:

- (L) M 2.1 IT kasutajate vastutuse ja reeglite kehtestamine
- (L) M 2.46 Krüpteerimise õige korraldus
- (L) M 2.161 Krüptokontseptsiooni väljatöötamine
- (M) M 2.162 Krüptoprotseduuride ja -toodete vajaduse määramine
- (M) M 2.163 Krüptoprotseduure ja -tooteid mõjutavate tegurite määramine
- (L) M 2.164 Sobiva krüptoprotseduuri valimine
- (L) M 2.165 Sobiva krüptotoote valimine
- (M) M 2.173 Veebiserveri turbestrateegia väljatöötamine

- (M) M 2.E12 E-ID rakendusjuhiste järgimine
- (L) M 2.E13 Asutusesisesed reeglid ID-kaardi/PKI kasutamiseks
- (L) M 2.E14 Digitempli turvaline evitamine asutuses
- (L) M 4.83 Võrgukomponentide riistvara ja tarkvara värskendamine ja täiendamine
- (M) M 4.88 Nõuded operatsioonisüsteemide turvalisusele krüptomoodulite kasutamise korral

Rakendamine:

- (L) M 2.9 Aktsepteerimata riist- ja tarkvara kasutuse keeld

[Eelkõige digiallkirjastamiseks ja -tembeldamiseks kasutatavad erinevad lahendused]

- (L) M 2.12 IT-kasutajate nõustamine
- (L) M 2.86 Tarkvara tervikluse tagamine
- (M) M 2.166 Krüptomoodulite kasutamist reguleerivad sätted
- (L) M 3.1 Uute töötajate esmane juhendamine ja väljaõpe
- (L) M 3.2 Uute töötajate kohustamine eeskirju järgima
- (L) M 3.4 Väljaõpe enne programmi tegelikku kasutamist
- (L) M 3.5 Turvameetmete koolitus
- (M) M 3.23 Sissejuhatus krüptograafia põhimõistetesse
- (L) M 4.7 Algparoolide muutmine

[Eelkõige ID-kaardi ja mobiil-ID PIN- ja PUK-koodide korral]

- (L) M 4.34 Krüpteerimise, kontrollsummade ja digitaalallkirjade rakendamine
- (M) M 4.41 Sobivate IT-süsteemide turvatoodete valimine
- (L) M 4.87 Krüptomoodulite füüsiline turve
- (M) M 4.88 Nõuded operatsioonisüsteemide turvalisusele krüptomoodulite kasutamise korral
- (L) M 4.114 Mobiiltelefonide turvamehhanismide rakendamine
- (M) M 4.177 Tarkvarapakettide tervikluse ja autentsuse tagamine
- (L) M 4.228 Pihuarvutite turvamehhanismide rakendamine

[Seadmetes, kus kasutatakse mobiil-ID lahendusi]

- (M) M 5.150 Penetratsioonitestide läbiviimine

[Kohustuslik ainult nendel juhtudel, kus digitembelduslahendus töötab ilma inimese vahetu juuresolekuta]

- (L) M 3.E2 Töötajate koolitus ID-kaardi/PKI lahenduste kasutamise osas
- (L) M 4.E1 ID-kaardi/PKI lahenduste turvaline seadistamine
- (M) M 4.E5 Nõuded ID-kaardi/PKI lahendusi kasutavale turvalisele autentimisele

- (L) M 4.E6 Keeld anda digiallkirja autentimisvõtmepaari ja PIN1-koodi kasutades

Kasutamine:

- (L) M 2.22 Paroolide deponeerimine

[Siinkohal PUK-koodid]

- (M) M 2.111 Juhendite hoidmine käepärast
- (L) M 2.224 Trooja hobuste tõrje
- (M) M 2.264 Krüpteeritud andmete regulaarne regenereerimine arhiveerimisel
- (M) M 2.265 Digitaalallkirjade õige kasutamine arhiveerimisel
- (L) M 2.E15 ID-kaardi või sarnase seadme PIN-ja PUK-koodide turvaline käitlemine
- (L) M 2.E16 Transpordikrüpto vormingute kasutuskeeld andmete säilitamiseks
- (L) M 2.E17 ID-kaardi või sarnase seadme kasutuskeeld tundmatute turvasätetega keskkonnas
- (L) M 2.E18 ID-kaardi või digi-ID edasiandmiskeeld teisele isikule (tavakasutaja)
- (L) M 2.E19w ID-kaardi või digi-ID kaasavõtmiskohustus arvuti juurest lahkumisel
- (L) M 2.E20 ID-kaardi või digi-ID edasiandmiskeeld teisele isikule (administraator)
- (L) M 4.3 Viirustõrjeprogrammi regulaarne kasutamine
- (L) M 4.229 Pihuarvutite turvaline kasutamine
- (L) M 4.E2 ID-kaardi/PKI lahenduste turvaline seadistamine
- (L) M 4.E3 ID-kaardi, digi-ID ja mobiil-ID ning nende sertifikaatide õigeaegne uuendamine
- (M) M 4.E4 Juurdepääsutõendiga määratud signeerimisressursi seire ja uuendamine

Kasutusest eemaldamine:

- (M) M 2.E21 Digitembeldussüsteemi tegevuse lõpetamine

Valmisolek hädaolukorraks:

- (L) M 5.E1 Sertifikaatide õigeaegne peatamine
- (M) M 5.E2 Varem antud digiallkirjade õigeaegne ülesigneerimine

Aste H: Turvameetmed kataloogist H, lisada astme M meetmetele
Kohustuslikud üldmeetmed:

- HG.78 Halduslike meetmete rakendamine korporatiivsete ja riiklike PKI-lahenduste jätkusuutlikuks kasutuseks
- HG.79z ID-kaardi või sarnase seadme perioodiline loendurikontroll

- HG.80zPin-pad'i kasutamine

Teabe käideldavus (K)

- HK.5 Mobiilseadme aku regulaarvahetus

[Seadmetes, kus kasutatakse mobiil-ID lahendusi]
Teabe terviklus (T)

- HT.29 Kombineeritud autentimise nõue

[Kombineeritud autentimine peab võimalusel kasutama Eesti rahvuslikke PKI vahendeid]

- HT.34 Digiallkirja kasutamine
- HT.48 Lisanõuded krüptolahenduste võtmehaldusele
- HT.49 Lisanõuded arhiveeritud andmete krüptoatribuutide regenereerimisele

Teabe konfidentsiaalsus (S)
-

ISKE kataloogid

M1: Infrastruktuur

Meetmete nimekiri

M 1.1 Vastavus normidele ja eeskirjadele

Vastutav algatuse eest: varustusjuht, planeerija
Vastutav elluviimise eest: ehitusjuht, paigaldusfirma

Peaaegu kõik tehnika valdkonnad on reguleeritud normide või eeskirjadega. Nimetatud regulatsioonid aitavad kaasa, et tehnilised seadmed tagaksid kasutajale vajaliku kaitse ning töökindluse.

Hoonete planeerimisel ja püstitamisel, nende ümberehitamisel, tehniliste seadmetega varustamisel (nt sisemised toitevõrgud, nagu telefonid või andmevõrgud) ning seadmete soetamisel ja kasutamisel tööprotsessis tuleb tingimata järgida vastavaid norme ja eeskirju.

M 1.2 Jaotusseadmete pääsueeskirjad

Vastutav algatuse eest: tehnikaosakonna juhataja
Vastutav elluviimise eest: tehnikaosakond

Jaotusseadmed (nt elektritoitele, andmevõrkudele, telefonitehnikale) tuleb võimalusel paigaldada tehnilise infrastruktuuri ruumidesse (vt moodul B 2.6 Tehnilise infrastruktuuri ruum). Seejuures tuleb järgida nimetatud moodulis kirjeldatud meetmeid.

Juurdepääs kõikidele toiteseadmetele (elektrivool, vesi, gaas, telefon, häiresignalisatsioon, torupost jne) hoones peab olema võimalik ja reguleeritud.

“Võimalik” tähendab, et:

- viimistlustööde teostamisel ei kaetaks jaotusseadmeid värvi või tapeediga, nii et neid on võimalik avada või üles leida vaid tööriistade abil,
- jaotusseadmeid ei blokeeritaks mööbli, seadmete, kaubaalustega jne,
- suletud jaotuskilpide avamiseks oleks olemas võtmed ning et lukustussüsteemid funktsioneeriksid.

Reguleeritud tähendab, et on kindlaks määratud, kes missugust jaotuskilpi tohib avada. Jaotuskilbid peavad olema suletud ning neid tohivad avada vaid vastava toiteseadme eest vastutavad isikud. Juurdepääsuvõimalusi on võimalik reguleerida mitmesuguste lukustusviiside ning nendele vastava võtmete halduse abil (vt M 2.14 Võtmete (ja kaartide) haldus).

Kui elektritoitevõrgu jaotuskilpidesse on paigaldatud sulavkaitsmed, peaks valmis olema vastavad varukaitsmed (jaotuskilbis). Jaotusseadmete dokumentatsioon tuleb sisse viia vastavalt meetmele M 2.19 Neutraalne dokumentatsioon jaotuskilbis .

Kõik jaotuskilpi paigaldatud seadmed peavad olema täpselt ja arusaadavalt pealkirjastatud.

Täiendavad kontrollküsimused:

- Kas juurdepääs jaotusseadmetele on reguleeritud?

M 1.3 Juhtmestuse kohandamine

Vastutav algatuse eest: tehnikaosakonna juhataja
Vastutav elluviimise eest: tehnikaosakond

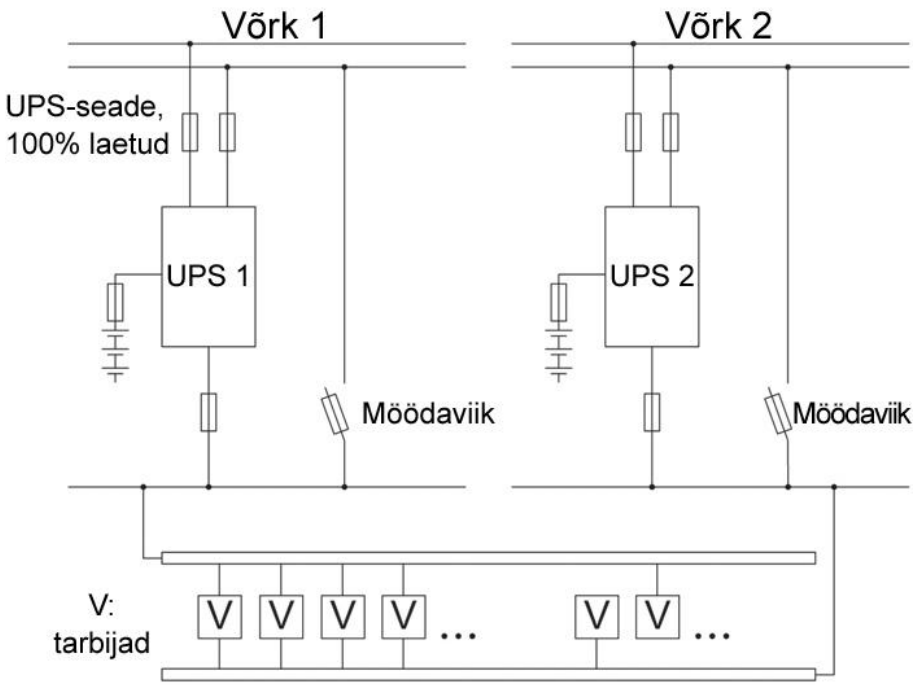
Kogemused näitavad, et aja möödudes ei pruugi ruumide algne elektriinstallatsioon enam vastata institutsiooni tegelikele vajadustele. Ruumide kasutusotstarbe muutumisel ning tehnilise sisseseade (nt IT, kliimaseade, valgustuse) muutuste ja täienduste korral on oluline elektriinstallatsiooni kontrollida ja seda vajaduse järgi kohandada. Lihtsamatel juhtudel võib piisata olemasoleva juhtmestiku ümberpaigutamisest. Seevastu raskematel juhtudel võib kohandamine tähendada ka seda, et paigaldada tuleb kas täiendavad või täiesti uued toiteühendused, elektrikaablid, elektrikilbid jms.

Nii turbe seisukohast kui ka seetõttu, et vaskkaablite andmeedastuskiirused muutuvad üha suuremaks, on väga soovitatav terve hoone elektrijaotusvõrk rajada TN-S-võrguna. Seda nõuab ka standard DIN VDE0100-444. Siinkohal on tähtis, et PE- ja N-juht paigaldataks alates potentsiaaliühtlustussiinist (PAS) eraldi juhtmena. Selle nõude täitmisel pole IT-seadmetes erinõuete järgimine üldjuhul enam vajalik. Samas tuleks siiski arvestada ka meetmes M 1.28 Puhvertoiteallikas esitatud soovitustega, mis puudutavad uute TN-S-võrkude rajamist juba ühendatud seadmete tarbeks.

TN-S-võrgu tõhususe ja pika kasutusea tagamiseks tuleb jälgida, et PE- ja N-juhi ühendusi PAS-iga (nulliga) oleks terve võrgu kohta ainult üks. Praktikas on aga sageli väga raske välistada, et uute seadmete ühendamisel või võrgus tehtavate lülituste käigus ei looda PE- ja N- juhiga kogemata siiski mõnda teist ühendust. Seetõttu tuleks andmevõrkudes tehtavad muudatused hoonetehnika osakonnaga alati kooskõlastada. Samuti tuleks TN-S-võrku regulaarselt kontrollida, et veenduda, kas maandus töötab õigesti. Seda võib teha kas kohustuslike elektrivõrgu kontrollide käigus või kahtluste korral (nt kui andmevõrgus esineb mõni pikemaajaline mittespetsiifiline tõrge). Ideaaljuhul võiks TN-S-võrk olla varustatud diferentsiaalvoolu pideva jälgimise süsteemiga.

Kui IT-süsteemidele on kehtestatud kas suured või väga suured käideldavusnõuded, on levinud ja sobiv lahendus see, kui igal IT-süsteemil on kasutada kaks eraldi toimivat toiteliini ja kasutatakse IT-süsteeme, millel on kaks eraldi toitejuhet.

Olulisemad tarbijad (salvestikomponendid, tsentraalsed võrgusõlmed, olulised serverid) ühendatakse eraldi toitevõrkude „Võrk 1” ja „Võrk 2” külge (vt joonis). Teised IT-komponendid, mille nõuded on väiksemad, jaotatakse ühtlaselt toiteliinide peale ära.



Kahe eraldi toiteliiniga turvaline elektrivarustus

Tavaliste ühendatud seadmete puhul on eriti tähtis jälgida just seda, et need seadmed, mis peavad üksteist dubleerima, ei oleks ühendatud ühe ja sama toiteliini külge. Lisaks tuleb tagada, et seadmed jagataks tarbimisvõimsuse järgi ühtlaselt mõlema liini peale ära.

Kontrollküsimused

- Kas vooluahelate turvalisust ja elektrisüsteemi vastavust tegelikele vajadustele kontrollitakse regulaarselt?
- Kas suurte käideldavusnõuete korral on IT-seadmete toide tagatud kahe eraldi toiteliiniga?

M 1.4 Piksekaitse

Vastutav algatuse eest: tehnikaosakonna juhataja
Vastutav elluviimise eest: tehnikaosakond

Pikselöögi otsest kahjustavat mõju hoonele (ehitise kahjustus, katusekonstruktsiooni põlemine jms) on võimalik ära hoida piksekaitse paigaldamisega. Lisaks välisele piksekaitsele on peaaegu hädavajalik sisemine piksekaitse, liigpingekaitse. Sest välimine piksekaitse ei kaitse hoones olevaid elektriseadmeid. See on võimalik vaid liigpingekaitse abil (vt M 1.25 Liigpingekaitse), millele tehtavad suured kulutused võrreldes kaitstava varaga peavad olema õigustatud.

Igakülgseks piksekaitseks on vajalik, et kõik kaitseseadmed vastaksid samale potentsiaalile. Välimine piksekaitse on seotud potentsiaaliühtlustuslatiga: See on omakorda ühendatud hoones asuva elektriinstallatsiooni PEN- või N- ja PE-juhiga. Pikselöögi korral muutub koormusvooluga proportsionaalne pinge piksekaitseseadme maandustakistuse kahjutuks. Potentsiaaliühtlustuslati ning sellega koos ka N- ja PE-juhtide potentsiaal hoones tõuseb ning võib ulatuda kümnete tuhandete voltideni. N-/PE-juhtide ja L1/L2/L3 juhtide vahel tekivad pinged, mis ületavad olulisel määral tavapärase 230/400 voldise pinge. Tagajärjeks on seadmete ja juhtmestiku kahjustus. Tasandusvoolud andme- ja elektritoite võrgu vahel, nt defektsete varjete tõttu, võivad viia IT-süsteemi hävimiseni (vt M 1.39 Tasandusvoolude vältimine varjes). Kõikide võrkude vaatluse alla võtmine (hoone juhtimis- ja kontrollsüsteem, laivõrgud - WAN) on võimalike paralleelsete paigalduste tõttu läbikostmist silmas pidades sama vajalik nagu hoonesse viivate välisliinide kaasamine (vt M 1.5 Välisliinide lahutuslülitid)

Näide

- Pikselöögi tagajärjel said ühe teenindusettevõtte filiaali IT-seadmed (arvutid, serverid, laserprinterid) *ca* 10 000 euro ulatuses kahjustatud. Pärast nimetatud sündmust varustati hoone välise piksekaitsega ilma sisemise piksekaitseta (liigpingekaitseta). Uus pikselöök tekitas vaatamata välise piksekaitse olemasolule kahju peaaegu samas ulatuses.

Täiendavad kontrollküsimused:

- Kas välise piksekaitse vajadus on tõepoolest olemas?
- Kas on ettekirjutusi ametiasutustelt või kindlustustelt?
- Kas toimub piksekaitseseadme reeglipärane kontroll ja hooldus?
- Kas hoones on olemas piisava tugevusega liigpingekaitse?

M 1.5w Välisliinide lahutuslülitid

Vastutav algatamise eest: tehnikaosakonna juhataja

Vastutav elluviimise eest: tehnikaosakond

IT-süsteemide tööd ning seeläbi ka nende käideldavust ja terviklust pärssivate tõrgete üks põhjus võib peituda elektrikaablites. See puudutab nt erinevat päritolu häirivate signaalide edasikandumist ja kõikvõimalikke, nt pikselöökidest ja lülitusprotsessidest tingitud liigpingeid. Sedalaadi tõrkeid saab üpris tõhusalt ennetada välisliinide galvaanilise lahutamisega, mis tõkestab elektrikõikumiste edasikandumise, kuid kahjuks ei ole see alati võimalik.

Tavapärase elektritoite ja vaskkaablitel põhineva andmeedastuse korral saaks küll paigaldada galvaanilise lahutuse tagamiseks isoleeriva trafo. Häirivad maksimumpinged ja muud häirivad signaalid kanduksid samas siiski siseliinidesse üks ühele edasi. Tõrgete mõju võib veidi pehmendada üksnes trafo ribapääsu funktsioon.

Kuna isoleerivad trafod ei paku siinkohal täit lahendust ja kuna neid ei saa andmekaabliliinides kasutada, siis eespool mainitud galvaanilist lahutamist praktikas ei kasutata. Isoleerivate trafode asemel võetakse tavapärase elektritoite ja vasest andmekaablitega seotud maksimumpingetest ja liigpingest tingitud tõrgete minimeerimiseks pigem liigpinge ennetamiseks mõeldud meetmeid. Lisateavet leiate meetmest M 1.25 Liigpingekaitse .

Andmekaablite puhul on hea lahendus kasutada vaskkaablite asemel valguskaableid või lahutada vaskkaablid vähemalt galvaaniliselt, paigaldades nende vahele optronid.

Samuti tuleks arvestada kõikvõimalike torustikega (jahutussüsteemide jahutusvedelik ja kondensatsioonivesi, tavapärased vee- ja gaasitorud jmt). Kui torustikus olev aine juhib elektrit, nt vesi (mis on ka jahutusvedelike põhikoostisosa), ei anna valdavalt vask- või terasmaterjalist ehitatud torustiku katkestamine plastdetailidega erilist efekti. Ka siin tuleb võtta hoopis liigpingekaitse meetmeid.

Ainukese erandi, mille puhul torustiku katkestamine elektrit mittejuhtiva detailiga võimaldab luua galvaanilise lahutuse, moodustavad gaasitorustikud. Kuna aga gaasitorustikke ei tohi niikuinii IT-valdkonna ruumidesse paigaldada, piirdub meetmete võtmine enamasti siiski ainult liigpingekaitse meetmetega.

M 1.6 Tuletõrje-eeskirjade täitmine

Vastutav algatuse eest: tehnikaosakonna juhataja, tuleohutuse eest vastutav töötaja
Vastutav elluviimise eest: tuleohutuse eest vastutav töötaja, tehnikaosakond

Tingimata tuleb täita olemasolevaid tuleohutuseeskirju ning ehitusjärelvalve poolt hoonete suhtes kehtestatud eeskirju. Tulekaitse planeerimisse tuleb kaasata kohalik tuletõrje.

Ruumide suhtes, milles asuvad tähtsad IT-seadmed ja andmekandjad (serverid, andmekaitseseadmed jne), tuleks järgida ka standardi EN 1047 osas 2 kindlaks määratud eeskirju.

Nõupidamis-, üritus- ja koolitusruumide suhtes tuleb teatud juhtudel järgida vastavaid nõupidamisruumidele kehtivaid tuleohutuseeskirju. Kuna vastavalt ruumide kasutamisele kehtivad erinevad lisanõuded nagu nt uste avamisviisi ja laiuse suhtes põgenemis- ja väljapääsuteedel ning teeviitadega varustamise suhtes, peaks ka nende planeerimisse kaasama kohaliku tuletõrje.

Tuleks määrata isik, kes on vastutav tuleohutuseeskirjade täitmise eest. Selleks võib olla tuleohutuse eest vastutav töötaja või keegi teine vastava alaga kursis olev isik, kes on läbi teinud ka vastava koolituse.

Eriti tähtis on evakuatsiooniteede varustamine teeviitadega. Selleks on vaja kasutada kindlaks määratud tähistusi ning järgida nende paigaldamise eeskirju. Evakuatsiooniteed peavad alati olema avatud, s.t et neid ei tohi blokeerida, nt koridori tõstetud inventariga ning evakueerimiseks ette nähtud uksed ei tohi olla lukustatud.

Et tuletõrje saaks põlengu korral kiiresti tule kustutamisega alustada, on tähtis, et tuletõrjesignalisatsiooni keskus, tuletõrjesignalisatsiooni puuteplaat ning kustutusveepunktid oleks paigaldatud teeviitade abil kiiresti leitavad.

Efektiivse tuleohutuse elluviimiseks on vajalik kõigi asjaosaliste koostöö. Nende hulka kuuluvad:

- tuleohutuse eest vastutav töötaja (vastutav tuleohutuseeskirjade täitmise eest on tööandja)
- tööohutuse spetsialist

- tuleohutuse eest vastutav töötaja

Täiendavad kontrollküsimused:

- Kas toimub koostöö kohaliku tuletõrjega?
- Kas on olemas tuleohutuse eest vastutav töötaja või keegi teine alaga kursis olev isik, kes on läbi teinud ka vastava koolituse?

M 1.7 Tulekustutid

Vastutav algatuse eest: tehnikaosakonna juhataja, tuleohutuse eest vastutav töötaja
Vastutav elluviimise eest: tuleohutuse eest vastutav töötaja, tehnikaosakond

Enamik põlengutest saab alguse väikestest, algul veel hästi kontrolli all hoitavatest tulekolletest. Eriti büroodes leiab tuli rikkalikult toitu ning võib kiiresti levida. Põlengute kohesel kustutamisel on seega väga suur tähtsus.

Tulekollete kohene kustutamine on võimalik vaid juhul, kui hoones on käepärast piisaval hulgal ja piisava suurusega (vastavalt kohapealse tuletõrje soovitusele) sobiva tuleklassi tulekustuteid. Seejuures tuleb püüelda selle poole, et need asuksid kaitset vajavate tsoonide ja selliste ruumide nagu serveriruumi, tehnilise infrastruktuuri ruumi või dokumentide arhiivi läheduses.

Veekustutid, mis vastavad tuleklassile A kuni 1000 V, sobivad vaid elektriseadmete kustutamiseks.

Elektrooniliste seadmete, nt arvutite põlengute jaoks peaks eelistatult käsutuses olema süsinikdioksiid-tulekustutid (tuleklass B). Tulekustuti toime saavutatakse hapniku väljatõrjumise teel, seepärast tuleb nende kasutamisel kitsastes, halvasti õhutatud ruumides olla ettevaatlik.

Pulberkustuteid, mis vastavad tuleklassidele A (tahked ained), B (põlevad vedelikud) ja C (gaasid), ei tohiks kasutada elektriliste ja elektrooniliste seadmete kustutamiseks, kuna kustutuse tagajärjel tekkinud kahjud on reeglina ülemäära suured. Seetõttu on soovitatav serveriruumide, andmekandjate arhiivide, tehnilise infrastruktuuri ruumide ja arvutuskeskuste vahetusse lähedusse mitte paigutada pulberkustuteid, vaid eranditult selleks sobivaid gaasikustuteid. Ainult nii on võimalik ära hoida seda, et põlengu tõttu tekkinud ärevushoos ei kasutataks ekslikult pulberkustutit.

Tulekustuteid tuleb regulaarselt kontrollida ja hooldada. Tulekustutid peavad olema paigutatud nii, et neid oleks põlengu korral kerge kätte saada. Töötajad peaksid endale lähima tulekustuti asukoha meelde jätma. Kustutite ja hüdrantide asukohad peavad olema tähistatud nõuetele vastavate siltidega. Kantavate tulekustutite lubatud kogukaal on kuni 20 kg. Arvamus, et enamasti kasutusel olevate 6 kuni 12 kg kustutitega ei ole võimalik kustutada suuremaid tulekoldeid, on võhiklik, sest hea ettevalmistuse korral on see võimalik. Kustutusvahendi täielik tühjenemine toimub vaid mõne sekundi jooksul. Seepärast tuleb tuletõrjeõppuste ajal töötajatele õpetada tulekustutite kasutamist.

Kontrollküsimused:

- Kas töötajad on teadlikud tulekustutite asukohast?

- Kas tulekustutite kasutamist harjutatakse?
- Kas tulekustutid on põlengu korral üldse kättesaadavad?
- Kas toimub regulaarne tulekustutite kontroll ja hooldus?

M 1.8 Ruumide tuleohutus

Vastutav algatuse eest: tehnikaosakonna juhataja, tuleohutuse eest vastutav töötaja
Vastutav elluviimise eest: tehnikaosakond, tuleohutuse eest vastutav töötaja

Põlemiskoormus tekib kõikide hoonesse paigutatud põlevate materjalide tõttu. See sõltub materjalide hulgast ning nende küttevääртusest. IT-seadmed ja juhtmestik tekitavad samuti põlemiskoormust nagu mööbel, põrandakatted ja kardinadki.

IT-seadmete, andmekandjate jne paigaldamisel mingisse ruumi tuleks eelnevalt läbi viia selle ruumi ja naabruses asuvate ruumide olemasolevate põlemiskoormuste hindamine. Näiteks ei tohiks andmekandjate arhiiv paikneda paberilao läheduses ega selle kohal.

M 1.9 Ruumide ja korruste tuleisolatsioon trassiavades

Vastutav algatuse eest: tehnikaosakonna juhataja, tuleohutuse eest vastutav töötaja
Vastutav elluviimise eest: tehnikaosakond, tuleohutuse eest vastutav töötaja

Elektrijuhtmed ja IT-kaabeldus kontsentreeritakse tavaliselt installatsioonitrassidesse. Tihti on nii, et trassid kulgevad mööda väljapääsu- ja evakuatsiooniteid, läbi maa-aluste garaažide, ladude, töökodade või transiittrassidena läbi võõra territooriumi.

Paljude tuletõkkesektsioonidega hoonete korral toimub elektrijuhtmete ja IT-kaabelduse paigaldamine vastavalt tuleohutusnõuetele. See puudutab eelkõige juhtmeid, mis läbivad tuletõkkesektsioone, seinu või lagesid või on paigaldatud liiklusteedesse. Eriti juhul, kui trasse kasutatakse tuletõrjesignalisatsiooni, häireseadmete, kustutustehnika või ohutusvalgustuse jaoks, tuleb järgida täiendavaid nõudeid elektrijuhtmete funktsiooni säilitamise suhtes põlengu korral. Seepärast tuleks trasside planeerimisse igal juhul kaasata tuleohutuse eest vastutav isik. Trassid peavad pakkuma nii tuleohutusalast kaitset kui ka kaitset sabotaaži vastu. Mõlemat on võimalik saavutada trasside nõuetele vastava tuleisolatsiooniga.

Kui elektrikaablid on küllaltki tihedalt paigaldatud tuleohutusele vastavalt eraldatud kaablikanalisse, võib tekkida suur temperatuuritõus. Selle tagajärjeks võib olla elektrilise eritakistuse tõus täiendava soojenemisega. Abi on võimalik saada juhtmete hulga vähendamise või piisava ventilatsiooni kaudu.

Tavapäraste ventilatsioonimeetodite või –tehnikate, nt õhutuskomponentide kasutamise puuduseks on, et need ei paku küllaldast kaitset sabotaaži vastu. See tähendab, et kõrge kaitsevajadusega juhtmed, mis läbivad kaitseta tsoone, nagu nt maa-alust garaaži, ei ole kaitstud seadusevastaste juhtumite vastu. Sel juhul on vaja rakendada individuaalseid planeerimismeetmeid. Selleks võib olla kanali piisav dimensioneerimine, mis teeb kanali õhutamise ohustatud tsoonis mittevajalikuks, või spetsiaalne õhutuskontseptsioon, mis on orienteeritud spetsiifilistele ohutusnõuetele.

Trassiavad tuleb pärast juhtmete paigaldamist vastavalt seina või lae tulepüsivusklassile isoleerida. Hilisema installeerimise kergendamiseks võib ajutiste meetmetena kasutada sobivaid materjale, nagu seda on pehmed tuletõkked või tulekaitsepadjad. Kaablitrassid venivad soojenemisel, nt põlengu mõjul ning selle tagajärjel võivad pehmed tuletõkked või tulekaitsepadjad hävida, kui need viiakse läbi seinte.

Sellepärast ei tohiks trasse viia läbi isolatsiooni, vaid need peaksid mõlemal pool seina vähemalt 10 cm enne seina lõppema. Selline praktika kergendab ka kaablite ja juhtmete hargnemise teostust, sest neid ei tohi viia läbi tuleisolatsiooni pundina, vaid üksikuna.

Tihti paiknevad ühes trassis erinevad kaablid, nt telefoni, kohtvõrgu (LAN) ja majas paiknevate tehniliste seadmete jaoks. Kui ees seisab muutuste tegemine kaabelduses, tuleb juba planeerimisfaasis kindlaks teha, kas ettenähtud ajavahemiku jooksul tuleb välja vahetada ka teisi kaablisüsteeme. Vastav projektide ühildamine viib ajakao miinimumini ning hoiab kokku mitmekordse tuleisolatsiooni paigaldamise kulud.

Kui planeeritava trassi rajamine ei ole tuleohutusnõuetele vastavalt võimalik, tuleb kontrollida võimalust rajada alternatiivtrass. Lisaks sellele tuleb installeerimistööde lõpetamise järel tuleisolatsiooni regulaarselt, näiteks kord aastas, kontrollida.

Täiendavad kontrollküsimused:

- Kas trasside planeerimisse kaasati tuleohutuse eest vastutav isik?
- Kas elektrijuhtmetega trasside planeerimine ja teostus on kontrollitud elektriinseneri poolt?
- Kas kontrolliti alternatiivtrasside paigaldamise võimalust?
- Kas pärast installatsioonitööde lõpetamist toimub regulaarne tuleisolatsiooni kontroll?

M 1.10z Turvauksed ja -aknad

Vastutav algatuse eest: tehnikaosakonna juhataja
Vastutav elluviimise eest: tehnikaosakond
Kui uksed ja aknad moodustavad ülemineku turvatsoonide vahel, peavad need pakkuma asjakohast kaitset. Välisuks peab kaitsma nt sissemurdmise eest, samuti tuleb kaitsta ligipääsetavaid aknaid. Siseruumides peavad uksed, mis moodustavad tuletõkke tsooni piiri, olema ise tulekindlad. Lisaks sellele võivad need või ka muud uksed moodustada sissemurdmisevastase kaitse teise liini.

Turvaustel ja –akendel on võrreldes tavaliste büroouste ja –akendega omad eelised:

- Vastavalt ISKE-le on ehituselemendid jagatud vastupidavusklassidesse (WK). WK1 kuni WK2 vastupidavusklassi kuuluvad uksed pakuvad oma stabiilsuse tõttu tõhusamat kaitset sissemurdmise vastu (nt keldri- ja tarnesissepääsud).
- Isesulguvad, tule- ning suitsutihedad uksed (nt suitsutihe uks aeglustab tule levikut).
- Arvutuskeskuste varustamisel tuleks ustel nende paigaldust arvestades rakendada DIN EN 1627-1630:2011 kohaselt miinimumväärtusena vastupidavusklassi RC3. Ainult juhul, kui turvalisuse tagamiseks on eriti soodsad tingimused, eriti, kui abijõudude sekkumisaeg on lühike (maksimaalselt 2 minutit), võib erandjuhtudel olla piisav RC2-uks. Kui abijõudude sekkumisaeg on seevastu 5 minutit või rohkem, ei piisa isegi RC3-uksest ja soovitatav on paigaldada RC4-uksed. Loomulikult kehtib sama põhimõte vastavalt ka kõikide muude, RZ-ümbrise komponentide kohta.

Tuleb garanteerida, et kõikide ruumi ümbritsevate ehituselementide ohutusmeetmed oleks võrdväärsed:

- Sissemurdmist takistavate uste kasutamisel tuleb fassaadi piirkonnas kaaluda sissemurdmist takistavate akende ja fassaadielementide kasutamist.
- Lisaks sellele ei ole kõrgeimasse vastupidavusklassi kuuluva ukse paigaldamine kipskartongseina otstarbekas.
- Tule- või suitsukindla ukse paigaldamisel tuleb tähelepanu pöörata asjaolule, et ka ümbritsev sein oleks tuld pärssiv ja suitsu mitte läbilaskev ning et laetulede või kaabli paigaldusavade tõttu tekiks möödaviik.

Ülevaate turvaustele esitatavatest nõuetest leiate meetmetest M 1.47 Eraldi tuletõkked ja M 1.19 Sissemurdmiskaitse .

Turvauste kasutamine on tuleohutuse seisukohalt otstarbekas lisaks ehitusjärelvalve ja tuletõrje poolt ette nähtud tsoonidele (vt M 1.6 Tuletõrje-eeskirjade täitmine) erilist kaitset vajavates ruumides nagu serveriruumis, dokumentide ja andmekandjate arhiivis. Tugevdatud kaitset vajavate ruumide jaoks on vaja koostada tasakaalustatud kaitsekontseptsioon, milles käsitletakse valvesignalisatsiooni ja alarmsüsteeme ning turvauste paigaldamist. Kui potentsiaalsel sissemurdjal on sissemurdmiseks aega terve nädalavahetus, ei takista teda oma eesmärgi saavutamisel, varastamisel, andmete või sisutuse hävitamisel ka kõige kvaliteetsem sissemurdmist takistav uks.

Nõuanne

- Sissemurdmise eesmärgiks võib olla ka andmete ja IT-süsteemidega manipuleerimine. Seepärast tuleks pärast sissemurdmist kontrollida tsentraalsete IT-süsteemide terviklust (vt ka M 6.60 Turvaintsidentide käsitlusprotseduurid ja teavitamiskanalid).

Tuleb hoolitseda selle eest, et tule- ja suitsukindlad uksed tõepoolest suletaks ning mitte (mis ei ole lubatud) nt kiilu abil lahti ei hoitaks. Alternatiivina võib kasutada uksi automaatse sulgurmehhanismiga, mis häire korral aktiveeritakse.
Peale selle tuleb regulaarselt kontrollida, kas turvauksed ja -aknad on töökorras. Need peavad olema korralikus mehhaanilises seisundis, avanema ja sulguma turvaliselt, ning kontrollpaigaldised, nagu sulgekontaktid, peavad töötama.

Kontrollküsimused:

- Kas on kindlaks tehtud, kuhu oleks otstarbekas paigaldada turvauksed ja -aknad?
- Kas toimub turvauste ja -akende regulaarne funktsioonikontroll?
- Kas arvutuskeskuse puhul on kooskõlastatud uste, akende ja muude ruumi moodustavate komponentide vastupidavusväärtused ühelt poolt ja abijõudude sekkumisaeg teiselt poolt?

M 1.11 Trasside plaanid

Vastutav algatuse eest: tehnikaosakonna juhataja
Vastutav elluviimise eest: tehnikaosakond

Vajalik on kõikide hoones ning selle juurde kuuluval maa-alal paiknevate toitejuhtmete (elekter, vesi, gaas, telefon, valvesignalisatsioon, torupost jne) plaanide olemasolu ning kõik juhtmeid puudutavad asjaolud tuleb dokumenteerida:

- juhtmete täpne paigaldamine (märkimine dimensioneeritud põhi- ja asendiplaanidele),
- täpsed tehnilised andmed (tüüp ja mõõtmed)
- võimalik olemasolev märgistus,
- juhtmestiku kasutamine, sellega ühendatud tarbijate nimetamine,
- ohupunktid ja
- olemasolevad ja kontrollimist vajavad kaitsemeetmed.

Plaanide abil peab olema võimalik lihtsalt ja kiiresti saada täpne ülevaade olukorrast. Ainult nii on võimalik viia oht, et juhtmestik saab tööde läbiviimisel kogemata kannatada, miinimumini. Kahjustatud kohta on võimalik kiiremini lokaliseerida ning rikked kiiremini kõrvaldada.

Tuleb tagada, et kõik juhtmestiku osas tehtavad tööd saaksid õigeaegselt ja täielikult dokumenteeritud. Plaane tuleb säilitada kindlas kohas ning pääs nende juurde peab olema reguleeritud, kuna need sisaldavad kaitset vajavat informatsiooni.

Täiendavad kontrollküsimused:

- Kes on vastutav plaanide eest?
- Kas plaane uuendatakse?
- Kas plaane hoitakse kindlas kohas ning kas need on kättesaadavad vaid volitatud isikutele?
- Millised plaanid on juba olemas?

M 1.12 Kaitstavate hooneosade märgistamata jätmine

Vastutav algatuse eest: tehnikaosakonna juhataja
Vastutav elluviimise eest: tehnikaosakond

Kaitset vajavad hooneosad on nt serveriruum, arvutuskeskus, andmekandjate arhiiv, klimaator, elektritoite jaotusseadmed, juhtimiskeskused, käitamisruumid, tagavaraosade ladu.

Sellistel ruumidel ei tohi olla uksesilte. Uksesildid nagu ARVUTUSKESKUS või ARHIIV annavad hoonesse pääsevale potentsiaalsele ründajale informatsiooni, mis aitab tal oma tegevuse eesmärgikindlamalt ning edukamalt ette valmistada.

Kui IT osakonda ei ole võimalik paigutada mujale kui ruumidesse või hoone osadesse, mis on väljastpoolt võõrastele kergesti aimatavad (vt ka M 1.13 Kaitset vajavate ruumide paigutus), tuleb tarvitusele võtta vastavad meetmed, et takistada nendesse sissevaatamist või need nii kujundada, et nende kasutusotstarve koheselt äratuntav poleks. Seejuures tuleb tähelepanu pöörata asjaolule, et varjet ei paigaldataks korrusel mitte ainult ühe akna ette.

Täiendavad kontrollküsimused:

- Milliste märkide järgi on võimalik väljastpoolt kindlaks teha ruumide paiknemist?
- Millised märgid ruumide paiknemise kohta on hoones?

M 1.13z Kaitset vajavate ruumide paigutus

Vastutav algatuse eest: planeerija, asutuse/ettevõtte juhatus
Vastutav elluviimise eest: ehitusjuht, tehnikaosakonna juhataja

Kaitstavad ruumid või hoone osad ei tohiks asuda kaitseta või ohustatud kohtades:

- Keldriruume ohustab vesi.
- Esimesel korrusel avalike liiklusteede ääres asuvad ruumid on ohustatud kallaletungidest, vandalismist ja vääramatust jõust (liiklusõnnetused hoone lähedal).
- Esimesel korrusel asuvad ruumid varjatud hoovidega on ohustatud sissetungidest ja sabotaažist.
- Lamekatuse all asuvaid ruume ohustab sissetungiv vihmavesi.

Reegline on kaitset vajavad ruumid või tsoonid hoone keskel paremini kaitstud kui selle välisservades. Optimaalne oleks neid aspekte juba uue hoone ehitusplaani või olemasoleva hoone korral ruumide kasutusplaani väljatöötamisel arvestada. Juba kasutuses olevate hoonete korral on ruumide kasutuskord tihti seotud hoonesiseste ümberkolimistega. Alternatiivina peaks niikuinii vajalikest muutustest ruumide kasutuses tulenevaid võimalusi järjekindlalt ära kasutama.

Täiendavad kontrollküsimused:

- Millised kaitset vajavad ruumid asuvad kaitsetus kohas?

M 1.14z Automaatne drenaaž

Vastutav algatuse eest: planeerija, asutuse/ettevõtte juhatus
Vastutav elluviimise eest: ehitusjuht, tehnikaosakonna juhataja

Kõik tsoonid, kuhu võib koguneda vesi või milles voolavat või seisvat vett ei avastata või alles liiga hilja avastatakse ning milles vesi võib põhjustada kahjustusi, peaksid olema varustatud automaatse drenaaži või veeanduritega. Nimetatud tsoonide hulka kuuluvad muu hulgas:

- keldrid,
- õhuruum tõstetud põrandate all,
- valgussahtid,
- kütteseade.

Kui drenaaž toimub passiivselt, niisiis sadeveekaevude kaudu otse heitveesüsteemi, on tagasivooluklapid hädavajalikud. Ilma nimetatud klappideta muutub taoline drenaaž heitveesüsteemi ülekoormuse korral vee sissevooluavaks. Eriti tugeva saju järgselt tungib vesi enamasti selle kaudu keldrisse. Tagasivooluklappide funktsioneerimist tuleb reeglipäraselt kontrollida.

Kui passiivne drenaaž ei ole võimalik, sest heitveesüsteem asub liiga kõrgel, võib kasutada pumpasid, mis lülituvad ujuvlülitite või veeandurite kaudu automaatselt sisse. Nimetatud tehnika kasutamisel on vaja tähelepanu pöörata järgmistele asjaoludele:

- Pumba võimsus peab olema küllaldane.
- Pumba survetorustik on varustatud tagasivooluventiiliga.
- Et vees ujuvad esemed ei blokeeriks pumpa, on vaja tarvitusele võtta vastavad abinõud (imifiltrid jne).
- Pumba käivitumisest märku andmine peaks toimuma automaatselt (nt majahoidja või tehnikaosakonna valve ruumis).
- Pumba ja lüliti funktsiooni tuleb reeglipäraste vahedega testida.
- Pumba survetorustik ei tohi olla ühendatud vahetus läheduses kulgeva heitveetorustikuga. Sellise torustiku lekke korral pumpaks pump vett vaid ringiratast.

Täiendavad kontrollküsimused:

- Kas vee poolt ohustatud ruumid on varustatud iseseisva drenaažiga?

M 1.15 Aknad ja uksed suletud

Vastutav algatuse eest: tehnikaosakonna juhataja
Vastutav elluviimise eest: tehnikaosakond, töötajad

Aknad ja välisuksed (rõdud, terrassid) tuleb lukustada ajaks, mil ruumi ei kasutata. Keldri- ja esimesel korrusel ning vastavalt fassaadikujundusele ka kõrgematel korrustel pakuvad need sissemurdjale ka töö ajal ideaalset sisenemisvõimalust.

Normaalse tööaja ja kaastöötaja lühikese äraoleku ajal teatud kindlal ajal ei ole bürooruumide ning nõupidamis-, ürituste ja koolitusruumide kasutamise reguleerimine hädavajalik.

Nõupidamis- ürituste- ja koolitusruumides ei ole tavaliselt võimalust hoida dokumente, IT-süsteeme ja muud taolist eraldatult luku taga. Seepärast peaks olema võimalik sellised ruumid lukustada, vähemalt ajaks, mil kõik koosolekust osavõtjad ruumist lahkuvad, või lasta oma asutuse töötajal sellel silma peal hoida.

Täiendavad kontrollküsimused:

- Kas on olemas korraldus akende ja välisuste sulgemiseks?
- Kas kontrollitakse reeglipäraselt akende ja uste lukustamist pärast ruumist lahkumist?

M 1.16 Hoone sobiv asukoht

Vastutav algatuse eest: asutuse/ettevõtte juhatus
Vastutav elluviimise eest: planeerija

Üürile võetava või ehitatava maja asukoha planeerimisel on soovitav lisaks tavapärastele aspektidele, nagu ruumide tarve või kulud, tähelepanu pöörata ka infoturvet mõjutavatele keskkonnateguritele:

- Seoses hoone konstruktsiooni nõrkusega võib hoone läheduses toimuvast liiklusest tingitud vibratsioon (autotee, raudtee, metroo) kahjustada IT- süsteeme.
- Peamagistraalide (riigiraudtee, kiirtee, riigitee) ääres asuvad hooned võivad saada kahjustatud liiklusõnnetuste tagajärjel.
- Väga heade liiklusteede, seega ka põgenemisteede lähedus võib kallaletungi läbiviimist kergendada.
- Raadiosaatejaamade läheduses võivad tekkida tõrked IT süsteemides.
- Veekogude läheduses ja madalikel tuleb arvestada tulvaveega.
- Jõujaamade ja vabrikute läheduses võib õnnetuste või rikete tõttu (plahvatus, ohtlike ainete leke) hoone kasutatavus (nt evakueerimise või paljude ruumide sulgemine) väheneda.

Täiendavad kontrollküsimused:

- Kas on asukohast tingitud ohtusid?
- Kuidas ollakse valmis nendele ohtudele vastu astuma?

M 1.17z Pääsla

Vastutav algatuse eest: siseteenistuse juht
Vastutav elluviimise eest: siseteenistus

Pääsla rajamine võimaldab hoonet mitmesuguste ohtude eest kaitsta, kuid seda vaid eeldusel, et pääsla töö korraldamisel peetakse kinni mõningatest põhiprintsiipidest.

Uksehoidjad jälgivad või kontrollivad kõiki nii pääsla kui ka teiste sissepääsude kaudu sisenevaid ja väljuvaid isikuid. Koos videovalvega saab uksehoidja jälgida ja juhtida ka pääslast kaugemal paiknevaid uksi ja väravaid (vt M 1.53 Videovalve). Uksehoidja peab oma institutsiooni töötajaid tundma. Ka avalikkusele tuntud isikute puhul on soovitatav, et nad enda isikut uksehoidja juures siiski tõendaks, nt esitaks isikut tõendava dokumendi. Kui töötaja lahkub institutsioonist, nt töölepingu lõppemise tõttu, või kui töötaja asub institutsiooni sees mõnele teisele ametipostile, tuleb sellest teavitada ka uksehoidjat, et ta teaks, keda ei tohi enam sisse lasta ning kelle pääsuõigused on muutunud.

Võõrad isikud (sh uus ja kõikidele seni veel võõras ülemus) peavad uksehoidjale enda isikut tõendama.Võõraste isikute sisenemine hoonesse võiks olla üles märgitud külastajate raamatusse. Külastajatele võiks kaaluda külastajakaardi või -tõendi väljastamist.

Külaline läheb külastatava juurde koos saatjaga või külastatav tuleb talle pääslasse järele. Kui külastajatel on lubatud hoonesse siseneda ilma saatjata, tuleb kõigepealt kindlaks teha, et sellega ei kaasne turvariske. Asjakohased raamtingimused peavad olema dokumenteeritud. Näiteks võib koostada nimekirja institutsiooni pidevalt külastavatest usaldusväärsetest isikutest, kellel on pärast külastajakaardi saamist lubatud hoonesse siseneda ka ilma saatjata.

Kui pääsla töötab ööpäev ringi, võib sinna koondada kas kõik või ka ainult väljaspool tööaega seire- ja teavitussüsteemides genereeritavad teated. Pääsla töötaja peab temani jõudnud süsteemiteated teavitusnimekirjade kohaselt kas vastutavatele valvetöötajatele või organisatsioonivälistele isikutele edasi toimetama.

Uksehoidja töötingimused peavad vastama tema tööülesannetele. Töökirjelduses peab olema siduvalt kindlaks määratud, millised on uksehoidja täiendavad, turvalisuse tagamisega seotud kohustuslikud tööülesanded (nt hoone lukustamine pärast tööpäeva lõppu, signalisatsiooni aktiveerimine, välisuste ja akende kontroll).

Tööülesannete kindlaksmääramisel tuleb arvestada, et töötajale pandavad kohustused ei tooks endaga kaasa uusi turvariske. Näiteks kui pääslas töötab ainult üks uksehoidja ja kui tal puudub võimalus pääslat ajutiselt sulgeda, ei

tohi tema töökohustuste hulka kuuluda nõue, et ta peab külastajaid isiklikult külastatava juurde saatma. Uksehoidjat ei tohi selleks ka ajutiselt kohustada.

Kontrollküsimused:

- Kas kõik pääslale esitatavad nõuded on selgelt dokumenteeritud?
- Kas töötajad ja külastajad peavad enda isikut pääslas tõendama?
- Kas külastajad lähevad külastatava juurde koos saatjaga või külastatav tuleb neile pääslasse järele?
- Kas uksehoidjatele antakse õigel ajal teada, kui töötajate sissepääsuõigused on muutunud?

M 1.18 Valve- ja tuletõrjesignalisatsioon

Vastutav algatuse eest: tehnikaosakonna juhataja, tuleohutuse eest vastutav töötaja, infoturbeosakond
Vastutav elluviimise eest: tehnikaosakond

Valve- ja tuletõrjesignalisatsiooni süsteem koosneb paljudest lokaalsetest anduritest, mis on ühenduses valvekeskusega, mille kaudu ka häiresignalisatsioon käivitub. Kui valvesignalisatsioon sissemurdmise, tulekahju, vee- või gaasiavarii jaoks on olemas ning kui seda on võimalik jõukohaste kulutustega täiendada, tuleks vähemalt IT peamised tsoonid (serveriruumid, andmekandjate arhiivid, tehnilise infrastruktuuri ruumid jms) valvesüsteemi kaasata. Sel viisil on võimalik tule, sissemurdmise, varguse tõttu tekkida võivaid ohtusid õigeaegselt ära tunda ning vastuabinõud tarvitusele võtta. Selle tagamiseks on hädavajalik ohusignaalide edasisuunamine alalise valvega kohta (portjee, valve- ja turvateenistus, tuletõrje jne). Seejuures peab olema kindlaks tehtud, et nimetatud koht on ka tehniliselt ja isikuliselt võimeline häiresignaalile reageerima. Siinkohal tuleb järgida vastavas asutuses kehtivaid eeskirju.

Valve- ja tuletõrjesignalisatsioon on kompleksne süsteem, mis tuleb planeerida ja installeerida vastavalt hoone omapärale ja võimalikele ohtudele. Seepärast peaks valvesignalisatsiooni installeerimise ja hooldamisega tegelema eksperdid. Kui neid oma asutuses pole, tuleb otsida abi väljastpoolt. Nii näiteks on olemas terve rida erinevaid valvesignalisatsiooni süsteeme, mille hulgast tuleb teha valik vastavalt püstitatud turvanõuetele ja keskkonnatingimustele. Sissemurdmiste avastamiseks võib kasutada nt liikumisandureid, klaasipurunemisandureid, avamisandureid, videokaameraid jne.

Andureid võib omavahel erineval viisil võrku ühendada. Olenevalt kaitstavate tsoonide liigist ja suurusest ning kehtivatele eeskirjadele tuleb välja valida ja installeerida sobivad süsteemid. Valve- ja tuletõrjesignalisatsiooni planeerimisel ja arendamisel tuleks tähelepanu pöörata asjaolule, et trassid võrgu loomiseks oleks piisavalt dimensioneeritud ning et trasside kasutamise suhtes võetaks ette võimalikult vähe muudatusi.

Et valve- ja tuletõrjesignalisatsiooni kaitsevõimet säilitada, on vaja planeerida selle regulaarne hooldus ja funktsioonikontroll. Kui valve- ja tuletõrjesignalisatsioon puudub või ei ole olemasolevat võimalik kasutada, tulevad miinimumlahendusena kõne alla lokaalsed valveandurid. Need töötavad täiesti iseseisvalt, ilma et oleksid ühendatud valvekeskusega. Häiresignaal hakkab tööle kohapeal või lihtsa kahejuhtmelise liini kaudu (nt telefoniliin) mõnes teises kohas.

Arvutuskeskuse tööks on vaja installeerida valve- ja tuletõrjesignalisatsioon põlengute ja sissemurdmiste avastamiseks. Hoone asukohta ja selle infrastruktuuri silmas pidades võivad osutuda otstarbekohaseks ka teised detektsiooni valdkonnad.

Tugevdatud kaitset vajavad nt serveriruumid ja andmekandjate arhiivid. Kui ei ole olemas tsentraalset valve- ja tuletõrjesignalisatsiooni, on vaja installeerida lokaalsed valveandurid. Lokaalsete valveandurite kasutamisel ohu varajaseks avastamiseks on vaja hoolitseda selle eest, et signaal oleks kuulda ka väljaspool kaitstavaid ruume. Signaali edastamine võib toimuda erineval viisil ning see peaks edasi antama kohta, mis on ööpäevaringselt hõivatud. Näiteks on olemas lahendusi töötajate informeerimiseks häirest PBX-seadme või raadio teel mobiiltelefonile edastatud teate kaudu.

Enne valve- ja tuletõrjesignalisatsiooni planeerimist tuleb vastava hoone jaoks välja töötada tihe kaitsekontseptsioon. Era- või äriobjektide valvesignalisatsiooniseadmete planeerimisel tuleks kindlustusandjaga kokku leppida, kas tuleks kõne alla kindlustusmakse vähendamine, eriti kui on sõlmitud murdvarguskindlustus.

Täiendavad kontrollküsimused:

- Kas on olemas ohtude avastamise, ohusignaalide edastamise ja häiresignalisatsiooni kontseptsioon ning kas kasutamisel toimub selle kohandamine muutustega?
- Kas toimub signalisatsiooniseadme reeglipärane hooldus ja kontroll?
- Kas töötajaid on teavitatud tegutsemisest häireolukorras?

M 1.19z Sissemurdmiskaitse

Vastutav algatuse eest: tehnikaosakonna juhataja, infoturbe osakond
Vastutav elluviimise eest: tehnikaosakond

Kogemused näitavad, et sissemurdjad valivad objektid välja selle järgi, kui suur on risk ja kulu võrreldes oodatava kasumiga. Seepärast peaks kõik meetmed olema suunatud kurjategijate eduväljavaadete minimeerimiseks. Sissemurdmiskaitse üldlevinud meetmed tuleks vastavusse viia kohalike oludega. Selle hulka kuuluvad:

- ruloode kaitseseadmed akendel ja ustel, mille kaudu võib toimuda sisemurdmine,
- spetsiaalsed lukustussilindrid, lisalukud ja riivid,
- keldri valgusšahtide kaitse,
- mittekasutatavate lisasissekäikude lukustamine,
- sissemurdmise vastu kindlustatud varuväljapääsud (kui kohaliku ehitusjärelevalve poolt lubatud),
- sissemurdmist takistavad uksed, nt mis vastavad ET1 või veel kõrgematele kvaliteedinõuetele, kui võimalikud ohud seda nõuavad,
- inimesi vedavate ja kaubaliftide lukustamine väljaspool tööaega.

Füüsiliste kaitsemeetmete planeerimisel tuleb tähelepanu pöörata asjaolule, et ei rikutaks tule- ja isikukaitse eeskirju, nt evakuatsiooniteede kasutatavust. See kehtib eriti tulekaitseelementide muutuste kohta, mille tüüpide suhtes puuduvad ettekirjutused. Töötajaid tuleb reeglite abil informeerida, millised meetmed on tähtsad sissemurdmiste ärahoidmiseks.

Ka hoonesse võib olla otstarbekas paigaldada sissemurdmist takistavaid elemente, neid võib kasutada nt kõrgendatud kontrolli vajavates tsoonides, nagu serveriruumides või arvutuskeskuse põhiüksustes.

Täiendavad kontrollküsimused:

- Kas toimub sissemurdmist takistavate meetmete järgimise kontroll?
- Kas töötajad on teadlikud sissemurdmiskaitse eeskirjadest?

M 1.20 Kaablite valimine füüsiliste/mehaaniliste omaduste järgi

Vastutav algatuse eest: planeerija, tehnikaosakonna juhataja, infoturbe juht, infoturbe osakond
Vastutav elluviimise eest: tehnikaosakond, IT-juht

Kaablite valikul tuleb ülekandetehniliste vajaduste kõrval arvestada ka keskkonnatingimustega nii kaablite paigaldamisel kui ka töö käigus. Erinevate nõudmiste rahuldamiseks pakuvad kaablite tootjad erinevat liiki kaableid või töötavad välja vastavad lahendused.

Kaabli paigaldamisel siseruumides või välitingimustes tuleb tähelepanu pöörata alljärgnevatele kaablimantlit puudutavatele kriteeriumitele:

- temperatuur,
- ümbritsev keskkond (vesi, heitvesi, hape, gaas, valgus),
- kaitse näriliste vastu, torke- ja labidalöögikindlus, kivilöögikindlus, veesurvekindlus,
- funktsiooni säilimine tuleohtlikes tsoonides,
- spetsiaalsed tõmbejõud nt õhuliinide kasutamise tõttu.

Lisaks sellele tuleb tähelepanu pöörata ette nähtud trassisüsteemidele, nagu kaablirennid, kaabliredelid, kaablikanalid, kaablikarbikud, betoonist kaablitorud, treppide piirkonnad ja õhuliinide paigaldamine.

Edasise kaabeldusega seoses tuleb arvestada alljärgnevate faktoritega:

- tõmbejõud masinatega paigaldamise tõttu, nt kaabli tõmbevints, sissepuhkesüsteem või käsipaigaldus,
- käänderaadius ja külgsurve stabiilsus vastavalt paigaldamise viisile ja stabiilsele asendile tööprotsessis,
- niisked ja märjad alad kaitsegeeliga vee kahjustava toime eest,
- spetsiaalsed tõmbejõud peale paigaldamist õhuliinide suurte ulatuskauguste ja toestamisvahede või ülisuurte tõusude tõttu,
- tugevad elektrilised ja induktiivsed häireväljad varjestatud kaablite tõttu.

Õige ja eeskirjadele vastav elektrikaablite valik ning vastavasisuliste normide ja eeskirjade ning tunnustatud tehniliste regulatsioonide järgimine loob aluse elektriinstallatsiooni valmisolekuks hädaolukorraks.

Individuaalseid nõudeid kaablite valikuks ei tohi defineerida ainuüksi IT, eriti kehtib see töötingimustes, kus tuleb arvestada keskkonnamõjude või spetsiaalsete ehituslike iseärasustega. Eriti tehnikaosakonna töötajad, kes on kursis töö kulu ja muude eritingimustega, peavad osalema planeeritud kaablite paigaldamisel, tähtsate mõjude ning seega kaablite paigaldamiseks vajalike erinõuete kindlaksmääramisel.

Täiendavad kontrollküsimused:

- Kas järgitakse igakülgselt asutuse eeskirju tulekaitse ja elektritoite kindlustamiseks?

- Kas kaabli valikul küsiti tehnilise sisseseade eest vastutajalt teadaolevate või oletatavate segavate keskkonnatingimuste kohta?
- Kas on kontrollitud võimalikke alternatiivseid võimalusi kaablite paigaldamiseks?

M 1.21 Liinide õige dimensioneerimine

Vastutav algatuse eest: planeerija, IT-juht, tehnikaosakonna juhataja
Vastutav elluviimise eest: tehnikaosakond

Kaablitrassid (nt põrandakanalid, aknalauakanalid, rennid, torutrassid väljaspool hoonet) tuleb õigesti dimensioneerida. Ühelt poolt peab olema küllaldaselt ruumi, et vajaduse korral oleks võimalik ette võtta võrgu laiendamist. Teiselt poolt tuleb läbikoste vältimiseks (kaablite vastastikune mõju) kinni pidada miinimumvahemaadest kaablite vahel. Eriti tähtis on ühiste energia- ja IT-kaabelduse trasside kasutamisel tagada trasside eraldamine eraldusteede abil. Juba lihtsa elektri- ja IT- kaablite eraldi paigaldamisega on enamasti võimalik vältida tõrkeid IT- süsteemis.

Kui ei ole võimalik rajada piisavate reservidega trasse, tuleks vähemalt pöörata tähelepanu asjaolule, et trassi kulgemise piirkonnas oleks küllaldaselt ruumi edaspidisteks laiendusteks. Kui seina- ja laeavad kujundatakse vajalikus suuruses, on hiljem võimalik loobuda lärmi, mustust ja kulusid tekitavatest töödest. Järelpaigaldatavate tuletõkete kasutamisel võib avad nii varustada, et tule- ja suitsukaitse on garanteeritud, samal ajal on aga kaablite juurdevedamine igal ajal probleemideta võimalik.

Tuleb arvestada asjaoluga, et tulepüsivusklassile vastavaid seinaavasid tohib koormata vaid 60% ulatuses, et oleks võimalik saavutada nende avade efektiivne isoleerimine. Vajadusel tuleks ka edaspidiste laienduste tarvis ette näha avad ning täita need algul pehme tuletõkke või tulekaitsepatjadega.

Tähtis on, et trasside dimensioneerimine planeeritaks alati koos kaablitüüpide valikuga (vt M 1.20 Kaablite valimine füüsiliste/mehaaniliste omaduste järgi ja M 5.3 Sidetehniliselt sobivad kaablitüübid) Mõnede mitmesooneliste kaablite kasutamisega paljude väiksemate kaablite asemel saab näiteks palju ruumi kokku hoida. Varjestatud kaablite või valguslainejuhtide kasutamisega on võimalik takistada läbikostet. Nii saab ka vähese ruumiga trassidel garanteerida tõrgeteta töö.

Kontrollküsimused:

- Kas on kontrollitud võimalust, teiste kaablitüüpide valikuga ruumi kokku hoida ja läbikostet vältida?

M 1.22z Liinide ja jaotuskilpide füüsiline kaitse

Vastutav algatuse eest: planeerija, tehnikaosakonna juhataja, IT-juht
Vastutav elluviimise eest: tehnikaosakond

Ruumides, kus liigub palju rahvast või hoone tsoonides, kus puudub ülevaade, võib olla otstarbekas, kindlustada juhtmestik ja jaotuskilbid täiendavalt mittevolitatud juurdepääsu vastu. Seda on võimalik saavutada mitmel viisil:

- juhtmestiku või kaablikanalite paigaldamisega krohvi alla,
- juhtmestiku paigaldamisega terastorusse,
- juhtmete paigaldamisega mehaaniliselt vastupidavatesse ning suletavasse kanalitesse,
- jaotuskilpide lukustamise ning
- jaotuskilpide ja kanalite elektrilise kontrolli teel.

Kohtade arv, kus paigaldatud kaablile on juurdepääs, tuleb viia miinimumini ning volitamatu juurdepääsu eest kaitstavate ühenduste arv võimalikult väiksena hoida.

Eriti elektritoite ja IT-kaabelduse tsentraalsete trasside ja kaablite kaitse tuleb kogu ulatuses võimalike ohtudega vastavusse viia. Maa-alustes garaažides ja koridorides, mida kasutatakse transporditeedena, tuleb trassi või kaabli stabiilse kattekihi abil luua sobiv kaitse juhuslike mehaaniliste kahjustuste ning võimaliku sabotaaži vastu.

Kui jaotuskilbid lukustatakse, on vaja regulatsioone, mis määravad kindlaks pääsuõigused jaotuskilpidele, võtmete jagamise ja juurdepääsu tingimused. Muu hulgas tuleb ka kindlaks määrata, mida tuleb teha enne muutuste läbiviimist kaablite ja jagajate juures ning pärast taoliste tööde teostamist. Tuleb garanteerida, et muutused kooskõlastataks ja heaks kiidetaks ning seejärel dokumenteeritaks.

Täiendavad kontrollküsimused:

- Kas kohtade arv, kus kaablile on juurdepääs, on viidud miinimumini?
- Kas kaitstavate ühenduste pikkus hoiti võimalikult väiksena?
- Kus pääsuõiguste andmine toimub piiratult? Kas seejuures arvestatakse personalivahetuse ja asendustega?
- Kas pääsuõiguste andmise õigustatust ja vajalikkust kontrollitakse regulaarselt?

M 1.23 Lukustatud uksed

Vastutav algatuse eest: tehnikaosakonna juhataja, IT-juht
Vastutav elluviimise eest: tehnikaosakond, töötajad

Tühjade ruumide uksed peaksid olema suletud. Seeläbi on võimalik takistada mittevolitatud isikute juurdepääsu nendes asuvatele dokumentidele ja IT seadmetele. Üksikute bürooruumide lukustamine on eriti sel juhul tähtis, kui need asuvad tsoonides, kus liigub palju külastajaid või nendesse sisenemine ei ole teiste meetmete abil kontrollitav.

Uste lukustamisest võib loobuda, kui neil on väljaspool iselukustuv lukk. Seejuures on eelduseks, et volitatud töötajatel oleks alati oma võti kaasas.

Mõningatel juhtudel, nt suurte avatud bürooruumide korral, ei saa büroosid lukustada. Sel juhul peaks iga töötaja äraoleku ajaks oma dokumendid ("puhta laua poliitika") ja isikliku töökoha sulgema: kirjutuslaud, kapp ja arvuti (disketidraivi lukk, klaviatuurilukk), telefon.

Uste lukustamisest võib loobuda, kui kaitstavad esemed nagu dokumendid ja andmekandjad ei ole avatult väljas ning volitamata juurdepääs IT-süsteemidele ruumis (ning nendega ühenduses olevatele IT süsteemidele) ei ole võimalik.

Töötava arvuti korral võib uste lukustamisest loobuda, kui on installeeritud kaitseseade, mis teeb arvuti kasutamise võimalikuks vaid parooli sisestamisega (parooliga kaitstud ekraanisäästja), ekraan kustutatakse või kui arvuti buutimiseks on vaja sisestada parool.

Väljalülitatud arvuti korral võib loobuda büroo sulgemisest, kui arvuti käivitamiseks on vajalik sisestada parool. Sama funktsioon on ka pääsumehhanismidel, mis baseeruvad lubamarkeritel (*token passing*) või kiipkaartidel.

Täiendavad kontrollküsimused:

- Kas kontrollitakse pisteliselt büroode lukustamist, kui sealt lahkutakse?
- Kas töötajatele antakse korraldus büroo lukustamiseks nende äraolekul?

M 1.24 Veetorude vältimine IT-ruumis

Vastutav algatuse eest: tehnikaosakonna juhataja, IT-juht
Vastutav elluviimise eest: tehnikaosakond, administraator

Ruumides või tsoonides, kus asuvad tsentraalsete funktsioonidega IT- seadmed (nt serverid), tuleks vältida igat liiki veetorusid. Ainsad veetorud võiksid olla, kui tingimata vajalik, külmavee-, kustutusvee- ja küttetorud. Küttekehade juurde viivad torud peaks asuma võimaluse korral väljaspool ruumi või tsooni ning olema varustatud sulgurventiilidega. Väljaspool kütteperioodi tuleb ventiilid sulgeda.

Kui veetorusid ei saa vältida, tuleb tarvitusele võtta meetmed, mis aitaks veeleket õigeaegselt avastada või negatiivseid mõjusid minimeerida. Minimaalse kaitseabinõuna võib torude alla paigaldada drenaaživanni või –renni, mille äravooluava viib ruumist välja. Selleks on soovitatav kasutada koridori, sest nii avastatakse võimalik toru kahjustus kiiremini. Veelekete ja ebatihedate torude varajaseks avastamiseks on õigustanud end lagede valgeks värvimine.

Valikuliselt võiks paigaldada veeandurid koos automaatselt töötavate magnetventiilidega. Nimetatud magnetventiilid tuleb paigaldada väljaspool ruumi või tsooni. Selleks, et ventiilid täidaks ka pärast elektrivoolu katkemist oma kaitsefunktsiooni, tuleb need sulgeda, kui nad pole voolu all.

Täiendava või alternatiivse meetmena on soovitav kasutada automaatset drenaaži (vt M 1.14 Automaatne drenaaž).

Kõik IT- ja tehnikaosakonna töötajad peaksid olema informeeritud, et kõrgete käideldavusnõuetega IT-süsteemidega hoone tsoonides on veetorud probleemiks ning millele nendega seoses tuleb tähelepanu pöörata.

Kontrollküsimused:

- Kas toimub olemasolevate veetorude reeglipärane tiheduse kontroll (vaatlus)?

M 1.25 Liigpingekaitse

Vastutav algatuse eest: IT-juht, tehnikaosakonna juhataja, infoturbe osakond
Vastutav elluviimise eest: tehnikaosakond, administraator

Vastavalt energiaettevõtte toitevõrgu ning oma elektrijuhtmestiku kvaliteedile ja väljaehitusele, sõltuvalt keskkonnast (teised voolutarbijad) ja geograafilisest asendist, võivad induktsiooni või pikselöögi tagajärjel tekkida elektrivõrgus ülisuured liigpinged. Liigpinge vastu suunatud kaitsemeetmed on vajalikud IT- seadmete võimalike kahjustuste vähendamiseks võrkudes otsese pikselöögi, ühendamise ja lülitustegevuse tagajärjel.

Ka teiste elektriliselt juhitud välisühenduste nagu telefoni, vee- ja gaasijuhtmete kaudu võivad liigpinged jõuda hoonesse ja seal töötavatesse IT- seadmetesse. Lisaks sellele võivad liigpinged jõuda ka sisemistesse juhtmetesse.

Täielik liigpingekaitse kontseptsioon arvestab kõigi väliste ja sisemiste elektriliselt juhitud ühendustega ning koosneb kolmest astmest, mis orienteeruvad peaasjalikult liigpingekategooriate transientliigpingetele:

- Põhikaitse hoone toitepunktis on võimeline kinni püüdma liigpinget, mis on tekkinud otsese pikselöögi tulemusena ning hoidma seda madalamana kui 6000 V. Olemasoleva välise piksekaitse korral peab põhikaitse olema võimeline kaitsma pikselöögi eest, kuna tuleb arvestada 100 kA voolutugevusega.
- Vahekaitse korruste jaotusseadmetes piirab järelejäänud liigpinge *ca* 1500 voldile ning tagab, et selle poolt maandatav liigpinge ei ületaks 6000 volti.
- Liigpingekaitse kõikide teiste juhtmete kontaktide ja pistikühenduste juures vähendab järelejäänud liigpinget tasemele, mis ei ohusta vooluvõrku ühendatud seadmeid. Elektriliste ja elektrooniliste seadmete tootjad enamikes maades on kohustatud varustama oma seadmed häireteta funktsioneerimiseks vajaliku liigpingekaitsega (sellele viitab CE-tähistus).

Iga astme kaitsemõju baseerub eelmisel. Ühest astmest loobumine muudab kogu liigpingekaitse peaaegu olematuks.

Kui liigpingekaitse ei ole võimalik kogu hoone ulatuses, võib vähemalt IT tähtsad osad (serverid jne) ümbritseda vastava kaitsetsooniga. Võrgud, millesse on ühendatud palju seadmeid, võib võimalike kahjustuste minimaalsel tasemel hoidmiseks optilise sidesti või liigpinge lahendi abil väiksemateks üksteise vastu kaitstud tsooniks jagada. Seejuures tuleb kaitstud ja kaitseta tsoonid kuni tagasi kaitseseadmeni, kus toimub jagamine, järjekindlalt eraldada. Toitejuhtmed tuleb paigaldada piisava vahemaaga, ühte kaablikanalisse - koos paigaldamine kõrvaldaks kaitsemõju. Liigpingekaitse seadmeid tuleks perioodiliselt ning teatud intsidentide järel kontrollida ning vajadusel asendada. Eriti uue liigpingekaitse kontseptsiooni koostamisel tuleb arvestada olemasolevate puhvertoiteallikate ja võrgu varuseadme paigaldamise ja talitlusviisiga.

Lisaks liigpingekaitsele toitevõrgus peab serveriruumides ja arvutuskeskuse kesksetes üksustes rakendama abinõusid elektrostaatilise lahenduse vastu. Põrandakatete kontakttakistus sellistes ruumides peab olema 10 ja 100 megaoomi vahel. Vastavalt nõuetele peavad need olema raskesti süttivad. Sama kehtib ka tõstetud põranda või installatsioonipõranda kohta.

Sõltumatult liigpingekaitse ulatusest ja kujundusest tuleb tähelepanu pöörata kahele põhilisele eeltingimusele:

- Juhtme pikkus liigpingekaitse ja kaitstavate seadmete vahel ei tohiks ületada 20 meetrit. Kui see siiski peaks nii olema, tuleb vahele lisada veel üks liigpingekaitse. Kui seadmel on liigpingekaitse pääsupunkti juures, langeb 20 meetri piirang ära.
- Funktsioneeriva liigpingekaitse jaoks on nõutav kõikide liigpingekaitsesse kaasatud elektriseadmete ulatuslik potentsiaaliühtlustus. Enamik IT- seadmete liigpinge tagajärjel tekkinud kahjustustest on tingitud mitte järjekindlalt rakendatud potentsiaaliühtlustusest.

Täiendavad kontrollküsimused:

- Kas pikse- ja liigpinge kaitseseadmeid kontrollitakse perioodiliselt ning teatud intsidentide järel ja vajadusel asendatakse?
- Kas on teostatud üldine potentsiaaliühtlustus?
- Kas täiendava installeerimise käigus pööratakse tähelepanu sellega kaasnevale potentsiaaliühtlustusele?

M 1.26w Toite avariilülitid

Vastutav algatuse eest: tehnikaosakonna juhataja, IT-juht
Vastutav elluviimise eest: tehnikaosakond

Ruumides, kus elektriseadmete kasutamine toimub selliselt, et nende heitsoojuse, tiheda paiknevuse või täiendava tulekoormuse olemasolu tõttu on kõrgenenud tuleohtlikkus, on otstarbekas installeerida avariilüliti. Sellisteks ruumideks on nt serveri- või tehnikaruumid. Kuna avariilüliti aktiveerimiseks on vajalik personali olemasolu, tuleb selle paigaldamine kõne alla vaid tsoonides, kus alati või enamasti keegi kohal on. Tsoonides, kus töötajad ei viibi või viibivad vaid vahetevahel, on oluliselt efektiivsem avarii-väljalüliti, mis aktiveerub põlengu avastamisel tulekahjuanduri kaudu.
Avariilüliti aktiveerimisega võetakse põlengult oluline energiaallikas, mis väiksemate põlengute korral võib viia nende kustumiseni. Vähemalt on aga elektripinge kaudu tekkiv oht tule kustutamisel kõrvaldatud.
Tähelepanu tuleb pöörata asjaolule, et kohalikud puhvertoiteallikad võtavad välise toitevoolu väljalülitamise järgselt üle vooluga varustamise ning ühendatud seadmed jäävad pinge alla. Seepärast tuleb avariilüliti installeerimisel jälgida, et ka puhvertoiteallikas lülitataks välja ning mitte ainult ei lahutataks välisest toiteallikast.
Avariilüliti tuleks paigaldada ruumi sisse ukse kõrvale (soovitavalt viitega asukohale ukse juures väljaspool ruumi) või ukse kõrvale väljaspool ruumi. Seejuures on aga võimalik, et avariilüliti aktiveerimine võib toimuda ka ekslikult või tahtlikult ilma ohuolukorrata. Seepärast tuleb avariilülitile paigaldada kate, et kaitsta seda eksliku aktiveerimise eest.
Kui tuletõrje nõuab avariilüliti olemasolu, võib selle paigaldada tuletõrje võtmelülitina. Seeläbi välistatakse enamasti selle kogemata või volitamatult sihilikult käivitamine.

Näide

- Keskmise suurusega ametiasutuse serveriruumi paigaldati umbes 10 serverit, 5 laserprinterit ja teisi seadmeid. Ruum oli sissemurdmiskaitse tagamiseks varustatud vastavate seinte, akende ja ustega. Avariilülitit ei olnud. Oli ainult kaks punkti, et nimetatud ruumist elektrivool välja lülitada: hoone peajaotuskilp keldris või ruumi jaotuskilp. See asus aga seinal sissepääsu vastas, põlengu korral peaaegu kättesaamatus kohas.

Kontrollküsimused:

- Kas on kõikide tehnikaruumide suhtes kontrollitud, kas avariilüliti installeerimine on otstarbekas?
- Kas kõik avariilülitid on ettekavatsematu aktiveerimise vastu kaitstud?
- Kas avariilüliti paigaldamisel võetakse arvesse, et selle käivitamisel ei lülitata välja üksnes asutusevälist toidet, vaid ka USV?

M 1.27 Konditsioneer

Vastutav algatuse eest: tehnikaosakonna juhataja, IT-juht
Vastutav elluviimise eest: tehnikaosakond

IT seadmete temperatuuri tagamiseks lubatud piirides ei piisa mõnikord ruumi normaalsest õhu- ja soojusvahetusest, nii et osutub vajalikuks konditsioneeri sisseehitamine. Selle ülesandeks on hoida ruumiõhku IT poolt ettenähtud piirides. Kui lisaks sellele esitatakse nõudeid õhuniiskusele, nt elektrostaatilise lahenduse vältimiseks, võib kliimaseade ventilatsiooni kaudu täita ka seda ülesannet. Selleks tuleb aga kliimaseade ühendada veetoruga (vt M 1.24 Veetorude vältimine IT-ruumis).

Kliimaseadme kaitsemõju säilitamiseks on vajalik selle regulaarne hooldus. Soovitav on kasutada koos konditsioneeriga täiendavat järelevalveseadet, eriti täiskonditsioneeri korral. Kuna kliimaseadme seiskumisel tuleb teatud juhtudel paljud (eriti tähtsad) IT süsteemid välja lülitada, peaks see olema paigaldatud kõrgetele käideldavusnõuetele vastavalt. See peaks olema dimensioneeritud suure võimsusreserviga, peale selle peaks see olema lihtsalt täiendatav. Hädaolukorraks valmisoleku planeerimisel (vt moodulit B 1.3 Hädaplaanimine) ei tohiks konditsioneeri unustada.

Serveriruumi või arvutuskeskuse jaoks vajaliku jahutusvõimsuse kindlaksmääramiseks tuleb läbi viia täpne soojuskoormuse arvutamine. Värske õhu juurdevool on vajalik juhul, kui konditsioneeritud ruumis (ruumides) viibivad pidevalt töötajad.

Samuti tuleb erinevatel päevaaegadel teostatud mõõtmiste abil kindlaks määrata, kas nimetatud ruumides on vajalik õhuniiskuse suurendamine või vähendamine. Siinkohal tuleb järgida ka rakendatud IT-komponentide tootjaeeskirju.

Soojusvaheti ja jahutusseadmed ei peaks asuma otseselt serveriruumis või arvutuskeskuses, et takistada kliimaseadme rikete, nt jahutusvedeliku lekete või lühiühenduste tõttu tekkivaid tõrkeid.

Kui konditsioneeri jahutusseadmed on paigutatud väljapoole hoonet, tuleb neid kaitsta otsese pikselöögi eest. Eriti kõrgete turvanõuetega tsoonides ei tohiks jahutusseadmetele igaüks juurde pääseda ning need peaksid olema füüsiliselt kaitstud ka sabotaaži vastu.

Täiendavad kontrollküsimused:

- Millistes IT-ruumides võivad esineda kõrgenenud temperatuurid?
- Kas toimub kasutuses olevate kliimaseadmete regulaarne hooldus?
- Millised on IT-ruumis lubatud temperatuuri ja õhuniiskuse piirväärtused?

M 1.28 Puhvertoiteallikas

Vastutav algatuse eest: tehnikaosakonna juhataja, IT-juht, infoturbe osakond
Vastutav elluviimise eest: administraator, tehnikaosakond

Lokaalse puhvertoiteallika (UPS) ülesanne on kaitsta üksikut IT-süsteemi või mõnda IT-seadet elektritoite lühiajaliste katkestuste tagajärgede eest. Selline eesmärk on seatud tavaliselt väiksemates IT-struktuurides, millel ei ole lisaks avariitoiteallikat.
Suuremate IT-struktuuride või isegi tervete hoonete varustamiseks kasutatakse peamiselt tsentraalseid UPS-süsteeme (vt M 1.70 Tsentraalne puhvertoiteallikas).
Ükskõik, kas kohalikku UPS-d kasutatakse kui lisaseadet või kui 19-tollist lisandmoodulit, on selle jõudlus ja toetusaeg kindlaks määratud seadme omadustega ja neid ei saa tavaliselt muuta.
Tänapäeval kasutatavate kohalike UPS-seadmete ja tavaliselt nende kaudu võimaldatud vähese jõudluse (vahemikus kuni u 1 kVA) korral on võimalik probleemideta katta kuni 120 minuti pikkused voolukatkestused (toetusaeg). Milline toetusaeg on tegelikult konkreetses olukorras vajalik, sõltub sellest, kui kaua ühendatud seadmete väljalülitamine (shutdown) kestab ja kui kaua tuleb oodata, et elektritoide jälle aktiveeruks (ooteaeg). Et suurem osa voolukatkestusi kestab üksnes mõned minutid, peaks toitevarustuse katkestuse kõrvaldamiseks tavaliselt piisama 15-minutilisest ooteajast. Kui toitevarustuse katkestus kestab ooteajast kauem ja kui varustatav IT-süsteem tuleb andmekadude vältimiseks peatada, tuleks kogu toetusaeg määrata valemi
toetuseaeg = ooteaeg pluss kahekordne väljalülitusaeg
järgi. Kahekordse väljalülitusajaga antakse turvavaru, kui peatamine kestab eeldatust kauem. IT-seadmete, mida varustatakse UPS-ga, igakordsel väljavahetamisel või täiendamisel tuleb uuesti kontrollida, kas olemasolev toetusaeg on piisav.
Eristada võib kolme UPSliiki:

- VFD-UPS
  VFD-UPS (VFD Voltage and Frequency Dependent) korral saavad ühendatud tarbijad tavarežiimis toidet otse vooluvõrgust. Väiksemad vooluvõrgu häired võivad jõuda seega kuni ühendatud tarbijateni. Alles siis, kui see rivist välja langeb, lülitub VFD-UPS iseseisvalt sisse ja võtab toitega varustamise üle. Selleks vajab see kuni 10 ms (ümberlülituspaus), mis on mõnede IT-seadmete jaoks juba liiga palju. VFD-UPS-d nimetati varem ka Offline-UPS-ks.
- VI-UPS (Voltage Independent)
  Selle puhvri korral reguleeritakse toitepinget väiksemate kõikumiste korral (VI – Voltage Independent), ilma et UPS kui selline võtaks täielikult üle ühendatud tarbijate varustamise. VI-UPS väljundi sagedus on aga nagu ka VFD-UPS puhul otseselt sõltuv vooluvõrgust. Ka VI-UPS korral võib akutoitel esineda ümberlülituspaus.
- VFI-UPS (Voltage and Frequency Independent)
  VFI-UPS(Voltage and Frequency Independent) puhul ei ole tavaliselt UPS-sisendi ja -väljundi vahel otsest ühendust. Elektrienergiat reguleeritakse sisendi poolel ja suunatakse vahevõrku. Sealt hoitakse akusid optimaalses

laadimisolekus ja varustatakse inverterit. See toodab ühendatud tarbijate jaoks vajalikku vahelduvvoolu.

Et väljundienergiat toodetakse sisendist sõltumatult pidevalt inverteri kaudu, siis ei teki ümberlülituspause. VFI-UPS-d nimetati varem Online-UPS-ks.
Et VFI-UPS töötab kõigist kolmest süsteemist ainsana tõesti katkestusteta, tuleks alati eelistada seda. Võttes arvesse muid, siin käsitlemata kvaliteediomadusi, kujutab UPS, mis on liigitatud DIN IEC 62040-3 järgi VFI-SS-111 kohaselt, endast IT-toite kõige optimaalsemat varianti.
Mõlemad puhvertoiteallikad võivad lisaks elektrivarustuse täielikust lakkamisest ja alapingest üleaitamisele tasandada ka liigpingeid. Ka siinkohal kehtib liigpingekaitse suhtes meetmes M 1.25 Liigpingekaitse ära toodud 20 meetri piirang.
Selleks, et vältida probleeme maanduslekkevooluga, ei tohiks lokaalse UPS kaudu toitega varustatavate IT-seadmete ühendamisel muude IT-seadmetega, mida varustatakse toitega muul moel, kasutada varjestatud kaableid (nt printerikaabel).
Et lokaalse UPS akusid kasutatakse väga harva nende optimaalses temperatuurivahemikus (tavaliselt 20 °C piires), on akude kasutusaeg lokaalsete UPS-seadmete puhul üsna lühike, parimal juhul kuni 5 aastat, enamasti vähem. Selle kasutusaja jooksul väheneb akude jõudlus pidevalt, mille tulemusel on lokaalse UPS toetusaeg kahe või kolme aasta pärast kahanenud võibolla kõigest pooleni uue seadme toetusajast. Selleks, et veenduda, kas UPS-l on olemas vajalik toetusaeg, tuleks umbes üks kord aastas välja selgitada tegelik toetusaeg. Mõnedel UPS-süsteemidel on selleks integreeritud kontrollmehhanismid. Kui see nii ei ole, võib väärtuse välja selgitada koormustestiga.
Nagu kõikide muudegi elektriseadmete korral tuleb ka UPS-süsteemide puhul pöörata tähelepanu sellele, et neid kasutataks tootja poolt nimetatud temperatuurivahemikus. Selle asjaoluga tuleb arvestada ka jahutuse dimensioneerimisel.
UPS kaitsemõju säilitamiseks tuleb seda regulaarselt hooldada. Selleks tuleb kinni pidada tootja ette nähtud UPS hooldusvälpadest.
Kui lokaalne UPSasub koos selle poolt varustatava IT-seadmega tulekahju seiretsoonis ja tulekahju seire käivitab seiretsoonis pinge aktiveerimise, tuleb ilmtingimata hoolitseda selle eest, et ka lokaalne UPS oleks täielikult välja lülitatud. See tähendab, et välja ei lülitata üksnes UPS toidet (UPS sisend). Välja tuleb lülitada ka inverter (UPS väljund) ja akud tuleb UPS elektriühendusest lahti ühendada.
Puhvertoiteallikas sildab lühiajalisest voolukatkestusest või säilitab vooluga varustatust nii kauaks, et on võimalik ühendatud arvutite ettenähtud korras mahalaadimine. See on eriti otstarbekas alljärgnevatel juhtudel:

- kui arvuti vahemällu salvestatakse suurel hulgal andmeid (nt Cache võrguserveris), enne kui need mittekaduvatele mäluseadmetele salvestatakse.
- kui voolu katkestuse tagajärjel läheks kaduma terve hulk andmeid, mida tuleks tagantjärele uuesti taastada,
- kui ei ole tagatud küllaldase stabiilsusega elektritoide.

Tehakse vahet kaht liiki puhvertoiteallikate vahel:

- offline puhvertoiteallikas: seejuures saavad võrku ühendatud tarbijad normaaljuhul toidet otse vooluvõrgust. Alles siis, kui see enam ei toimi, lülitub puhvervooluallikas automaatselt sisse ning võtab toitefunktsiooni üle.

- online puhvertoiteallikas: sel juhul on puhvertoiteallikas alaliselt võrgu ja tarbijate vahele ühendatud. Kogu elektritoide kulgeb kogu aeg puhvertoiteallika kaudu.

Kui IT seadmeid TN-S-võrguga hoones (vt M 1.39 Tasandusvoolude vältimine varjes) varustatakse lokaalse puhvertoiteallika kaudu, tuleb tähelepanu pöörata alljärgnevatele asjaoludele: Et TN-S võrgu kaitsemõju tasandusvoolude suhtes andmeside liinide varjes säilitada, tuleb tähelepanu pöörata asjaolule, et puhvertoiteallikal ei ole väljaminekul ühendust N- ja PE-juhi vahel (kaitsemaandus). Vajadusel tuleb sellised seeriatootmise käigus sisseehitatud ühendused enne paigaldamist TN-S võrku eemaldada.

Puhvertoiteallika dimensioneerimisel võib reeglina lähtuda tavapärasest umbes 10 kuni 15 minutilisest sildamisajast. Enamasti likvideeritakse voolukatkestused 5 kuni 10 minuti jooksul, nii et pärast nimetatud ajavahemiku möödumist jääb veel 5 minutit aega üle, et võrku ühendatud IT ettenähtud korras alla laadida, kui voolukatkestus peaks kestma kauem. Enamik moodsatest puhvertoiteseadmetest pakuvad arvutiliideseid, mis võivad eelnevalt kindlaks määratud aja järgi, vastavalt IT ajavajadusele ja puhvertoiteseadme võimsusele algatada õigeaegse automaatse mahalaadimise. Spetsiaalsete rakendusjuhtumite korral (nt PBX-seadmed) võib vajalik sildamisaeg kesta ka mitmeid tunde.

Puhvertoiteallika kaitsemõju säilitamiseks on vajalik selle regulaarne hooldus. Kui katkematu elektritoide on võimalik mingi teise allika kaudu (nt ühendamisel keskse puhvertoiteallikaga), on tegemist alternatiiviga lokaalsele puhvertoiteallikale.

Kontrollküsimused:

- Kas peetakse kinni puhvertoiteallikate hooldusintervallidest?
- Kas on ette nähtud automaatne mahalaadimine?
- Kas toimub reeglipärane puhvertoiteallika mõjususe testimine?
- Kas on toimunud muudatusi, nii et olemasoleva puhvertoiteallika võimsusest enam ei jätku?
- Kas UPS-seadmete ja IT-seadmete jaoks on olemas ülepingekaitse?
- Kas välditakse varjestatud juhtmetega ühendusi UPS-ga kaitstud IT-seadmete ja muul moel toitega varustatavate IT-seadmete vahel?
- Kas jahutuse ja ruumitemperatuuri dimensioneerimisel kontrollitakse tootja poolt antud UPS-seadmete temperatuurivahemikke?
- Kas aku tegelikku võimsust ja koos sellega UPS toetusaega testitakse korrapäraselt?
- Kas peetakse kinni UPS hooldusvälpadest?
- Kas IT-süsteemi BMA-ga juhitud pinge aktiveerimise korral lülitatakse täielikult välja ka lokaalne UPS?

M 1.29z IT-süsteemi õige paigutus

Vastutav algatuse eest: tehnikaosakonna juhataja, IT-juht
Vastutav elluviimise eest: tehnikaosakond, kasutaja

IT-süsteemi paigaldamisel tuleb tähelepanu pöörata mitmesugustele eeldustele, mis parandavad tehniliste seadmete turvalisust ja usaldusväärsust, pikendavad nende eluiga ning pööravad tähelepanu ergonoomilisusele (vt ka M 3.9 Ergonoomiline töökoht), näiteks:

- IT-süsteem peaks olema võimalikult nii paigaldatud, et ainult volitatud kasutajad saavad näha monitoripildi sisu. Kui arvuti on paigaldatud akna või ukse lähedusse, on võimalik monitoril olevat teksti väljastpoolt jälgida.
- IT-süsteemide manipuleerimise vältimiseks peaksid need olema paigaldatud nii, et ainult volitatud isikutel oleks juurdepääs. Tsoonides, kus liigub tihti võõraid, tuleb IT-süsteeme kaitsta täiendavate meetmetega varguse ja manipuleerimise vastu.
- Ülekuumenemise vältimiseks ei tohiks IT-süsteemi paigaldada küttekolde vahetusse lähedusse.
- IT-süsteem ei tohiks asuda otsese päikesekiirguse käes.
- Vältida tuleks tolmu ja mustust, mis võib kahjustada mehaanilisi komponente (eemaldatavate meediate draivid, mehaaniline hiir, kõvakettad).
- Paigalduskoht tuleks valida nii, et oleks võimalik vältida välismõjudest nagu üleujutustest, torude purunemisest, kõrgenenud õhuniiskusest, elektrilisest vahelesegamisest, elektromagnetilisest kiirgusest tingitud kahjustusi.

Kõik töötajad peaksid olema informeeritud, millised mõjud on IT- süsteemidele kahjulikud, et nad saaksid nende vältimisele kaasa aidata. Nende hulka kuuluvad näiteks määrdumine söökide või jookidega, sigaretisuitsu- või –tuhaga, aga ka puhastusvahendite vale kasutamise tõttu.

Olenevalt aluspinnast võib olla otstarbekas kasutada IT-süsteemide kaitseks täiendavaid abivahendeid, nagu nt klaviatuuri katteid, monitori ekraanifiltreid, mis takistavad selle nägemist kõrvalt.

Täiendavad kontrollküsimused:

- Kas IT-süsteemid on paigutatud nii, et need on kaitstud volitamatu juurdepääsu eest.
- Kas varem on täheldatud süsteemi paigutuskohast tingitud tõrkeid?

M 1.30 PBX-arveldusandmetega andmekandjate kaitse

Vastutav algatuse eest: PBX-seadmete eest vastutav töötaja, andmekaitse eest vastutav töötaja
Vastutav elluviimise eest: administraator

PBX-seadmetele laekuvad töö käigus arveldusandmed. Need sisaldavad alljärgnevat informatsiooni:

- jutuajamise kellaaeg ja kuupäev
- helistaja ja vastuvõtja number ning
- kõne kestus.

Nimetatud andmed võivad olla salvestatud nii PBX-seadme enda kõvakettale kui ka välisele arveldusarvutile. Paljudel juhtudel on tegu kombinatsiooniga mõlematest variantidest. Arvuteid tuleb — kui vähegi võimalik — kaitsta nii, et ainult volitatud isikutel oleks juurdepääs arveldusandmetele. Seepärast on nõutav, et arveldusarvuti oleks paigaldatud hästi turvatud ruumi (vt moodulit B 2.4 Serveriruum). Seadmete suhtes, millele on salvestatud arveldusandmed, tuleb lisaks realiseerida meetmed M 1.23 Lukustatud uksed , *M 2.5 Vastutuse ja ülesannete jaotamine* , *M 2.6 Sissepääsuõiguste andmine* , M 2.7 Süsteemi ja võrgu pääsuõiguste andmine , M 2.8 IT-rakendustele ja andmetele pääsuõiguste andmine , M 2.13 Tundlike ressursside jäljetu hävitamine ja M 2.17 Sisenemisreeglid ja reguleerimine .

Samuti tuleb dokumenteerida, millistel isikutel millistes rollides on ligipääs arveldusandmetele.

Täiendavad kontrollküsimused:

- Kellel on õigus juurdepääsuks arveldusandmetele?
- Kuidas realiseeritakse juurdepääsukaitse?
- Kas ainult õigustatud huviga kasutajatel on juurdepääsuõigus?
- Kus asuvad varukoopiad ja kellel on nendele juurdepääs?
- Kuidas toimub andmekandjate hävitamine?
- Kui kauaks andmed salvestatakse?

M 1.31z Tõrgete kaugindikatsioon

Vastutav algatuse eest: IT-juht, PBX-seadmete eest vastutav töötaja, infoturbe osakond
Vastutav elluviimise eest: administraator

IT-seadmed ja tugiseadmed, mis ei nõua või nõuavad vaid harva teenindamist mõne isiku poolt, paigutatakse tihti suletud ja lukustatud ruumidesse (nt serveriruumi). Tulemuseks on, et rikked, mis varases staadiumis veel IT-le mõju ei avalda ja lihtsalt kõrvaldatavad on, avastatakse alles liiga hilja, enamasti mõju tõttu IT-le. Tuli, puhvertoiteallika funktsioonihäired või konditsioneeri seiskumine oleks näideteks taolistest “hiilivatest” ohtudest.

Kaugindikatsiooni abil on võimalik taolisi tõrkeid varem avastada. Paljud seadmed, mida peab usaldama, ilma et oleks võimalik neid pidevalt kontrollida ja jälgida, on kaasajal ühendatud tõrgete kaugindikatsiooniseadmega. Tehnilised võimalused ulatuvad seejuures lihtsatest kontaktidest, mille kaudu saab hoiatuslambi sisse lülitada kuni arvutiliidesteni selle juurde kuuluva tarkvarapaketiga levinud talitlussüsteemide jaoks. Liideste kaudu on tihti isegi võimalik igal ajal kindlaks teha ühendatud seadmete tööseisundit ning nii tõrgetele õigeaegselt vastu astuda.

Täiendavad kontrollküsimused:

- Kas kaugindikatsiooni kaudu häiresignaali saanud isikud teavad, mida tuleb häire korral ette võtta?

M 1.32 Printerite ja koopiamasinate turvaline paigutus

Vastutav algatuse eest: IT-juht, infoturbeosakond
Vastutav elluviimise eest: administraator

Et takistada printeritega manipuleerimist ning prinditud materjalide kopeerimist või lugemist mittevolitatud isikute poolt, tuleks printerid nii paigutada, et neile oleks juurdepääs vaid selleks volitatud isikutel. Vähemalt ei tohi printereid paigutada kohtadesse, kus viibib tihti võõraid inimesi, näiteks nõupidamis-, ürituste- ja koolitusruumide lähedusse. Erandiks on vaid printerid, mis on spetsiaalselt ette nähtud selliste kohtade, näiteks koolitusruumide jaoks.

Printeriruumides on tihti ka koopiamasinad. Turvalisuse seisukohalt tuleb järele mõelda, kas ei teki oht, et valmistatakse kättesaadavatest väljatrükkidest kiiresti koopiad. Teiselt poolt näitab kogemus, et isegi kui väljatrükid lihtsalt kaasa võetakse, kiruvad kogemuste kohaselt enamik kasutajaid tehnikat ning ei mõtle sellele, et keegi teine võis väljatrüki pahade kavatsustega kõrvaldada.

Selliste probleemide vältimiseks on otstarbekohane printerid ja koopiamasinad nii paigutada, et need oma personalile hästi nähtavad oleks. Näiteks ei tohiks printereid ja koopiamasinaid paigaldada hämarasse nurka, vaid need peaksid olema läbi klaasukse sekretariaadist nähtavad. Parem on aga paigaldada printerid ja koopiamasinad suletud ruumi, kuhu pääsevad vaid volitatud isikud. See on soovitatav kõrgema kaitsevajaduse korral.

Veelgi parem on, kui väljatrükid jagatakse usaldusväärse isiku poolt sahtlitesse, millele on juurdepääs vaid nende omanikel. Väljatrükkidele tuleb seepärast lisada adressaadi nimi. See võib toimuda automaatselt trükiprogrammide abil. Väga kõrge kaitsevajaduse korral tuleks kontrollida, kas nimetatud lahendus on sobiv.

Kasutajad avastavad tihti alles printeri juures, et on vale dokumendi välja trükkinud või et tuleb teha veel väike muudatus. Sellised väljatrükid visatakse tihti otse printeri juures asuvasse lahtisesse paberikorvi. Kuna nii võivad konfidentsiaalsed dokumendid valedesse kätesse sattuda, on soovitav paigaldada kohe võrguprinterite kõrvale paberihunt. Selle puudumisel tuleb kasutajate tähelepanu juhtida asjaolule, et taolisi dokumente ei tohi vedelema jätta ning et need tuleb mingil muul viisil hävitada.

Täiendavad kontrollküsimused:

- Kas printerid ja väljatrükitud materjalid on kaitstud volitamata isikute kätte sattumise eest?

M 1.33 Kaasaskantavate IT-süsteemide hoidmine reisil

Vastutav algatuse eest: IT-juht, infoturbeosakond
Vastutav elluviimise eest: kasutaja

Kuna keskkonnatingimused IT-süsteemide mobiilsel kasutamisel asuvad enamasti väljaspool kasutaja mõjusfääri, peavad nad kindlustama kaasaskantavate IT-süsteemide, nt sülearvutite või pihuarvutite turvalise säilitamise ka väljaspool töökohta.

Kaasaskantavate IT-seadmete nagu sülearvutite, mobiiltelefonide, tahvelarvutite ja PDA-de puhul tuleb jälgida, et neid hoitaks ka väljaspool asutust ringi liikudes turvaliselt. Mõned soovitused seadmete mobiilseks kasutamiseks:

- Kaitse varguse eest
- Vastavalt võimalustele peaks olema aeg, mil seade järelevalveta jäetakse, minimaalne.
- Kui kaasaskantavat süle- või pihuarvutit hoitakse autos, ei tohi see olla väljast nähtav. Abi on seadme kinnikatmisest või lukustamisest kohvriruumi. Mobiilne IT-süsteem võib olla suure väärtusega, mis meelitab ligi potentsiaalseid vargaid, kuna kaasaskantavaid IT- süsteeme on kerge ärandada.
- Kui mobiilset IT-süsteemi kasutatakse võõrastes bürooruumides, tuleb see ruum vastavalt võimalustele ka lahkumisel lühikeseks ajaks lukustada või arvuti kaasa võtta. Kui ruumist lahkutakse pikemaks ajaks, tuleks lisaks sellele mobiilne IT-süsteem välja lülitada ning pääsukaitse aktiveerida, et takistada volitamatut kasutamist.
- Hotelliruumides ei tohiks mobiilne IT-süsteem olla avatuna juurdepääsetavas kohas. Seadme lukustamine kappi hoiab ära juhusliku varguse.
- Mõningaid uusi seadmeid on lisaks võimalik ketiga kinnitada. Varastamise eelduseks on sel juhul tööriistade olemasolu.
- Mobiilset IT-süsteemi ei tohi kunagi hoida ekstreemsetel temperatuuridel. Iseäranis aku, aga ka monitor võivad saada kahjustada. Eriti tuleks vältida IT-seadmete ja akude jätmist pargitud autodesse.
- Samuti tuleks mobiilseid terminale kaitsta kahjulike keskkonnamõjude, näiteks vihma ja pritsmeveest tingitud niiskuse eest.
- Mobiilsed terminalid võivad puruneda, seepärast tuleks neid ka lühikeste marsruutide korral transportida võimalikult põrutuste eest kaitstuna. Sülearvutid peavad transpordi ajal olema suletud, kuna nii šarniirid kui ka monitor võivad tõuke ajal saada kahjustada. Põhimõtteliselt on alati soovitatav kasutada transpordiks turvalist vahendit.

Soovitav on koostada mobiilsete IT-süsteemide kasutajate jaoks infoleht, mis sisaldab tähtsamaid nõuandeid ja ettevaatusabinõusid seadmete nõuetele vastavaks hoidmiseks ja turvaliseks transpordiks.

Kontrollküsimused

- Kas kaasaskantavate IT-süsteemide kasutajate tähelepanu juhitakse seadmete õigele hoidmisele?

M 1.34 Kaasaskantavate IT-süsteemide hoidmine põhiasukohas

Vastutav algatuse eest: IT-juht, infoturbeosakond
Vastutav elluviimise eest: kasutaja

Kaasaskantavad IT-süsteemid nagu sülearvutid, pihuarvutid või mobiiltelefonid on oma ehituse tõttu alati armastatud varguse objektideks. Seepärast tuleb neid ohtude eest kaitsta ka juhul, kui need asuvad oletatavalt turvalises bürooruumis. Seepärast tuleb järgida moodulis B 2.3 Bürooruum kirjeldatud meetmeid. Kuna kaasaskantavaid IT-süsteeme on eriti kerge transportida ja varjata, tuleks seade väljaspool kasutusaega luku taha panna, näiteks kappi või kirjutuslaua sahtlisse või kinnitada ketiga.

Kontrollküsimused

- Kuidas hoitakse kaasaskantavaid IT-süsteeme büroodes?

M 1.35z Kaasaskantavate IT-süsteemide ühisladustus

Vastutav algatuse eest: IT-juht, infoturbeosakond
Vastutav elluviimise eest: administraator

Kui asutuses või ettevõttes on (mobiilses) kasutuses palju kaasaskantavaid IT-süsteeme ning kui nende kasutajad tihti vahelduvad, võib ajutiselt mitte kasutatavaid sülearvuteid ühisladustuses (*Pool*) hoida. Selleks kasutatav ruum peaks vastama moodulis B 2.6 Tehnilise infrastruktuuri ruum kirjeldatud nõuetele.

Seejuures tuleb kindlustada sülearvutite varustamine toitevooluga, et seadmete patareid võimaldaks nende kohest kasutamist. Lisaks sellele tuleb dokumenteerida kaasaskantavate IT-süsteemide väljastamine ja tagastamine.

Täiendavad kontrollküsimused:

- Kellel on juurdepääs IT-süsteemide ühisladustusele?
- Kas sülearvutite väljastamine ja tagastamine dokumenteeritakse?

M 1.36 Andmekandjate transpordieelne ja –järgne turvaline säilitus

Vastutav algatuse eest: infoturbe osakond
Vastutav elluviimise eest: kasutaja, postipunkt

Enne andmekandja teelesaatmist tuleb kindlustada, et andmete andmekandjale salvestamise ja transpordi vahelisel ajal oleks andmetele tagatud piisav kaitse volitamatu juurdepääsu vastu. Kirjeldatud andmekandjaid tuleks nii säilitada, et nendele oleks juurdepääs ainult volitatud isikutel, olenemata, kas tegu on analoog- või digitaalandmekandjatega. Kui üleantavad andmed on konfidentsiaalsed, tuleb andmekandjaid transpordini hoida lukustatud hoiukohas (kapp, hoiulaegas). Transpordi või kättetoimetamise eest vastutajate (nt postipunkt) tähelepanu tuleb juhtida andmekandjate nõuetele vastavale ja turvalisele säilitamisele ja käsitsemisele.

Kontrollküsimused

- Kas töötajate tähelepanu on juhitud asjaolule, et transporti ootavad andmekandjad ei hoitaks nii, et need oleks kõigile juurdepääsetavad.

M 1.37 Faksiaparaadi õige paigutus

Vastutav algatuse eest: Infoturbe osakond, tehnikaosakonna juhataja
Vastutav elluviimise eest: kasutaja, faksi eest vastutav töötaja, tehnikaosakond

Faksiaparaat tuleks paigaldada tsooni, mis ei ole kõigile ligipääsetav. Otstarbekas on sisse viia kontroll nimetatud tsooni sisenemise ja faksiaparaadi kasutamise üle. Seda on võimalik saavutada faksi paigaldamisega pidevalt kasutuses olevasse ruumi (nt asjaajamisruum, sekretariaat, postipunkt). Väljaspool tööaega või volitatud kasutajate äraolekul peaks seade olema lukustatud ruumi või kappi. Tähtis on ära hoida, et sissetulnud faksisaadetisi näeksid mittevolitatud isikud või et need satuksid nende kätte (vt M 2.48 Faksioperaator).

Täiendavad kontrollküsimused:

- Kes saab faksiaparaati kontrollimatult kasutada?
- Millistel aegadel on faksiaparaadi kasutamine võimalik?
- Kuidas kontrollitakse juurdepääsu faksiaparaadile?
- Kuidas kaitstakse faksiaparaati väljaspool tööaega?

M 1.38 Modemi õige paigutus

Vastutav algatuse eest: IT-juht, infoturbeosakond
Vastutav elluviimise eest: kasutaja, administraator

Modemi väärkasutamise vältimiseks tuleb tagada, et sellele oleks füüsiline juurdepääs ainult volitatud isikutel. Väärkasutamine tähendab ühelt poolt volitamatute andmeülekannete teostamist, mis võib põhjustada kulutusi, võib sisse tuua või levitada väljapoole viirusi ning teiselt poolt volitamatut modemi konfiguratsiooni muutmist või valimist, mistõttu võivad tekkida turvaaugud.

Et kindlustada füüsilist juurdepääsu välisele või PCMCIA modemile, tuleb tagada nt pidevalt kasutuses oleva modemi ruumi lukustamine või ainult ajutiselt kasutatava modemi korral mitteaktiivse modemi turvaline hoidmine kapis. Järgida tuleb meetmeid vastavalt moodulile B 2.3 Bürooruum .

Sisemisel modemil on IT-süsteemi sisseehitamise tõttu kõrgem loomuomane füüsiline kaitse. Nende puhul peaks piisama meetmetest, mida on kirjeldatud moodulites B 2.3 Bürooruum või B 2.4 Serveriruum .

Kui modemi või modemipuuli *(Modem pool)* kaudu luuakse pääs sisevõrku, tuleb rakendada moodulit B 3.301 Turvalüüs (tulemüür) . Modemite kaudu ei tohi luua pääsu sisevõrku, hiilides mööda olemasolevast tulemüürist. Kui modemipuuliga tuleb luua väliseid ligipääse tulemüüriga kaitstud võrgule, tuleb see paigaldada tulemüüri kindlustamata poolele (vt ka M 2.77 Serverite integreerimine tulemüüri). Modemipuul peaks koos selle juurde kuuluva serveriga olema paigaldatud turvanõuetele vastavasse serveriruumi. Järgida tuleb moodulis B 2.4 Serveriruum kirjeldatud meetmeid.

M 1.39 Tasandusvoolude vältimine varjes

Vastutav algatuse eest: IT-juht
Vastutav elluviimise eest: tehnikaosakond

IT infrastruktuuri normides on kirjeldatud nii varjestatud kui ka varjestamata andmekaabeldusi, samuti ka nimetatud seadmete maandamisele ja varjestamisele esitatavad nõudeid. Varjestatud andmeliinide kasutamisel eristatakse normides tehnikaruume (nt serveriruumid ja arvutuskeskus) ning üldise IT-kasutusega ruume. Tehnikaruumide jaoks on ette antud mõlemapoolne varjestamine ja tihe süsteemide ja komponentide sidustamine. IT-infrastruktuuri üldiseks kasutuseks, nagu korruste kaabelduseks hoonetes, nähakse normides ette ühepoolne varjestus. Mõlemapoolne varjestus on valikuline.

Kui võrgu funktsioneerimist segavad varjestatud juhtmete kasutamisel tasandusvoolud, peaks kõigepealt analüüsima selle põhjust. Üha kõrgemaks muutuva lainesagedusega IT ülekandemeetodite tõttu muutuvad seadmed tundlikumaks kõrgsageduslike häirete suhtes. Lisaks sellele muutuvad need teatud juhtudel ka ise kõrgsageduslikeks segajateks ümbritsevatele seadmetele ja süsteemidele. Kui tuvastatakse tegevushäireid, tuleb sõltuvalt kohapealsetest tingimustest õige lahendus leida. Kuna selleks on vaja palju erialaseid teadmisi, on soovitav teha ekspertiisi läbiviimine, analüüs ja lahenduse väljatöötamine ülesandeks erialafirmale. Näiteks tasandusvoolude ärahoidmiseks andmeliinide varjestustel hoonetes on erinevaid võimalusi.

Tasandusvoolusid võib vältida TN-C-võrgus sellega, et varjestatud andmeliinide kaudu ühendatakse omavahel vaid sellised IT-seadmed, mis on ühendatud ühise elektrijaotuskilbiga. Andmevõrgu laiendamisel tuleb nimetatud tingimuse olemasolu kontrollida ja garanteerida. Meetmena tasandusvoolude vältimiseks TN-C- või TN-CS-võrgus soovitatakse tihti erandlikku andmeliinide ühepoolset varjestust. Tasandusvoolude ärahoidmiseks on nimetatud tegevusviis tõepoolest mõjus. Teistel põhjustel tuleks aga nimetatud vahendit kui erandit rakendada eriti piiratult.

- Ühepoolse varjestusega juhtmetele mõjuvad palju tugevamini välised kiirgusemissioonid. Samal ajal kiirgavad need ise tugevamini kui varjestamata sümmeetrilised juhtmed. Ühepoolse varjestuse korral tuleb niisiis arvestada rohkemate häiretega andmete ülekandmisel (nt käideldavuse või tervikluse osas, kui kõikide teiste kaablite korral.
- Taoliste juhtmete mõõdetava kiirguse tugevam väljastamine kujutab endast riski informatsiooni konfidentsiaalsuse hindamisel.
- Isegi kui leppida ühepoolse varjestuse puudustega, jääb alles tervikliku realiseerimise probleem. Kõikide tööde suhtes andmevõrkudega on vaja teostada järjekindlat kontrolli, et garanteerida, et ühepoolseid varjestusi siiski

kunagi mõlemapoolselt ei varjestataks. Selliseid valesid varjestusi on hiljem võimalik avastada vaid väga suuri kulutusi tehes.

Turvalisuse seisukohalt on optimaalne, kui elektrijaotusvõrk kogu hoones paigaldatakse tervenisti TN-S-võrguna. Seejuures paigaldatakse PE- ja N-juht alates potentsiaaliühtlustuslatist eraldi. Üksikmeetmete rakendamine IT-seadmete juures ei ole sel juhul tavaliselt enam vajalik. Järgida tuleb siiski nõuannet M 1.28 Puhvertoiteallikas uue TN-S-võrgu moodustamisel ühendatud seadmetele.

Et TN-S-võrk oleks kestvalt efektiive, tuleb tagada, et ühendus PE- ja N-juhi vahel kaitsemaanduse juures oleks võrgus ainuke. Praktikas ei saa aga välistada, et uute seadmete ühendamisel või lülitustööde korral võrgus luuakse eksikombel veel üks ühendus PE- ja N-juhi vahel. Seepärast peaks muutused andmevõrgus tehnikaosakonnaga kooskõlastada. Lisaks sellele tuleks TN-S-võrku regulaarselt korrektse kaitsemaanduse suhtes kontrollima. See võib toimuda toitevõrgu regulaarse kontrolli käigus ning kahtluste korral (näiteks kauem kestvad mittespetsiifilised tõrked andmevõrgus). Ideaalne oleks, kui TN-S-võrk varustataks alalise rikkevoolu kontrolliga.

Täiendavad kontrollküsimused:

- Milline võrgu liik on maavaldusel olemas?
- Kas on olemas reeglid, millal tuleks kontrollida, kas toitevõrgu kaitsemaandus on korrektne?
- Kas mõõteväärtusi kontrollitakse iga päev võimaluse korral olemasoleva pideva rikkevoolu kontrolli kaudu?

M 1.40 Kaitsekappide sobiv paigutus

Vastutav algatuse eest: infoturbe osakond
Vastutav elluviimise eest: siseteenistus

Kuna kaitsekapid kaaluvad tavaliselt palju, peab enne nende paigaldamist kontrollima paigalduskoha põranda kandevõimet. Kaitsekapid, mida nende suhteliselt väikese suuruse tõttu on lihtne minema viia, tuleks kinnitada seina või põranda külge. Järgida tuleb olemasolevaid tootjanõuandeid nende sobivaks paigaldamiseks (nt vabad õhutusavad, kaablikarbikud).

Kontrollküsimused

- Kuidas takistatakse kaitsekapi vargust?

M 1.41z Kaitse elektromagnetilise kiirguse eest

Vastutav algatuse eest: infoturbe osakond
Vastutav elluviimise eest: soetaja, tehnikaosakond

Kui kaitsekapis hoitakse informatsioonitehnilisi seadmeid, võivad naabruses asuvad seadmed toota elektromagnetilist kiirgust, mis kahjustab seadmete funktsiooni (eriti tööstuslikes tootmisettevõtetes). Täiendavate filtrite ja uksetihendite paigaldamisega saab kaitsekapis olevat kiirgust vähendada. Samaaegselt takistavad need meetmed ka kapis olevate seadmete ohustava kiirguse levikut.

Täiendavad kontrollküsimused:

- Kas on olemas elektromagnetilise kiirguse oht?

M 1.43 Võrgu aktiivkomponentide turvaline paigutus

Vastutav algatuse eest: IT-juht, infoturbeosakond, planeerija

Vastutav elluviimise eest: tehnikaosakond, administraator

Et kindlustada manipuleerimisest vaba võrgu tööd, tuleb võrgu aktiivkomponente (nt marsruuterid, kommutaatorid, ISDN-marsruuterid) käitada turvalises keskkonnas. See võib olla kas serveriruum (vt B 2.4 Serveriruum) või serverikapp, kui ei ole olemas eraldi serveriruumi (vt B 4.4 Virtuaalne privaatvõrk (VPN)). Volitamata isikutel ei tohi seadmete paigalduskohta olla järelevalveta juurdepääsu.

Seejuures tuleb arvestada asjaoluga, et kaitsekappide tootjad kasutavad tihti standardlukkusid, nii et kappide tootja ükskõik millise võtmega on võimalik avada kõik kapid. Seepärast tuleb kaitsekapi seeriaviisiliselt toodetud lukk välja vahetada individuaalse vastu.

Lisaks sellele peaksid seadmed olema paigaldatud selliselt, et need oleks kaitstud elektromagnet- või magnetväljade mõju eest. Peale selle peaksid need olema varustatud kontrollimehhanismidega, mis annavad märku niiskuse ja temperatuuri lubatud piirväärtuste ületamisest.

Marsruuterite ja kommutaatorite kaitse volitamatu juurdepääsu eest on ka seepärast väga tähtis, et paljude seadmete password-recovery protseduurid paroolide lähtestamiseks on teada, mis eeldab enamasti füüsilist ligipääsu seadmetele (konsoolühendus). Tihti on seadmetel ka PCMCIA-pesad. Vastavaid PCMCIA-kaarte võib kasutada andmete üldiseks salvestamiseks ning need pakuvad mugavat võimalust konfiguratsiooniandmete väljavahetamiseks, värskendamiseks või pildifailide salvestamiseks.

Seeriaviisiline konsoolühendus (RS-232-Port) võimaldab arvuti või terminali ühendamist administreerimis- või konfigureerimistööde läbiviimiseks. Konsooli ligipääsuparooli tuleb hoida kirjalikult turvalises kohas (vt M 2.22 Paroolide deponeerimine).

Lisaks tuleb ära hoida varguse, vandalismi ja seadme volitamatu väljalülitamise tõttu tekkinud ohud.

Kontrollküsimused

- Kas aktiivsed võrgukomponendid on paigutatud suletud kappidesse?
- Kas standardlukud on välja vahetatud?
- Kas konsool on kaitstud turvalise parooliga?
- Kas paroolid on deponeeritud?

M 1.44 Kodutöökoha sobiv konfiguratsioon

Vastutav algatuse eest: tehnikaosakonna juhataja, töötajate nõukogu/ettevõtte nõukogu, ülemus

Vastutav elluviimise eest: tehnikaosakond, töötajad

Koduse töökoha korral on soovitav tööruumi olemasolu. Vähemalt peaks kodune töökoht olema ülejäänud korterist uksega eraldatud.

Ruumi sisustus peaks olema selline, et see vastaks ergonoomia-, turvalisuse- ja tervisekaitsealastele nõuetele. See tähendab muu hulgas, et on tagatud:

- küllaldaselt ruumi mööblile ja kuvariga töökohale,
- reguleeritav ruumitemperatuur ning piisavad õhutusvõimalused,
- varjestus müraallikate vastu,
- päevavalgus ning küllaldane kunstlik valgustus,
- ekraanifilter, kui monitori on võimalik läbi akna näha,
- segavate pimestuste, reflekteerumiste või peegeldumiste vältimine töökohal ning
- telefoni ja elektri ühenduskontaktid.

Ametiasjus kasutatavad IT-seadmed peaks paigaldama tööandja, et vältida nt tööjuhendite abil IT-seadmete kasutamist isiklikuks otstarbeks.

Kontrollküsimused:

- Kas kodus töötajatelt küsitakse regulaarselt või aeg-ajalt, kas töökoht vastab tervishoiu- või tööalastele nõuetele?

M 1.45 Äridokumentide ja –andmekandjate sobiv talletus

Vastutav algatuse eest: tehnikaosakonna juhataja, infoturbeosakond

Vastutav elluviimise eest: töötajad

Äridokumentidele ja andmekandjatele tohib olla juurdepääs vaid selleks volitatud kaastöötajatel. Seda nõuet tuleb järgida ka väljaspool ametlikku büroohoonet, niisiis kodutöökohas või mobiilses töökohas. Väljaspool kasutusaega tuleb neid hoida nii, et volituseta isikutel ei oleks neile juurdepääsu.

Hoidmine büroos

Kõikidel töötajatel peaks olema võimalus bürooruumis, kus on nende töökoht, tähtsaid ja eelkõige kõrge kaitsevajadusega andmekandjaid ja dokumente luku taga hoida. Selleks võib kasutada näiteks lukustatavaid kirjutuslauasahtleid, ratastega konteinereid ja kappe.

Nimetatud hoiukohtade lukud peaksid vastu pidama vähemalt rünnakutele lihtsalt valmistavate või kättesaadavate (kirjaklambrid, muukrauad) muukimisvahenditega. Kasutama peaks vähemalt 4 kara ja 1000 sulgemisvariandiga mööblilukke. Lisaks sellele tuleb jälgida, et lukust ei oleks võimalik lihtne mööda hiilida, nt tagaseina eemaldamise teel. Kokkuvõttes peaks hoiukoha kaitsemõju vastama selles hoitavate dokumentide ja andmekandjate turvanõuetele.

Hoidmine kodus

Ka koduse töökoha juurde peaks sel põhjusel kuuluma vastava kaitsemõjuga lukustatav hoiukoht (kirjutuslaud, ratastel konteiner, kapp või midagi taolist).

Hoidmine reisil

Mobiilse töökoha korral ei tohiks äridokumendid ega mobiilsed IT-süsteemid jääda järelevalveta. Need peaksid olema kaitstud vähemalt lihtsa äravõtmise vastu, niisiis olema näiteks varustatud varguskaitsega, lukustatud kappi või kaitstud teiste lihtsamate meetmete abil. Peale selle on äridokumente ja mobiilseid IT-süsteeme soovitav transportida lukustatavas dokumendikohvris.

Kontrollküsimused:

- Kas kõikide büroo ja koduste töökohtade juurde kuulub vähemalt üks lukustatav hoiukoht?
- Kas töötajaid on instrueeritud, et kõrge kaitsevajadusega andmeid sisaldavaid dokumente ja andmekandjaid tuleks hoida lukustatud hoiukohas?

M 1.46z Vargusetõrjevahendid

Vastutav algatuse eest: IT-juht, infoturbeosakond

Vastutav algatuse eest: IT-juht

Vargusetõrjevahendite kasutamine on õigustatud kõikjal, kus tuleb kaitsta suuri väärtusi või seal, kus teisi meetmeid – nt nõuetele vastav kontroll juurdepääsu üle töökohtadel – ei ole võimalik rakendada, nagu näiteks sülearvutite mobiilsel kasutamisel. Lisaks sellele on vargusetõrjevahendite kasutamine otstarbekas kohas, kus liigub palju külastajaid või on kasutajate vaheldumine väga tihe. Seejuures tuleks aga alati meeles pidada, et kaitstavate väärtuste hind on palju kõrgem uue seadme hankimiskuludest, seepärast tuleb sülearvutite ja sarnaste IT-süsteemide korral arvestada nendele salvestatud andmete hinda.

Vargusetõrjevahenditega tuleks olenevalt kaitstavast objektist varustada lisaks IT-süsteemile ka monitor, klaviatuur ja muud lisaseadmed.

Turul on saadaval erinevaid vargusetõrjevahendeid. Neid võib eelkõige jagada mehaanilisteks ja elektroonilisteks kaitsevahenditeks.

Mehaaniliste kaitsevahendite hulka kuuluvad muu hulgas kaablikaitsed, korpusekaitsed (et kaitsta korpust avamise eest), kaitseplaadid ja kaitsekorpused. Ühelt poolt on olemas riistvara kaitsevahendid, mis hoiavad ära IT-seadmete varguse, nt IT-süsteemi ühendamise abil kirjutuslauaga. Teiselt poolt on olemas ka terve rida kaitsemehhanisme, mille ülesandeks on takistada korpuse avamist, et hoida ära seadme osade vargust või ohutuse seisukohal tähtsate seadistuste manipuleerimist, nagu nt turvakaartide eemaldamist.

Mehaaniliste kaitsevahendite soetamisel on tähtis valida hea lukk, millel on vastavatele vajadustele kohandatud lukustusmehhanism. Olenevalt tootest on võimalikud erinevad lukustusmehhanismid:

- Ühtmoodi sulguvad: üks võti sobib kõigile asutuse, osakonna jne seadmete kaitsemehhanismidele. Eeliseks on väiksemad kulutused võtmete haldamisele. Puuduseks on aga asjaolu, et ringluses võib olla väga palju ühesuguseid võtmeid ning et kahju korral ei ole tõendite tagamine tihti võimalik.
- Erinevalt sulguvad: igal seadme kaitsemehhanismil on oma isiklik võti. Puuduseks on suuremad kulutused võtmete haldamisele. Eeliseks on aga asjaolu, et on vähem võtme koopiaid.
- Peavõtmesüsteem: igal seadmekaitsel on oma isiklik võti, kuid seda saab avada ka peavõtme abil. Eeliseks on väiksemad kulutused võtmete haldamisele. Puuduseks on aga asjaolu, et selliste süsteemide soetamine on kallim.

Enamikul sülearvutitest– aga ka paljudel teistel seadmetel – on väike pilu, mis on tähistatud keti- või luku sümboliga. See väike ava (ca 3 x 7 mm) asub seadme küljel või taga. Saadaval on suur valik kaablikaitseid ja teisi tooteid, mida saab kinnitada nimetatud avasse seadmete kaitseks.

Kaablikaitsete korral tuleb vaid kaablisilmus panna ümber läheduses asuva vastupidava objekti, juurdekuuluv lukk läbi tekkinud aasa tõmmata ja lukustada.

Seadmete jaoks, millel puuduvad nimetatud avad – või ei ole need küllalt tugevad – on olemas turvatooted, mille puhul liimitakse seadmele stabiilne plaat. Selle külge kinnitatakse kaitsekaabel.

Lisaks on olemas elektroonilised kaitsevahendid, mis vallandavad näiteks seadme juures akustilise hoiatussignaali, mis peaks potentsiaalsed vargad seadmetest eemale peletama.

Uute IT-seadmete soetamisel tuleks jälgida, et seadme juures oleks avad, et neid saaks teiste seadmete külge kinnitada ning et korpused oleks suletavad.

Kontrollküsimused:

- Kas viimastel aastatel on varastatud IT-süsteeme või –komponente?
- Kuidas kaitstakse IT-süsteeme või komponente varguse eest?

M 1.47 Eraldi tuletõkked

Vastutav algatuse eest: asutuse/ettevõtte juhatus

Vastutav elluviimise eest: planeerija

Tuletõkkesektsioonide kindlaksmääramine on arvutuskeskuse tuleohutuse seisukohalt suure tähtsusega. Usaldusväärsete tule- ja suitsutõkkesektsioonide mõju on end paljude suurpõlengute korral veenvalt õigustanud. Arvutuskeskuste tuletõkkeseina või tuletõkkesektsioonide suurusele esitatud nõuded peaksid ületama asjakohastes normides esitatud nõuded. Tuletõkkesein või tuletõkkesektsioon ei peaks olema mitte ainult inimeste ja hoone, vaid ka inventari ja selle käideldavuse kaitseks. Seega ei ole eesmärgiks takistada mitte ainult tule levikut leekidena ja kuumi suitsugaase, vaid ka soojuskiirgust ning külma suitsu levikut.

Standardite järgi veel lubatud soojuskiirgus võib hoone sisustusele, eriti soojatundlikus IT-tsoonis, juba hävitavalt mõjuda. Seepärast tuleks ehitusplaani sisse viia mitmed tule- ja suitsutõkkesektsioonid, mis oleks nii suured, kui vajalik ning nii väiksed, kui võimalik. Arvutuskeskuse puhul on vaja kontrollida, millisel määral on vaja luua veel sisemisi tuletõkkesektsioone. Kui peaks olema nõutav eraldi tuletõkkesektsioon põhiüksuste (IT-ruumid, andmekandjate arhiivid) jaoks, peaksid seinad, uksed ja ka vajalikud seina- ja laeavad vastama tulepüsivusklassi F90 nõuetele.

Järgida tuleb maksimaalset õhuniiskust vastavalt standardile EN 1047-2. Lisaks tuleks arvutuskeskuste, serveriruumide ja andmekandjate arhiivide puhul järgida ka normi EN 1047-2, milles on kindlaks määratud maksimaalne suhteline õhuniiskus. Kui arvutuskeskuse tuletõkkesektsiooni kuuluvad ka nt bürood, piisab tuletõkkesektsiooni piirides büroode vahel ja arvutuskeskuse põhitsoonis F30 seintest ja T30 ustest. Bürood tuleb sel juhul kaasata tuletõrjesignalisatsiooni. Planeerimisel ja tööprotsessis tuleb kindlustada, et arvutuskeskuse tuletõkkesektsioonis asuvates ruumides ei oleks suurt tulekoormust.

Kontrollküsimused:

- Kas ruumid on jagatud tuletõkkesektsioonideks otstarbekalt?

M 1.48 Tuletõrjesignalisatsioon

Vastutav algatuse eest: asutuse/ettevõtte juhatus

Vastutav elluviimise eest: planeerija

Lisaks spetsiaalselt IT-valdkonna jaoks kohandatud tuleohutuseeskirjade koostamisele ning häire- ja reageerimisplaanidele omab suurt tähtsust ka tuletõrjesignalisatsiooni installeerimine. Kuna rohkem kui 90% kõikidest arvutuskeskustes tule poolt tekitatud kahjudest on põhjustatud põlengutest lähiümbruses, on soovitav nimetatud tsoonid tuletõrjesignalisatsiooni järelevalvesüsteemi integreerida. Kasutada võiks impulss- või optilist andurit. (optiline valguse hajutamise printsiip).

Tööle hakkava anduri identifitseerimine peab olema võimalik. Tulekolde ja tule leviku lokaliseerimiseks on tuleandurite identifitseerimine eriti tähtis. Infrastruktuuri tuletõrjesignalisatsiooni soovitav minimaalne konfiguratsioon koosneb:

- kanalianduritest konditsioneeri ventilatsioonikanalites
- anduritest värske õhu juurdevoolul, värske õhu juurdevoolu automaatse tõkestamisega, kui avastatakse häireseisund.

Kõik tuletõrjesignalisatsioonid, samuti ka häireteated tuleks, niivõrd kui see on võimalik, olla suunatud mingisse alaliselt hõivatud kohta, nt pääslasse. Võimalusel peaks järgnema otseühendus elukutselise tuletõrjega.

Näide

- Juhatuse tasemel nõupidamise ajal ühes arvutuskeskuses märkas üks osaleja, kes viibis korraks kõrvalruumis, juhuslikult suurpõlengu puhkemist lähedal asuvas keemiatehases. Tema põlengule osutamine võimaldas arvutuskeskuse juhatajal värske õhu juurdevoolu välja lülitada. Vaid mõne minuti pärast oleks tahmane põlengusuits tõmbeventilaatori kaudu, millel ei olnud detektorit, arvutuskeskuse ruumidesse pääsenud.

Regulaarne kontroll

Tulekahjusignalisatsiooni kõikide komponentide funktsioonivõimet tuleb regulaarselt kontrollida. Kui tulekahjusignalisatsiooni korrashoid ja kasutus toimub hooldusfirma kaudu, peaksid kaks töötajat tundma seadme elementaarseid põhifunktsioone (vähemalt kõigi kasutusseisundite ja seisunditeadetega) ning olema hooldusfirmale kontaktisikuks. Aeg-ajalt tuleks mõningate anduriliinide funktsioonivõimet käsitsi kontrollida.

Kontrollküsimused:

- Millal kontrolliti viimati tulekahjusignalisatsiooni funktsioonivõimet?

M 1.49 Tehnilised ja organisatsioonilised nõuded arvutuskeskusele

Vastutav algatuse eest: asutuse/ettevõtte juhatus

Vastutav elluviimise eest: planeerija

Kogu turvatsoonil e arvutuskeskusel peaks võimaluse korral olema ainult üks või kaks ust ja mitte ühtegi akent, sest kõiki juurdepääsuvõimalusi tuleb valvata (vt ka M 1.10z Turvauksed ja -aknad).Juurdepääs peaks olema kaitstud kvaliteetsete juurdepääsu kontrollmehhanismidega (vt ka M 1.73 Arvutuskeskuse kaitse volitamata juurdepääsu eest). Arvutuskeskus tuleks kavandada suletud turvatsoonina. Sellel peaks olema võimaluse korral vaid üks uks ning mitte ühtki akent, nii et kõikide sissepääsuteede üle oleks võimalik teostada kontrolli. Sissepääs peaks olema reguleeritud rangete kontrollmehhanismidega. Arvutuskeskuse planeerimisel või sobivate ruumide valimisel tuleks keskkonnamõjudest tingitud potentsiaalsed ohud võimalikult minimeerida. Nii tuleb potentsiaalsetele ohtudele, mis on tingitud vee sissetungimisest lamekatuse korral või kogunemisest keldritesse samuti vastu astuda nagu EMV-tõrgetele, nt mobiilsideseadmetest või kolmefaasilistest agregaatidest tingitud.

Sissemurdmiskaitse

Arvutuskeskuse jaoks on hädavajalik ehituslikult ja tehniliselt sobiv sissemurdmiskaitse (Vt M 1.19 Sissemurdmiskaitse).

Varu

Arvutuskeskuses kasutatavatele IT-komponentide käideldavusele esitatakse paljudel juhtudel kõrgeid nõudeid. Neid nõudeid on võimalik täita, paigaldades infrastruktuuri ja tehnilised seadmed varuga (Vt M 1.52 Tehnilise infrastruktuuri varud).

Raske- ja täppistehnika eraldamine

Et vältida raske- (elektritoide, kliimatehnika) ja täppistehnika (arvutid) segamini paigutamist arvutuskeskuses, tuleks selleks planeerida eraldi ruumid. Arvutuskeskuse tehniline infrastruktuur tuleb installeerida eraldi ruumidesse. Kõrgete käideldavusnõuetega arvutuskeskustes ei tohi kaitsekontseptsiooni koostamisel tähelepanuta jätta kommunikatsiooni- või infotehnilisi komponente, mida kasutatakse “väliskommunikatsiooniks”. Kui nendele ei ole tagatud samaväärset kaitset kui tehnilistele põhikomponentidele, ei ole käideldavus garanteeritud. Näiteks tuleb arvestada asjaoluga, et väliskommunikatsioonis osalevate võrgu aktiivkomponentide (nt marsruuterid ja kommutaatorid) kaitsetarve vastaks arvutuskeskuse põhivaldkondade kaitsetarbele. See puudutab nii materiaalset kaitset, kui ka detektsiooni, teadete edastamist ja alarmeerimist.

Soovitav on, et alltoodud seadmed ja ruumid paikneksid eraldi (soovi korral ka eraldi tuletõkkesektsioonides):

- informatsioonitehnika
- kliima- ja õhutuseadmed,
- energiatoide,
- ladu jne

Toiteliinide vältimine

Planeerimisel tuleks tähelepanu pöörata ka asjaolule, et hoone toiteliinide trassid, nt vee või gaasitorud, (vt M 1.24 Veetorude vältimine IT-ruumis) ei kulgeks arvutuskeskuse vahetus läheduses ega läbi selle tundlike tsoonide.

Sissepääs vaid administraatoritele

Arvutuskeskus on ohutuse seisukohalt tähtis tsoon, seepärast tohiks sinna paigaldatud IT-süsteemidele olla juurdepääs ainuüksi administraatoritel. Kooskõlastatud pääsuõiguste reguleerimisega tuleb kindlustada, et omad töötajad ning eriti veel ajutused töötajad, nt hooldustööde läbiviimise ajal arvutuskeskuses, ei omaks juurdepääsu süsteemidele, mis ei puuduta nende tegevusvaldkonda. Kaasaskantavate IT-süsteemide, mobiiltelefonide või kaamerate kaasavõtmine arvutuskeskusesse peaks olema keelatud, kui nimetatud seadmed ei ole vastava asutuse kontrolli all. Mobiiltelefonide kasutamine arvutuskeskustes peaks olema põhimõtteliselt keelatud, kuna need võivad IT-süsteemide talitlust oluliselt häirida. Erandid peavad olema kooskõlastatud (vt M 2.188 Mobiiltelefonide kasutamise eeskirjad ja turvasuunised).

Arvutuskeskuse ümberehitamisel või uue planeerimisel tuleks tähelepanu pöörata alljärgnevalt kirjeldatud parameetritele. Arvutuskeskuse ruumi jaoks on end praktikas õigustanud laiuse ja kõrguse suhe 1:1 kuni 2:3. Selline suhe kergendab IT-komponentide ja nende kaabelduse struktureeritud paigaldamist arvutuskeskuses. Niivõrd kui ehituslikud tingimused võimaldavad, on soovitav installeerida tõstetud põrand. Selle kõrgus sõltub tehnilisest varustusest ja kasutamisest. Kui tõstetud põrandat kasutatakse konditsioneerimiseks, peaks see olema ca 50 cm kõrgune.

IT-ruumide planeerimisel on soovitav kinni pidada alljärgnevatest mõõtmetest:

Ruumi sisekõrgus alates tõstetud põrandast	3,00 m
Tugipostide vahekaugused	6,00 m
Täitmata ukseava laius	1,10 m
Täitmata ukseava kõrgus	2,10 m

Lagede ja tõstetud põrandate kandejõud peab olema vähemalt 1000 kg/m ^{2}. Tõstetud põrand peaks olema väga hea sobivustäpsusega ja alates 20 cm kõrgusest suletuna vastama tulepüsivusklassi F 30 nõuetele.

Nõuanne: Tõstetud põrandad ja ripplaed peavad lõppema IT-ruumis. Selliste konstruktsioonide kaudu ei tohi luua kaitseta sissepääsuteid.

Koridoride laius peaks olema vähemalt 1,80 m ning põrandad peaksid olema kaetud libisemisekindlate, siledate kattematerjalidega, mis peavad vastu suuremale transpordikoormusele. Arvutuskeskuses kasutatavate liftide kui vertikaalsete transporditeede kandejõud peaks olema vähemalt 1500 kg. Kabiini sisemised mõõtmed peaksid olema vähemalt: sügavus – 2,80 m, laius – 1,50 m ja kõrgus – 2,20 m.

Kontrollküsimused:

- Kas on tehnilisi ja organisatsioonilisi nõudeid arvutuskeskusele?
- Kas arvutuskeskus on kavandatud suletud turvatsoonina?
- Kas sissepääs serveriruumi on reguleeritud?
- Kas planeerimisel pöörati küllaldast tähelepanu raske- ja täppistehnika eraldamisele.

M 1.50 Kaitse suitsu eest

Vastutav algatuse eest: asutuse/ettevõtte juhatus

Vastutav elluviimise eest: planeerija

Suits kujutab endast tulekahjude korral suurimat ohtu inimestele. Rohkem kui 90% põlengu ohvritest on hukkunud suitsu kahjuliku mõju (mürgituste) tagajärjel. Ka IT-riistvara võib suitsu tõttu oluliselt kannatada saada. Seepärast tuleb omistada suurt tähtsust kaitsele suitsu eest.

Seejuures on soovitav järgida alljärgnevaid soovitusi:

- Tulekaitseuksed peaksid olema ka suitsukindlad.
- Suitsukindlad uksed - Suitsukindlad uksed koridorides peaks olema juhitavad suitsutundlike lülititega. Sellised uksed võivad alati lahti olla, kuna need suitsu avastamisel iseenesest sulguvad.
- Õhutuseadme või konditsioneeri abil peaks olema võimalik IT ruumidest suits välja juhtida.
- Kanaliandur - Konditsioneeri kanalitesse (ventilatsioon) tuleks installeerida kanaliandurid.
- Värske õhu juurdevooluavale tuleks installeerida andurid, mis need kohe sulgevad, kui tuvastatakse häireolukord (suits).

Töötajaid on vaja instrueerida, millised hoiatussignaalid on suitsukaitse komponentidel ning kuidas nendele tuleb reageerida.

Kõikide suitsukaitse komponentide talitlusvõimet tuleb regulaarselt kontrollida.

Kontrollküsimused:

- Millal kontrolliti viimati suitsukaitse komponentide talitlusvõimet?

M 1.51 Tulekoormuse vähendamine

Vastutav algatuse eest: asutuse/ettevõtte juhatus

Vastutav algatuse eest: planeerija, IT-juht, tehnikaosakonna juhataja

Suurte tulekoormuste põhjuseks on nt IT-süsteemide koondumine, ehitusmaterjalide vale valik, kergesti süttiv büroo sisustus ning suur paberi hulk. Paljudel juhtudel on selliseid tulekoormusi võimalik lihtsal viisil vältida. Juba arvutuskeskuste, nii nagu ka teiste hoonete planeerimisel tuleks mõelda, kuidas vähendada mittevajalikku tulekoormust. Nende väljaehitamisel tuleks eelistada mittepõlevaid materjale (ehitusmaterjalide klass A).

Et garanteerida tuleohutuse seisukohalt kindlat tööprotsessi ning mitte ületada piirväärtusi, peaks juba planeerimisfaasis toimuma hilisemate tulekoormuste ligikaudne väljaarvestamine. Seejuures tuleb arvestada sisustuse või ehitusmaterjalide tuleklassidega. Seeläbi on võimalik tagada hoone vastamine tuleohutuseeskirjadele ning vältida raskusi selle vastuvõtmisel ehitusjärelevalve asutuste ja tuletõrje poolt? Teiselt poolt tuleb arvutuskeskuse tööprotsessi ajal hoolitseda selle eest, et tõstetud põrandatest eemaldataks näiteks tulekoormused mittevajalike kaablite näol.

Bürooruumidest tuleks eemaldada mittevajalikud aktid ning paigutada need selleks ettenähtud arhiividesse. Üks sagedamaid näiteid mittevajalikest tulekoormustest IT-ruumides on pakkematerjalid, näiteks papp või vahtpolüsterool (stüropor). IT-ruumidest tuleb pakkematerjal viivitamatult eemaldada ning selleks ettenähtud loaruumidesse transportida, kui seda veel vaja läheb.

Kontrollküsimused:

- Kas kontrollitakse regulaarselt, ega kasutuses olevatesse ruumidesse ei kuhju tulekoormused?

M 1.52z Tehnilise infrastruktuuri varud

Vastutav algatuse eest: asutuse/ettevõtte juhatus

Vastutav elluviimise eest: planeerija

Kui arvutuskeskuse või serveriruumi käideldavuse suhtes on kehtestatud spetsiaalsed nõudmised, tuleb luua ka tehnilise infrastruktuuri varud.

N+1 printsiip

Kliimaseadmete töösserakendamisel on soovitav hoida kasutusvalmis küllaldaselt varukomponente. Kui näiteks mingit komponenti vajatakse 6 tükki, peaks soetama 7. Nii saadakse hakkama tippkoormuse ajal, nt kuumadel suvepäevadel ning ka mingi seadme rikke või hooldustööde teostamisel ajal säilib konditsioneeri üldine kasutatavus.

Ka sideliinide osas tuleks kontrollida, millistes valdkondades on varud vajalikud (vt M 6.18 Varuliinid). See kehtib eriti juhul, kui kesksed võrgusõlmed või kesksed aktiivkomponendid asuvad kontrollimata valdkondades. Arvutuskeskus peab olema varustatud ka varutoite allikaga. Soovitusi selleks leiate M 1.56 Varutoite allikas . Kui varutoite allikas ei asu naaber-tuletõkkesektsioonis, tuleks mõelda elektritoite varukaabeldusele.

Kontrollküsimused:

- Kas kaitsevajaduse kindlaksmääramisest tuleneb vajadus tehnilise infrastruktuuri varude järele?

M 1.53z Videovalve

Vastutav algatuse eest: asutuse/ettevõtte juhatus
Vastutav elluviimise eest: planeerija

Meetmeid hoone väliskesta kaitseks (vt M 1.56 Varutoite allikas) ning sisenemiskontrolliks võib täiendada videotehnika abil. Iseseisvad või teisi turvatehnika liike täiendavaid videovalveseadmeid kasutatakse alljärgnevatel kaitseeesmärkidel:

- hirmutamiseks
- fassaadi valveks
- identifitseerimiseks
- valveks
- alarmeerimiseks
- ohtude avastamiseks ja lokaliseerimiseks
- kahjustuste vältimiseks
- reeglitest kõrvalekallete dokumenteerimiseks ja hindamiseks.

Videovalve planeerimisel tuleb tähelepanu pöörata selle tihedale integreerimisele kogu kaitsekontseptsiooni. See kehtib eriti juhul, kui valveterminalid asuvad kaitstavast tsoonist kaugel. Videovalvel ilma analüüsi- ja häiremehhanismideta on ainult hirmutav funktsioon. Vajalikud kesksed tehnilised komponendid tuleb paigaldada vajalikku keskkonda ning neid tuleb kaitsta.

Videovalve planeerimisse või installeerimisse peaks kaasama ka andmekaitse eest vastutava isiku ja töötajate või ettevõtte nõukogu.

Kontrollküsimused:

- Kas videovalve on tihedalt kaitsekontseptsiooni sisse viidud?
- Kas toimub regulaarne videovalveseadme talitlusvõime kontroll?

M 1.54z Põlengu varajane avastamine / automaatkustutuse tehnoloogia

Vastutav algatuse eest: asutuse/ettevõtte juhatus

Vastutav elluviimise eest: planeerija

IT-seadmete põlengute korral võib piisata juba elektri väljalülitamisest, et põlengut vaos hoida või lõpetada.

IT-süsteemide valveks võib kasutada objektile suunatud valvet nn multidetektorite abil. Tavapärase tuletõrjesignalisatsioonitehnika (ruumi geomeetriline valve) kõrval kujutab objektivalve (üksikute IT-komponentide sisene valve) endast täiendavat signalisatsiooniseadme tasandit. Neid multidetektoreid võib kaasata nii objektide kustutamisse kui ka vastava seadme toiteenergia väljalülitamiseks.

Kui vajalikuks peetakse ka täiendavat kustutamist, on soovitav kulude ja isikukaitse seisukohalt kindlustada kustutusgaasidega vaid üksikud objektid (nt 19-tollised kapid) individuaalselt. Objektikaitseseadmed peaksid lähtuma planeerimise, tuletõrjesignalisatsiooni ja kustutamise kohta käivatest VdS direktiividest 2304 ning ka tootjate installeerimisnõuannetest ja eeskirjadest talitluses ja töökorras hoidmiseks.

Ruumi valveks IT valdkonnas sobib optiliste suitsuandurite installeerimine. Ka tõstetud põranda valveks võib kasutada samasuguseid suitsuandureid. Kui arvutuskeskuse või serveriruumi käideldavuse suhtes on kehtestatud spetsiaalsed nõuded või sisaldavad need eriti väärtuslikke või raskesti soetatavaid komponente, tuleb kaaluda inertgaasidega (süsihappegaas, inergen, argoon, lämmastik, FM 200 jne) automaatse kustutusseadme kasutuselevõttu.

Lämbumisoht kustutusgaaside kasutamisel

Leekide kustutamiseks vajalik lämmatav toime mõjub ka inimestele, kui kasutatakse hapnikku välja tõrjuvaid kustutusgaase. Nii tekib süsihappegaasi suurema kui 8 mahuprotsendilise kontsentratsiooni korral tõsine eluoht. Kustutusgaasiseadme planeerijaks peaks põhimõtteliselt olema vaid erialaspetsialist.

Kontrollküsimused:

- Kuidas tagatakse põlengute võimalikult varajane avastamine?

M 1.55z Perimeetri kaitse

Vastutav algatuse eest: asutuse/ettevõtte juhatus

Vastutav elluviimise eest: planeerija

Kui hoone või arvutuskeskus asub krundil, millele on võimalik installeerida täiendavaid turvaseadmeid, tuleks tarvitusele võtta meetmed, et väljastpoolt mõjuvaid ohtusid arvutuskeskusest eemal hoida. Siinkohal võib eriti otstarbekaks osutuda esimese astme loomine sissepääsu- ning eelkõige juurdesõidu reguleerimiseks.

Olenevalt kaitsevajadusest ja topoloogilistest asjaoludest võib perimeetri kaitse koosneda alljärgnevatest komponentidest:

Väline tarastus - Väline piire või tarastus, nt tara, müüritis ja tara valve, mis pakub kaitset krundi piiride ettekavatsematu ületamise eest, krundi piiride ületamise eest ette kavatsetult jõudu kasutamata ja krundi piiride ületamise eest ette kavatsetult jõudu kasutades

Avamaa turvameetmed - Avamaa turvameetmed, nt maa-ala kujundus, sissesõidutõkked, maa-ala ja hoone valgustus, turvafirma, videovalve ja detektorite süsteem maa-alal, mis hoiab ära märkamatuks jääva sissetungimise tara ja hoone vahelisele alale.

Isikute ja sõidukite kontroll - Väline isikute ja sõidukite identifitseerimine, nt videotelefon, turvalüüs isikutele või sõidukitele, ukse- või värava avamise ja sissepääsukontrolli üksused, mis pakuvad sissepääsukontrolli kontseptsiooni esimese astmena kaitset äratuntavalt (visuaalselt, akustiliselt või sensoorselt) volitamatute sissepääsukatsete eest. Seda funktsiooni võib toetada portjee-teenusega pääslas (vt ka M 1.17 Pääsla).

Enne perimeetri kaitse valdkonna meetmete realiseerimist tuleb igal juhul välja töötada sobiv kaitsekontseptsioon, mis hõlmab ülalnimetatud aspekte ja hoone kaitset. Teiselt poolt on oht, et rakendatakse võrdlemisi kalleid turvameetmeid, näiteks kalleid tarasid ja väga põhjalikult välja töötatud maa-ala videovalvesüsteeme, mis ei sobi aga kokku hoone kaitsega ning ei ole seetõttu otstarbekohased. Kaitsekontseptsioon peaks olema nii välja töötatud, et olemasolevate ressurssidega saaks üles ehitada võimalikult efektiivse turvameetmete süsteemi. See puudutab eriti perimeetri kaitset. Siinkohal tarvitusele võetavad meetmed peaksid üldist turvalisust tõstma ning mitte jätma ainult muljet kõrgetasemelisest kaitsest, kuna kvalifitseeritud sissemurdjad ei loobu tavaliselt kõrgete tarade ja videovalve pärast oma kavatsustest.

Näide:

- Kui sissemurdjal kulub üle tara majani jõudmiseks kaks minutit ning seejärel ainult pool minutit hoonesse tungimiseks, ei ole suhe õige. Seda võib väita eriti juhul, kui kohaliku politseiüksuse kohalejõudmiseks pärast eraturvafirma kaudu häiresignaali saamist kulub näiteks kaheksa minutit. Selle ajaga võib sissemurdja olla juba kuriteo korda saatnud ning maa-alalt lahkunud. Sissemurdjat võib olla küll märgatud ja videole salvestatud, kuid hea maskeeringu korral ei ole tema isikut võimalik identifitseerida.

Kontrollküsimused:

- Kas on olemas kaitsekontseptsioon, mis hõlmaks nii perimeetri kui ka hoone kaitset?

M 1.56 Varutoite allikas

Vastutav algatuse eest: tehnikaosakonna juhataja, IT-juht, infoturbeosakond

Vastutav elluviimise eest: tehnikaosakond

Primaarset toiteallikat energiaettevõtte võrgust tuleb kõrgenenud nõuete korral käideldavuse suhtes täiendada ise meetmetega arvutuskeskuse avariitoiteks. Seejuures ei tohi unustada ka teisi hoone tähtsaid infrastruktuuri osi, nagu nt avariivalgustus ja tuletõrjeliftid. Arvutuskeskuse varutoitesüsteem koosneb sel juhul tavaliselt arvutuskeskuse tsentraalsest puhvertoite- ning varutoiteallikast. Kui kohalikud tingimused ja nõuded arvutuskeskuse käideldavusele võimaldavad, võib varutoiteallika asemel seda asendusfunktsiooni täita ka toide teise energiavõtte võrgust. Kui online-puhvertoiteallikas (vt M 1.28 Puhvertoiteallikas) sildab voolukõikumisi või lühiajalisi voolukatkestusi, katab varutoiteallikas lisaks sellele ja pikemaajalisi voolukatkestusi.

Kogu IT-süsteemile lülitatakse ette tsentraalne online-puhvertoiteallikas. Nimetatud puhvertoiteallika tööd reguleeriv elektroonika peab hoolitsema õige sageduse ja faasidega ühenduse eest varutoiteallika käivitumisel ning energiatoite taaskäivitumisel energiaettevõtte võrgust.

Avariitoiteagregaatide dimensioneerimisel tuleks jälgida, et asendustoitevõrgu nimivõimsus ületaks arvutuskeskuse täistöövõimsuse. Sellega saab garanteerida, et varutoiteallikas, nt mitmete tarbijate samaaegsel voolutarbimisel, oleks võimeline varustama tarbijaid vajaliku võimsusega.

Toite üleandmisel puhvertoiteallikalt varutoiteallikale tuleb tagada, et toimuks samm-sammuline edasilülitamine ilma varutoiteallika ülekoormamiseta ning sellest tingitud puhvertoiteallika taaskäivitumiseta. Seejuures tuleb kooskõlastatud koormuse juhtimise abil arvestada IT infrastruktuuri ja teiste varutoiteallikaga varustatavate hoone osade individuaalseid vajadusi.

Tsentraalse puhvertoiteallika patareide dimensioneerimiseks on otsustavaks sildamisaeg toiteallika väljalangemisel. See koosneb alljärgnevatest faktoritest:

- Ooteaeg toitevõrgu taaskäivitumiseks. Varutoiteallikas käivitub alles pärast 1- kuni 5-minutilist ooteaega.
- Ümberlülitamisaeg kuni koormuse ülevõtmiseni varutoiteallika poolt. Sel ajal varustab puhvertoiteallikas kõiki IT-seadme tarbijaid vooluga.
- Aeg vähendatud tarbimisvõimsusega. Patareide laadimisvõimsuse langemisel tuleks üle minna vähendatud tarbimisvõimsusele. Selleks tuleb vähemkriitilised tarbijad võrgust eraldada.
- Aeg vähendatud tarbimisvõimsusega vajalikele kriitilistele tarbijatele. Patareide võimsuse edasisel langemisel tohib vooluga varustada vaid kõige tähtsamaid tarbijaid. Hiljemalt siin peab toimuma automaatselt IT-talitluse avariiline sulgemine, isegi juhul, kui tuleb arvestada reversiivse andmekaoga.

Puhvertoiteallika kaitsemõju säilitamiseks on vajalik selle regulaarne hooldus.
Kontrollküsimused:

- Kas peetakse kinni puhver- ja varutoiteallika hooldusintervallidest?
- Kas puhver- ja varutoiteallikate funktsioonivõimet kontrollitakse regulaarse testimisega reaalsel koormusel?
- Kas diisliga töötavate varutoiteallikate korral kontrollitakse regulaarselt kütuse olemasolu paagis?

M 1.57 Infrastruktuuri ja hoone uusimad plaanid

Vastutav algatuse eest: asutuse/ettevõtte juhatus

Vastutav elluviimise eest: planeerija

Ehitusplaanid, evakuatsiooniteede plaanid, teeviidad tuletõrjele jne (vt ka M 1.11 Trasside plaanid ja M 5.4 Kaabelduse dokumenteerimine ja märgistus) tuleks uuendada kohe pärast iga ümberehitust, infrastruktuuri ja ohutustehnika laiendamist. See on vajalik, selleks et:

- hoida defineeritud turvalisuse taset,
- olla optimaalselt valmis ohuolukordadeks,
- kergendada auditi läbiviimist ning
- planeerida ja realiseerida täielikult ja nõuetele vastavalt vajalikke meetmeid.

Ei ole piisav, kui plaane hoitakse vaid nende eest vastutavas ehitusosakonnas. Kahjustuste või avariide korral, nt kaablite kahjustuse või veetorude purunemise korral võib rikete lokaliseerimiseks ja kõrvaldamiseks vajaminev tähtis aeg kaduma minna. Plaanide haldaja asutuses, nt valvetöötaja, peaks olema võimeline neid ka lugema. Vajadusel tuleb personali vastavalt koolitada ja instrueerida.

Kontrollküsimused:

- Kas arhitekt või asukoha planeerija sai ümberehituse planeerimisel ülesandeks ka plaanide uuendamise?

M 1.58 Tehnilised ja organisatsioonilised nõuded serveriruumidele

Vastutav algatuse eest: asutuse/ettevõtte juhatus

Vastutav algatuse eest: infoturbe osakond

Serveriruum tuleks kavandada suletud turvatsoonina. Sellel peaks olema võimalikult hästi kaitstavad uksed ja aknad, kuna kõik sissepääsuteed peavad olema valve all (vt M 1.10 Turvauksed ja -aknad). Sissepääs peaks olema reguleeritud rangete kontrollimehhanismidega. Serveriruumi planeerimisel või sobivate ruumide väljavalimisel tuleks keskkonnamõjudest tingitud potentsiaalsed ohud võimalikult minimeerida. Nii tuleb potentsiaalseteks ohtudeks, mis on tingitud vee sissetungimisest lamekatuse korral või kogunemisest keldritesse samuti valmis olla nagu elektromagnetkiirguse taluvuse tasemest tingitud tõrgeteks, nt mobiilsideseadmete või kolmefaasiliste agregaatide tõttu.

Toiteliinide vältimine

Planeerimisel tuleks jälgida, et hoone toiteliinide trassid, nt vee või gaasitorud, (vt M 1.24 Veetorude vältimine IT-ruumis) ei kulgeks arvutuskeskuse vahetus läheduses ega läbi selle tundlike tsoonide. Arvutuskeskuse IT-komponentidele esitatakse paljudel juhtudel kõrgeid nõudeid käideldavuse suhtes Neid nõudeid on võimalik täita, paigaldades infrastruktuuri ja tehnilised seadmed varuga (vt M 1.52 Tehnilise infrastruktuuri varud).

Sissepääs vaid administraatoritele

Serveriruum on ohutuse seisukohalt tähtis tsoon, seepärast tohiks sinna paigaldatud IT-süsteemidele olla juurdepääs ainult nende administraatoritel. Kooskõlastatud pääsuõiguste reguleerimisega tuleb kindlustada, et omad töötajad ning eriti veel ajutused töötajad, nt hooldustööde läbiviimise ajal, ei omaks juurdepääsu süsteemidele väljaspool oma tegevusvaldkonda. IT-süsteemid, mida hooldavad mittekoosseisulised töötajad, peaks olema paigutatud eraldi ruumidesse. Peale selle oleks otstarbekohane paigaldada erineva kaitsetarbega või erinevate valdkondade IT-süsteemid eraldi ruumidesse, et sissepääsuõigusega isikute arvu väiksena hoida.

Serveriruumis ei tohiks mitte mingil juhul paikneda seadmed või varustus, millele peaks olema juurdepääs suurel hulgal kasutajatel, nt faksiaparaat või fotokoopiamasin. Põlevad materjalid, nagu koopiapaber, ei tohiks olla ladustatud serveriruumis. Kaasaskantavate IT-süsteemide, mobiiltelefonide või kaamerate kaasavõtmine serveriruumi peaks olema keelatud, kui nimetatud seadmed ei ole vastava asutuse kontrolli all. Mobiiltelefonide kasutamine arvutuskeskustes peaks olema põhimõtteliselt keelatud, kuna need võivad IT-süsteemide talitlust oluliselt häirida. Erandid peavad olema kooskõlastatud (vt M 2.188 Mobiiltelefonide kasutamise eeskirjad ja turvasuunised).

Kontrollküsimused:

- Kas on tehnilisi ja organisatsioonilisi nõudeid serveriruumidele?
- Kas serveriruumid on kavandatud suletud turvatsoonina?
- Kas sissepääs serveriruumi on reguleeritud?

M 1.59 Arhiivisüsteemide asjakohane rajamine

Vastutav algatuse eest: IT-juht

Vastutav elluviimise eest: IT-juht, administraator

Kuna salvestus- ja arhiivisüsteemides hoitakse kontsentreeritult asutuse või ettevõtte tähtsaid andmeid, peavad nende IT-komponendid olema paigaldatud turvatud ruumidesse, kuhu on sissepääs vaid volitatud isikutel. See puudutab lisaks kasutusse võetud serveritele ja võrgukomponentidele eriti salvestusüksusi (plaadimassiivid, magnetlintsalvestid, ketassalvestid).

Nimetatud IT-komponentide asjakohaseks paigaldamiseks tuleb realiseerida kõik olulise tähtsusega meetmed, mida on kirjeldatud IT-etalonturbe kataloogides ning mis on vajalikud infrastruktuuri kaitseks. Olenevalt salvestus- või arhiivisüsteemi tüübist ja suurusest tuleb kaasata ka moodulid B 2.1 Hooned , B 2.4 Serveriruum , B 2.7 Kaitsekapid ja B 2.9 Arvutuskeskus . Seejuures tuleks erilist tähelepanu pöörata infrastruktuuriliste komponentide (voolutoide, jne) piisavale usaldusväärsusele. Salvestussüsteemide kasutamisel tuleb luua vastavad tehnilise infrastruktuuri varud (vt M 1.52 Tehnilise infrastruktuuri varud), et toetada nii hästi kui võimalik nende tsentraalsete ressursside käideldavust.

Kasutatud arhiivi-andmekandjate pikaajaliseks säilitamiseks tuleb järgida meetmes M 1.60 Arhiivi-andmekandjate asjakohane säilitus nimetatud säilitustingimusi. Eelkõige tuleb tähelepanu pöörata andmekandjate, aga ka arhiivisüsteemide otstarbekohasele konditsioneerimisele.

Säilitustingimused salvestuskomponentides

Tihti realiseeritakse elektroonilised arhiivid nii, et arhiivi-andmekandjatele on salvestusüksuste kaudu pidev juurdepääs. Lisaks sellele kasutatakse mitmeotstarbelisi salvestusüksusi, mis haldavad ja paigutavad iseseisvalt sisse eemaldatavaid andmekandjaid, näiteks magnetlintsalvestite robotid või kettaseadmed. Kui salvesti- või arhiivisüsteem sisaldab selliseid komponente, ei võeta reeglina arhiivi-andmekandjaid terve eluea vältel enam salvestusüksusest välja. See tähendab, et arhiivi-andmekandjatele esitatavaid nõudeid hoiutingimuste suhtes (kaasa arvatud õhu konditsioneerimine, juurdepääsukaitse, jne) tuleb täita ja kontrollida juba salvestuskomponendis. Salvestus- või arhiivisüsteemi valikul tuleb tähelepanu pöörata asjaolule, et arhiivi-andmekandjatele esitatavatest hoiunõudeid saaks salvestuskomponentides täita või millised lisakulud on sellega seotud.

Kontrollküsimused:

- Kas salvestussüsteemi või elektroonilise arhiivi paigutuskohale ette nähtud IT-etalonturbe meetmed on realiseeritud?
- Kas arhiivi-andmekandjate hoiutingimused on teada ja dokumenteeritud?
- Kas kasutatavates pikaajalistes salvestusüksustes peetakse kinni arhiivi-andmekandjate hoiutingimustest?

M 1.60 Arhiivi-andmekandjate asjakohane säilitus

Vastutav algatuse eest: IT-juht

Vastutav elluviimise eest: IT-juht, administraator

Arhiivi-andmekandjate pikaajalisel kasutamisel tuleb erilist tähelepanu pöörata juurdepääsukaitsele ja klimaatilistele hoiutingimustele ning kontrollida nendest kinnipidamist.

Online -juurdepääs

Niivõrd kui arhiivi-andmekandjatele on online -juurdepääs, s.t. et neid hoitakse arhiivisüsteemis või mäluseade draivides, ei ole arhiivisüsteemi ja arhiivi-andmekandjate ruumiline eraldamine realiseeritav. Arhiivi-andmekandjate asjakohaseks säilitamiseks tuleb rakendada soovitusi, mis on nimetatud M 1.59 Arhiivisüsteemide asjakohane rajamine .

Offline -säilitamine

Kui arhiivi-andmekandjaid säilitatakse väljaspool arhiivisüsteemi, nn “ offline ”, tuleb rakendada B 2.5 Andmekandjate arhiiv kirjeldatud meetmeid, pöörates erilist tähelepanu õhu konditsioneerimise suhtes esitatud nõuetele.

Konditsioneer

Klimaatilised nõuded arhiivi-andmekandjate säilivusele sõltuvad kasutatud arhiivi-andmekandjatest. Tootjad annavad üksikuid mittekohustuslikke nõuandeid hoiutingimuste (nt temperatuuri ja õhuniiskuse) ning andmekandjate säilivusaja suhtes. Elektrooniliste arhiivisüsteemide pikaajaliseks kasutamiseks tuleb tootjatelt kindlasti nõuda konkreetset informatsiooni kasutuses olevate arhiivi-andmekandjate hoiutingimuste kohta. Kuna sellest sõltub arhiivi-andmekandjate säilivusaeg, tuleks enne kasutusele võetavate arhiivi-andmakandjate valikut välja selgitada alljärgnevad tingimused (vt ka M 4.169 Sobiva arhiveerimis-andmekandja valimine):

- **Tootjapoolne kasutusjuhend** - Vaadeldavate arhiivi-andmekandjate klimaatilised ja füüsilised hoiutingimused peaks olema tootja poolt küllaldaselt detailselt kirjeldatud (kaasa arvatud mõjud maksimaalsele säilivusajale). Nimetatud kasutusjuhend peaks olema kohustuslik, kui vähegi võimalik, peaks selle juurde kuuluma tootja garantiikiri hoiutingimustest kinnipidamisel.
- **Tehnilise teostatavuse kontroll** - Asjakohase hoidmise tehniline realiseerimine võib teatud tingimustel olla väga kompleksne. Olenevalt olemasolevatest tehnilistest ja infrastruktuurilistest nõuetest võivad teatud arhiivi-andmekandjad olla täiesti sobimatud. Seepärast tuleb eelnevalt kontrollida asjakohase hoidmise tehnilise realiseerimise võimalusi ning sellega seotud kulutusi.

Hoiutingimused peaksid olema dokumenteeritud arhiivisüsteemi kasutusjuhendis. Lisaks sellele tuleb garanteerida, et nõudeid hoiutingimustele pidavalt täidetaks ning kontrolli all hoitaks (vt M 1.27 Konditsioneer).

Füüsilise kaitse meetmed

Lisaks klimaatiliste tingimuste täitmisele tuleb kasutatavaid arhiivi-andmekandjaid kaitsta volituseta isikute juurdepääsu ja mehaanilise kahjustuse või muutmise eest. Siinkohal on asjakohane järgida eriti B 2.5 Andmekandjate arhiiv nimetatud meetmeid.

Juurdepääsukontroll

Lisaks sisenemiskontrollile andmekandjate ruumi, tuleohutusele ja kaitsele vee kahjustava mõju eest tuleb olenevalt arhiivi-andmekandjate liigist rakendada ka

teisi meetmeid, nt kaitseks magnetväljade mõju eest magnetlintidele. Selleks on vajalik nõuda tootjatelt siduvad soovitused mehaaniliste hoiutingimuste suhtes ning neid järgida.

Häire ja reaktsioon

Hoiutingimustest mitte kinnipidamisele peab järgnema häire ja reaktsioon. Selleks on vaja määratleda organisatsioonile omased eskalatsiooniprotseduurid ja -meetmed.

Kontrollküsimused:

- Kas on olemas tootjapoolselt siduvalt kindlaks määratud klimaatilised ja füüsilised hoiutingimused?
- Kas tootja poolt soovitatud klimaatilisi ja füüsilisi hoiutingimusi suudetakse järgida?
- Kas hoiutingimused on arhiivisüsteemide kasutusjuhendis dokumenteeritud?
- Kas hoiutingimuste mittejärgimise puhuks on välja töötatud eskalatsiooniprotseduurid?

M 1.61 Mobiilse töökoha sobiv valimine ja kasutamine

Vastutav algatuse eest: infoturbe osakond, kasutaja, ülemus

Vastutav elluviimise eest: kasutaja

Tänu ikka väiksemaks muutuvatele ja tõhusatele IT-süsteemidele on tänapäeval võimalik peaaegu kõikjal töötada. Seetõttu võib ükskõik millisest kohast saada mobiilne töökoht, selleks võib olla näiteks hotellituba, istekoht rongis või lennukis või mõni ruum kliendi juures. Selliseid mobiilseid töökohti saavad IT-kasutajad vaid väga piiratult sisustada ning neid tuleb üldiselt kasutada sellistena, nagu need kasutamise hetkel on. Seepärast peab iga IT-süsteemide mobiilne kasutaja kõigepealt otsustama, kas vastav koht on sobiv kasutamiseks mobiilse töökohana. Selle vastu võiksid rääkida alljärgnevad põhjused:

- Töötlemisele kuuluvad andmed on liiga tundlikud, et neid väljaspool büroruumi töödelda (vt ka M 2.217 Teabe, rakenduste ja süsteemide hoolikas liigitamine ja käitlus ja M 2.218 Andmekandjate ja IT-komponentide kaasavõtmise protseduurid).
- Koht ei võimalda varjata töödeldavaid andmeid kolmandate isikute eest, nt lähestikku istekohtade korral rongis või lennukis.
- Puudub elektritoide või võrguühendus.
- Mobiilsete IT-seadmete kasutamine on keelatud, nt lennukis või võõrastes büroodes.

Alljärgnevalt on loetletud veel mõned mobiilseks töötamiseks soovitatavad tingimused:

- Peaks olemas olema stabiilne koht mobiilsete IT-süsteemide paigutamiseks. Paljud mobiilsed IT-süsteemid purunevad kukkumise tagajärjel.
- Koht ei tohiks olla liiga kärarikas.
- Koht peaks olema küllaldaselt valgustatud, monitori valgusest üksi ei aita. Vältida tuleks pimestamist, reflekteerumist või peegeldumist.
- Monitori peaks olema võimalik paigutada nii, et selle ekraanil olevaid andmeid ei oleks võimalik kõrvalt näha. Sülearvutite jaoks on olemas ka spetsiaalsed monitori ekraanifiltrid, mis takistavad ekraanile nägemist kõrvalt.
- Lisaks eelnimetatule peaks koht olema selline, et ei kahjustaks IT-süsteeme, niisiis mitte liiga niiske, liiga külm või liiga soe. IT-seadmete kasutamise ajal on kasutaja sellest loomulikult ka ise huvitatud, aga ka väljaspool tööaega tuleks IT-seadmeid nõuetele vastavalt hoida.
- Mobiilseid IT-seadmeid tuleks kaitsta varaste eest (vt M 1.46 Vargusetõrjevahendid). Koht peaks pakkuma selleks vajalikke tingimusi. Et kindlustada näiteks sülearvutit kaablilukuga lihtsa äravõtmise vastu, peab olema võimalus, kinnitada kaablilukk mingi tugeva eseme külge. Kui võimalik, tuleks mobiilse töökoha aknad ja uksed lahkumisel sulgeda. See on näiteks võimalik hotellitubades või nõupidamisruumides, rongis aga enamasti raske.

Võõras kohas, nt hotellides, on ka alati soovitav teha endale selgeks, kuidas tuleb käituda põlengute ja teiste hädaolukordade korral, tähtis on näiteks häiresignaalide ja evakuatsiooniteede tundmine.

Kontrollküsimused:

- Kas töötajaid informeeritakse, millele nad mobiilse töökoha valikul ja kasutamisel peavad tähelepanu pöörama?

M 1.62 Kaablijaotusseadmete tulekaitse

Vastutav algatuse eest: tuleohutuse eest vastutav töötaja

Vastutav elluviimise eest: tehnikaosakond, tuleohutuse eest vastutav töötaja, planeerija

Nii majavõrgu sisemised kui ka avaliku võrgu välimised juhtmed kuhjuvad mingil moel kaablijaotusseadmetele või –paneelidele, millelt need on ühendusjuhtmete kaudu seotud serverite ning marsruuteritega jne. Et takistada nimetatud kaablijaotusseadmete ja -paneelide kahjustumist aktiivsete IT-seadmete (serverid, marsruuterid, jne) põlemise tagajärjel, tuleb need vastavate tuletõketega nimetatud aktiivsetest IT-seadmetest isoleerida.

Kui tehnilise infrastruktuuri ruumis paiknevad kaablijaotusseadmed ja –paneelid ühelt poolt (vt B 2.6 Tehnilise infrastruktuuri ruum) ning serveriruumis paiknevad serverid, marsruuterid jne teiselt poolt (vt B 2.4 Serveriruum) on paigutatud üksteisest korralikult eraldatuna, võib vastava tuleisolatsiooni sobivate meetmete abil realiseerida ehitises. Kui ei ole võimalik kasutada eraldi ruume ning kaablijaotusseadmed ja -paneelid tuleb paigutada serveriruumi, on võimalus kasutada nende paigaldamiseks nõuetele vastavaid seinale või põrandale paigaldatavaid jaotuskilpe, mis säilitavad vajaliku funktsionaalsuse. Seejuures tuleb aga erilist tähelepanu pöörata asjaolule, et ka kõiki majast ja avalikust võrgust ruumi tulevaid toitejuhtmeid kaitstaks ruumis samal viisil (nt asjakohaste kaablikanalite kaudu) põlengu eest.

Mõlemate lahenduste korral tuleb jälgida, et ühendusjuhtmete viimine kaablijaotusseadmetelt ja –paneelidelt IT-seadmete juurde läbi tulekaitsekonstruktsiooni oleks igal ajal asjakohaste tulekaitsevahenditega blokeeritud. Et saaks lihtsalt ja kiiresti nimetatud läbiviikude juures töid teostada, ning et alati ei peaks kulukat tulekaitset uuesti paigaldama, on soovitav kasutada tulekaitsepatjasid või (harvemate tööde korral) puistekivim. Kasutatavaid tulekaitsepatju tuleb lisaks sellele kindlustada väljakukkumise vastu.

Kontrollküsimused:

- Kas toitejuhtmed on küllaldaselt kaitstud?
- Kas valitud ja realiseeritud funktsiooni säilitamine (E-30 või E-90) vastab olemasolevatele võimalustele tuletõrjesignalisatsiooni ja tulekustutamise osas?
- Kas läbiviigud suletakse pärast tööde teostamist jaotuspiirkonnas vastavalt nõutud korrale?
- Kas kasutatavad tulekaitsepadjad kindlustatakse väljakukkumise vastu?

M 1.63 Sobiv pääsupunktide paigutus

Vastutav algatuse eest: IT-juht, infoturbe osakond

Vastutav elluviimise eest: siseteenistus, administraator

Pääsupunktide turvaline montaaž

Pääsupunktidega manipuleerimise ärahoidmiseks peaksid need olema paigutatud metallkorpusesse või kinnitatud metallklambritega, mis võimaldavad monteerimist seinale. Võimalik on paigutamine tõstetud põrandatesse, vahelagede või ripplagede peale ning välisantennide kasutamine. Olenevalt antenni kujust ei tunne isegi spetsialist ära, kas tegemist on tuletõrjesignalisatsiooni või pääsupunkti antenniga.

Ruumid või kohad, milles mitteusaldusväärsed isikud võivad pikemat aega ilma järelevalveta viibida, ei sobi põhimõtteliselt montaažikohaks (väline maa-ala, trepikojad) nähtavatele ja ilma maskeeringuta pääsupunktidele. Nendesse piirkondadesse võib aga siiski paigaldada pääsupunktid, millel pole marsruutimise funktsiooni. Selle kaudu ei saa volituseta isikud informatsiooni võrgu detailse ülesehituse kohta. Sellega vähendatakse juurdepääsuala raadiokohtvõrgule (WLAN) ja teatud juhtudel sellega seotud LAN-võrgule. Minimaalse kaitsena peaks pääsupunktid kinnitama kindlalt kohta, kus need ei ole ilma abivahenditeta ligipääsetavad või mittenähtavasse kohta.

Pääsupunktide positsioneerimine

Pääsupunktide paigaldamise ja reguleerimise kaudu mõjutatakse oluliselt raadiokohtvõrgu (WLAN) ülekandekvaliteeti ja jõudlust. Üldkehtiv on, et raadiolainete levi alade, mida ei tule katta raadiokohtvõrgu (WLAN) kaudu, tuleb võimalikult minimeerida. Sel viisil ei vähendata mitte ainult juurdepääsuala, vaid kaetakse paremini ka tegelikult soovitud ala. Selleks võib kasutada suundantenne, mis koondavad elektromagnetiliste lainete kiirguse teatud suundadesse ruumis ning saavutavad nii suunast sõltuva tugevdusefekti (nimetatakse antenni võimenduseks). See tugevdusefekt tuleb vastavusse viia saatevõimsusega pääsupunktis. Mõned pääsupunktid toetavad saatevõimsuse paindlikku seadistamist. Sel viisil saab katteala vajaliku võimsusega katta ja juurdepääs raadiokohtvõrgule (WLAN) väljast muutub samal ajal raskemaks, kuna siin valitsevad nüüd võrdlemisi halvad vastuvõtutingimused. Eelduseks on pääsupunktide või antennide sobiv positsioneering. See saab toimuda vastava kattevõimsuse mõõtmise baasil.

Välisantennide kaitse

Välisalade katmisel tuleb välisinstallatsioone (antennid ja võimalikud pääsupunktid) kaitsta nõuetele vastavalt ilmastikumõjude, elektrilahenduste ja volitamatu juurdepääsu eest. Pääsupunktide paigaldamist väljaspool hoonet tuleb võimalusel vältida.Antennide paigaldamine hoone katusele peab toimuma nii, et antenn oleks kaitstud pikselöögi eest. Antenn peaks olema piksevardast piisavalt palju madalamal ning kaugus piksevardast peaks olema piisav. Sama kehtib ka kauguse kohta kõrgepingeliinidest. Väljaspool hoonet olevad antennid, mida ohustab elektrilahendus (kehtib antennide kohta, mis on monteeritud katusele), peaksid olema ühendatud spetsiaalse liigpingekaitsega, mis avastab kiiresti ja juhib eemale elektri- ja pingelained. Nimetatud liigpingekaitse monteeritakse antenni ja pääsupunkti (tavaliselt hoones sees või sama moodi kaitstud punktis) vahele ning sellel peab olema küllaldane maandus. Pääsupunkte ei tohiks põhimõtteliselt installeerida elektrilahenduste mõjupiirkondadesse.

Kui pääsupunktid installeeritakse erandkorras väljapoole asjakohaselt konditsioneeritud hoonet, tuleb tagada, et pääsupunkt oleks küllaldaselt sissetungiva

niiskuse, külma ja kuumuse eest kaitstud. Välisantenne tuleb sobival viisil kaitsta lume kuhjumise eest. Need tuleb paigaldada kaitstult tuule eest või peab paigaldus olema ka tugeva tuule korral nii vastupidav, et antenni suund ei muutu.

Kontrollküsimused:

- Kuidas kaitstakse pääsupunkte volitamatu juurdepääsu eest?
- Kas on garanteeritud, et pääsupunktid katavad vaid soovitud ala? Kas nende alade katmine on optimaalne?

M 1.64 Elektriliste süttimisallikate vältimine

Vastutav algatuse eest: tuleohutuse eest vastutav töötaja, tehnikaosakonna juhataja

Vastutav elluviimise eest: tehnikaosakond, töötajad

Enamik ehituslikest tuleohutusmeetmetest on suunatud põlengute leviku piiramisele, aga ka inimeste evakuatsioonile ja päästetöötajate tegevusele kaasaaitamisele. Põlengute tekkele avaldavad nimetatud meetmed vaid vähest mõju.

Nende vältimiseks peavad inimesed oma igapäevatööd tehes olema tähelepanelikud ja hoolsad. Lisaks üldtuntud ja tõenäolistele tuleallikatele nagu tuhatoosid, sigaretikonid paberikorvis või jõuluküünlad, tuleb tähelepanu pöörata ka vähemtõenäolistele elektrilistele süttimisallikatele.

Elektriseadmed

Uute isiklike majapidamisseadmete ostmisel kasutatakse veel funktsioneerivaid vanu seadmeid “annetusena” ettevõttes edasi. Seejuures unustatakse, et just vanad elektriseadmed kujutavad endast oma vanadusest tingitud tõenäoliste defektidega eriti suurt tuleohtu.

Isiklike elektriseadmete kasutamine ettevõttes või asutuses vajab seetõttu täpset reguleerimist. See võiks olla lubatud vaid erandkorras, kui seadmed on enne elektriala spetsialisti poolt kontrollitud ning ohutuks tunnistatud. Lubatud seadmed tuleks spetsiaalselt märgistada, nii et mittelubatud seadmeid oleks kerge ära tunda ja kasutusest kõrvaldada.

Eriti külmkappe, mis töötavad alaliselt ja kohvimasinaid, mis on tihti tundide kaupa sisse lülitatud, tuleks kasutada vaid ruumides, mis on selgesõnaliselt ja ehituslikult selleks ette nähtud (kööginurgad jne).

Pikendusjuhtmed

Ükskõik kui palju pistikupesasid arhitektid ka ette poleks näinud, neid on ikka vähe ning need on vales kohas. Puuduvate pistikupesade asendamiseks kasutatakse tihti pikendusjuhtmeid. Kui need on ebapiisava kvaliteediga või kasutatakse neid mitteotstarbekohaselt (vt ka G 4.62 Ebapiisav pistikupesade arv), kujutavad need pikendusjuhtmed endast ohtlikku süttimisallikat.

Pikendusjuhtmete kasutamist tuleb nii palju kui võimalik vältida. Puuduvad pistikupesad tuleks elektriala spetsialisti poolt olemasolevasse kanalisüsteemi paigaldada või nõuetele vastavalt krohvile monteerida. Kui see ei ole võimalik ning seega ei ole võimalik vältida ka pikendusjuhtmete kasutamist, tuleb tähelepanu pöörata alljärgnevale:

- Kasutada tohib vaid kõrgekvaliteetseid pikendusjuhtmeid, mis on elektriala spetsialisti poolt kontrollitud ning kasutuskõlblikuks tunnistatud.
- Paljude väheste pistikupesadega pikendusjuhtmete asemel tuleks kasutada piisavalt paljude pistikupesadega pikendusjuhtmeid.
- Pikendusjuhtmeid ei tohiks mitte mingil juhul ühendada järjestikku.
- Pikendusjuhtmeid ei tohiks mitte mingil juhul üle koormata. Tavaliselt on piiriks 3500 vatti. Seejuures tuleb kindlasti tähelepanu pöörata tüübisildile.
- Pikendusjuhtmed ei tohi mitte mingil juhul olla töökoha juures põrandal ega ka aladel, kus inimesed liiguvad.

Elektrijaotussüsteem

Kogu elektrijaotussüsteem, enamasti kaitselülitid ja kruvi- ning klemmühendused vananevad täpselt samuti nagu teised tehnilised seadmedki. Sellepärast on seda vaja regulaarselt kontrollida.

Ventilaatorid

Tolmu tõttu blokeeritud ventilaatorid võivad põhjustada jahutamist vajavate IT-seadmete ülekuumenemist, aga ka ise süttimisallikaks muutuda (vt G 4.63 Tolmunud ventilaatorid). Seega tuleb ventilaatorite vaba pöörlemist ja tolmusust regulaarselt kontrollida ning neid puhastada. See peaks toimuma vähemalt kord aastas ning äratuntava vajaduse korral ka tihedamini (vt M 2.4 Hooldus- ja remonditööde reeglid).

Protokollimine

Kõik kontrollimised ja nende tulemused tuleb ettenähtud kujul dokumenteerida.

Kontrollküsimused:

- Kas on olemas kirjalikud eeskirjad isiklike elektriseadmete ja pikendusjuhtmete kasutamiseks, elektrijaotusseadmete ja ventilaatorite kontrollimiseks?
- Kas on olemas elektriala spetsialist, kes teostab ülalnimetatud kontrolli?
- Kas kontrolli teostus ja tulemused protokollitakse?

M 1.65z IT kaabelduse uuendamine

Vastutav algatuse eest: planeerija, tehnikaosakonna juhataja, IT-juht

Vastutav elluviimise eest: tehnikaosakond

Informatsioonitehnika ning eriti uute IT-rakenduste tõttu esitatavate nõuete kiire areng viib vanema kaabeldusega hoonetes tihti mõttele, IT-kaabeldus uuendada või täielikult välja vahetada. Kulutusi, mis tekivad olemasoleva IT-kaabelduse täieliku asendamise tõttu uue sekundaarse ja tertsiaarse kaabeldusega, ei tohi alahinnata. Kogemus näitab, et juba enne ulatusliku moderniseerimisprojekti finantsiliste ja organisatoorsete kulude esmast vaatlust langetatakse enamasti otsus, et olemasolevat IT-kaabeldust tuleks kasutada nii kaua kui võimalik.

IT-kaabelduse ulatuslik uuendamine tuleks ette võtta vaid juhul, kui on kindel, et olemasolev IT-kaabeldus asutuse äritegevust enam vajalikul määral ei toeta. Selged märgid sellest, et olemasolevat IT-kaabeldust enam kasutada ei saa, on näiteks alljärgnevad:

- Kaablite täiendav paigaldamine, mis on vajalik uute tarbijate ühendamiseks võrku, kutsub esile pidevaid häireid võrgu töös.
- Olemasoleva võrgu töö kannatab pidevate tõrgete all, nt lühiühenduste tõttu lubaringvõrgus või kontuuri moodustamisel defektsete ühenduste tõttu IBM IVS tüüp 1 Ethernet'i kaablitel.
- Olemasolev kaabeldus ei saa enam vastata nõuetele võimsuse osas, kuna nt terved korrused on ühendatud IBM IVS tüüp 1 kaabeldusega, niisiis maksimaalse edastuskiirusega 10 Mbit/s.

Kui IT-kaabeldus nõuab uuendamist, tuleb läbida kõik planeerimisfaasid, nagu esmakordsel paigaldamisel (vt M 2.395 IT-kaabeldusele esitatavate nõuete analüüs). Ka siin tuleb alustada nõuete analüüsist ja vajaduste arengu hindamisest.

Vana tüüp 1 kaablite väljavahetamisel tuleb eriti tertsiaarvaldkonnas kontrollida, kas kaabliteed võivad ka uue kaabelduse korral samaks jääda. Kuna tüüp 1 kaablite maksimaalseks pikkuseks võib olla 150 meetrit, võib osutuda vajalikuks installeerida sobivatesse kohtadesse korruste jagajad, kuna 5. või kõrgema kategooria kaablite ühenduspikkuseks võib olla maksimaalselt 100 meetrit. Seejuures arvestatakse ühenduspikkus tertsiaarkaabli pikkusest, lisades sellele patchkaabli pikkuse.

Kui tühjalt seisvat hoonet moderniseerima hakatakse, võib ümberpaigutamiseks ette võtta puhtalt tehnilise planeerimise. Hoonete korral, mida kasutatakse büroona, mitte puhtalt laohoonena, tuleb olemasoleva IT-kaabelduse üleviimisel uuele kaabeldustehnikale koostada moderniseerimisplaan.

Selles tuleb ette näha, kuidas IT-kaabelduse paigaldamist töö käigus nii korraldada, et tööprotsessi võimalikult vähe häirida.

Kontrollküsimused:

- Kas moderniseerimisplaani teostamiseks on olemas kirjalik nõuete analüüs?

- Kas olemasoleva kaabelduse kaabliteed on mõõdetud?

M 1.66z Normidele vastav IT-kaabeldus

Vastutav algatuse eest: IT-juht

Vastutav algatuse eest: IT-juht

Mõiste all “andmesidevõrgud” avaldati 1995. aastal esmakordselt norm, mis kirjeldab kindlaksmääratud omadustega ülekandeliinide topoloogiat ja klassifikatsiooni, samuti ühtset liidest lõppseadmete ühendamiseks. Nimetatud normid ei kehti ainult büroohoonetes, vaid neid on võimalik rakendada ka teistes kasutusvaldkondades. Vastutust järelevalve eest nimetatud normide täitmise, rahvusvaheliste standardiorganisatsioonidega (ISO/IEC) kooskõlastamise ja vajadusel edasiarendamise ja täpsustamise eest kannab Euroopa Elektrotehnika Standardikomitee (CENELEC).

Normid on kasutajatele abiks hoonete planeerimise, kaabelduse kavandi koostamise, andmesidekaablite planeerimise, realiseerimise ja kasutamise faasides. Lisaks normile EN 50173-1 Andmesidevõrgud, üldised nõuded ning nimetatud dokumendi väljatöötamise ajal kavandina kasutatavatele osadele 2 Büroohooned , 3 Tööstushooned , 4 Eluruumid ja 5 Arvutuskeskused on veel norme, mis leiavad kasutust IT-kaabelduse planeerimisel ja teostamisel.

Kantuna üle IT-etalonturbe kataloogide faasimudelile on norme võimalik liigitada alljärgnevalt:

- **Hoonete planeerimine**

EN 50310 – meetmete rakendamine potentsiaalide ühtlustamiseks ja maanduse teostamiseks informatsioonitehnikaga hoonetes
5.2: Ühine potentsiaalide ühtlustamise seade (CBN) ühes hoones.
6.3: Vahelduvvoolu jaotus ja kaitsejuhi (TN-S) ühendamine

- **Kaabelduse kavand**

EN 50173-1 - Andmesidevõrgud, üldised nõuded ja bürooruumid
4: Topoloogia
5: Ülekandeliinide potentsiaal
7: Nõuded kaablitele
8: Nõuded ühendustehnikale
9: Nõuded juhtmetele
A.1: Vahekauguste piirväärtused

- **Planeerimine**

EN 50174-1 - Andmesidekaablite paigaldamine, spetsifikatsioon ja garanteeritud kvaliteet
4: Kaalutlused spetsifikatsioonide kindlaksmääramiseks
5: Kvaliteedi garantii
7: Kaabelduse haldamine
EN 50174-2 – Andmesidekaablite paigaldamine, paigalduse projekteerimine ja paigaldamine hoonetes
4: Nõuded turvalisusele
5: Üldised nõuded metall- ja valguskaablite paigaldamiseks
6: Lisanõuded metallkaablite paigaldamiseks
7: Lisanõuded valguskaablite paigaldamiseks

EN 50174-3 – Andmesidekaablite paigaldamine, paigalduse projekteerimine ja paigaldamine välitingimustes

EN 50310 – meetmete rakendamine potentsiaalide ühtlustamiseks ja maanduse teostamiseks informatsioonitehnikaga hoonetes

5.2: Ühine potentsiaalide ühtlustamise seade (CBN) ühes hoones.

6.3: Vahelduvvoolu jaotus ja kaitsejuhi (TN-S) ühendamine

- **Realiseerimine**

EN 50174-1 - Andmesidekaablite paigaldamine, spetsifikatsioon ja garanteeritud kvaliteet

6: Dokumentatsioon

7: Kaabelduse haldamine

EN 50174-2 – Andmesidekaablite paigaldamine, paigalduse projekteerimine ja paigaldamine hoonetes

4: Nõuded turvalisusele

5: Üldised nõuded metall- ja valguskaablite paigaldamiseks

6: Lisanõuded metallkaablite paigaldamiseks

7: Lisanõuded valguskaablite paigaldamiseks

EN 50174-3 – Andmesidekaablite paigaldamine, paigalduse projekteerimine ja paigaldamine välitingimustes

EN 50310 – Meetmete rakendamine potentsiaalide ühtlustamiseks ja maanduse teostamiseks informatsioonitehnikaga hoonetes

5.2: Ühine potentsiaalide ühtlustamise seade (CBN) ühes hoones.

6.3: Vahelduvvoolu jaotus ja kaitsejuhi (TN-S) ühendamine

EN 50346 – Kaablite paigaldamine, paigaldatud kaabelduse testimine

4: Üldised nõuded

5: Sümmeetrilise kaabelduse kontrollparameetrid

6: Valguskaablite kontrollparameetrid

- **Kasutamine**

EN 50174-1 - Andmesidekaablite paigaldamine, spetsifikatsioon ja garanteeritud kvaliteet

5: Kvaliteedi garantii

7: Kaabelduse haldamine

8: Remont ja korrashoid

M 1.67 Kapisüsteemide dimensioneerimine ja kasutus

Vastutav algatuse eest: IT-juht

Vastutav elluviimise eest: IT-juht

Serverite, aktiiv- ja passiivkomponentide töökindluse parandamiseks peaksid need seadmed olema monteeritud või paigaldatud kapisüsteemidesse. Kapisüsteeme nimetatakse olenevalt kasutamise viisist tihti 19-tollisteks püstikuteks, serverikappideks või ka võrgukappideks. Kapisüsteeme on erinevate sise- ja välismõõtudega. Kõige rohkem on levinud kapid netomahuga 42 püstikuühikut (U). Sõltuvalt sellest, kas kapisüsteemid on paigutatud suletud jaotusruumidesse või kõigile juurdepääsetavatesse kohtadesse, peavad neil olema uksed, külgseinad ja lukud, mis vastavad kaitsevajadustele igal konkreetsel juhul. Kappide all paiknevad soklid kergendavad vajaliku kaabelduse paigaldamist. Tänu soklile jääb IT-süsteemide ja põranda vahele täiendav vahekaugus. Sel juhul ei saa IT-süsteemid vee võimaliku sisseimbumise tagajärjel automaatselt kahjustada, kuna need asuvad põrandast kõrgemal. Nõuetele vastavalt kindlustatud jaotusruumide korral võib pärast keskkonnatingimuste kontrollimist loobuda ustest ja külgseintest.

Kapi sisemuse ülesehituse juures tuleb tingimata arvestada hooldustehnilisi aspekte. Näiteks peaks olema võimalik kiiresti välja vahetada komponente lülitussüsteemis ilma naabersüsteeme kahjustamata. See eeldab kõikide komponentide ettenägelikku sissepaigutamist ning vastavat patchkaablite haldamist. Eeliseks seejuures on, et elektrikaablid ja IT-kaabeldus saaks paigaldatud stabiilselt ja kaitstult. Paljud kapisüsteemide tootjad pakuvad komponente, mille abil saab kapisisest kaabipaigutust vastavusse viia kasutaja spetsiifiliste nõuete ja soovidega. Vältida tuleb üleliigse pikkusega patchkaableid.

Kappide kasutamise planeerimisel tuleb silmas pidada, et kapi mahutavus on enamasti piiratud sellesse paigutatud seadmete soojusemissiooniga, mitte aga paigaldatavate seadmete mõõtmetega. Kui sisse monteeritud seadmete termiline koormus on liiga suur, võivad tekkida soojuse ärakande probleemid. Sarnased probleemid võivad tekkida võrgukappides, milles on väga palju passiivkomponente (jaotuspaneele) ning väga tihedalt kaableid. Sel juhul võib kapi õhuvahetus olla niivõrd häiritud, et detailidel või aktiivkomponentidel tekivad funktsioonihäired. Ka nimetatud aspekti tuleb kappide kasutamisel silmas pidada.

Üksteise kõrvale paigutatud kappide korral tuleb täiendavat tähelepanu pöörata aktiivkomponentide õhu juhtimisele kõrval asuvates kappides. Kindlasti tuleb vältida, et komponentidest eralduv soe õhk takistaks külma õhu juurdevoolu naabruses asuvale komponendile. Kappide reas paiknevate üksikute kappide isoleerimisega saab seda probleemi lahendada. Selleks, et aktiivkomponente saaks käitada ettenähtud temperatuuridel, tuleb kapid isoleerida. Lihtsamal juhul aitab kapi passiivsest jahtumisest piisavalt külma ruumiõhu tingimustes. Suletud kappide korral võib sellele kapis paiknevate ventilatsioonisüsteemidega

kaasa aidata. Kui soojuskoormused on liiga suured, võib kasutada erinevaid aktiivjahutussüsteeme. Seejuures tuleb ühelt poolt eristada ruumi jahutamise võimalusi ning teiselt poolt jahutussüsteeme, milliseid võib paigaldada kappide külge või peale.

Et oleks võimalik käitada IT-komponente, millel on suur soojusemissioon ning mis võtavad samal ajal vähe ruumi, võib kaaluda spetsiaalsete iseseisvate konditsioneeridega kapisüsteemide kasutamist. Kappe, mille sisemuses on enamasti vaid vedelikjahutus, tohiks kasutada vaid pärast põhjalikku vajadus- ja riskianalüüsi.

Igasugune õhu konditsioneerimise viis eeldab täpset planeerimist, millega kaasneb kõikide mõju avaldavate parameetrite arvestamine, kaasa arvatud majanduslikkus. Konditsioneeriga kappide kasutamisel tuleb lisaks tähelepanu pöörata asjaolule, et külgseintele või ustele paigaldatud kliimaseadmed võivad vähendada kapiuste avanemisnurka ning teatud juhtudel evakuatsiooniteedele ulatuda. Ruum peaks võimalusel olema selliselt planeeritud, et kappidel paiknevaid kliimaseadmeid oleks võimalik täiendada.

Soovitav on kehtestada asutuses ühtsed nõuded kapisüsteemide sisustamiseks ja kasutamiseks. Ka kappide kaabeldus üksteise all tuleb hoolikalt planeerida (vt M 1.69 Kaabeldus serveriruumides).

Kontrollküsimused:

- Kas kapid on paigaldatud ja täidetud selliselt, et hooldustööde tegemisel pääseb probleemideta kõikide IT-süsteemide juurde?

M 1.68 Nõuetele vastav installatsioon

Vastutav algatuse eest: IT-juht

Vastutav elluviimise eest: IT-juht

IT-kaabelduse paigaldamine nõuab väga head asjatundlikkust ja hoolikust. Niivõrd kui kaablite ja passiivkomponentide tootjad pakuvad garantiid, mis ületab seaduslikud miinimumpiirid, kehtib see tihti vaid eeldusel, et installeerimise teostab tõestatud kvalifikatsiooniga ettevõte. Tellija peaks IT-kaabelduse paigaldamise kõikides etappides kontrollima tähtsate kriteeriumide täitmist, mis tagaksid nõuetele vastava teostuse. Materjali kättetoimetamisel tuleb kõigepealt kontrollida, kas on tarnitud õiged kaablid ja ühenduskomponendid. Esimesena tuleb kontrollida, kas kaablid ja ühenduskomponendid (nt varje) üksteisega sobivad. Kui tarnitud kaableid ja nende juurde kuuluvaid materjale ei paigaldata kohe, tuleb tagada nende nõuetele vastav hoidmine. Hoiukoht peab olema kuiv ja tugevate klimaatiliste mõjude eest kaitstud. Soovitav on hoida lattu paigutatud materjali kuni installeerimiseni originaalpakendis.

IT-kaablite paigaldamisel tuleks eriti hoolitseda selle eest, et montaažiga ei kaasneks kaablite kahjustust ning et kaabliteed oleks valitud nii, et hoone normaalsel kasutamisel ei saaks paigaldatud kaablid kahjustada. Lisaks sellele tuleb jälgida, et IT-kaablid paigaldataks eraldi elektrikaablitest. Juba eraldusteed ühiselt kasutatavatel trassidel aitavad tavaliselt takistada elektrikaablite mõju IT-kaablitele. Kaablite paigaldamisel tuleb järgida kaitsemeetmeid ning kinni pidada koormuspiirangutest.

- Enne kaablite paigaldamist tuleb müüriavadelt ja muudelt sarnastelt läbiviiguavadelt eemaldada teravad servad ning need ümardada, et vältida kaablite läbiviimisel ja kinnitamisel kaabimantli kahjustusi.
- Kaabli paigaldamisel ja tööprotsessis ei tohi minimaalne painderaadius olla väiksem kehtestatud normist. Kui see pole kaablile märgitud, kehtib vastavalt normile EN 50173, et väikseim lubatud painderaadius ei tohi olla väiksem kui kaabli kaheksakordne väline läbimõõt. Tagada tuleb, et painded kaablikanalites ja kaablitrassides vastaksid lubatud painderaadiustele.
- Vajadusel annab tootja andmelehtedes kaablite kohta olenevalt nende tüübist kaks painderaadiust: suurema väärtusega painderaadius näitab maksimaalset paindekoormust kaabli sissetõmbamisel. Väiksem suurus kehtib juba paigaldatud kaabli kohta.
- Andmelehelt leiab ka andmed kaablitüübi maksimaalse tõmbekoormuse kohta.
- Kaabli sissetõmbamisel tohib abivahendina kasutada vaid sobivaid määrdeaineid. Üldiselt tohib kasutada õli- ja rasvavabasid määrdeaineid (nt talgipulber).
- Kaablite kinnitamisel kaablitrassidele klemmide või klambritega ei tohi kaableid mitte mingil juhul muljuda.

Kaablid tuleb paigaldada krohvi alla, kaablikanalitesse või kaablitrassidele. Kaablite katteta paigaldamine on täiesti lubatud, tuleb vaid tagada, et ei toimuks selle kahjustamist büroomööbli või transpordivahenditega ülesõitmisel.

Kontrollküsimused:

- Kas kontrolliti ja järgiti tootjapoolselt kindlaks määratud nõudeid kaablite sissetõmbamiseks ja paigaldamiseks?

- Kas kaablite kinnitamisel ja kasutamisel välditakse kaablite survekoormust?
- Kas enne kaablite paigaldamist kontrolliti trasse ja läbiviiguavasid?

M 1.69z Kaabeldus serveriruumides

Vastutav algatuse eest: IT-juht

Vastutav elluviimise eest: planeerija, IT-juht

Serveriruumides ja arvutuskeskustes tuleb järgida struktureeritud kaabelduse põhimõtteid vastavalt standardile EN 50173 – 1“ Arvutivõrkude tehnoloogia – Andmesidevõrgud – 1. osa: Üldised nõuded ”. Normi kavandina on ilmunud spetsiaalselt arvutikeskuste jaoks välja töötatud täiendav standard EN 50173 – 5. Sellega kergendatakse kasutaja jaoks normi nõuete realiseerimist.

Asutuse olemasolevast või planeeritud võrgukontseptsioonist johtuvad nõuded on aluseks IT-kaabelduse struktureerimisele serveriruumides ja arvutuskeskustes. Struktuur määrab kindlaks, kuidas toimub serverite võrku ühendamine ning kuidas toimub nende ühendamine kohtvõrku (LAN), välisvõrkudesse ja kommunikatsioonisüsteemide ühendusepakkujatega. Ettenägelikult tuleb arvesse võtta asutuses kasutatavaid või planeeritavaid tööprotsessi toetavaid süsteeme, nagu nt terminalserverid, KVM kommutaatorid ning SAN/NAS (Storage Area Network, Network Attached Storage) süsteemid. Sellega on analoogselt korruse- ja hoonejagajatega hoonestruktuuridele kindlaks määratud IT-kaabelduse niinimetatud juurdepääsu- ja kontsentreerumiskohtade struktuuri alused.

Suuremates installatsioonides jaotatakse kappide grupid, millesse serverid on paigutatud, tihti teatud “võrgukapi” juurde. Võrgukappide ja nende juurde jaotatud serverikappide vahele paigaldatakse püsiv kaabeldus või spetsiaalne serveriruumide süsteemikaabeldus. Võrgukapid on jälle omavahel seotud asutuse nõudmistele vastavalt. Et serveriruumi või arvutuskeskuse pinda parimal viisil ära kasutada, on vajalik töötada välja nõudmistele vastav ruumi plaan. Nimetatud ruumi plaanis tuleb vajalikud pinnad asutuses kasutusel olevate süsteemidega kappidele (lisaks serveritele ka salvestussüsteemid ja võrgu aktiiv- ning passiivkomponendid) jaotada tulevikule mõeldes reservidega. Seejuures tuleb arvesse võtta ohutusalaseid aspekte, nagu evakuatsiooniteede ettevalmistamine, tööalaseid aspekte, nagu transporditeede ettevalmistamine ning ka õhu konditsioneerimist puudutavaid aspekte. Selle põhjal on võimalik planeerida elektritoite ja trasside paigaldamist.

Serveriruumides ja arvutuskeskustes on soovitav kasutada suurele koormusele vastupidavat tõstetud põrandat (vt M 1.49 Tehnilised ja organisatsioonilised nõuded arvutuskeskusele). Kui tõstetud põrand kaasatakse kapi konditsioneeri õhu juhtimisse, tuleb arvestada trassisüsteemidega. Paljude lõikuvate trasside tõttu tõstetud põrandates olevate värske õhu juurdevooluavade ning kaugemal seisvate kappide vahel, millel on suur soojuskoormus, võivad tekkida “kuumad kohad” (hot spots) . Kuigi on kindlaks tehtud, et konditsioneeri võimsus ruumi jaoks on küllaldane, jätkub mõnedele kappidele ja nendes olevatele IT-komponentidele liiga vähe jahutatud õhku. Selle tagajärjeks võivad olla serverite või võrgu

aktiivkomponentide tõrked ülekuumenemise tõttu. Lisaks sellele tuleb kindlasti suurt rõhku panna mittetolmavale põrandakattele- või toorpõrandale.

Soovitav on nii ulatuslikult kui võimalik kaablid kindlalt paigaldada. See aitab kaasa trassisüsteemide nõuetele vastavale paigaldamisele tõstetud põrandates või lae all. Servereid ei tohiks võimalusel ühendada patchkaablitega ilma täiendavate trassisüsteemideta keskselt ruumi paigaldatud serveri kommutaatoritega ka juhul, kui seda kaabeldusliiki praktikas tihti kasutatakse. Selline “lahtine kaabeldus” on eriti ohustatud täiendava kaablite paigaldamise korral.

Asutuse nõuetega vastavusse viidud kapisüsteemid, millesse on eelnevalt monteeritud süsteemid kaabli paigaldamiseks ja üleliigse kaabli hoiukoht, võimaldavad ülevaatlikku ja hästi hooldatavat kaabli paigaldamist kapis.

Kui ka võrku ühendatakse vaid vähesed kapid, on otstarbekohane installeerida kapisüsteemidesse jaotuspaneelid serverite ühendamiseks ning nende jaotuspaneelide kindel ühendus võrgusõlmedega serveriruumis. Kui koostamisel on uus kontseptsioon, tuleb näiteks kaaluda kõikide kappide eelnevat varustamist jaotuspaneelidega 6. või 7. kategooria vaskkaablite jaoks (CAT-6 või CAT-7, sobiv 10 gigabitise ühenduse jaoks) ning vastavalt vajadusele lisaks LWL-jaotuspaneeliga. Viimase abil saab näiteks ühendada servereid salvestusvõrku. Loomulikult tuleb kappide eelvarustamine viia vastavusse asutuse strateegiaga.

Kui ei ole ehituslikke takistusi, tuleb paljudel juhtudel kaablite paigaldamisele tõstetud põranda kaudu eelistada kaablite paigaldamist serveriruumi lae all kulgevate trasside kaudu. Eriti juhul, kui tõstetud põrand täidab konditsioneeri rolli, võib tõstetud põrandasse paigaldatud kaabeldus takistada vajaliku jahutusõhu liikumist. Lisaks sellele varjab kaablite paigaldamine tõstetud põrandasse endas kõrgendatud ohtu, et mittevajalikke kaableid ei eemaldata. Kui kaablid on paigaldatud hästi juurdepääsetavatesse laetrassidesse, on vanade kaablite eemaldamine tavaliselt märksa kergem.

Kontrollküsimused:

- Kas ka serveriruumis järgitakse struktureeritud kaabelduse põhimõtteid?
- Kas kapisüsteemide soetamisel ja täitmisel järgitakse asutuse nõudeid ja strateegiat?

M 1.70 Tsentraalne puhvertoiteallikas

Algatamise eest vastutavad: Infoturbe spetsialist, IT juht, tehnikaosakonna juhataja

Rakendamise eest vastutavad: administraator, tehnikaosakond

Eesti oludes ei ole mõistlik kõiki seadmeid puhvertoiteallika taha ühendada, seetõttu jääb rakendaja otsustada läbi riskianalüüsi, mis seadmed ta ühendab puhvertoiteallikaga ja mida mitte. Puhvertoiteallikas (UPS) sildab lühiajalisest voolukatkestust või säilitab vooluga varustatust nii kauaks, et on võimalik seadmete ettenähtud korras väljalülitamine. See on eriti otstarbekas järgmistel juhtudel:

- kui arvuti vahemällu salvestatakse suurel hulgal andmeid (nt Cache võrguserveris), enne kui need mittekaduvatele mäluseadmetele salvestatakse;
- kui voolu katkestuse tagajärjel läheks kaduma terve hulk andmeid, mida tuleks tagantjärele uuesti taastada;
- kui ei ole tagatud küllaldase stabiilsusega elektritoide.

Eristatakse kolme puhvertoiteallika (UPS) liiki:

- **VFD-UPS (Voltage and Frequency Dependent)** - Selle korral saavad võrku ühendatud tarbijad normaalkäituse korral toidet otse vooluvõrgust. Alles siis, kui see enam ei toimi, lülitub puhvertoiteallikas automaatselt sisse ning võtab toitefunktsiooni üle. Selleks vajab VFD-UPS kuni 10 ms ümberlülitamisaega, mis mõnede IT-seadmete jaoks võib olla liiga palju. Kuna VFD-UPS normaalkäituse korral võrku ühendatud tarbijate vooluga varustamisel ei osale, nimetati seda varem ka offline- UPS. VFD tähendab Voltage and Frequency Dependent ning tagab selle, et normaalkäituse korral on UPSi väljundvool nii pinge kui ka sageduse poolest otseselt sõltuv sisendvoolust. See tähendab, et väiksemad tõrked toitevõrgus võivad jõuda otse VFD-UPSi kaudu toidet saavate tarbijateni.
- **VI-UPS (Voltage Independent)** - VI-UPS reguleerib väiksemate kõikumiste korral toitepinget (VI tähendab Voltage Independent), ilma et UPS võtaks täielikult üle võrku ühendatud tarbijate vooluga varustamise. Sagedus VI-UPS väljumisel on aga nagu VFD-UPS korralgi, otseselt sõltuv toitevõrgust. Ka VI-UPS korral võib ümberlülitamisel patareivoolule tekkida ümberlülitamisest tingitud katkestusi vooluga varustamisel.
- **VFI-UPS (Voltage and Frenquency Independent)** - VFI-UPS korral ei ole normaaljuhul enam otsest ühendust UPSi sisendi ja väljundi vahel. Kogu elektrienergia alaldatakse sisendi pool ning suunatakse alalisvoolu vahelülisse. Sealt toimub patareide optimaalses laadimisseisundis hoidmine ja vaheldi varustamine vooluga. Alles see toodab võrku ühendatud tarbijatele vajalikku vahelduvpinget. VFI-UPS on niisiis alaliselt lülitatud võrgu ja tarbija vahele. Seetõttu ei teki ümberlülitumisest tingitud katkestusi vooluga varustamisel, mistõttu ainult VFI-UPS tagab kindlalt katkematu vooluga varustamise. Kuna siin toimub kogu vooluga varustamine alati UPSi kaudu, nimetati seda varem ka online-UPS- ks.

Kui neid kolme UPS tüüpi omavahel võrrelda, ei ole kahtlust, et VFI-UPS on parimate lähteomadustega ja soovitatav vähemalt tundlike IT-süsteemide vooluga

varustamiseks. Pidades silmas teisi, siinkohal mitte käsitlust leidvaid kvaliteeditunnuseid, pakub UPS parimat võimalust IT-seadmete vooluga varustamiseks. Vastupidiselt ikka ja jälle avaldatud arvamusele ei kaitse ükskõik milline UPSi mudel selle sõna otseses tähenduses liigpinge eest. UPS suudab küll normaalse funktsioneerimise käigus liiga kõrgeid pingeid võrku ühendatud tarbijatest eemal hoida. Liigpingete korral, mille kõrvalejuhtimiseks vajatakse liigpingekaitse seadmeid, ei ole aga puhvertoiteallikast kindlasti mingit abi. Vastupidi – UPS vajab nagu kõik teisedki elektritarbijad sobilikke kaitsemeetmeid rakendades liigpinge vastast kaitset (M 1.25 Liigpingekaitse).

Puhvertoiteallika dimensioneerimisel tuleb tähelepanu pöörata kahele aspektile: tugiaeg ja lähtevõimsus.

Tugiaja kindlaksmääramisel tuleb arvesse võtta UPS-süsteemi kasutuselevõtu otstarvet, vooluga varustatava IT-süsteemi liiki ja teisi energiaga varustamise tagamiseks rakendatavaid meetmeid. Kui UPS-toitega IT–süsteem on pärast järsku voolu väljalülitamist ja selle taastumist võimeline probleemideta käivituma ja edasi töötama, on küllalt, kui paigaldada UPS lühiajalisteks voolukatkestusteks. Kuna enamik voolukatkestusi kõrvaldatakse väheste minutite jooksul, on 10- kuni 15-minutiline sildamisaeg küllaldane.

Kui on vajalik IT-süsteemi ettenähtud korras seiskamine, ei piisa nii lühikesest tugiajast. Sel juhul on mõttekas pärast voolukatkestuse algust kõigepealt veidi oodata ja süsteeme mitte kohe seisata. Ooteajaks võiks arvestada umbes 10 minutit. Seiskamiseks (shutdown) vajalik aeg võib olla väga erinev ning tuleb võrku ühendatud IT-süsteemide jaoks individuaalselt kindlaks määrata.
Tugiaja arvestamine toimub järgmise valemi järgi:

Tugiaeg = ooteaeg pluss kahekordne seiskamisaeg

Tugiaja tüüpiline väärtus jääb 30 ja 60 minuti vahele. Seiskamisaja kahekordistamisega saavutatakse turvapuhver.

Spetsiaalsete rakendusjuhtumite korral (nt PBX-seadmed) võib vajalik tugiaeg kesta ka mitmeid tunde. UPS-toitega seadmete igakordsel väljavahetamisel ja täiendamisel tuleb uuesti kontrollida, kas olemasolev tugiaeg on piisav.

Vajaliku tugiaja muudatusi on küllaltki lihtne sisse viia patareide võimsuse kohandamise teel. Väljundvõimsuse puhul on teisiti. Maksimaalne väljundvõimsus määratakse kindlaks alaldisse ja vaheldisse paigaldatud elektrooniliste komponentide abil. Siin ei ole varustuse täiendamine ja sellega koos väljundvõimsuse suurendamine enamasti võimalik, või on võimalik vaid ulatuslike ümberehituste abil. Lähtevõimsuse kindlaksmääramisel tuleks niisiis planeerida piisavad reservid.

UPSi kõige tundlikum osa on patareid. Patareide maksimaalne võimsus ja eluiga on tagatud vaid juhul, kui neid hoitakse tootja poolt ette nähtud optimaalsel temperatuuril (tavaliselt umbes 20 °C juures). Iga 10 ° Kelvini kohta, mille võrra ettenähtud temperatuur ületatakse, vähenevad patareide võimsus ja eluiga umbes 50% võrra. Sellest nähtub, et eriti suurte UPS-süsteemide korral ei tohi külmemat kliimat armastavaid patareisid ja soojust tootvat jõuelektroonikat mitte mingil juhul ühes ruumis hoida. Et olla kindel, kas UPS tagab vajaliku tugiaja, tuleks umbes kord aastas kindlaks määrata tegelik tugiaeg. Mõnedel UPS süsteemidel on selleks sisse ehitatud kontrollmehhanismid. Kui need puuduvad, on selle pikkust võimalik kindlaks määrata koormustesti abil. Kuna UPS on viimane kindlustus voolu väljalangemise vastu enne IT-riistvara, tuleb selle kättesaadavuse tagamisele omistada suurt tähtsust. Seda on vaja kaitsta samuti nagu UPS-toitega IT-seadmeid. Kui UPS toitega IT-süsteemid on paigaldatud varuga, peaks olema paigaldatud ka varuga UPS-süsteemid. Täiendavalt olgu viidatud meetmele M 1.52 Tehnilise infrastruktuuri varud .

Lisaks sellele tuleb UPS-süsteemi puhul erilist tähelepanu pöörata kaitsele volitamata isikute juurdepääsu, põlengute ja veekahjustuste vastu. Asjakohane tuleohutus teeb üksteisele varu pakkuvate UPS-seadmete paigaldamise erinevatesse tuletõkkesektsioonidesse peaaegu vältimatuks. Ainult nii on võimalik ära hoida, et ühe seadme põlengu korral veidi aja pärast ka teised põlengu tagajärjel rivist välja langevad.

UPS-seadmete puhul, nagu kõikide teiste elektriseadmete puhulgi, tuleb tähelepanu pöörata asjaolule, et neid tuleb käitada tootja poolt ette nähtud temperatuurivahemikus. Sellega tuleb arvestada jahutuse dimensioneerimisel. UPS-süsteemi kaitsemõju säilitamiseks tuleb seda regulaarselt hooldada. Selleks tuleb järgida tootja poolt ettenähtud hooldusintervalle.

Kontrollküsimused:

- Kas patareisid hoitakse ettenähtud temperatuurivahemikus?
- Kas järgitakse puhvertoiteallikate hooldusintervalle?
- Kas patareide tegelikku võimsust ja sellest sõltuvat puhvertoiteallika tugiaega testitakse regulaarselt?
- Kas pärast muudatuste sisseviimist tarbijate juures kontrollitakse uuesti, kas tugiaeg on piisav?

M 1.71 Tehnilise infrastruktuuri funktsioonikontroll

Algatuse eest vastutavad: Infoturbe spetsialist, tehnikaosakonna juhataja
Elluviimise eest vastutab: tehnikaosakond

Tehnilise infrastruktuuri valdkonnas korraldatakse tõelist funktsioonikontrolli kahjuks ikka veel küllaltki harva. Näiteks kontrollitakse liiga harva energiaga varustamise nõuetele vastavat funktsioneerimist avariiolukorras või kliimaseadme ja tuleohutuse kokkusobivust. Paljudel juhtudel tehakse suuri kulutusi tõrgete vältimiseks, tihti aga ei testita rakendatavaid meetodeid, kuna kardetakse testimise tagajärjel tekkivaid kahjusid. Nende asemel korraldatud kontrolltestimise abil ei ole aga võimalik kontrollida kogu reaktsioonide ahelat, nii nagu see reaalselt kulgema peab. Põhimõtteliselt on siiski parem korraldada testimine ning käsitleda võimalikke tekkinud kahjusid testimise käigus (ja nendest õppida), kui kannatada ootamatult tekkinud kahju reaalse kasutamise käigus, kui avariimeetmed aktiveeritakse. Tehnilise infrastruktuuri järelevalve piirdub tavaliselt üksikult vaadeldavate tehniliste seadmetega, näiteks energiatoite seadmetega. Äärmisel juhul käsitletakse veel funktsionaalselt seotud seadmete liideseid.

Tavaliselt ei vaadelda aga kogu funktsioonide ahelat tervikuna. Tüüpiline funktsioonide ahel on reaktsioonide järjestus “Toiteallikas langeb välja, varutoiteallikas käivitub automaatselt”. Funktsioonide ahelat ei ole võimalik küllaldaselt testida, kui varutoiteallikas käivitatakse käsitsi ning seejärel lülitatakse välja toide, sest selline kontroll ei näita, kuidas toimib funktsioonide ahel primaarenergiaallika spontaanse väljalangemise korral. Üldiselt ei ole klassikalise kontrollimise käigus võimalik piisaval tasemel kindlaks teha, kas kogu reaktsiooniahel funktsioneerib nii, nagu ette nähtud. Seepärast juhtub tihti, et vaatamata optimaalsele kontrollile ja üksikute seadmete tehnilisele hooldusele ei funktsioneeri kogusüsteem avarii korral plaanipäraselt.

Näide:

- Ühel konkreetsel juhul olid varutoiteallikas ja toitevõrgu väljalangemisest teatamise seade koos vastava signaaliga testitud ja tunnistatud funktsioneerimisvõimeliseks. Vooluvõrgu äralangemisel reageeris toitevõrgu väljalülitumisest teatamise seade õigesti ning edastas signaali varutoiteallikale. Varutoiteallikas aga ei interpreteerinud teadmata põhjustel signaali õigesti ning ei käivitunud, kuigi kontrollimisel toimus seadme juhtimine selle valmistajate ettenähtud signaaliga ning seade reageeris selle testi korraldamisel ettenähtud korras.

Seepärast on reaktsiooniahela funktsioonikontrolli (reaaltesti) korraldamine möödapääsmatu. See tähendab, et testitavad seadmed tuleb ühtse süsteemina viia vastastikku probleemiga, mille lahendamiseks on nad ette nähtud. Kuna sellise reaaltesti eesmärgiks on ainult kogusüsteemis äratuntavate vigade kindlakstegemine, tuleb arvestada, et esinevad sellised vead ning seadmed ei reageeri ettenähtud korras. Seepärast ei tohiks reaaltestimist korraldada põhitööajal ning tuleks teha ettevalmistusi, et võimalike rikete tõttu tekkinud tagajärgede

kõrvaldamisega hakkama saada. Viimati nimetatu peaks kindlasti olema üks osa hädaolukorraks valmisoleku kontseptsioonist.

Arvutikeskuse tehnilise infrastruktuuri reaaltestide korraldamine peaks toimuma aastaste või kaheaastaste vahedega, samuti pärast süsteemi ümberehitamist ja ulatuslike parandustööde teostamist.

Hindamisküsimused

- Kas kõikide olulise tähtsusega reaktsiooniahela osade suhtes korraldatakse funktsioonitestid?
- Kas funktsioonitestisid korraldatakse regulaarsete vaheaegade järel?

M 1.72z Ehitustööde teostamine jooksva töö käigus

Algatuse eest vastutavad: asutuse/ettevõtte juhatus, infoturbe spetsialist

Rakendamise eest vastutab: infoturbe spetsialist

Majanduslikel põhjustel on tihti soovitatav uue serveriruumi või arvutuskeskuse ehitamise asemel laiendada olemasolevate IT-ruumide pinda naabruses asuva pinna integreerimise teel. Sellise pinna laiendamise tagajärjeks on tihti olemasoleva ehitise struktuuri muutmine, kuna seinu tuleb ümber ehitada, eemaldada või uusi ehitada. Lisaks sellele tuleb laiendatud pind sisustada vastava infrastruktuuriga (tõstetud põrand, elektritoide, kliimaseade, ohutustehnilised seadmed jne), nii et ka siin on palju tööd.

Et asutuse äritegevust mitte piirata, osutub tihti vajalikuks olemasoleva infrastruktuuri ehitustööde ajal käigus hoidmine. Samaaegselt ei tohi ehitustööde teostamist töötavate infotehnoloogiliste seadmete tõttu piirata või nõuetele allutada, et kulud liiga suureks ei läheks.

Kõigepealt tuleb planeerimise ja infrastruktuuri ettevalmistavate muudatuste abil tagada, et toetav tehnika, näiteks elektritoide, kliimaseade, valve- ja alarmseadmed, ei saaks ehitustööde käigus kahjustada ja funktsioneeriks edasi. Lisaks sellele tuleb territooriumi, millel asuvad töötavad IT-seadmed, kaitsta mustuse, kuid ka volitamata juurdepääsu eest. Samaaegselt ei tohiks aga ehitustöid asjatult takistada. Kaitseks mustuse eest sobivad järgmised meetmed:

- kilest tolmukaitseseina paigaldamine;
- kipskartongplaatidest tolmukaitseseina paigaldamine;
- vuukide ja ehituspragude kinnikleepimine või täitmine
- õhupuhastite kasutamine;
- alarõhu loomine ehitusterritooriumil;
- spetsiaalsete töömeetodite kasutamine.

Kilest tolmukaitseseina paigaldamine tuleb kõne alla vaid lühiajaliste ehitustööde ja minimaalse tolmu tekke korral. Selleks paigaldatakse raske ehituskile puidust aluskonstruktsioonile. Ehitusdetailidega piirnemisel tekkivad vuugid ja avaused kiles (näiteks vajalike juhtmete jaoks), suletakse kleeplindiga.

Sellise lahenduse puhul on ikkagi oht, et kile purunemisel ei kaitse see enam tolmu eest. Sel viisil ei ole ka võimalik turvaliselt tõkestada läbipääsu, mistõttu on vaja rakendada lisameetmeid, et volitamata isikud ei pääseks tööterritooriumile.

Lihtsad kilest tolmukaitseseinad (ilma tugeva aluskonstruktsioonita) paigaldatakse tihti ajutiselt, et oleks võimalik ehitada kipskartongist tolmukaitsesein, mille puhul tänu vajalikele puurimisavadele võib arvestada väiksema tolmu hulgaga.

Enamikel juhtudest on kipskartongist tolmukaitseseina ehitamine vägagi soovitatav. Seejuures saavutatakse piisav kaitse tolmu eest juba siis, kui aluskonstruktsioonile paigaldatakse ühepoolne topeltvooderdus. Topeltvooder takistab kaitset vajava territooriumi saastumist peentolmuga, mis muidu võib tungida raskusteta läbi plaatide ühenduskohtade.

Olemasoleva ehitisega ühendatud pinnad ning vältimatud töövuugid tuleks tihendada elastse tihendusmassiga, et vältida tolmu läbitungimist. Avausi seinas ja kaablite paigaldusavasid tuleb vältida. Kui see ei ole võimalik, tuleb need sobivat isolatsioonimaterjali kasutades sulgeda, et viia tolmu läbitungimine miinimumini.

Uste integreerimine tolmukaitseseintesse on põhimõtteliselt võimalik, kujutab endast aga nõrka kohta tolmukaitses. Ukseava tuleks tingimata kujundada lüüsiks, et vältida tõmbetuult ja sellega kaasnevat tolmu sattumist IT-ruumidesse. Sellise lüüsi kujundamine kahekordse üksteise taha riputatud ehituskile abil ei ole mingil juhul piisav.

Paigaldada tuleb tõmbekindlad uksed. Väga suured praod kasutatavas tolmukaitseukses võib näiteks kummiribaga tihendada.

Sellisel massiivsel tolmukaitseseinal on ka teine eelis: see eraldab ehitusterritooriumi füüsiliselt arvutuskeskusest, kuna pärast kipskartongseina paigaldamist ei ole ehitustöölistel otsest juurdepääsu arvutuskeskuse territooriumile.

Ehitustöödel on end õigustanud ehitusterritooriumil alalise alarõhuga töötamine. Selle meetodi kasutamisel imeb ventilaator õhu ehitusterritooriumil endasse ja juhib selle läbi suletud süsteemi välja. Sellega tagatakse, et suur osa tekkivast tolmust juhitakse otse välja ning alles jäänud tolm ei satu naaberterritooriumile. Võimalike ebatihedate kohtade kaudu imetakse äärmisel juhul arvutuskeskuse tolmuvaene õhk ehitusterritooriumile. Selle meetme puuduseks on, et fassaadis peab olema ava heitõhu väljajuhtimiseks.

Kui töö käigus tekib palju tolmu, on soovitav kasutada ehitusterritooriumil õhupuhasteid. Seejuures tuleb eelistada õhu puhastamist õhu filtreerimise (niinimetatud tolmueraldaja) abil. Õhu puhastamisel vee baasil niisutatakse õhku kuni küllastumispiirini, nii et kõrgema ruumitemperatuuri korral raskendab „subtroopiline” kliima tööde kulgu.

Muude tolmukaitse meetmetena võib kasutada spetsiaalseid töövõtteid:

- spetsiaalsete märgpuurimis- ja –lõikamismeetodite kasutamine;
- tolmu imemine kohe selle tekkekohal püsivalt installeeritud või mobiilse imiseadme abil (õhu kohene väljutamine või filtreerimine);
- puuravast tolmu imemine tolmuimeja abil;
- lammutusmaterjali kogumine ja transport tolmuimejate või sobivate pühkimismasinatega;
- puhastamise välistamine luua või suruõhu abil.

Tellija või tema poolt määratud turvalisuse ja tervisekaitse koordinaator peaks regulaarselt kontrollima kehtivate eeskirjade järgimist. Ehitustööde lõppemisel tuleb korraldada põhjalik ehitusterritooriumi puhastus.

Näide:

- Pärast suurema serveriruumi ümberehitamist tegi töövõtja näiliselt põhjalikku lõpp-puhastuse. Puhastatud ruumide kontrollimise tagajärjel selgus, et tõstetud põranda plaadid olid puhastamata. Tõstetud põranda kogu tugikonstruktsioonil oli veel palju saetolmu. See oleks ilma kontrollita ja täiendava puhastuseta ruumide käikuandmisel ventilatsiooniseadmete poolt õhku paisatud ja oleks kahjustanud juba paigaldatud IT-komponente, näiteks kaablijaotusseadmeid, kommutaatoreid ja servereid.

Lisaks tolmukaitsele tuleb ümberehitustööde teostamisel tagada, et edasitöötavaid IT-seadmeid küllaldaselt jahutataks. Õhu jahutamisel tuleb arvestada ümberehitustöödest tingitud lisatolmukoormusega.

Arusaamatuste ja töövõtjate kallite lisateenuste vältimiseks on soovitav kõikide rakendatavate meetmete jaoks kirjeldatud nõuanded tööde ja teenuste nimekirja kanda.

Ehitustööde teostamine ei häiri aga mitte ainult töö tegemist ega tekita tolmu, tähelepanematuse või vale planeerimise tõttu võib kahjustatud saada ka olemasolev tehnika (näiteks juhtmete läbipuurimine). Lisaks sellele on tavaliselt paljudes kohtades üheaegselt tööle rakendatud ka vahelduv väline tööjõud. Sellega seoses tuleb tagada, et välisel tööjõul silma peal hoitaks või territoorium, millel paiknevad IT-seadmed, ehitustööde territooriumist nii eraldataks, et volitamata juurdepääs seadmetele oleks välistatud.

Kontrollküsimused:

- Kas nõuded tolmukaitsemeetmete rakendamiseks on detailselt IT-ruumide ümberehitustööde hanke teksti sisse kirjutatud?
- Kas välise tööjõu järelevalve alal, millel paiknevad töötavad IT-seadmed, on ehitustööde toimumise ajal tagatud?
- Kas kõikide tolmukaitsemeetmete ettenähtud korras funktsioneerimist kogu ehitustööde toimumise ajal kontrollitakse piisavalt tihedate ajavahemike järel personali poolt, kes ise ehitustöödes ei osale?

M 1.73 Arvutuskeskuse kaitse volitamata juurdepääsu eest

Algatamise eest vastutavad: Infoturbe spetsialist, IT juht, tehnikaosakonna juhataja

Rakendamise eest vastutab: tehnikaosakonna juhataja

Arvutuskeskus kujutab endast tähtsat tsentraalset üksust ja sellega seoses funktsionaalset üksust, mille kaitsmiseks volitamata juurdepääsu eest tuleb rakendada spetsiaalseid meetmeid. Arvutuskeskuse kaitsmiseks volitamata sissepääsu eest on tingimata vajalik rakendada meetmeid M 2.6 Sissepääsuõiguste andmine ja M 2.17 Sisenemisreeglid ja reguleerimine . Reeglitest üksi siin aga ei aita. Reeglite täitmise tagamiseks tuleb rakendada teisi meetmeid.

Sissepääsuks madalate turvanõuetega hoone osadesse kontrollitakse tavaliselt ühte kahest kriteeriumist – millegi omamist (näiteks kaart) või millegi teadmist (näiteks PIN). Arvutuskeskustes on tunduvalt kõrgemate turvanõuete tõttu nõutav volitamata sissepääsu vältimiseks tugevamate kontrollimehhanismide rakendamine.

Esimese sammuna tuleb kõne alla vähemalt kahe kriteeriumi kontrollimine kolmest – millegi omamine, millegi teadmine ja biomeetrilised tunnused. Praeguste seisukohtade järgi ei ole soovitav turvakaamerata territooriumil kasutada ainsa sissepääsukontrollina turvatsooni biomeetrilisi meetodeid. Kahe kriteeriumi kombineeritud kontrollimise abil saab piisava kindlusega tagada, et kasutatud kriteeriumid tõepoolest vastavale isikule kuuluvad.

Kõikidele külastajatele tuleb määrata kindlad isikud, kes nende eest külastuse käigus vastutavad ja neil pidevalt silma peal hoiavad. Normaalses keskkonnas aktsepteeritav asjaolu, et volitatud isik võtab teised isikud, näiteks külalised, lihtsalt niisama pääsukontrolliga turvatud territooriumile kaasa, ei tule arvutuskeskuses kõne allagi. Siin on vajalik iga isiku iga sissepääs ühemõtteliselt fikseerida. Külaliste sissepääsu tuleb reguleerida nii, et iga külaline saab näiteks temale isiklikult väljastatud tõendi, näiteks külastajakaardi. Teise kriteeriumi puudumine kompenseeritakse sellega, et külastajakaart seotakse külastuse eest vastutava isikuga.

Arvutuskeskuses tuleb iga sissepääs protokollida, see puudutab nii volitatud isikuid kui ka isikuid, kellel on ajutine sissepääsuluba. Näiteks võiks arvutuskeskusesse sisenenud võõraste isikute nimed külalisteraamatusse kanda. Külalisteraamatu kasutamine ei võimalda volitamata isikute sissepääsu reguleerida, kuid võimaldab seda dokumenteerida. Raamatul, mis on arvutuskeskuses vaatamiseks välja pandud, ja millesse külastajad kannavad end ilma, et selleks volitatud isik kontrolliks otseselt nende andmete õigsust, ei ole tugeva sissepääsukontrolli teostamisel mingit väärtust.

Takistamaks, et volitatud isik võtaks teised isikud sissepääsukontrolliga turvatud alale kaasa, on mõttekas rajada eralduslüüs. Kui see ei ole võimalik, tuleb ra-

kendada organisatoorseid ja tehniliselt toetatud eeskirju. Tehnilise toetusena võib kasutada anti-passback funktsiooni. Selle puhul peab isik, kes sai sobivate kriteeriumide abil sissepääsuloa teatud territooriumile, territooriumilt lahkudes end ka välja möllima. Isik, kes jätab selle tegemata, ei saa järgmisel sisenemiskatsel sisenemisluba, kuna ta on registreeritud pääsukontrolli süsteemis territooriumil viibijana ja ei saa seetõttu sellele uuesti siseneda. Isik, kes on ilma registreerimata kaasa läinud, tunnistatakse väljumisel territooriumil mitte viibinuks. Tagajärjeks võib näiteks olla, et väljaviiv uks ei avane või kõlab meeldetuletus, et sisenemisreegleid tuleb täita. Lisaks anti-passback funktsiooni kasvatuslikule mõjule kaasamineku vastu, on võimalik lisaks sisenemisele tuvastada kindlalt ka väljumine. See on turvaintsidentide käsitlemisel oluline eelis. Anti-passback väljumise registreerimine võib piirduda vaid ühe kriteeriumi küsimisega. Selleks võiks olla näiteks külastajakaart.

Kontrollküsimused

- Kas sisenemisel arvutuskeskusesse nõutakse vähemalt kahe autentimistunnuse kontrollimist?
- Kas on tagatud, et iga külastaja registreeritakse sisenemiskontrolli käigus individuaalselt?
- Kas kõikidele külastajatele määratakse saatjad, kes neil pidevalt silma peal hoiavad?
- Kas rakendatakse anti-passback meetodit?

M 1.74z Virtuaalse taristu planeerimine

Algatamise eest vastutavad: IT-juht, infoturbespetsialist

Rakendamise eest vastutavad: administraator

Virtuaalse taristu rajamise suure keerukuse tõttu tuleb seda kindlasti detailselt planeerida. Seetõttu tuleb juba kontseptsiooni väljatöötamise ja projekteerimise käigus vajalikke raamtingimusi täpselt analüüsida.

Virtualiseerimistehnoloogia kindlaksmääramine

Seetõttu tuleb esimese planeerimisetapina virtualiseerimisele kuuluvate IT-süsteemide kontseptsiooni puhul määrata kindlaks, millisel virtualiseerimistehnoloogial (serveri või operatsioonisüsteemi virtualiseerimine) virtuaalne taristu põhinema hakkab. Seejuures lähtutakse järgmistest kriteeriumidest:

- Serveri virtualiseerimine, mille puhul virtuaalselt luuakse kogu server koos kõigi riistvarakomponentidega, sobib eriti hästi väga erinevate ja mitmekesiste ülesannetega virtuaalsete IT-süsteemide puhul. Serveri virtualiseerimise alusel toimivate süsteemide puhul on võimalik ühes virtualiseerimisserveris käitada samaaegselt erinevaid operatsioonisüsteeme (Windows, Linux, Solaris), kuna iga virtualiseerimissüsteem saab kasutada oma operatsioonisüsteemi tuuma. Serveri virtualiseerimise abil on saavutatav virtuaalsete IT-süsteemide väga tugev kapseldumine, mis tähendab, et virtuaalne IT-süsteem ei kasuta näiteks virtualiseerimisserveri ega teiste virtuaalsete IT-süsteemide operatsioonisüsteemi komponente või tarkvarateeke. Peale selle on virtuaalsüsteemid serveri virtualiseerimise puhul üksteisest paremini isoleeritud kui operatsioonisüsteemi virtualiseerimise puhul, s.t vastastikune funktsionaalne mõjutamine on suuresti välistatud.
- Operatsioonisüsteemi virtualiseerimine võimaldab ühel virtualiseerimisserveril lihtsalt käitada suurt hulka sarnaseid servereid, mistõttu selle süsteemi puhul on võimalik saavutada andmete kõrge pakkimisaste (virtualiseeritud IT-süsteemide ja virtualiseerimisserverite suhe). Operatsioonisüsteemi virtualiseerimisega ei ole aga tavaliselt võimalik virtuaalsel kujul käitada erinevaid operatsioonisüsteeme ühel serveril, kuna virtuaalsed IT-süsteemid kasutavad enamasti virtualiseerimisserveri operatsioonisüsteemi tuuma ja tarkvarateeke. See on võimalik piiratud kujul mõningate toodete puhul ühe operatsioonisüsteemipere sees. Näiteks Parallels Virtuozzo võimaldab kasutada operatsioonisüsteemi Microsoft Windows Server 2003 erinevaid versioone. Virtuaalsed IT-süsteemid ei ole üksteisest nii isoleeritud kui serveri virtualiseerimise puhul. Näiteks kasutatakse ühiseid tarkvarateeke ja virtuaalsed IT süsteemid kasutavad sama operatsioonisüsteemi tuuma. Virtuaalse IT-süsteemi kapseldus ei ole enamasti isegi saadaval või on ainult väga nõrgalt välja arendatud, kuna nad kasutavad ka virtualiseerimisserveri tark- ja riistvarakomponente.

Selline virtuaalse IT-süsteemi nõrk kapseldus operatsioonisüsteemi virtualiseerimise puhul toob kaasa selle, et ühel virtualiseerimisserveril ei saa väga erinevate kaitsenõuetega virtuaalseid IT-süsteeme hõlpsasti käitada. Serveri virtualiseerimisel põhinevate lahenduste puhul see tavaliselt nii ei ole, kuna virtuaalsüsteemide kapseldus on tugevamini väljendatud, kuid see, kas erineva kaitsevajadusega virtuaalseid IT-süsteeme ühel virtualiseerimisserveril koos käitada saab, sõltub peale kasutatud toote ka konkreetsetest ohtudest ja organisatsiooni või virtuaalse IT-süsteemi nõuetest. Seetõttu tuleb planeerimise käigus hinnata, mil

määral kõnealune virtualiseerimistehnoloogia erineva kaitsevajadusega virtuaalsete IT-süsteemide ühel virtualiseerimisserveril koos käitamiseks sobib.

Virtualiseerimistoote valimine

Kui virtualiseerimistehnoloogia on välja valitud, tuleb konkreetse toote sobivust antud juhul kontrollida. Sel puhul rakendatavad nõuded lähtuvad virtuaalkeskkonnas kasutatavate protsessorite liigist ja nende funktsioonidest, samuti vajaminevate seadmete emulatsioonide või liideste käideldavusest. Võimalikult varases planeerimisfaasis tuleb kontrollida ja otsustada, millise tehnika abil virtuaalsed IT-süsteemid arvutuskeskuse võrguga seotakse: serveri füüsiliste võrgukaartide otsese virtuaalsetele IT-süsteemidele allutamise teel või virtuaalsete süsteemide sidumise teel nn virtualiseerimisserveri kommutaatori kaudu. Sellelt aluselt saab kindlaks määrata, kuidas rakendada meetmete M 2.141 Võrgukontseptsiooni väljatöötamine , M 5.61 Sobiv füüsiline segmenteerimine ja M 5.62 Sobiv loogiline segmenteerimine alusel välja töötatud eeskirju ja reegleid. Nii on virtualiseerimisserveri ja juurdekuuluva taristu parameetrid juba varakult olemas. Pärast sihtkeskkonnale esitatavate nõuete kindlakstegemist saab valida sobiva virtualiseerimislahenduse ja sellele vastavad füüsilised IT-süsteemid.

Kogu arvutuskeskust hõlmav planeerimine

Virtualiseerimisserveril saab käitada arvukalt virtuaalseid IT-süsteeme. Neil virtuaalsetel IT-süsteemidel, mis kujutavad endast tavaliselt erinevate operatsioonisüsteemidega serverisüsteeme, saab käitada arvukalt erinevaid rakendusi, mis vajavad omakorda alusteenuseid nagu DNS, kataloogiteenused autentimiseks või andmebaasid. Seetõttu peavad virtualiseerimisserverid ligi pääsema kõigile nii virtualiseerimisserveri enda kui virtuaalsete IT-süsteemide käitamiseks vajalikele ressurssidele. Virtualiseerimisprojekti planeerimisel tuleb silmas pidada järgmisi nõudeid. Virtualiseerimisserverid vajavad:

- füüsilist ühendust kõigi võrkudega, milles virtuaalsed IT-süsteemid töötavad.
- ühendusi salvestusvõrkudega juurdepääsuks massimälukomponentidele.
- juurdepääsu taristusüsteemidele nagu DNS-, DHCP- ja kataloogiteenuse server.

Seetõttu peavad kõik nende teenuste osutamisega tegelevad administraatorite rühmad virtualiseerimise teatud määral osalema, et nad saaksid teha virtualiseerimisprojekti ka omapoolseid ettepanekuid ja esitada nõudeid.

Rollide ja vastutuse planeerimine

Kuna virtualiseerimisserverid võimaldavad sageli virtuaalsete IT-süsteemide ja neil käitatavate rakenduste kaudu juurdepääsu arvutuskeskuse alusteenustele ja -võrkudele ning salvestusvõrkudele, kujutavad nad virtuaalse IT-süsteemi enda seisukohalt arvutuskeskuse taristu koostisosa. Seetõttu soovitatakse viia võrkudele ja salvestusvõrkudele juurdepääsu reeglid ja eeskirjad virtuaalse taristu nõuetega kooskõlla. Kui näiteks peatüki M 5.130 Salvestisvõrgu (SAN-i) kaitse segmenteerimise abil järgi määratakse kindlaks salvestusvõrgu segmenteerimise ja ketaste ressurssidele juurdepääsu tingimused, tuleb tagada, et neid saaks rakendada ka virtuaalses taristus. Virtualiseerimisserveri puhul peab juurdepääs salvestusressurssidele olema võimalikult laialdane, kuna neil peab olema juurdepääs paljude virtuaalsetele IT-süsteemide salvestusressurssidele, et need omakorda saaksid

anda ressursse virtuaalsete IT-süsteemide käsutusse. Sellest hoolimata tuleb rakendada nimetatud meetme mooduli B 3.303 Salvestisüsteemid ja salvestivõrgud poolt esitatavaid nõudeid, mille rakendamine peab aga olema võimalik kasutatud virtualiseerimislahenduse poolt pakutavate vahenditega. See näitab, et virtualiseerimisserveri administraatoritel võib osutuda vajalikuks täita ülesandeid, mida on eelnevalt oma valdkonnas lahendanud salvestusvõrgu või salvestuskomponentide administraatorid.

Sama kehtib võrguadministraatorite ülesannete puhul. Virtuaalsete IT-süsteemide sidumise IT-koosluse erinevate võrkudega määravad virtualiseerimisserveri puhul kindlaks selle administraatorid, kuna nemad allutavad virtuaalsed IT-süsteemid virtualiseerimisserveri füüsilistele võrguühendustele. See on võrguadministraatori traditsiooniline ülesanne. Kui ühel virtualiseerimisserveril käitatakse virtuaalseid IT-süsteeme erinevates võrkudes, vastutavad õige võrgujaotuse ja selle kontrollimise eest virtualiseerimisserverite administraatorid. Peale selle tuleb silmas pidada, et võrgu segmenteerimisega taotletav eesmärk tõsta IT-süsteemide arvutuskeskuse eri harude vahel jagamisega turvalisust ei jääks virtuaalsete IT-süsteemide puuduva kapselduse ja isolatsiooni tõttu täitmata.

Seetõttu tuleb virtuaalse infosüsteemi planeerimisel otsustada, kuidas virtualiseerimisserveri administraatorid hakkavad realiseerima võrgu- ja salvestusvõrgu administraatorite ülesandeid, kui see osutub valitud virtualiseerimislahenduse puhul vajalikuks. Peale selle tuleb kontrollida, kas võrgu- või salvestusvõrguadministraatorite ülesandeid on võimalik delegeerida virtualiseerimisserverite administraatorite kaudu võrgu- ja salvestusvõrgu administraatoritele. Vastutus kehtivate reeglite ja eeskirjade rakendamise eest tuleb kindlaks määrata üheselt ja selgelt.

Taristu kooskõlastamine virtualiseerimisega

Klassikaliste IT-koosluste puhul on nii IT-süsteemid kui serverid enamasti seotud ainult ühe, harvem mitme võrguga, kuid kui virtualiseerimisserveril tahetakse käitada virtuaalseid IT-süsteeme erinevates võrkudes, peab server olema seotud mitme võrguga. Seetõttu soovitatakse kohandada moodulite B 3.302 Marsruuterid ja kommutaatorid , B 4.1 Heterogeensed võrgud , M 2.141 Võrgukontseptsiooni väljatöötamine , M 2.142 Võrguplaani väljatöötamine , M 4.81 Võrgutoimingute audit ja logimine , M 4.206 Kommutaatori portide turvamine , M 5.61 Sobiv füüsiline segmenteerimine , M 5.62 Sobiv loogiline segmenteerimine ja M 5.77 Alamvõrkude rajamine meetmeid virtualiseerimisserveri eripärade ja nõuetega. Tähelepanu tuleb pöörata sellele, et virtualiseerimisserver suudaks täita ühes virtuaalses taristus kõiki virtuaalse IT-süsteemi ühenduse nõudeid.

Näiteks kui kommutaatori portidel kasutatakse MAC-filtreid (vt M 4.206 Kommutaatori portide turvamine), peab nende filtrite konfiguratsioon olema kooskõlas virtuaalse infosüsteemi nõuetega, kui mitte, ei saa virtuaalseid IT-süsteeme, millel on mõnede virtualiseerimislahenduste puhul oma MAC-aadress, ühelt virtualiseerimisserverilt teisele viia. Kuna neid funktsioone vajatakse virtuaalsete IT-süsteemide jaotamiseks virtualiseerimisserverile jõudlustõrgetele reageerimise otstarbel, on virtuaalsete IT-süsteemide käideldavus ilma filtrireeglite piisava kooskõlastamiseta ohustatud.

Ka järgnevate mooduli B 3.303 Salvestisüsteemid ja salvestivõrgud kohaste meetmete puhul tuleb vajadusel silmas pidada virtualiseerimistehnoloogiate kasutamisest tulenevaid nõudeid:

- M 2.352 Kohtvõrgu salvesti (NAS-süsteemi) turvapoliitika väljatöötamine
- M 2.353 SAN-salvestivõrgu turvapoliitika väljatöötamine

- M 4.275 Salvestisüsteemide turvaline kasutamine
- M 5.130 Salvestisvõrgu (SAN-i) kaitse segmenteerimise abil

Virtualiseerimisserveri ressursside planeerimine

Ressursside planeerimisel tuleb lisaks M 2.315 Serveri kasutuselevõtu planeerimine silmas pidada ka teatud eripärasid, mis tulenevad asjaolust, et ühel virtualiseerimisserveril käitatakse tavaliselt mitmeid virtuaalseid IT-süsteeme. Seetõttu tuleb välja selgitada, kui palju protsessori võimsust, põhimälu ja kõvakettaruumi virtuaalse IT-süsteemi käigushoidmiseks vaja läheb. Peale selle tuleb kindlaks teha, milliseid võrguühendusi ja virtuaalseid IT-süsteeme vajatakse (vt M 5.135 Turvaline meediatransport SRTP abil).

Sobiva virtualiseerimisserveri valimiseks tuleb välja selgitada planeeritava virtuaalse IT-süsteemi jõudluse ja ressursside koguvajadus. Alles seejärel saab kindlaks määrata vajaminevate virtualiseerimisserverite arvu ja võimsuse.

Juba edukalt käigusolevate füüsiliste IT-süsteemide ülekandmisel virtuaalsesse keskkonda tuleb välja selgitada ka tegelik ressursivajadus, milleks ei piisa vaid ressursside kokkuliitmisest, vaid tuleks mõõta virtualiseeritavate süsteemide jõudlust ja määrata virtualiseerimisserverile esitatavad nõuded kindlaks mõõdetud füüsilise serveri jaoks vajaminevate jõudlusparameetrite alusel.

Peale piisavate ressursside üksikute virtuaalmasinate jaoks tuleb silmas pidada ka virtuaalse taristu muid võimsusi, mida on vaja virtualiseerimistarkvara enda jaoks. Nii on rohkem massimäluvõimsust vaja virtualiseerimisserveri snapshot'ide, sündmuste protokollide ja saatefailide salvestamiseks. Virtualiseerimisserveri hüperviisor vajab samuti protsessori võimsust ja põhimäluruumi.

Test- ja arenduskeskkondades ei tule eeltoodud parameetreid järgida. Nende keskkondade planeerimisel tuleb silmas pidada, et ei tekiks soovimatuid vastastikuseid mõjutusi tegelike süsteemidega, mistõttu test- ja arenduskeskkonnad tuleb tegelikest keskkondadest piisavalt eraldada.

Virtuaalse infosüsteemi käideldavus

Juba planeerimisfaasis soovitatakse silmas pidada, et virtualiseerimisserveri käideldavusele esitataks võimalikult kõrged nõuded, sest virtualiseerimisserveritel töötab arvukalt IT-süsteeme. Kui mõni virtualiseerimisserver välja langeb, lakkavad toimast ka kõik sellel töötavad virtuaalsed IT-süsteemid. Seetõttu kanduvad kõik üksikute virtualiseeritud IT-süsteemide käideldavusnõuded üle virtualiseerimisserverile (kumulatsiooniprintsiip). Mõistlik on kontrollida, kas virtualiseerimisserverile tuleks valida kõrgkäideldav või vigade suhtes tolerantne arhitektuur või kas ühes paljudest virtualiseerimisserveritest moodustatud taristus on olemas mehhanismid ühe või mitme virtualiseerimisserveri väljalangemise kompenseerimiseks.

Kontrollküsimused:

- Kas protseduur virtualiseerimisserverite ja virtuaalsete IT-süsteemide kasutamiseks on IT-süsteemide, rakenduste, võrkude ja salvestusvõrkude käitamise reeglite ja eeskirjadega kooskõlas?
- Kas üksikute administraatorirühmade (rakendus-, serveri-, võrgu- ja salvestusvõrguadministraatorite) ülesanded on üksteisest selgelt eraldatud?
- Kas vastutus virtuaalse taristu üksikute komponentide (virtualiseerimisserver, virtuaalsed IT-süsteemid, salvestusvõrk, võrk) käitamise eest on selgelt reglementeeritud ja kas vastutajad suudavad oma ülesandeid ka tehniliselt realiseerida?

- Kas virtuaalne taristu sisaldab käideldavusnõuete rahuldamiseks piisavalt liiasusi?

M 1.75 Hoonetesisene tuleohutusmärgistus

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond

Rakendamise eest vastutavad: planeerijad

Hoone ja tehnorajatiste tuleohutus, tuleohutusmärgistus ja inimeste õigeaegne teavitamine tulekahju korral on elementaarsed meetmed, millega kaitstakse hoones viibivate inimeste elu ja tervist. Lähtekohaks on põhimõte, et iga hoone puhul eksisteerib alati tulekahju oht, olenemata hoone kasutusotstarbest ja ehitusviisist. Et kaitsta inimesi ja panna tulekahjule võimalikult ruttu piir, on tarvis tulekahju teke võimalikult kiiresti tuvastada.

Tulekahju kiireks tuvastamiseks on soovitatav kasutada suitsuandureid. Soovitatav on paigaldada piisaval arvul suitsuandureid kõikidesse hoonetesse. Lokaalseid andureid saab juhtida ja nende seisundit analüüsida tsentraalse tulekahju alarmisüsteemiga. Kõikvõimalikud andurid ja tsentraalne tulekahju alarmisüsteem moodustavad kokku tulekahju teavitussüsteemi.

Minimaalsed soovitatavad komponendid on järgmised:

- suitsuandurid kõikide koridoride lagedes;
- suitsuandurid kõikide tehnikaruumide lagedes, samuti ruumides, mis tagavad elektrivarustuse (elektrikilbid, UPS-id).
- suuremates hoonetes on mõistlik kasutada tsentraalset tulekahju alarmisüsteemi, millesse on lülitatud kõik andurid.
- kui ruumides kasutatakse ventilatsiooniseadet, peab alarmisüsteem hõlmama ka selle õhukanaleid. Ventilatsiooni- ja kliimaseadet peab olema võimalik tsentraalsest tulekahju alarmisüsteemist välja lülitada, et takistada suitsu edasikandumist.

Suitsuandurid tuleb paigaldada korrektselt, s.t järgides tootja juhiseid ja EV seadustest tulenevaid nõudeid. Kui hoones on tulekahju teavitussüsteem juba olemas, tuleks tagada, et kõik süsteemi teated, k.a tõrketeated, oleksid suunatud kohta, kus on alati keegi, kes neid teateid ka jälgib, nt uksehoidja kabiini. Kõikide suitsuandurite, s.t kõikide tulekahju teavitussüsteemi komponentide töökorda tuleb pidevalt kontrollida. Mõnede teavitusahelate töökorda tuleks pisteliselt ka käsitsi kontrollida. Suitsu tuvastamisele peab hoones järgnema alarm ning põlenguohust teavitamine peab olema korraldatud nii, et vajalik info jõuab kõikide hoones viibivate inimesteni.

Inimesed peavad saama hoonest ohutult lahkuda, mistõttu tuleb tagada, et olemasolevad evakuatsiooniteed oleksid alati kasutatavad. Evakuatsiooniteedel ei tohi olla takistusi, nt mööblit ega ka elektrilisi seadmeid (nt printereid või koopiamasinaid), sest need suurendavad tulekoormust ning võivad kitsendada inimestele evakuatsiooniks ette nähtud liikumisruumi. Regulaarselt tuleb kontrollida, kas evakuatsiooniteid saab nõuetekohaselt kasutada ning kas sinna pole kuhjatud liikumist takistavaid esemeid.

Kontrollküsimused

- Kas hoones on olemas piisav hulk suitsuandureid?
- Kas evakuatsiooniteid kontrollitakse regulaarselt, et sinna poleks kuhjatud liikumist takistavaid esemeid?

M 1.76 Lokaalse töökoha valimine ja kasutamine

Algatamise eest vastutavad: infoturbespetsialist, töötajad, ülemused

Rakendamise eest vastutavad: ülemused, töötajad

Töökoha asukoht ja varustus peavad olema kooskõlas tehtava tööga. Töökohtade paigutamisel hoones tuleb leida tasakaal üldkehtivate töötingimuste, reaalsete tööprotsesside ja nende turbevajaduse vahel. Töökohad, kuhu on juurdepääs ka klientidel ja külastajatel, tuleb paigutada selliselt, et kliendid ega ka külastajad ei peaks liikuma läbi alade, mis on turbe seisukohalt olulised. Tööprotsessid, mille puhul on väga tähtis tagada töödeldavate dokumentide konfidentsiaalsus, peaksid toimuma ruumides, millele puudub vaba juurdepääs nii külastajatel kui ka teiste osakondade töötajatel.

Tehniline varustus, mööbel, töökoha mõõtmed ja üldised töötingimused peavad vastama eelkõige töö iseloomule. Üldise vajamineva tööpinna kõrval peab töökohal olema ka piisavalt ruumi asjakohaste tegevuste tarbeks.

- Töökohas peab olema piisavalt ruumi arvuti, telefoni, kaustade ja muude töövahendite jaoks.
- Tuleb tagada, et töökohas oleks piisavalt võimalusi töömaterjalide paigutamiseks (nt lukustatavad kapid), et kaitsta neid volitamata juurdepääsu eest.
- Töökohas peab olema piisav hulk pistikupesasid (nt elektri, IT-võrkude ja telefoni jaoks) nii töötajatele kui ka kolleegidele või külastajatele.
- Töökeskkonna temperatuuri peab saama reguleerida. Töökohas peab olema piisavalt õhutusvõimalusi ning piisav valgustus ja heliisolatsioon, mis võimaldaks produktiivselt töötada.
- Kohtades, kus tööülesandeid täidetakse rühmadena, peab olema piisavalt ruumi ühiste nõupidamiste jaoks. Samuti peavad sellisel juhul olemas olema rühmatööks vajalikud erivahendid, nagu tahvlid, kaardilauad või projektorid ja ekraanid, ning ka piisavalt palju ruumi, et neid otstarbekalt kasutada.

Töötajate ja töörühmade puhul, kelle töö on seotud kas suure või väga suure turbevajadusega, on soovitatav tööruumid koondada kokku selliselt, et ka sanitaarruumid ja ühiselt kasutatavad tööruumid (nt koosolekutoad ja kohvinurgad), samuti printerid ja koopiamasinad asuksid kõik ühes kokkukuuluvas ja teistest valdkondadest eraldatud hooneosas. Sellises eraldatud hooneosas saab ka kerge vaevaga sisse seada nt autonoomse juurdepääsukontrolli ala. Töötajate võimalused töökohta enda jaoks paremaks muuta on sageli väga piiratud. Enamasti tuleb neil leppida olemasolevate lahendustega. Seetõttu peavad iga töökoha puhul alati ennekõike ülemused otsustama, kas töökohas saavutatav turbeaste on töö jaoks piisav või mitte.

Kontrollküsimused:

- Kas lokaalse töökoha varustus on sealsete tööülesannete täitmiseks piisav?
- Kas lokaalsete töökohtade turbeaste vastab seal töödeldavate andmete turbevajadusele?

M 1.77z Inimeste kliimaseadmed

Algatamise eest vastutavad: tehnikajuht, IT-juht

Rakendamise eest vastutab: tehnikaosakond

Suuremates hoonetes kasutatakse piisava õhuvarustuse tagamiseks ventilatsiooni- ja kliimaseadmeid. Ventilatsiooni- ja kliimaseadmed transpordivad õhku (ventilatsioon) ning muudavad selle temperatuuri (kliimaseade). Ventilatsiooni- ja kliimaseadmed peavad ruumis looma töötajatele sobiva sisekliima. Lisaks peavad need hoolitsema selle eest, et siseruumi õhk oleks hügieeniliselt laitmatu kvaliteediga. See tähendab, et ventilatsiooni- ja kliimaseadmes töödeldud õhk ei tohi ohustada töötajate füüsilist ega vaimset tervist, õhus ei tohi olla ebameeldivaid lõhnu ning peab olema tagatud piisav soojusmugavus. Hea õhukvaliteedi saavutamiseks ei piisa üksnes ventilatsiooni- ja kliimaseadmetest. Ruumi sisekliimaga tuleb arvestada ka hoone ehituseks kasutatavate ehitusmaterjalide, põrandakatete ja mööbli valikul, sest ka neist võib ruumi eralduda suur hulk kahjulikke aineid.

Büroode ja muude ruumide puhul, kus inimesed viibivad pidevalt, kehtivad õhu kvaliteedile rangemad nõuded kui nendes ruumides, kus inimesed viibivad ainult aeg-ajalt. Selleks, et ruumi tulevastele kasutajatele luua õiged tingimused, peab ehitustööde tellija esitama ehitusettevõttele kliimasüsteemi puudutavad õiged. Ruumi vastuvõetava sisekliima tagamisel pole sageli suur probleem mitte jahedus, vaid ülemäärane suvine kuumus. Kuumadel suvepäevadel läheb vastuvõetava sisekliima tagamiseks peale ventilatsiooni- ja kliimaseadme tarvis ka tõhusaid aknakatteid.

Ventilatsiooni- ja kliimaseadmete puhul on hädavajalik nende regulaarne tehnohooldus. Tehnohooldustööd tagavad ventilatsiooni- ja kliimaseadmete tõrkevaba töö ning hoones töötavatele inimestele piisavad hügieenitingimused, mis säästavad nende tervist. Hooldusintervallide järgimine, hoolikate puhastustööde tegemine ja filtrite vahetamine on tööd, mida tuleb kontrollida ja dokumenteerida. Ventilatsiooni- ja kliimaseadmed ei tohi olla kõikidele vabalt ligipääsetavad ning vajaduse korral tuleb need ka füüsiliselt eraldada, et vältida nende saboteerimist.

Ventilatsiooni- ja kliimaseadmete tööga tuleb arvestada ka hädaolukordadeks valmisoleku planeerimisel (vt moodul B 1.3 Hädaplaanimine), eriti puudutab see seadmete väljalülitamist ja taaskäivitamist.

Kontrollküsimused

- Kas ventilatsiooni- ja kliimaseadmed vastavad hoone kasutusnõuetele?
- Kas ventilatsiooni- ja kliimaseadmetele tehakse regulaarselt tehnohooldust?

M 1.78 Hoone kasutuse turvakontseptsioon

Algatamise eest vastutavad: asutuse/ettevõtte juhtkond, infoturbespetsialist

Rakendamise eest vastutavad: planeerija, infoturbespetsialist

Reaalselt rakendatava ja kulutõhusa hoonekasutuse turvakontseptsiooni koostamiseks tuleb välja selgitada hoones aset leidvate tööprotsesside turbevajadused ja üldkehtivad turvaeesmärgid, mis lähtuvad väga sageli organisatsiooni tegevusvaldkonnast. Turvaeesmärkide hulka kuuluvad näiteks majandustegevusega seotud kauba kaitse, osa või kõikide töötajate tavapärasest suurem kaitse rünnete vastu, teatud ruumidesse või spetsiaalsetele aladele sisenemise tõkestamine või neil aladel ja ruumides hoitavate esemete kaitse.

Hoone puhul tuleb arvestada väga erinevate valdkondadega alates tuleohutusest ja elektrisüsteemist ning lõpetades juurdepääsu kontrollimisega. Olenevalt institutsiooni ja selle hoone suurusest võib juhtuda, et eri valdkondade eest vastutavad erinevad töötajad. Seetõttu tuleb erinevate töötajate rollid ja tööülesanded omavahel kokku sobitada. Vastutavad töötajad peaksid ülesanded omavahel ära jagama, et erinevate valdkondade turbe tagamiseks õnnestuks välja valida võimalikult head ja püstitatud eesmärkidele vastavad turbemeetmed.

Hoonete puhul on väga levinud tava vaadata hoonet esmalt tsoonide kaupa (vt M 1.79 Turvatsoonide rajamine). Paljusid turvaeesmärke on võimalik saavutada juba sellega, kui luuakse olukord, kus väiksema turbeastmega tsoonist pole tarvis ega ka võimalik ilma piiranguteta edasi pääseda suurema turbeastmega tsoonidesse. Selleks tuleb esmalt välja selgitada, kuidas jaotub hoone ruumideks ning kuidas on kavas neid ruume kasutada (vt M 1.13 Kaitset vajavate ruumide paigutus). Erinevate turvatsoonide vahel tuleks sisse seada selgelt äratuntavad ja võimalikult kerge vaevaga kaitstavad üleminekukohad. Seejärel on tarvis tsoonidevahelised üleminekukohad muuta piisavalt turvaliseks, s.t kohandada turbevajadusega. Keelatud üleminekukohad tuleb kas likvideerida või erimeetmetega turvaliseks muuta. Näiteks tuleb tavapärasest suurema turbeastmega turvatsoonide evakuatsiooniuksed väljastpoolt piisavalt turvaliseks muuta, et volitamata isikutel poleks võimalik väljast ruumi pääseda. Turbevajadust tuleb arvesse võtta ka hoone uste ja akende kaitsmisel (vt M 1.10 Turvauksed ja -aknad).

Igas turvatsoonis peaksid toimuma ainult sellised tööprotsessid, mille turbenõuded langevad kokku turvatsooni turbeastmega. Samuti peaks olema igasse tsooni juurdepääs ainult neil inimestel, kelle tööülesanded seda nõuavad. Turvatsoonide juurdepääsusid tuleb vastavalt nende turbevajadusele ka kontrollida, et välistada volitamata isikute sisenemine nendesse tsoonidesse.

Sellist tegevusviisi tuleb siiski peaaegu alati täiendada meetmetega, mis käsitlevad volitamatut sissetungimist ja -hiilimist. Sellekohase ülevaate leiate meetmest M 1.19 Sissemurdmiskaitse .

Kui hoone teatud ruumid on avalikud või poolavalikud või kui näiteks läbi akende, mille vaade avaneb tänavale, on võimalik näha hoone sisemust, tuleb arvestada meetmega M 1.12 Kaitstavate hooneosade märgistamata jätmine .

Kõikidel juhtudel, kus on tarvis hoolikalt kaitsta hoones hoitavaid asju, olgu siis tegu kas kaubaga või hoone tehnilise taristuga, peab hoone kasutuse turvakontseptsiooni loomisel arvestama ka veekahjustuste vältimisega. Lisateavet selle kohta leiate meetmest M 1.14 Automaatne drenaaž .

Kõiki turvaeesmärkidele kohandatud meetmeid, mida kasutatakse kahjude ennetamiseks ja minimeerimiseks, tuleb täiendada ka tuvastamist võimaldavate meetmetega (vt M 1.18 Valve- ja tuletõrjesignalisatsioon). Hoone kasutuse turvakontseptsioon saab täiuslikuks alles siis, kui kontseptsiooni planeerimisel ja rakendamisel võetakse piisavalt meetmeid oluliste ohtude ärahoidmiseks ning kui rakendatakse piisavat kontrolli, mis tagab, et kahjutoovad sündmused ning kaitse- ja turvameetmete vastased juhuslikud ja planeeritud ründed tuvastatakse võimalikult vara. Vaid sellisel juhul saab võtta vastumeetmeid.

Hoone kasutuse turvakontseptsioon peab olema kooskõlas institutsiooni üldkehtiva turvakontseptsiooniga. Hoone kasutuse turvakontseptsiooni tuleb regulaarselt ajakohastada, eriti pärast seda, kui hoone kasutuses esineb muutusi, nt kui muudetakse institutsiooni töökorraldust.

Kontrollküsimused

- Kas hoone jaoks on olemas kasutuse turvakontseptsioon?
- Kas kõiki hoone juurdepääse kontrollitakse, et tõkestada volitamata isikute juurdepääs kaitstud aladele?

M 1.79w Turvatsoonide rajamine

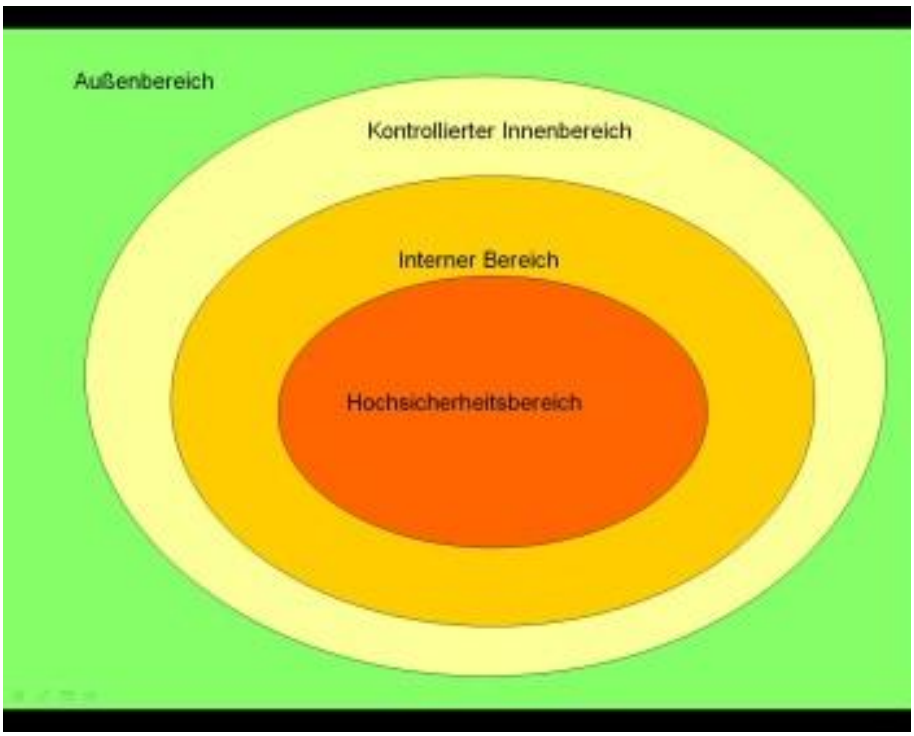
Algatamise eest vastutavad : infoturbespetsialist, sisemise kommunikatsiooni juht, planeerija

Rakendamise eest vastutab: sisemise kommunikatsiooni osakond

Hoone erinevate ruumide kaitsevajaduse määrab kindlaks nende kasutusotstarve. Ruumis võetavad kaitsemeetmed peavad olema kooskõlas selle kaitsevajadusega. See tähendab, et nõuetele peavad vastama nii seinte, akende ja uste ehituskonstruktsioon kui ka ruumidesse paigaldatud turva- ja seiretehnoloogia. Seetõttu tuleks uue hoone kavandamisel või olemasoleva hoone hindamisel sarnase turbeastmega ruumid koondada tsoonidesse. Nii saab sarnaste ohtudega tegelda korraga ja ülevaatlikult ning vähendada seeläbi meetmetega seotud väljaminekuid.

Et vältida olukorda, kus iga ruum peab olema pidevalt lukus või valve all, tuleb suure turbevajadusega tsoonid eraldada külalistele avatud tsoonidest. Seetõttu peaksid avalikud ruumid, nt söökla, kus einestavad ka külalised, ning poolavalikud ruumid, nt koosoleku- ja koolitusesaalid ning muud ürituseruumid, asuma hoones võimalikult sissepääsu lähedal. Nii saab juurdepääsusid hoones ainult sisekasutuseks ette nähtud ruumidele, nt bürooruumidele, väga lihtsalt valvata uksehoidja. Eriti suure kaitsevajadusega ruume, nt arendusosakonda, hoone juhttehnoloogiat sisaldavaid ruume ja IT-ruume, tuleks alati kaitsta täiendava juurdepääsukontrolliga.

Hoone ja vajaduse korral ka selle juurde kuuluva kinnistu füüsilise kaitse tagamisel on end seni hästi tõestanud mitmetasandiliste meetmetega turvakontseptsioon (sibulakoore põhimõte). Levinud on turvatsoonide jaotamine neljaks: välistsooniks, kontrollitud sisetsooniks, sisetsooniks ja üliturvaliseks tsooniks.



Joonis. Turvatsoonide mudel (lugeda väljastpoolt sissepoole)

Turvatsooni 0, s.t välise turvatsooni piir on kinnistu piir. Kui olukord seda võimaldab, on soovitatav kinnistu juriidiline piir ka füüsiliselt piirdega tähistada. Esmane juurdepääsu- ja sissesõidukontroll võib aset leida juba kinnistu piiril. Sellesse tsooni tuleks liigitada kõik avalikus kasutuses olevad hooneosad.

Turvatsoon 1 on kontrollitud sisetsoon. Sellesse tsooni võivad siseneda ainult volitatud inimesed (töötajad ja kutsutud külalised) ning sisenemiseks peavad nad läbima juurdepääsukontrolli, mida võib teha nt uksehoidja, kuid selleks võib kasutada ka juurdepääsukontrolli süsteemi. Tavapärasest suurema kaitsevajaduse korral peaks juba selles tsoonis töötajatele kehtima kohustus kanda lubasid alati endaga kaasas ja nähtaval kohal. Turvatsooni 1 välimist piiri (hoone välispiiri) tuleks ehituslike ja tehniliste meetmetega kaitsta sabotaaži ja sissemurdmise eest.

Turvatsoon 2 on sisetsoon, kuhu võib siseneda üksnes piiratud arv selleks volitatud töötajaid. Siin kehtivad määratletud juurdepääsuõigused. Tsooni 2 kuuluvatel ruumidel või hooneosadel peaks olema alati ainult üks juurdepääs. Ülejäänud juurdepääsud võivad olla ette nähtud vaid evakuatsiooniks ja päästetöödeks ning tavakasutuse ajal peavad need olema alati suletud. Sellised juurdepääsud peavad olema pideva seire all ja neile peavad olema paigaldatud elektromehaanilised kaitseseadmed (evakuatsiooniteede turvasüsteemid), mis hoiavad ära nende väärkasutuse.

Turvatsoon 3 on üliturvaline tsoon (nt juhtkonna tööruumid, kriitilise tähtsusega IT-ruumid). Juurdepääsuõigusega isikute ring on väga väike. Turvameetmed peavad olema piisavalt ranged. Näide: sissepääsuks tuleb läbida turvaväravad, kus sisenemisel rakendatakse kahefaktorilist autentimismeetodit ja inimeste ühekaupa läbilaskmist, väljumisel aga ühefaktorilist autentimismeetodit ja inimeste ühekaupa läbilaskmist. Juurdepääsude üle peetakse arvet, s.t niipea kui kõik töötajad on tsoonist lahkunud, lülitub automaatselt tööle sissemurdmisest teavitav signali-

satsioon.

Posti, tarnete ja kauba vastuvõtuks ja laadimiseks ette nähtud alad peaksid asuma turvatsoonis 1. Need alad tuleks sisustada selliselt, et tarnete vastuvõtmiseks ei pea kauba kohaletoimetajad sisenema hoone teistesse aladesse. Selliste alade uksed ei tohiks olla pikka aega niisama avatud. Tavapärasest suurema kaitsevajaduse puhul tuleks olukord lahendada nii, et avada saab kas ainult välisust või ust, mille kaudu pääseb sisemistesse aladesse. Saabunud saadetiste ohutust tuleks vastuvõtualas kontrollida (vt M 2.90 Kohaletoimetuse kontroll). Kontrolli liik ja põhjalikkus olenevad ohupotentsiaalist (nt kirjapommide oht). Sisenevaid ja väljuvaid saadetisi tuleks hoida võimalikult eraldi.

Kontrollküsimused

- Kas hoone ja kinnistu jaoks on välja töötatud turvakontseptsioon ja kas see on dokumenteeritud?

M 1.80 Juurdepääsu kontrolli süsteem ja volituste haldus

Algatamise eest vastutab: ametiasutuse/ettevõtte juhtkond

Rakendamise eest vastutavad: organisatsiooni juht, hoones kasutatava tehnoloogia juht

Põhjus, miks on vaja tõkestada volitamata isikute juurdepääs hoonele, kaitstud hooneosadele või ruumidele, seisneb vajaduses täita sageli mitut turvaeesmärki. See ei pruugi olla seotud üksnes omandi, s.t nii organisatsiooni kui ka selle töötajate omandi kaitsmisega, vaid ka töökaitse, oskusteabe kaitse ja võib-olla ka isikukaitsega. Lisaks võib lepingulistest suhetest tingitud või seadustega kehtestatud järelevalvenõuete (compliance) tõttu olla institutsioonid kohustatud kontrollima juurdepääsuvolituste väljastamist ja kasutamist. Institutsiooni juurdepääsukontrolli süsteemile esitatavad nõuded peavad olema dokumenteeritud piisavalt detailselt.

Mehaanilised lukusüsteemid koos oma võtmete ja rühmavõtmetega võivad väga kiiresti kujuneda probleemiks, kui keegi peaks oma võtme ära kaotama ja sellele on tarvis kiirelt reageerida või kui hoone kasutusotstarbe muutused eeldavad kiiret ümberseadistust. Seetõttu kasutatakse sageli IT-toega juurdepääsukontrolli süsteeme, mis vastavad standardite EVS-EN 60839-11-1:2013/AC:2015 „Häiresüsteemid – turvaotstarbelised juurdepääsu kontrolli süsteemid" nõuetele. Standard on tasuliselt kättesaadav, kuid kui on vajadus standarditega tutvuda või saada täpsemaid juhiseid läbipääsusüsteemide kohta, pöörduda küsimusega Riigi Infosüsteemi Ameti poole.

Selline süsteem koosneb erinevatest põhikomponentidest, mis toimivad erinevates kihtides. Juurdepääsukontrolli server haldab tsentraalset andmehulka, s.t nende isikute andmeid, kellele volitusi antakse, ning reegleid (kes, millal, kuhu), mis määravad kindlaks volituste haldamise ja nende rakendamise. Juurdepääsukontrolli serveri külge on ühendatud juhtseadmed. Nendesse juhtseadmetesse edastab server läbi IT-võrgu uste, väravate ja tõkkepuude volituste profiilid. Kõik otsused süsteemi ühendatud uste jms juhtimise kohta langetab vastav detsentraalne juhtseade. Niimoodi saab ust juhtida ka siis, kui ühendus tsentraalse serveriga puudub. Juhtseadmetes on andmemälu, kuhu salvestatakse kõik liikumisega seotud andmed.

Juhtseadmete külge on ühendatud andurid (lugemisseadmed), täiturid (nt reguleerimisseadised, ukse avamise mehhanismid, lüüsid) ja detektorid.

Kasutajate identifitseerimiseks (ja osaliselt ka autentimiseks) kasutatakse pääsukaarte või loakaarte (token), mida loevad lugemisseadmed. Pääsu- ja loakaarte nimetatakse üldistavalt identifitseerimistunnuste kandjateks. Load peaksid olema kõikidel samasugused ning hästi loetavate eristavate tunnustega (nt nimi ja osakond). See võimaldab kiiresti ära tunda, kas kaitstud alale on sisenenud mõni ilma volituseta isik.

Juurdepääsuvolituse kinnitamiseks peab töötaja oma loa asetama lugemisseadmesse. Lugemisseade saadab töötaja loa seest väljaloetud ID edasi enda juhtseadmesse. Pärast seda, kui juhtseade on tuvastanud, et selle loaga tohib vastavat ust avada, käivitatakse täitur ja uks avaneb.

Valdkondades, kus turbenõuded on tavapärasest suuremad, tuleks rakendada kahefaktorilist autentimist. Sellisel juhul täiendatakse töötaja valduse kontrollimist (nt volitatud kiipkaardi olemasolu) tema teadmiste kontrollimisega (nt palutakse tal sisestada PIN-kood) või loa valdaja biomeetriste tunnuste kontrollimisega.

Juurdepääsukontrolli süsteemi võib kasutada ka volituste, identifitseerimistunnuste kandjate ja tavapäraste võtmete kättejagamiseks. Sama süsteemiga tuleks hallata ka erivolitusi, nt töötajatele antavaid parkimislubasid ja lühikest aega kehtivaid külastajalubasid. Serverisse kogutakse kokku ka kõik juurdepääsukontrolli süsteemi kasutusega seotud logid. Juurdepääsukontrolli süsteem, millega hallatakse ka tavapäraseid mehaanilisi võtmeid, peaks olema sellise jõudlusega, mis suudaks tagada kõikide meetmes M 2.14 Võtmete (ja kaartide) haldus .

Juurdepääsukontrolli süsteem peab võimaldama mis tahes ajahetkel kergesti järele kontrollida, millistele töötajatele on väljastatud turbe seisukohalt kriitilistesse hooneosadesse sisenemist võimaldavad pääsuvolitused ning milliste lubadega ja mis ajal on uksi kasutatud. Sellise süsteemiga on väga lihtne volitusi ka muuta ja tühistada, nt kui töötaja tööülesanded peaksid muutuma või kui töötaja lahkub institutsioonist. Sel juhul ei ole tarvis töötajalt nõuda eseme, nt võtme tagastamist, piisab üksnes sellest, kui töötaja käsutuses olevast loakaardist eemaldatakse vastavad volitused.

Siinkohal tuleb arvestada, et otsuse, millistele töötajatele hooneosa kasutusvolitusi anda, peab langetama ja selle eest ka vastutama konkreetse hooneosa kasutamise eest vastutav töötaja. Juurdepääsukontrolli süsteemi administraator vastutab seejärel ainult saadud juhiste korrektse rakendamise, mitte pääsuvolituste andmise eest.

Kuna logimise ja andmeanalüüsi funktsioonid (nt töötajate liikumisandmete analüüsimine) on väga laialdased, tuleks sellise süsteemi kasutuselevõtt esmalt kooskõlastada andmekaitsespetsialistiga ning kaasata protsessi ka töötajate esindus.

Juurdepääsukontrolli süsteemi planeerimisel tuleb arvesse võtta institutsiooni erivajadusi. Sellise süsteemi liidestele, nt ukseliidestele ja videojälgimise liidestele, esitatavate nõuete kindlaksmääramisel ja rakendamisel tuleb lähtuda eesmärgiks seatud turbeastmest. Kindlasti on tarvis tegelda ka eriprobleemidega, mis puudutavad evakuatsiooniuste juhtimist ja seiret. Muu hulgas tuleks arvestada ka ohuga, mida võib põhjustada liigne sõltuvus ühest tarnijast, nt kui süsteemi on tarvis muuta või laiendada. Seetõttu tuleks juurdepääsukontrolli süsteemi esmasel soetamisel ja olemasoleva süsteemi suuremate muudatuste korral konsulteerida spetsialistidega.

Kontrollküsimused

- Kas institutsioonis juurdepääsukontrollile seatud nõuded on dokumenteeritud?
- Kas nende isikute töökorraldus, kes väljastavad identifitseerimistunnuste kandjaid, ja kandjate väljastamine on piisavalt dokumenteeritud?

M 1.81 Integreeritud süsteemide füüsiline kaitse

Vastutav algatamise eest: infoturbespetsialist, IT-juht
Vastutav elluviimise eest: planeerija, administraator, arendaja

Integreeritud süsteemid ei tohi tolmu või määrdumise tõttu rivist välja langeda või üles öelda. Integreeritud süsteeme tuleb nende ettenähtud kasutusviisi ja kasutuskoha kohaselt kaitsta tolmu ja määrdumise eest. Integreeritud süsteemi võib paigaldada seda ümbritsevasse tugevasse korpusesse või kaitstud kohale seda ümbritseva süsteemi sees või sisse ehitada kandvasse taristusse.

Kui süsteeme ei ole võimalik vajaliku õhu juurdevoolu tõttu piisavalt katta, tuleb paigaldada õhufiltrid. Need peavad sobima ettenähtud kasutusviiside jaoks, pidades silmas dimensioneerimist ja filtri võimsust.

Abinõusid kaitseks tolmu ja määrdumise eest tuleb arvesse võtta juba planeerimisel.

Kontrollküsimused:

- Kas nõudmisi tolmu ja määrdumise kaitseks analüüsiti integreeritud süsteemide jaoks juba planeerimise ajal?
- Kas tolmu ja määrdumise kaitse abinõud on kooskõlas üldise süsteemi nõudmistega?
- Kas integreeritud süsteemil on piisav kaitse tolmu ja määrdumise vastu?

M2: Organisatsioon

Meetmete nimekiri

M 2.1 IT kasutajate vastutuse ja reeglite kehtestamine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond
Rakendamise eest vastutavad: IT-juht, organisatsiooni juht

IT kasutus ja IT turvalisus on valdkonnad, kus lisaks vastutusalale tuleb määratleda ka tegutsemisõiguste piirid. IT kasutuse puhul tuleb defineerida nii spetsialistide vastutusala kui ka kollektiivne vastutus. Spetsialistid vastutavad erialaste suuniste väljatöötamise eest, mida tuleb järgida IT rakendamise käigus.

Kollektiivne vastutus hõlmab muu hulgas järgmisi ülesandeid:

- andmehõive,
- töö planeerimine ja ettevalmistus,
- andmetöötlus,
- väljastatud andmete järeltöötlemine,
- andmekandjate haldus ja
- rakendusmeetodite kontrollimine.

IT kasutuse ühe osana tuleb kehtestada IT kohustuslikud turvareeglid. Soovitatavad reguleerimisvaldkonnad on järgmised:

- andmevarundus,
- andmete arhiveerimine,
- andmekandjate transportimine,
- andmeedastus,
- andekandjate hävitamine,
- IT rakendusmeetodite, tarkvara ja konfiguratsioonide dokumenteerimine,
- paroolide kasutamine,
- sissepääsuõigused,
- süsteemi pääsuõigused,
- ligipääsuõigused,
- ressursside reguleerimine,
- riistvara ja tarkvara ostmine ja liisimine,
- hooldus- ja remonditööd,
- tarkvara: vastuvõtuprotseduurid,
- tarkvara: rakenduste arendamine,
- andmekaitse,
- kaitse arvutiviiruste eest,
- audit,
- valmisolek hädaolukorraks ning
- tegevusplaan turvapoliitika rikkumiste korral.

Vastava info leiate järgnevatest meetmete kirjeldustest. Lisaks eelnevale tuleb arvestada ka sellega, et informatsiooni enda turvalisus ei tohi samuti kahe

silma vahele jääda. Kõnealuses valdkonnas tuleks IT turvaline kasutamine ja konfidentsiaalsuse kaitse omavahel sobival viisil ühendada.

Siia alla kuuluvad näiteks:

- sobilik ümberkäimine tööks vajaliku strateegilise informatsiooniga,
- konfidentsiaalsuskokkulepped,
- andmeturbe eest vastutavate isikute kaasamine töödesse ja projektidesse, mis sisaldavad strateegilist infot,
- töötajate koolitus seoses strateegilise infoga ümberkäimisega, nt kokkupuuted klientidega ja tööreisid,
- informatsiooni klassifitseerimine selle turbeastme alusel.

Kõik vastuvõetud eeskirjad tuleb asjaomastele töötajatele sobival moel teatavaks teha (vt M 3.2 Uute töötajate kohustamine eeskirju järgima). Vastavad teavitamised tuleks soovitatavalt dokumenteerida. Lisaks eelnevale tuleb tagada, et kõik eeskirjad oleksid teatud kindlas kohas kõige uuemal kujul olemas ja õigustatud huvi korral ka ligipääsetavad. Eeskirjade muudatused tuleb dokumentidesse võimalikult ruttu sisse viia, et vääritimõistmised, selgusetus seoses vastutusaladega ning võimalikud vastuolud oleksid juba eos välistatud. Kõik eeskirjad peaksid olema varustatud kas vastuvõtukuupäeva või versiooninumbritega, et kõige uuemaid andmeid oleks võimalikult kerge üles leida.

Kontrollküsimused:

- Millised eeskirjad on hetkel jõus?
- Kas eeskirjade läbitöötamine toimub pidevalt?
- Kas eeskirjad tehakse töötajatele teatavaks?

M 2.2 Ressursside haldamine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtorgan

Rakendamise eest vastutavad: IT-juht, organisatsiooni juht

IT kasutuse ressursid (töövahendid) on kõik tööks vajaminevad komponendid, nagu riistvara (arvuti, klaviatuur, printerid jne), tarkvara (süsteemitarkvara, individuaalsed programmid, standardsed programmid jms), andmekandjad (magnetlindid, disketid, striimeri lindid, kõvakettad, eemaldatavad andmekandjad, CD-ROM-id jms).

Ressursside reguleerimine hõlmab järgmisi ülesandeid

- töövahendite hankimine,
- kasutuseelne kontrollimine,
- märgistamine ja
- laomajandus.

Hankeprotsessi reeglid

Töövahendite hankimise protsess on infotehnoloogiliste vahendite kasutamisel olulise tähtsusega. Kindlaksmääratud soetamisprotseduur aitab kaasa infotehnoloogia kasutamisele esitatud nõudmiste täitmisele – jõudluse kasv, majanduslikkus, kommunikatsioonivõimaluste parendamine. Lisaks selgelt majanduslikele kaalutlustele saab reguleeritud hankeprotsessiga, mida on võimalik tsentraliseeritult läbi viia, pöörata rohkem tähelepanu infotehnoloogia uuendustele ja edasiarendusele.

Majasisesed standardid

Tsentraliseeritud hankeprotsessi plussiks on lisaks muule ka nn majasisese standardi juurutamine ja järgimine, mis muudab töötajate koolituse ja seadmete hooldustööd palju lihtsamaks. Töövahendite kindlaksmääratud kontrolliga enne nende kasutuselevõttu on võimalik ennetada erinevaid ohtusid.

Näited:

- Kauba tervikluse kontrollimine, st kas tarnepakendi sisu on täielik (nt käsiraamatud, ühenduskaablid).
- Uut arvutitarkvara ja eelformaaditud andmekandjaid tuleks enne nende kasutuselevõttu testida viirusetõrjetarkvaraga.
- Uut tarkvara tuleks eelnevalt testida testimissüsteemide peal, et nende kasutuselevõtt töösüsteemides kulgeks ilma tõrgeteta.
- Väärostude vältimiseks tuleks enne uute riistvara- ja tarkvarakomponentide ostmist kontrollida, kuidas need ühilduvad olemasoleva süsteemiga.

Korralikult toimiv laomajandus võimaldab hinnata nõudlust seoses ressurssidega ja on abiks nende õigeaegsel juurde tellimisel. Lisaks aitab täpne arvepidamine kontrollida seadmekomplektide terviklust, tuvastada rakenduses oleva tarkvara

kasutuslubasid või nende puudumist ning aitab muu hulgas jälile saada ka võimalikele ärastamistele. Süsteemi toimimiseks tuleb peamised töövahendid selgelt märgistada, kusjuures vastavad märgistused peavad olema üheselt mõistetavad (nt grupeeritud järjestikused inventarinumbrid). Lisaks sellele tuleks üles kirjutada kasutatavate seadmete, nt monitoride, printerite, kõvaketaste jne seerianumbrid, et varguse korral oleks võimalik neid tuvastada.

Inventari loetelud

Laomajanduse tarbeks tuleb töövahendite kohta koostada vastavad loetelud. Inventari loetelu peab sisaldama alljärgnevat informatsiooni:

- identifitseerimistunnused,
- hankimise koht, tarne saabumise aeg,
- töövahendite asukoht,
- laovarude arv,
- esemete laost väljastamise eeskirjad ning
- hooldusleping, hooldusvälbad.

Kustutamine ja hävitamine

Andmete väärkasutuse vältimiseks peab olema kindlaks määratud töövahendite kustutamise ja hävitamise kord. Erilist tähelepanu nõuab vanapaberiga ümberkäimine. Kõrgema tundlikkusega kuluvahendite käitlemiseks tuleks kasutada nt purusteid või paberi puhul paberihunte. Purusteid on saadaval erinevate kuluvahendite hävitamiseks, nagu nt paber, magnetlindid, disketid ja CD-d. Lisaks liigitatakse purusteid erinevatesse turvaklassidesse, kus on muu hulgas määrava tähtsusega asjaolu, kui väikesteks osadeks hävitamist vajav materjal töödeldakse.

Kõik kuluvahendid, millest on võimalik saada informatsiooni, nagu nt fakside vahekopeerlindid või ebaõnnestunud väljatrükid, tuleb enne minemaviskamist kas ise hävitada või lasta need kõrvalda infokaitseteenust pakkuvatel firmadel. Sama kehtib ka informatsiooni sisaldavate varuosade vahetamisel, nagu nt koopiaseadmete fotoelektrilised trumlid.

Kontrollküsimused:

- Kas laomajanduse seis võimaldab täielikku seadmete kontrolli?
- Millised on enne kasutuselevõttu läbitavad testimisprotsessid? Millised tulemused saavutati?
- Kas hankeprotsess on kindlalt määratletud või on hankeprotsessis võimalik laomajanduse arvepidamisest mööda hiilida?
- Kui värske on inventari loetelu info?
- Mil moel toimub selliste kulumaterjalide hävitamine, mida enam ei vajata?

M 2.3 Andmekandjate haldus

Algatamise eest vastutavad: organisatsiooni juht, IT-juht

Rakendamise eest vastutavad: arhiivi juhataja, spetsialist

Andmekandjate halduse kui ressursside reguleerimise ühe osa eesmärk on tagada mõistliku aja jooksul juurdepääs vajalikus koguses andmekandjatele. Selle tagamiseks on tarvis andmekandjaid süstemaatiliselt hallata, mistõttu muutub vajalikuks üheselt mõistetav märgistus ja laonimekirjade pidamine. Lisaks kuulub andmekandjate halduse alla veel andmekandjate õige käsitsemine ja ladustamine, nende korrakohane kasutamine ja transportimine ning viimaks ka andmekandjate kustutamine või hävitamine. Analoogsete andmekandjate puhul on enamikel institutsioonidel välja kujunenud oma läbiproovitud haldusmeetod, milleks on klassikaline arvepidamine. Seetõttu pööratakse selles meetmes põhitähelepanu digitaalsete andmekandjate haldusele, kuid eraldi väljatoodud soovitused kehtivad vastavaid eripärasid arvesse võttes kõikidele andmekandjate liikidele. Inventari loetelud tagavad kiire ja eesmärgikohase juurdepääsu andmekandjatele. Inventari loeteludest saab infot näiteks asukoha, asukohas hoidmise aja ning õigustatud juurdepääsuga isikute kohta.

Andmekandjate väline märgistamine võimaldab neid kiiresti identifitseerida. Märgistus ei tohi võimaldada järeldusi andmekandja sisu kohta (nt magnetlindi tähistamine pealkirjaga „Telefoniarved", kuna vastasel korral muutub nende väärkasutamine volitamata isikutele liiga kergeks. Andmekandjate loetelude grupeerimist hõlbustab tähistuse kindel struktuur (nt kuupäev, asukoha struktuuriüksus, jooksev number). Andmekandjate otstarbekohase käsitsemise juhised on enamjaolt ära toodud tootjafirma juhistes, mis on reeglina kirjas toodete pakendite peal.

Andmekandjate hoidmise puhul on ühelt poolt olulised nende ladustamistingimused (magnetvälja, tolmu, kliimamuutuste eest kaitstud) ja teiselt poolt volitamata juurdepääsu tõkestamine (sobivad hoidjad, kapid, ruumid). Andmekandjate saatmine või transportimine peab toimuma selliselt, et nende kahjustumine oleks võimalikult välistatud (magnetlindi saatmiskott, mullikilega turvaümbrikud). Andmekandja pakend tuleb valida selle kaitsevajaduse alusel (nt suletav transpordimahuti). Määratleda tuleb saatmise ja transportimise eriliigid (nt kullerteenus), samuti saatmist tõendavate dokumentide kasutamine (saatekirjad, saatelehed) ning saadetise kättesaamise kord (nt adressaadi kinnitus). Andmekandja ei tohi lisaks saadetavatele andmetele sisaldada mitte mingisuguseid „jääkandmeid". Seda on võimalik saavutada füüsilise kustutamisega. Kui vastavad vahendid puuduvad, tuleks andmekandja vähemalt formaatida. Sealjuures tuleks kindlustada, et kasutatava operatsioonisüsteemiga ei oleks võimalik käsku tagasi võtta. Lisaks tuleb veel jälgida, et enne tähtsat infot sisaldavate andmekandjate loovutamist tehtaks ka tagavarakoopiad. Täiendavat informatsiooni andmekandjate saatmise ja transportimise kohta leiate moodulist B 5.2 Andmekandjatel toimuv andmevahetus .

Organisatsioonisiseseks andmekandjate edasiandmiseks on võimalik juurutada erinevaid kontrollimehhanisme, nagu kviitungisüsteem, äratoomise/kaasavõtmise volitused ning arvepidamine andmekandjate asukoha üle. Juhtumite puhuks, kus andmekandjad on saadud kolmandate isikute käest, tuleb määratleda protseduurid, mis tuleb läbida enne nende kasutamist. Kui tegu on näiteks digitaalsete andmete edastamisega, tuleks üldjuhul enne andmekandja või andmekirje kasutamist

teha sellele arvutiviiruse kontroll. Sama kehtib uutele andmekandjatele enne nende esmakordset kasutuselevõttu. Digitaalsete andmekandjate puhul on soovitatav teha viirusekontroll mitte ainult nende vastuvõtmisel, vaid ka nende väljasaatmisel. Andmekandjate kindlaksmääratud kustutamise ja hävitamise protsess aitab vältida salvestatud andmete väärkasutamist. Enne andmekandjate taaskasutamist tuleb eelnevalt salvestatud andmed sealt kustutada (vt M 2.167 Andmete kustutamiseks või hävitamiseks sobivate lahenduste valik).

Kontrollküsimused:

- Kas inventari loetelu on saadaval kõige värskemas (päeva kaupa) versioonis?
- Kas arhiivis kontrollitakse andmekandjat sooviva isiku asjakohaseid volitusi?
- Kas inventari nimekirjade alusel kontrollitakse andmekandjate terviklust?

M 2.4 Hooldus- ja remonditööde reeglid

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: IT-juht, administraator, kasutaja

IT rikete vältimiseks on reeglipäraselt läbiviidavad hooldustööd väga olulised. Hooldustööde õigeaegne algatamine ja nende läbiviimise kontroll peaks toimuma tsentraalselt (nt kohast, mis tegeles nende soetamisega). Sealjuures tuleks jälgida, et kui oma töötajad hooldustöid läbi viia ei suuda, peaksid seda tegema usaldusväärsed isikud või ettevõtted. IT tootjajuhistest tuleb hooldustööde käigus ilmtingimata kinni pidada. Reeglipäraste hooldustööde pideval sisseostmisel tuleks kaaluda hooldusleping sõlmimist. Iga IT-süsteemi puhul tuleb kirja panna, millal toimus selle hooldus ja millised olid hoolduse käigus likvideeritud vead (nt seadmepass või seadme/konfiguratsiooni haldussüsteem). Lisaks eelnevale on soovitatav sisse seada hooldus- ja parandustööde infosüsteem. Vastava süsteemi abil saab planeerida eesseisvaid töid, dokumenteerida läbiviidud töid ja jälgida protsessi. Süsteemis peaks olema dokumenteeritud ka see, kes on seadmete hooldamise või parandamise eest vastutav.

IT-seadmete regulaarne puhastamine

Turvalisus = kord + puhtus! Igasuguseid IT-seadmeid tuleb regulaarselt puhastada. Soovituslikud hooldusvälbad sõltuvad suuresti seadme tüübist ja kasutuskeskkonnast. Sellele vaatamata peaks IT-seadmeid puhastama vähemalt kord aastas ja seda mitte ainult seetõttu, et määrdunud seadmetega on ebamugav töötada, vaid ka sellepärast, et mustus võib kahjustada seadmete tööfunktsiooni.

Näited:

- Klaviatuure tuleks puhastada hiljemalt siis, kui need on muutunud kleepuvaks või kui üksikud nupud on kinni kiilunud.
- Personaalarvutit tuleks aeg-ajalt ka seestpoolt tolmust puhastada, välja arvatud juhtudel, kui tootjafirma juhised sellest erinevad.
- Printerite puhul võib pealiskaudne puhastamine alandada nende trükikvaliteeti või viia masinaosade kahjustumiseni. Tüüpilised probleemsed kohad on printeri trummel ja trükipea.
- Liigne tolm võib põhjustada IT-süsteemide ülekuumenemist. Mustuse kogunemine plaatide peale (eriti efektiivne on tolmu, tõrva ja nikotiini ladestumise koosmõju) võib põhjustada elektri pindmisi ülelööke.

Tootjapoolsete juhiste järgimine

Ladestunud mustus tuleb seega ettevaatlikult eemaldada. Eriti oluline on tagada kõikide IT-süsteemide piisav ventileerimine. Kõik ventilaatorid ja ventileerivad detailid tuleb hoida puhtana, et mustus ei takistaks nende tööd. IT-seadmete puhastamisel tuleb ilmtingimata järgida tootja juhiseid, seda nii puhastusmeetodi ja tööriistade valikul kui ka minimaalsete hooldusvälpadega arvestamisel.

Organisatsioonisisesed hooldus- ja remonditööd

Majasiseste parandus- ja hooldustööde puhuks, eriti kui neid viivad läbi isikud väljastpoolt, tuleb vastu võtta reeglid vastavate töötajate järelevalve kohta. Kõnealuses valdkonnas pädev inimene peaks jälgima tööde käiku nii palju, et tal

oleks võimalik hinnata, kas tööde teostajad ületasid neile antud volitusi või mitte. Lisaks vajab ka kontrollimist, kas hooldustellimus täideti kokkulepitud mahus.

Enne ja pärast hooldus- ja parandustöid tuleks planeerida järgmist:

- Töödest etteteatamine – hooldus- ja parandustöödest tuleb asjassepuutuvaid töötajaid eelnevalt õigeaegselt teavitada.
- Hooldustehnikud peavad nõudmisel oma isikut tõendama.
- Hooldustehnikute ligipääsu andmetele tuleks vältida nii palju kui võimalik. Vajaduse korral tuleb andmekandjad eelnevalt süsteemist eemaldada või kustutada (muidugi alles pärast täielikku andmevarundust), eriti juhul, kui töid viivad läbi väljastpoolt organisatsiooni tulevad isikud. Juhul kui kustutamine ei ole võimalik (nt defekti tõttu), tuleb töid jälgida ka väljaspool organisatsiooni või sõlmida spetsiaalsed lepingud selleks sobilike usaldusväärsete firmadega.
- Hooldetehnikute õiguste minimeerimine – hooldustehnikutele tööde ajaks antud sissepääsu-, juurdepääsu- ja pääsuõigused ei tohi olla suuremad kui töödeks hädavajalik ning pärast tööde lõppu tuleb need õigused tühistada.
- Paroolid tuleb pärast ära muuta! – peale hooldus- ja parandustööde lõppu võib olenevalt sellest, kui „sügavale" hooldetehnikud oma töödes tungisid, osutuda vajalikuks paroolide muutmine. Personaalarvutitele tuleks teha viirusetõrje kontroll.
- Tehtud hooldustööd tuleb dokumenteerida (tööde ulatus, tulemused, töö tegemise aeg, firma nimi ning vajaduse korral ka tööd teostanud hooldustehniku nimi).
- Hoolduslepingu – hooldustöid teostav firma peab kirjalikult kinnitama, et nad järgivad üldkehtivaid eeskirju ja direktiive (nt tuleohutuse, keevitus-, jootmis- ja ketaslõikamistööde eeskirjad). Sama kehtib kõikide tegevuste kohta, mis võivad põhjustada kas otsest või kaudset ohtu hoonele või inimestele. Lõppkokkuvõttes on tähtis, et kohapeal tööle rakendatav personal oleks nende eeskirjadega kursis.
- Funktsiooni kontroll peale tööde lõppu – hooldus- ja parandustööde lõppedes tuleb kontrollida, kas seade töötab ootuspäraselt või mitte. Eriti hoolikas tuleb olla nende tööde vastuvõtmisel, mis viidi läbi millegi testimiseks.

Organisatsioonivälised hooldus- ja remonditööd

Kui IT-süsteemide hooldamine või parandamine toimub organisatsioonist väljaspool, tuleb kõik andmekandjatel olevad tundlikud andmed eelnevalt füüsiliselt kustutada. Juhul kui andmete kustutamine ei ole võimalik, kuna defekti tõttu on juurdepääs andmekandjale häiritud, tuleb parandustöid teostavat firmat kohustada kinni pidama vajalikest IT turbemeetmetest. Andmekaitset puudutavate kirjalike konfidentsiaalsusnõuete väljatöötamisel tuleb lähtuda meetmest M 3.2 Uute töötajate kohustamine eeskirju järgima. Eriti tähtis on kokku leppida, et andmed, mis hooldustööde käigus välisele andmekandjale salvestati, saaksid peale tööde lõppu hoolikalt kustutatud. Samuti tuleb täpselt määratleda organisatsioonivälise hooldustehnikute kohustuste ja volituste piirid.

Hooldustööde protokollimine

Väljapool organisatsiooni tehtud hooldustööde puhul tuleb protokollida, millised IT-süsteemid või nende komponendid millal ja kellele paranduseks üle anti, kes andis vastava käsu, missuguseid töid hooldamine või parandus hõlmab, mis ajaks peaksid parandustööd olema lõpule viidud ning millal seade tagasi tuuakse. Järjepidevalt toimiva protokollimise tagamiseks tuleb IT-süsteemid või selle osad märgistada, et selle kaudu oleks võimalik välja lugeda, millisele organisatsioonile need seadmed kuuluvad ja milline on seadmete koht selle organisatsiooni teatud kindlas struktuuriüksuses. IT-süsteemide osade saatmisel või transportimisel tuleb hoolt kanda selle eest, et kahjustuste ja varguste oht oleks võimalikult väike. Juhul kui IT-süsteemid sisaldavad tundlikke andmeid, tuleb seadmete transpordil rakendada vastavaid turvameetmeid, st näiteks lukustatav pakend, või kasutada kullerteenust. Lisaks tuleb hoolitseda, et nii saatmine (parandustööde tellimus, saatelehed) kui ka saadetise vastuvõtmine (vastuvõtu kinnitus) oleksid kirjalikult tõestatavad. Vastavad dokumendid tuleb arhiveerida.

Paroolid

Paroolkaitsega varustatud IT-süsteemide hooldustöödeks tuleb hooldustehnikule olenevalt parandustööde ulatusest ja paroolkaitse liigist avalikustada kas kõik või osad paroolid, või tuleb süsteemid ümber lülitada kindlaksmääratud seadistusele „HOOLDUSTÖÖD”.

Tehtud tööde kontrollimine

Pärast IT-süsteemide või selle osade tagasisaamist tuleb kontrollida komplekti terviklust. Kõik paroolid tuleb ära muuta. Personaalarvuti andmekandjad tuleb peale tagasisaamist uuendatud viirusetõrjetarkvaraga üle kontrollida. Kõikidele parandusest tulnud seadmes olevatele failidele ja programmidele tuleb teha tervikluse kontroll.

Kaughooldus

Kaughooldust puudutavad nõuded leiate meetmest M 5.33 Kaughoolduse turve
.

Kontrollküsimused:

- Kas töötajad on teadlikud, et majas läbiviidavaid hooldustöid on kohustuslik jälgida?
- Kas läbiviidud hooldustööde kohta kogutakse ja säilitatakse tõendeid?
- Kas hooldustööde läbiviimiseks on koostatud hooldusgraafikud?

M 2.5 Vastutuse ja ülesannete jaotamine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtorgan

Rakendamise eest vastutavad: IT turvaosakond, IT-juht, organisatsiooni juht

Määratlemist vajavad ametiasutuse või ettevõtte IT kasutuse funktsioonid. **Eristada tuleb kahte tasandit:**

- esimene tasand koosneb funktsioonidest, mis võimaldavad või toetavad IT kasutamist, nagu näiteks töö ettevalmistamine, andmete järeltöötlus, käitamine, programmeerimine, võrgu administreerimine, õiguste haldus ja audit;
- teise tasandi moodustavad funktsioonid, mis rakenduvad IT protseduuridele ja on vajalikud ülesannete täitmiseks.

Vastavate funktsioonide näited on järgmised:

vastutav spetsialist, IT-kasutuse juhendaja, andmesisestaja, spetsialist ja arvete laekumist kontrolliv raamatupidaja.

Järgmise sammuna tuleb määratleda funktsioonide lahusus ja seda põhjendada, st defineerida, millised funktsioonid tuleb üksteisest lahutada, et üks inimene ei saaks samal ajal täita erinevaid omavahel ühildumatuid ülesandeid. Siinkohal aluseks võetavad nõuded võivad pärineda nii ülesande püstitamisest endast kui ka seadusesätetest,

näiteks:

- õiguste haldamine ja auditeerimine,
- võrgu administreerimine ja auditeerimine,
- kasutatava tarkvara programmeerimine ja testimine,
- andmesisestus ja makselaekumiste kontrollivolitused,
- auditeerimine ja volitused maksmisele kuuluvate maksete allkirjastamiseks.

Ilmekalt tuleb esile see, et käitamisfunktsioone ei ühendata tihti kontrollifunktsioonidega. Pärast vaatluse all olevate funktsioonide üksteisest lahutamist võib hakata tegelema tööülesannete jaotamisega töötajate vahel. Ülesannete jagamisel tuleb määratleda ja dokumenteerida ka asenduste kord (vt M 3.3 Asendamise korraldamine). Vastuvõetud otsused tuleb kindlasti kirja panna ja võimalikud muudatused alati dokumentatsiooni sisse viia. Juhul kui tööülesannete jaotamisel ei õnnestu vältida olukorda, kus ühele töötajale langeb omavahel ühildumatute tööülesannete täitmine, tuleb see tööülesannete jaotust kajastavas dokumentatsioonis selgelt välja tuua.

Kontrollküsimused:

- Kas vajalike tööülesannete loetelu on piisav?
- Kas tööülesanded on piisavalt teineteisest eraldatud?
- Kas tööülesannete eraldatust järgitakse pidevalt?

M 2.6 Sissepääsuõiguste andmine

Algatamise eest vastutavad: IT-juht, IT turvaosakond

Rakendamise eest vastutavad: organisatsiooni juht, majas kasutatava tehnoloogia juht

Enne sissepääsuõiguste jagamist töötajatele tuleb määratleda erinevate ruumide turvaklassid, nt büroo, andmekandjate arhiiv, serveriruum, käitamisruum, masinasaal, dokumendiarhiiv, arvutuskeskus. Ruumide turvavajadused tuleb kindlaks teha nendes paikneva infotehnoloogia ning kasutatavate IT-rakenduste ja nendes sisalduva info kaitsevajaduse alusel. Seejärel tuleb kindlaks teha, milliseid sissepääsuõigusi vajavad töötajad oma tööülesannete täitmiseks. Siinjuures tuleb järgida eelnevalt läbiviidud tööülesannete jaotust (M 2.5 Vastutuse ja ülesannete jaotamine). Ebavajalikke sissepääsuõigusi tuleb vältida.

Sissepääsuõiguse arvukuse piiramiseks tuleks juba ruumides kasutatavate IT-süsteemide planeerimisel arvestada inimeste tööülesannete lahutamise printsiibiga. Näiteks IT varuosade ja andmekandjate eraldi ladustamisega saab vältida hooldustehnikute juurdepääsu andmekandjatele. Sissepääsuõiguste andmine ja tühistamine tuleb dokumenteerida. Sissepääsuõiguse tühistamisel peab olema tagatud, et töötaja tagastaks ka sissepääsu võimaldava vahendi. Lisaks tuleb kirja panna võimalikud konfliktid, mis tekkisid töötajatele sissepääsuõiguste jagamisel. Konfliktide põhjused võivad seisneda näiteks tööülesannete iseloomus, kui töötajate sissepääsuõigused ja tööülesannete lahutamine ei ole omavahel kooskõlas, või siis ruumilistes piirangutes (vt M 3.3 Asendamise korraldamine).

Õiguste kontseptsioon

Sissepääsuõiguste jälgimiseks võib kasutada töötajaid (uksehoidjad, sulgemisteenus) või tehnilisi lahendusi (pääsukaardi lugejad, biomeetrilised lahendused, nagu silmaiirise skannerid või sõrmejälje skannerid, uste turvalukud või sulgemissüsteem), (vt M 2.14 Võtmete (ja kaartide) haldus). Kaitset vajavatesse ruumidesse tohib volitamata personal (nt külastajad, koristajad ja hooldustehnikud) sisse pääseda vaid juhul, kui ruumis viibib või kui neid saadab sissepääsuõigusega töötaja. Sarnaselt oma töötajaskonnale tuleb määrata ka väljastpoolt tuleva personali ja külastajate sissepääsuõiguste jagamise ja tagasivõtmise kord.

Kontrollküsimused:

- Kas on olemas dokumentatsioon, milles kirjeldatakse erinevate IT-ruumide kaitsevajadusi?
- Kas kaitset vajavate ruumide ja sissepääsuõigusi omavate isikute dokumentatsiooni uuendatakse pidevalt?
- Kas asendustel kehtivaid õigusi kajastavat nimekirja uuendatakse pidevalt?

M 2.7 Süsteemi ja võrgu pääsuõiguste andmine

Algatamise eest vastutavad: IT-juht, IT turvaosakond

Rakendamise eest vastutavad: organisatsiooni juht, majas kasutatava tehnoloogia juht

Enne sissepääsuõiguste jagamist töötajatele tuleb määratleda erinevate ruumide turvaklassid, nt büroo, andmekandjate arhiiv, serveriruum, käitamisruum, masinasaal, dokumendiarhiiv, arvutuskeskus. Ruumide turvavajadused tuleb kindlaks teha nendes paikneva infotehnoloogia ning kasutatavate IT-rakenduste ja nendes sisalduva info kaitsevajaduse alusel. Seejärel tuleb kindlaks teha, milliseid sissepääsuõigusi vajavad töötajad oma tööülesannete täitmiseks. Siinjuures tuleb järgida eelnevalt läbiviidud tööülesannete jaotust (M 2.5 Vastutuse ja ülesannete jaotamine). Ebavajalikke sissepääsuõigusi tuleb vältida.

Sissepääsuõiguse arvukuse piiramiseks tuleks juba ruumides kasutatavate IT-süsteemide planeerimisel arvestada inimeste tööülesannete lahutamise printsiibiga. Näiteks IT varuosade ja andmekandjate eraldi ladustamisega saab vältida hooldustehnikute juurdepääsu andmekandjatele. Sissepääsuõiguste andmine ja tühistamine tuleb dokumenteerida. Sissepääsuõiguse tühistamisel peab olema tagatud, et töötaja tagastaks ka sissepääsu võimaldava vahendi. Lisaks tuleb kirja panna võimalikud konfliktid, mis tekkisid töötajatele sissepääsuõiguste jagamisel. Konfliktide põhjused võivad seisneda näiteks tööülesannete iseloomus, kui töötajate sissepääsuõigused ja tööülesannete lahutamine ei ole omavahel kooskõlas, või siis ruumilistes piirangutes (vt M 3.3 Asendamise korraldamine).

Õiguste kontseptsioon

Sissepääsuõiguste jälgimiseks võib kasutada töötajaid (uksehoidjad, sulgemisteenus) või tehnilisi lahendusi (pääsukaardi lugejad, biomeetrilised lahendused, nagu silmaiirise skannerid või sõrmejälje skannerid, uste turvalukud või sulgemissüsteem), (vt M 2.14 Võtmete (ja kaartide) haldus). Kaitset vajavatesse ruumidesse tohib volitamata personal (nt külastajad, koristajad ja hooldustehnikud) sisse pääseda vaid juhul, kui ruumis viibib või kui neid saadab sissepääsuõigusega töötaja. Sarnaselt oma töötajaskonnale tuleb määrata ka väljastpoolt tuleva personali ja külastajate sissepääsuõiguste jagamise ja tagasivõtmise kord.

Kontrollküsimused:

- Kas on olemas dokumentatsioon, milles kirjeldatakse erinevate IT-ruumide kaitsevajadusi?
- Kas kaitset vajavate ruumide ja sissepääsuõigusi omavate isikute dokumentatsiooni uuendatakse pidevalt?
- Kas asendustel kehtivaid õigusi kajastavat nimekirja uuendatakse pidevalt?

M 2.8 IT-rakendustele ja andmetele pääsuõiguste andmine

Algatamise eest vastutavad: IT-juht, IT turvaosakond

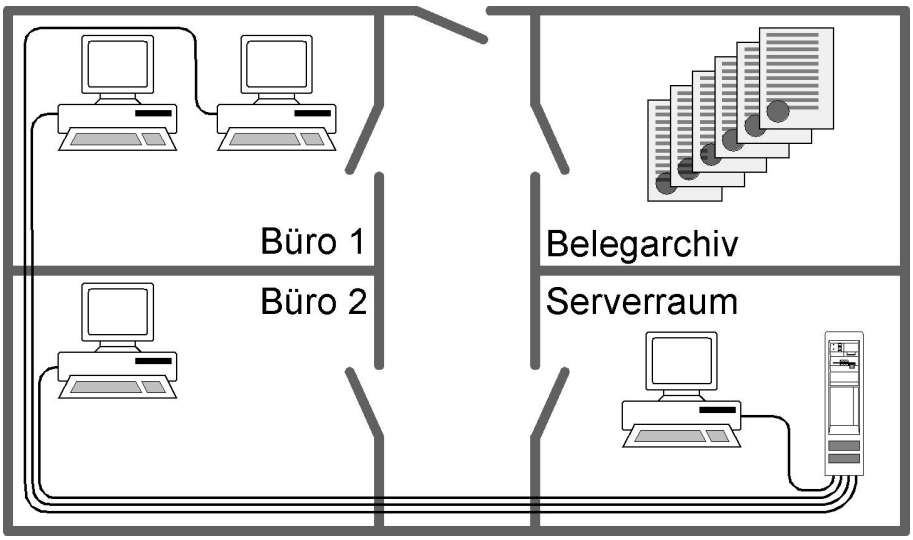
Rakendamise eest vastutavad: administraator, vastutav spetsialist

Rakenduste ja andmete pääsuõigustega määratakse kindlaks isikud, kellele antakse nende tööülesannete täitmise raames õigused teatud IT-rakenduste ja andmete kasutamiseks. IT-rakenduste, rakenduste erinevate osade või andmete kasutamise pääsuõigused (nt lugemine, kirjutamine, töötamine) sõltuvad suuresti iga töötaja tööülesannetest, milleks võib olla nt kasutajate juhendamine, töö ettevalmistamine, süsteemi programmeerimine, rakenduste arendamine, süsteemi administreerimine, audit, andmesisestus ja andmetöötlus. Pääsuõigusi tuleks töötajatele väljastada ainult sellises mahus, mis on hädavajalik nende tööülesannete täitmiseks (teadmistarbe printsiip). Pääsuõiguste korrakohase kasutuse peab tagama IT-süsteemi pääsuõiguste korrektne haldus. Suur osa IT-süsteeme võimaldavad õiguste grupeerimist, st lubavad defineerida õiguste profiilid (nt profiiligrupp nimega andmesisestus). Niisugune õiguste defineerimine annab tehnilise lahenduse ühe funktsiooni erinevate õiguste andmiseks. IT-süsteemi õiguste administreerimiseks on vastavate gruppide loomine vägagi soovitatav, kuna seeläbi saab õiguste jagamist ja uuendamist märgatavalt lihtsustada. Rakenduste ja andmete pääsuõiguste määramise ja muutmise peab algatama selle eest vastutav töötaja ning vastav tegevus tuleb dokumenteerida.

Dokumentatsioon peab sisaldama järgmist infot:

- erinevate tööülesannete täitmiseks antud pääsuõigused, mis lähtuvad tööülesannete lahutamise printsiibist (M 2.5 Vastutuse ja ülesannete jaotamine),
- loodud grupid ehk pääsuõiguste profiilid,
- loetelu töötajatest ja nende tööülesannetest,
- töötajale väljastatud töörollist lähtuvad pääsuõigused (siinkohal tuleks loetleda ka asendavate töötajate pääsuõigused) ning
- konfliktid, mis kerkisid esile rakenduste ja andmete pääsuõiguste jagamisel. Konfliktid võivad tekkida näiteks sellest, et teatud töötaja võtab enda kanda tööülesande, mis ei ole eelnevalt kokku lepitud, või sellest, et teatud IT-süsteemides ei pruugi olla võimalik pääsuõigusi üksteisest eraldada.
- hädaolukorras teatud inimestele antavad pääsuõigused, nt kriisistaapi kuuluvad töötajad.

Tööülesannete eraldamist ja pääsuõiguste jagamist kirjeldab järgnev näide. Vaatlusalune IT-rakendus on reisikulude hüvitamise süsteem. Vastavad ruumid on näidatud järgnevatel skeemidel. IT-süsteem koosneb kohtvõrgust, kuhu lisaks juhtkonsoolile on ühendatud kolm töökohaarvutit.



Joonis: Büro 1 – büroo nr 1, Büro 2 – büroo nr 2, Belegarchiv – kuludokumentide arhiiv, Serverraum – serveriruum

1. etapp: vastutuse ja ülesannete jaotamine

Vaadeldava töölähetuste kuluhüvitussüsteemi toimimiseks on vajalikud järgmised funktsioonid:

1. kohtvõrgu (LAN) administreerimine,
2. audit,
3. andmesisestus,
4. andmetöötlus ja arvutuste õigsuse kontroll,
5. andmetöötlus ja kulude põhjenduse kontroll,
6. andmetöötlus ja ettekirjutuse tegemise õigus.

Järgmised funktsioonid ei ole oma ülesande tõttu üksteisega ühendatavad:

- funktsioon nr 1 ja funktsioon nr 2 (administreerimisega tegelevad isikud ei tohi ennast ise kontrollida);
- funktsioon nr 2 ja funktsioon nr 6 (ettekirjutusi tegev isik ei tohi ennast ise kontrollida);

_ funktsioonide nr 4 või nr 5 kombineerimine funktsiooniga nr 6 (neljasilmaprintsiip läheks vastuollu väljamaksete korraldustega).

Loetletud funktsioone täidavad järgmised isikud:

		hr Mets	pr Kask	hr Kuusk	pr Tamm
1.	LAN võrgu administreerimine	X			
2.	Audit		X		

3.	Andmesisestus	X	
4.	Andmetöötlus ja arvutuse kontroll	X	
5.	Andmetöötlus ja kulupõhjendus	X	
6.	Ettekirjutuse tegemise õigus		X

2. etapp: sissepääsuõiguste andmine

Järgnevalt toimub üksikute ruumide kaitsevajaduse põhjendamine ja töötajate sissepääsuõiguste dokumenteerimine tabeli alusel.

- Serveriruum: kuna kogu rakenduse kättesaadavus, terviklus ja konfidentsiaalsus sõltub sellest kesksest komponendist, tuleb vältida volitamata isikute juurdepääsu serveriruumile.
- Kuludokumentide arhiiv: raamatupidamise tarbeks tuleb säilitada kuluhüvitiste aluseks olevad dokumendid. Tuleb tagada, et dokumendid säiliksid täies mahus ja muudatusteta.
- Büroo 1: selles bürooruumis sisestatakse kuluhüvitiste aluseks olevad andmed ning kontrollitakse kuluhüvitiste arvutuslikku õigsust ja nende põhjendatust. Nende protsesside korrektsuse säilitamiseks tuleb tagada, et volitamata isikutel puuduks juurdepääs nendele töökohaarvutitele.
- Büroo 2: selle büroo tööarvuti taga toimub töölähetuskulude väljamaksmisotsuse tegemine. Nimetatud ülesannet tohib täita vaid selleks volitatud isik. Volitamata isikutele on juurdepääs keelatud.

		Serveriruum	Kuludokumentide arhiiv	Büroo 1	Büroo 2
1.	LAN võrgu administreerimine	X			
2.	Audit	X	X	X	X
3.	Andmesisestus			X	
4.	Andmetöötlus ja arvutuse kontroll		X	X	
5.	Andmetöötlus ja kulupõhjendus		X	X	

6.	Ettekirjutuse tegemise õigus	X	X	X

3. Samm: süsteemi ja võrgu pääsuõiguste andmine

Lähtudes isikute tööülesannetest, pandi paika järgnevad süsteemi ja võrgu pääsuõigused:

		Serveri operatsiooni-süsteem	Protokollide läbitööta-mine	Andme-sisestus	Kuludokumentide läbitööta-mine
1.	LAN võrgu admini-streerimine	X			
2.	Audit	X	X		X
3.	Andmesisestus			X	
4.	Andmetöötlus ja arvutuse kontroll				X
5.	Andmetöötlus ja kulupõh-jendus				X
6.	Ettekirjutuse tegemise õigus				X

4. Samm: Rakenduste ja andmete pääsuõiguste andmine

Järgnevalt kirjeldatakse pääsuõiguseid, mida töötajad oma tööülesande täitmiseks vajavad. Selgitus:

- U = rakenduse/tarkvara kasutamise õigus
- R = andmete lugemise õigus
- C = andmete kirjutamise, st andmete tekitamise õigus
- A = andmete muutmise õigus
- D = andmete kustutamise õigus
- S = väljamaksete allkirjaga kinnitamise õigus

		Serveri operatsiooni-süsteem	Protokollide läbitööta-mine	Andme-sisestus	Kuludokumentide läbitööta-mine
1.	LAN võrgu admini-streerimine	U,R,C,A,D			

2.	Audit	U,R	U,R,D		U,R
3.	Andmesisestus			U,C	
4.	Andmetöötlus ja arvutuse kontroll				U,R,A
5.	Andmetöötlus ja kulupõh-jendus				U,R,A
6.	Ettekirjutuse tegemise õigus				U,R,S

Niisugune dokumentatsioon hõlbustab õiguste jagamist. Oletame näiteks, et pr Kask on vahetanud töökohta ja talle tuleb leida asendaja. Eespool toodud tabeli abil on suhteliselt lihtne teada saada, millised varem pr Kasele kuulunud õigused tuleb kustutada ja uue töötaja jaoks uuesti sisse seada. Juhul kui uus töötaja peaks lisaks oma tavapärastele töökohustustele täitma asenduse korras ka veel andmetöötluse ülesandeid koos ettekirjutuse tegemise õigusega, tuleb kohustusliku õiguste jaotamise protsessi käigus ilmsiks konflikt, st uuel töötajal oleks niisugusel juhul võimalik andmetega märkamatult manipuleerida.

Kontrollküsimused:

- Kas välja jagatud pääsuõiguste dokumentatsiooni hoitakse ajakohasena?
- Kas pääsuõiguste taotlusi ja väljajagatud õiguste muutumist kinnitab ja kontrollib selle eest vastutav töötaja?
- Kas seoses rakenduste ja andmete pääsuõiguste äravõtmisega on olemas kindel kord?

M 2.9 Aktsepteerimata riist- ja tarkvara kasutuse keeld

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT-juht, IT turvaosakond

Rakendamise eest vastutavad: IT-juht

On vägagi tavapärane, et töötajad kasutavad kas tööülesannete täitmiseks või siis lihtsalt tööl olles isiklikke riist- ja tarkvaralahendusi, nagu nt mobiiltelefonid, pihuarvutid või kaamerad. Kuna lisariistvara kasutamine muutub standardsete ühenduste (nt USB) ja aina rohkem levivate isehäälestuvate funktsioonide tõttu üha lihtsamaks, tuleb nende kasutamist reguleerida. USB kaudu töötavad salvestid (nt kõvakettad, mälupulgad) ja isiklikus kasutuses olevad pihuarvutid võivad mõjutada IT turvalisust. Seetõttu peab olema reguleeritud, kuidas tohib vastavat riist- ja tarkvara vastu võtta, installeerida ja kasutada. Kohustuslikud meetmed nimetatud valdkonnas on näiteks järgmised: M 2.62 Tarkvara vastuvõtuprotseduurid ja M 2.216 IT-komponentide kinnitamise protseduur , täpsemalt moodul B 1.10 Tüüptarkvara .

Tüüptarkvara ning meede M 4.4 Eemaldatavate andmekandjate draivipilude ja väliste andmekandjate nõuetele vastav kasutamine .

Mittesoovitud riist- ja tarkvara installeerimine ja kasutamine tuleb keelata ja muuta see lisaks ka tehniliste lahendustega nii palju kui võimalik võimatuks. Enamik operatsioonisüsteeme võimaldab seda teha kasutajakeskkonna piiramisega. Piiramise eesmärk on hoida ebasoovitavad programmid ja nende mõjud süsteemist eemal. Lisaks eelnevale tuleb tagada, et süsteemi ei oleks võimalik kontrollimatult kasutada väljaspool selle kindlaksmääratud funktsioone. Mõttekas võib olla ka kasutamiskeelu laiendamine isiklike andmete importimisele (nt makroviiruste leviku ennetamiseks). Tarkvara puhul tuleb dokumenteerida, millised käitusfailide versioonid on aktsepteeritud (koos faili loomiskuupäeva ja faili suurusega). Aktsepteeritud programmide puhul tuleb reeglipäraselt kontrollida, kas on tekkinud muudatusi. Aktsepteerimata riist- ja tarkvara kasutuskeeld tuleb fikseerida kirjalikult ning teha kõikidele töötajatele teatavaks. Erandeid puudutav regulatsioon peab sisaldama ka erandite tagasivõtmise õigust.

Kontrollküsimused:

- Kas riist- ja tarkvara puhul on olemas kasutusloa saamise ja registreerimise protsess?
- Kas kasutamiskeelud on kirjalikult fikseeritud?
- Kas kõik töötajad on kasutuskeeldudest teadlikud?
- Kas töötajaid teavitatakse kehtivatest kasutuskeeldudest regulaarselt?
- Mil moel on võimalik keelatud tarkvara installeerida ja kasutada?
- Millised on võimalused üksikutel arvutitel tarkvara iseseisvalt edasi arendada?
- Kas efektiivsete tüüptarkvara makrode, nt tekstitöötlus, tabelarvutus ja andmebaasid, programmeerimine ja edasiandmine on reguleeritud?
- Kas aktsepteeritud käitusfailide versioonide kohta on olemas nimekirjad, mis sisaldavad muu hulgas ka loomiskuupäeva ja faili suurust?
- Kas kontrollitakse regulaarselt, ega aktsepteeritud käitusfailide versioone pole muudetud?

- Kas tehnilised võimalused tarkvara installeerimise takistamiseks on olemas?
- Kas väliste salvestite (nt USB mälupulkade, kaamerate, pihuarvutite ja mobiiltelefonide) kasutamine on reguleeritud?

M 2.10 Riistvara ja tarkvara inventuur

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT-juht, IT turvaosakond, juhatajad

Rakendamise eest vastutavad: IT turvaosakond

Keelatud riist- ja tarkvara kasutamise tuvastamiseks on hädavajalik, et riist- ja tarkvara inventuuri tehtaks regulaarselt. Juhul kui IT-süsteemide arv on väga suur, võib kasutada pistelist kontrollimeetodit. Inventuuri tulemused tuleb dokumenteerida, et ka korduvaid rikkumisi oleks võimalik avastada. Kui inventuuri käigus leitakse keelatud riistvara, tuleb hoolitseda selle eest, et vastavate IT-komponentide eeskirjadevastane kasutamine lõpetataks. Sellele lisaks tuleb välja selgitada, kes on väärkasutuse eest vastutav, et olukorrale vastavalt reageerida.

Konkreetsete kahtluste korral tuleks riistvara inventuuri tehes uurida võimalikku seadmetega manipuleerimist ja otsida lisaseadmeid, mida võidakse kasutada nt klaviatuuri klahvivajutuste salvestamiseks. Keelatud tarkvara leidude korral tuleks korraldada ka nende eemaldamine. Inventuuride läbiviimiseks peab kontrollival organil olema ettevõtte või ametiasutuse väljastatud sellekohane luba. Lisaks peab kontrollivale organile olema teada, millistel IT-süsteemidel millist tarkvara kasutatakse (kasutatava tarkvara loetelu). Kuna reeglina on kasutuses oleva tarkvara loetelu väga mahukas, tuleks kasutatava tarkvara loetelu efektiivseks koostamiseks kasutada sobiliku programmi abi. Tüüpilise klient-server-keskkonna tarbeks peaks see olema võrgu toega.

Enne riist- ja tarkvarainventuuri läbiviimise reeglite kehtestamist tuleks sellesse kaasata ka ettevõtte või ametiasutuse töötajate esindajad. Üksikute IT-süsteemide puhul, mis ei ole terviksüsteemi igapäevatöös määrava tähtsusega, nt testimissüsteemid, võib reeglipärase kontrollimise asemel kasutada vajadusest lähtuvat kontrollimeetodit. Näiteks võib vastavaid IT-süsteeme kontrollida neil juhtudel, kui konfiguratsiooni on muudetud või kui vastav IT-süsteem on eelnevalt pikemat aega seisnud. Eelduseks on siiski, et meede M 2.9 Aktsepteerimata riist- ja tarkvara kasutuse keeld .

Kontrollküsimused:

- Millise ajavahemiku tagant toimub riistvara ja tarkvara inventuur?
- Kas on esinenud aktsepteerimata tarkvara kasutamise juhtumeid?
- Kuidas toimitakse rikkumise avastamise korral?

M 2.11 Paroolide kasutamise reeglid

Algatamise eest vastutavad: IT-juht, IT turvaosakond

Rakendamise eest vastutavad: IT turvaosakond, kasutajad

Juhul kui IT-süsteemis rakendatakse kasutajate autentimiseks paroole, sõltub süsteemi kasutus- ja pääsuõiguste turvaline haldus suurel määral sellest, kas paroole kasutatakse korrektselt või mitte. Seetõttu on soovitatav koostada paroolide kasutamise reeglid ja kasutajad vastava infoga kurssi viia.

Reaalne kompromiss

Paroolide kasutamise reeglistik peab kujutama endast alati reaalset kompromissi järgmiste turvaeesmärkide vahel:

- parool peaks koosnema erinevatest sümbolitest ja olema piisavalt keeruline, et seda oleks raske ära arvata;
- võimalike paroolide arv peaks etteantud skeemis olema piisavalt suur, et lühikese aja jooksul ei oleks võimalik läbiproovimise teel õige paroolini jõuda;
- parool ei tohi olla liiga keeruline, et kasutajal oleks võimalik seda ilma suure pingutuseta meelde jätta.

Reeglid kasutajatele

Paroolide kasutamisel tuleb pöörata tähelepanu järgmistele reeglitele:

- parool ei tohi olla kergesti aimatav. Seetõttu ei sobi paroolideks näiteks nimed, auto numbrimärgid, sünnikuupäevad jms;
- paroolis tuleks kasutada vähemalt ühte sümbolit, mis ei ole täht (märk või number);
- kui parooli jaoks on võimalik valida tähti ja numbreid, peab parool olema vähemalt kaheksakohaline.

Tõkestus pärast ebaõnnestunud katseid

- juhul kui parooliks on võimalik valida ainult numbreid, peaks parool olema vähemalt kuuekohaline ja lisaks peaks autentimissüsteem ebaõnnestunud sisenemiskatsete korral juurdepääsu sulgema (teatud ajaks või püsivalt);
- testimisega tuleb välja selgitada, kui palju parooli sümbolikohti arvuti reaalselt kontrollib;
- eelseadistusega määratud paroolid (nt tootja poolt süsteemide tarnimisel) tuleb asendada isiklike paroolidega;
- paroole ei tohi salvestada programmeeritavate funktsiooniklahvide alla;
- parooli tuleks hoida saladuses ja seda peaks teadma vaid kasutaja.

Parooli deponeerimine kinnises ümbrikus

- parooli talletamiseks tuleks see kindluse mõttes kirja panna, kuid vastaval juhul tuleb see kindlasti suletud ümbrikus kindlasse kohta hoiule panna. Kui parool kirjutatakse veel kuhugi üles, tuleb seda hoida vähemalt sama turvalistes oludes, nagu hoitakse tšekiraamatut või raha (vt M 2.22z Paroolide deponeerimine);

- parooli tuleb regulaarselt muuta, nt iga 90 päeva tagant;
- kui volitamata isikud on parooli teada saanud või kui tekib sellekohane kahtlus, tuleb parool ära muuta;
- pärast paroolide muutmist ei tohiks vanu paroole enam uuesti kasutada;
- parooli sisestamine ei tohiks toimuda kõrvaliste isikute pilgu all.

Nõuded IT-süsteemidele

Kui IT-süsteemi tehnilised võimalused seda lubavad, tuleks arvestada järgmiste raamtingimustega:

- triviaalsete kombinatsioonide valimist paroolideks (nt. „BBBBBBBB", „123456") tuleks takistada;
- kõigil kasutajatel peab olema võimalus oma parooli igal ajal muuta.

Ühekordsed paroolid

- uute kasutajate esmakordseks süsteemi sisenemiseks tuleks neile jagada ühekordsed paroolid, mis tuleb kohe pärast esimest kasutamist ära muuta. Võrkudes, kus paroolid edastatakse krüpteerimata kujul, on soovitatav kasutada ühekordseid paroole pidevalt (vt M 5.34z Ühekordsed paroolid);
- pärast kolmekordset parooli valesti sisestamist peaks autentimissüsteem vastava juurdepääsu sulgema (teatud ajaks või püsivalt). Suletud paroole võivad taastada ainult vastavate õigustega isikud, nt selleks volitatud administraatorid või spetsiaalsed kasutajate haldamisega tegelevad töötajad. Täpsemat teavet selle kohta leiate meetmest M 2.402z Paroolide uuendamine ;
- võrguühendusega süsteemides ei tohiks krüpteerimata paroolide edastamist kasutada isegi mitte intraneti autentimisprotsessis. Kui autentimisprotsess toimub läbi ebaturvalise võrgu, ei tohi paroole mingil juhul edastada krüpteerimata kujul;
- parooli sisestamisel ei tohi parool olla arvutiekraanil näha;
- paroolid peavad olema süsteemi salvestatud selliselt, et neile ei oleks võimalik ligi tungida, nt ühesuunaline krüpteerimine (räsifunktsioonid);
- süsteem peaks kohustama kasutajat regulaarselt parooli muutma;
- IT-süsteem peaks takistama vanade paroolide kasutamist parooli vahetamisel (paroolide ajalugu).

Kontrollküsimused:

- Kas töötajad on saanud koolituse paroolide korrektseks kasutamiseks?
- Kas paroolide sobivust kontrollitakse?
- Kas paroolide vahetamine on kohustuslik?
- Kas iga võrgus olev kasutaja on varustatud isikliku parooliga?
- Kas kasutajatel on soovitatud kasutada piisava keerukusega paroole, mis vastavad kaitsevajadusele?
- Kas testitakse, mitut parooli sümbolikohta IT-süsteem tegelikult kontrollib?

- Kas paroolid vahetatakse kohe ümber, kui need on saanud teatavaks volitamata isikutele või on olemas selline kahtlus?
- Ebaõnnestunud sisselogimiskatsete korral: ega ei anta teada, kas kasutajatunnus ja/või parool olid valed?

M 2.12 IT-kasutajate nõustamine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT-juht

Rakendamise eest vastutavad: IT-juht

IT-süsteemide kasutamine eeldab ka töötajate laiaulatuslikku koolitust. Lisaks nendele koolitustele, mis peavad õpetama töötajaid IT-süsteeme otstarbekohaselt kasutama, läheb tarvis ka IT kasutajate pidevat abistamist ja nõustamist tööülesannete täitmisel esilekerkivate probleemide lahendamisel. Vastavate probleemide põhjused võivad näiteks peituda riistvara defektides või tarkvara vigases installeerimises, samuti võib põhjuseks olla IT väär kasutamine. Kõik kasutajad peaksid teadma, kelle poole nad oma IT-d puudutavate probleemidega peavad pöörduma.

IT tugitöötajad peaks oma töös märkama ka viiteid võimalikele turvaprobleemidele ja edastama need sobivasse kohta, nt IT turvaosakonnale.

Operatiivne IT-tugi

Suuremate institutsioonide puhul võib olla mõttekas koondada IT kasutajate tugi ühte keskusesse, kuhu kõik töötajad võivad soovi korral pöörduda. Suure arvu detsentraliseeritud IT-süsteemide, nagu nt PCde kasutamisel võib vastav lahendus olla koguni hädavajalik. Niisuguse lahenduse korral on tarvis tagada, et IT-tugi oleks töötajatele nende tööajal kättesaadav, et tagada IT-alaste probleemide kiire lahendamine. Muutuva töögraafiku tõttu ei pruugi kõik IT kasutajad alati kindlatel kellaaegadel kohal viibida, seetõttu tuleks määrata teatud tugiteenuse osutamise ajad, mis arvestavad institutsiooni vajaduste ja kellaaegadega, mil suurem osa töötajatest viibib oma töökohal.

Telefoni abiliin

IT kasutajate nõustamiseks tuleks sisse seada telefoni abiliin, kuna paljusid probleeme on võimalik telefoni teel kiiremini lahendada kui kirjavahetusega. Ainult e-postil põhinev IT-tugi ei ole piisav, kuna IT-süsteemi, serveri või võrgu väljalangemise korral ei pruugi probleemi kirjeldamine seda kanalit pidi enam võimalik olla.

Kontrollküsimused:

- Kelle poole võivad IT kasutajad oma probleemidega pöörduda?
- Kas on tagatud, et IT-alaste probleemide lahendamine toimub operatiivselt?

M 2.13 Tundlike ressursside jäljetu hävitamine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT-juht, IT turvaosakond

Rakendamise eest vastutavad: tehnika juht, kasutaja

Tundlikku informatsiooni sisaldavaid kulu- ja töövahendeid, (väljatrükid, disketid, striimeri lindid, magnetlindid, kõvakettad, CD-ROM-id, USB mälupulgad ning spetsiaalsed toonerikassetid, kopeerpaber või kopeerlindid), mida enam ei kasutata või mis tuleb defekti tõttu kasutusest kõrvaldada, tuleb käidelda selliselt, et seal olnud andmeid ei oleks võimalik enam kasutada. Töökorras andmekandjatel olevad andmed tuleks füüsiliselt kustutada. Defektsed või ühekordselt kirjutatavad andmekandjad, nagu nt CD-ROM-id tuleb mehaaniliselt hävitada (vt M 2.216 IT-komponentide kinnitamise protseduur). Tundlikku infot sisaldava materjali käitlemine tuleks reguleerida eraldi ettekirjutusega ja tagada tuleks vastavate käitlusvahendite olemasolu. Juhul kui tundlikku infot sisaldav materjal kogutakse enne käitlemist kokku, tuleb seda hoida luku taga ja takistada volitamata isikute juurdepääsu. Kui ettevõte või ametiasutus ei suuda ise keskkonnasõbralikku ja turvalist käitlemist tagada, tuleb käitlemisega tegelevad firmad, kelle käest vastavat teenust ostetakse, kohustada vajalikest IT turvameetmetest kinni pidama.

Kontrollküsimused:

- Kas nimetatud reeglistik hõlmab igat liiki tundlikke materjale?
- Kas käitlemise protsess on usaldusväärne?
- Kas nimetatud käitlemiseeskirjadest peetakse kinni?
- Kas tundlike ressursside hävitamiseks on hangitud asjakohased vahendid, nt paberipurustajad?
- Kui hävitamisele eelneb kogumine, siis kas hävitamiseks mõeldud tundlikud ressursid on kaitstud volitamata juurdepääsu eest?
- Kas ressursside hävitamisteenust osutavates ettevõtetes kontrollitakse regulaarselt, kas hävitamise protseduur vastab nõuetele?

M 2.14 Võtmete (ja kaartide) haldus

Algatamise eest vastutavad: organisatsiooni juht, IT turvaosakond

Rakendamise eest vastutavad: tehnikajuht

Kõikide hoones kasutatavate võtmete kohta (korrused, koridorid ja ruumid) tuleb koostada lukustusskeemid. Võtmete tegemine, hoidmine, haldamine ja väljastamine peaks toimuma tsentraliseeritult. Võtmetest peavad olemas olema ka varukomplektid ning neid tuleb hoida turvalises paigas. Sama kehtib ka identifitseerimisvahendite, nagu magnet- või kiipkaartide kohta.

Tähelepanu tuleks pöörata alljärgnevale:

- kui hoones on olemas sulgemissüsteem, tuleb kaitset vajavad ruumid jaotada eraldi lukustusgruppidesse. Vajaduse järgi tuleb üksikud ruumid lukustusgrupist välja jätta ja varustada eraldi suletava süsteemiga;
- väljastamata võtmeid ja võtmete varukoopiaid tuleb hoida selliselt, et volitamata isikute juurdepääs oleks välistatud;
- võtmeid tohib väljastada vaid volitatud isikutele, kui vastav soov on põhjendatud ja mõistetav, võtmete vastuvõtjad peavad väljastamise kinnitama ning protsess peab olema dokumenteeritud. Ka asenduste korral ei tohi töötajad võtmeid lihtsalt üksteisele edasi anda. Töötaja annab võtme ära ja asendaja saab võtme kohast, kus neid väljastatakse. Ainult niisugust süsteemi järgides on võimalik tagada, et võtmete asukohad on alati teada ja vastav dokumentatsioon täielik;
- kindlaks tuleb määrata meetmed, mis võetakse üksikute võtmete kadumise korral (kadumisest teatamine, asendamine, kulude hüvitamine, olenevalt olukorrast uurida tagastamisnõude kohaldamist hooletuse tõttu, luku väljavahetamine, lukustusgruppide väljavahetamine jne);
- töötajate vastutusala muutumisel tuleb üle vaadata ka lukustamise volitused ja ebavajalikud võtmed tagasi võtta;
- töötajate lahkumisel tuleb kõik võtmed tagasi nõuda (lahkumislehel tuleb viimaste kohustuslike tööülesannete loetellu lisada ka võtmete tagastamine);
- erilist kaitset vajavate ruumide lukke ja võtmeid (vastavaid võtmeid tuleks väljastada vaid üksikud eksemplarid) tohib kahtluse korral vahetada ka ilma eelneva etteteatamiseta, et kõrvaldada võimalus illegaalselt juurde tehtud võtmete kasutamiseks.

Kontrollküsimused:

- Kuidas on reguleeritud võtmete haldamine?
- Kas asenduste puhul kehtivast võtmetega ümberkäimise korrast peetakse kinni?
- Kas töötajad aktsepteerivad vastavaid reegleid?

M 2.15 Tuleohutuse kontroll

Algatamise eest vastutavad: tehnika juht, IT-juht

Rakendamise eest vastutavad: tuleohutusspetsialist

Hoonete ehitamisel ja kasutamisel tuleb järgida kõiki kehtivaid tuleohutuse eeskirju. Vastavaid eeskirju täiendavad ehitusjärelvalve eeskirjad (vt M 1.6 Tuletõrjeeeskirjade täitmine). Kogemused näitavad, et hoones kasutuselevõtmisel ja igapäevatöös jäetakse vastavad tuleohutuseeskirjad üha rohkem tagaplaanile ning vahel eiratakse neid täielikult. Mõningad näited:

- Väljapääsud on tõkestatud mööbli või paberivarudega.
- Tule- ja suitsukindlaid uksi hoitakse lahti ukse alla pistetavate kiilude abil.
- Lubatud tulekoormust ületatakse kaablite lisamise või kasutuse muutmisega.
- Tööde käigus avatakse ja/või vigastatakse tuletõkked ning pärast tööde lõppu ei asetata neid tagasi oma kohtadele.
- Niinimetatud suitsunurga ligiduses olevad suitsuandurid lülitatakse teadlikult välja.

Tuleohutuse kontrollkäigud peaksid toimuma üks kuni kaks korda aastas etteteatamisega või ilma. Kuna reeglina ei ole töötajate poolt tehtud vead ajendatud halbadest kavatsustest, vaid tööst tulenevast hädavajadusest või mugavusest, ei saa tuleohutuse kontrollkäikude eesmärgiks seada rikkujate leidmist ja karistamist. Pigem peaks kontrollkäigu eesmärgiks olema võimalike puuduste, võimalusel ka nende põhjuste, kohene likvideerimine.

Kontrollküsimus:

- Kas tuleohutuse kontrollkäike tehakse regulaarselt ning kas tuvastatud puudused likvideeritakse?

M 2.16 Välispersonali ja külastajate valve ja saatmine

Algatamise eest vastutavad: organisatsiooni juht

Rakendamise eest vastutavad: töötajad

Kas ma saan Teid aidata?

Isikud, kes ei kuulu institutsiooni koosseisu, nagu nt külastajad, remonditöölised, hooldetehnikud ja koristajad, ei tohiks ruumides viibida ilma järelevalveta, välja arvatud ruumides, kus see on sõnaselgelt lubatud (vt M 2.6 Sissepääsuõiguste andmine). Kõikidele töötajatele tuleb selgitada, et võõrad isikud, keda kohatakse ametiasutuse või ettevõtte territooriumil ilma saatjata ringi liikumas, tuleb alates kohtumise hetkest oma hoolitsuse ja järelevalve alla võtta. See ei ole vajalik mitte ainult turvalisuse tagamiseks, vaid jätab võõrastele ka organisatsioonist hea mulje. Juhul kui väljastpoolt pärit isik tuleb büroosse üksi jätta, tuleks paluda mõnel kolleegil senikaua ruumis viibida või juhatada isik mõne kolleegi juurde. Kui väljastpoolt tulnud isikuid ei ole võimalik pidevalt saata või valvata (nt koristajad), tuleks vähemalt isiklik töökeskkond lukustada: kirjutuslaud, kapp ja PC (disketiseadme lukk, klaviatuurilukk), vt M 2.37 Korrastatud töölaud.

Ka oma kodus ei tohi tööpabereid laokile jätta

Ka koduse töökoha puhul kehtib nõue, et perekonnaliikmed ja külalised tohivad üksi koduses töökohas viibida vaid juhul, kui kõiki töödokumente hoitakse luku taga ja kasutatav IT-süsteem on vastavate pääsuõiguste abil kaitstud. Vastavad meetmed tuleb turvapoliitikasse sisse kirjutada ja nende hädavajalikkust tuleb töötajatele selgitada. Võõraste isikute kohalviibimise dokumenteerimiseks võib kasutada külalisteraamatut.

Kontrollküsimused:

- Kas töötajaid on korduvalt teavitatud sellest, millist käitumist neilt oodatakse?
- Kuidas asjad majas tegelikult toimivad?

M 2.17 Sisenemisreeglid ja reguleerimine

Algatamise eest vastutavad: organisatsiooni juht, majas kasutatava tehnoloogia juht

Rakendamise eest vastutavad: tehnikajuht, töötajad, planeerijad

Sisenemine kaitset vajavatesse majaosadesse ja ruumidesse peab olema reguleeritud ning seda tuleb kontrollida (vt M 2.6 Sissepääsuõiguste andmine). Meetmed võivad selle puhul alata lihtsa võtmete väljastamise kontrolliga ja lõppeda keeruliste isikuid eristavate identifitseerimissüsteemidega, kusjuures luku avamine mehaanilise võtmega võib samuti sisenemise reeglite hulka kuuluda.

Sisenemise reguleerimiseks ja kontrollimiseks on vajalik:

- selgelt märgistada reeglite alla kuuluv ala,
- hoida sissepääsuõigusi omavate inimeste ring nii väike kui võimalik; vastavad isikud peaksid teadma üksteise volitusi, et võõraid isikuid oleks võimalik võõrastena tuvastada,
- enne sisenemisloa andmist võõrastele isikutele (külalistele) kontrollida, kas see on vajalik,
- väljastatud sissepääsuload dokumenteerida.

Õiguste jagamisest üksi ei piisa, õigustest kinnipidamist ja üleastumisi tuleb kontrollida. Kontrollimehhanismide väljatöötamisel tuleks lähtuda põhimõttest, et lihtsad ja teostatavad lahendused on tihti sama tõhusad kui keeruline tehnoloogia.

Mõningad näited:

- informatsioon ja õiguste tundlikumaks muutmine,
- teavitamine õiguste muutumisest,
- majalubade kandmine nähtaval kohal, vajadusel külastajapääsmete väljastamine,
- külastajate saatmine,
- kindlaksmääratud käitumine volituste ületamise avastamisel ning
- volitamata sissepääsu tõkestamine (nt ühepoolselt avatav uks, volitatud isikutele ukselukk ja võti, külalistele kella helistamise võimalus).

Sisenemise kontrollimiseks läheb tarvis erinevaid ehituslikke, organisatsioonilisi ja isiklikke meetmeid. Nende koostoime peaks olema reguleeritud sissepääsu kontrollikontseptsiooniga, mis määrab üldnõuded turvaala, hoone ja seadmete kaitsmiseks.

Siia alla kuuluvad:

- Turvatsoonide piiritlemine - Kaitsmist vajavate alade hulka võivad kuuluda kinnistud, hooned, serveriruumid, lisaseadmetega ruumid, arhiivid, kommunikatsiooniseadmed ja hoones kasutav tehnika. Kuna vastavate alade turvanõuded on teineteisest erinevad, võib olla mõttekas jaotada need eraldi turvatsoonidesse.
- Sissepääsuõiguste andmine (vt M 2.6 Sissepääsuõiguste andmine)
- Sissepääsu kontrollimise eest vastutava töötaja määramine - Sissepääsuõiguste jagamisel üksikutele töötajatele lähtub vastav isik turvapoliitikas määratud üldpõhimõtetest.

- Ajalise sõltuvuse defineerimine - Tuleb välja selgitada, kas sissepääsuõigustele on tarvis kehtestada ajalisi piiranguid. Ajalisteks piiranguteks võivad olla näiteks sisenemisluba ainult töö ajal, luba siseneda kord päevas või teatud kindla kuupäevani kehtiv sissepääsuluba.
- Tõestamisprotsessi määratlemine - Siinkohal on tarvis määrata, millised andmed tuleb kaitstud alasse sisenemisel ja sealt väljumisel protokollida. Eriti hoolikalt tuleb läbi kaaluda süsteemi käitaja turvalisuse huvid ja iga üksiku süsteemikasutaja privaatsfääri kaitsmise huvid.
- Erakorralisteks sündmusteks ettevalmistumine - Muuhulgas on tarvis tagada, et tulekahju korral oleks võimalik töötajatel kiiresti ohutsoonidest lahkuda.
- Täiendavalt võib olla mõttekas erineva kvaliteediga lubade lugemisseadmete, lüüside ja töötajate separaatorite paigaldamine. Võtmete haldamise kohta lugege meedet M 2.14 Võtmete (ja kaartide) haldus .

Arvutuskeskuste tähtsamate osade puhul tuleb ilmtingimata kasutada rangeid sissepääsu kontrollimehhanisme. Identifitseerimis- ja autentimismeetoditena tulevad siinkohal kõne alla omand, teadmised ja biomeetrilised tunnused. Tugev sissepääsukontroll peab arvestama vähemalt ühe eelnevalt loetletud meetodiga. Praegu saadaolevale informatsioonile toetudes võib öelda, et biomeetrilistest kontrollimehhanismidest üksi ei piisa. Sissepääsu kontrollivaid terminale tuleb kaitsta võimalike manipulatsioonide eest. Selleks tuleb terminalid paigaldada nõnda, et andmete sisestamisel säiliks nende konfidentsiaalsus. Lisaks peaksid kõik andmesisestuseks vajalikud mehhanismid olema seadmes omavahel kombineeritud, nt klahvistik PIN koodi sisestamiseks. Juhul kui kõik andmesisestuse mehhanismid ei ole koondatud ühte seadmesse, peaks nendevaheline andmete edastamine toimuma krüpteeritult. Näiteks kontaktivaba pääsulubade lugemisseadme kasutamise puhul peab kaardi ja lugemisseadme vaheline andmeedastus olema krüpteeritud.

Kontrollküsimused:

- Kas sissepääsu kontrollimiseks on olemas vastav kontseptsioon?
- Kas sissepääsu kontrollimeetodite tõhusust kontrollitakse pidevalt?

M 2.18z Kontrollringkäigud

Algatamise eest vastutavad: tehnikaosakond, IT turvaosakond

Rakendamise eest vastutavad: tehnikaosakond, IT turvaosakond

Igasugused meetmed toimivad nii hästi kui hästi neid osatakse ellu viia. Kõige lihtsam lahendus kohustuslike meetmete rakendamise ning eeskirjade ja juhiste järgimise kontrollimiseks on teha vastavaid kontrollkäike. Kontrollkäikude põhieesmärk ei tohiks olla reeglite eirajate tuvastamine, et neid seejärel karistada. Esmajoones peaks kontrollkäikude eesmärk olema see, et võimalikud vajakajäämised saaksid kohe kõrvaldatud (akende sulgemine, laokil dokumentide hoiustamine jne). Tähtsuselt järgmine tegevus on võimalike põhjuste tuvastamine, et neid vajakajäämisi tulevikus vältida. Kontrollkäike võib läbi viia ka tööajal, kuna samal ajal on võimalik töötajaid ka reeglitest teavitada. Niimoodi aktsepteeritakse reegleid paremini, kuna mõistetakse, et reeglid on mõeldud abistamiseks, mitte ahistamiseks.

M 2.19 Neutraalne dokumentatsioon jaotuskilbis

Algatamise eest vastutavad: tehnikajuht

Rakendamise eest vastutavad: tehnikajuht, planeerija

Igas jaotuskilbis peaks olema vastav dokumentatsioon, mis kajastab hetkel kasutuses olevaid jaotusi ja juhtmete hõivamist. Vastava dokumentatsiooni sisu tuleb hoida võimalikult neutraalsena. Loetleda tuleks vaid kasutuses olevad ühendused. Erinevate kaablite kasutusala kirjeldusi tuleks vältida, välja arvatud juhud, kui seadus seda kohustab (tuleohutussüsteemide kaablid). Kaablinumbrid, jaotuskilbi ja ruumide numbrid on paljudel juhtudel infoks täiesti piisavad. Kogu täiendav informatsioon tuleb koguda auditidokumentidesse.

Kontrollküsimused:

- Kuidas tagatakse dokumentatsiooni pidev värskena hoidmine?
- Kuidas tagatakse, et vastav dokumentatsioon ei sisaldaks lubamatuid andmeid?

M 2.20 Liinide kontroll

Algatamise eest vastutavad: tehnikajuht, IT-juht

Rakendamise eest vastutavad: tehnikajuht, planeerija

Kõik juhtmestiku jaotuskohad ja jaotuspesad tuleb regulaarselt (vähemalt pisteliselt) üle kontrollida.

Sealjuures tuleb pöörata tähelepanu järgnevale:

- Kas suletud jaotuskohtades esineb jõuga lahtimurdmise tundemärke?
- Kas jaotuskohas olev dokumentatsioon on värske või aegunud?
- Kas tegelikud lülitus- ja jaotusgrupid ning sellekohane dokumentatsioon langevad omavahel kokku?
- Kas mittevajalike kaabliliinide lühiühendused ja maandused on puutumata?
- Kas esineb volitamata täiendusi või muudatusi?

Lisaks vaatluskontrollile võib täiendavalt läbi viia ka funktsiooni kontrollimist. Funktsiooni testimisel tehakse kindlaks, kas vastavaid liine on tarvis ning kas nende tehnilised näitajad vastavad normidele. Kaabliühenduste puhul, mis jäävad väljapoole kaitstud alasid, tuleks vastav kontroll läbi viia kahel juhtumil:

- Ühendused, mida kasutatakse väga harva ja mille puhul pole võimalik manipulatsioone kohe ära tunda.
- Ühendused, mille kaudu edastatakse tihti ja reeglipäraselt eriti konfidentsiaalset informatsiooni.

Kõik kõrvalekaldumised, mis vaatluskontrolli või funktsiooni testimise käigus avastatakse, tuleb viivitamata kirja panna ja edastada organisatsiooni vastutavale osakonnale, et vajalike vastumeetmete algatamine toimuks võimalikult operatiivselt. Tähtis on, et leitud kõrvalekaldumised ei saaks mitte ainult kõrvaldatud, vaid et selgitataks välja ka nende põhjus.

Kontrollküsimused:

- Milliste ajavahemike järel toimub olemasolevate liinide kontrollimine?
- Kas leitud kõrvalekaldumised pannakse kirja ja neid uuritakse?
- Kas on määratud, kellele tuleb leitud kõrvalekaldumisest teatada?
- Kelle vastutusealasse kuulub puuduste kõrvaldamine ning kes peab vastavaid töid kontrollima?

M 2.21 Suitsetamiskeeld

Algatamise eest vastutavad: tehnikajuht

Rakendamise eest vastutavad: töötajad

Ruumides, kus hoitakse IT-seadmeid või andmekandjaid (serveriruumis, andmekandjate arhiivis, aga ka kuludokumentide arhiivis), kus tulekahjud või määrdumine võivad põhjustada suuri kahjusid, peaks kehtima suitsetamiskeeld. Lisaks tuleohtlike olukordade ennetamisele, aitab suitsetamiskeeld tagada ka IT-seadmete mehaanilist tööfunktsiooni.

Kontrollküsimus:

- Kas kaitset vajavates ruumides peetakse suitsetamiskeelust kinni?

M 2.22z Paroolide deponeerimine

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: kasutajad

Paroolkaitsega varustatud IT-süsteemide puhul tuleb võtta meetmed, mis võimaldavad selle süsteemi kasutamist ka siis, kui töötaja viibib eemal, nt puhkusel või haiguslehel, et ka tema asendajale oleks tagatud juurdepääs IT-süsteemile. Selleks on olemas erinevaid võimalusi, mis sõltuvad kasutatavatest IT-süsteemidest, täpsemalt IT-rakendustest ja vastava organisatsiooni turvapoliitikast. Üks võimalus on näiteks paroolide deponeerimine sobivas kohas. Tavapäraste mitme kasutajaga süsteemide puhul võib administraator väljastada vajaminevad kasutajaõigused või muuta olemasolevat parooli. Paljud IT-süsteemid ja IT-rakendused võimaldavad kasutajagruppide loomist, mille abil saab sisestada võimalikud asendajad ja defineerida nende kasutajaõigused. Kõikidel äsja loetletud lahendustel on nii oma eelised kui ka puudused, mistõttu tuleb täpselt kaaluda, milline lahendus vastavasse olukorda kõige paremini sobib.

Selgituseks toome siinkohal järgmised näited:

Raamatupidaja pr Kuusk töötab Windowsiga töötava personaalarvutiga, mis on ühendatud kliendina kohtvõrku (LAN). Selleks, et tema asenduse ajal saaksid kõik esile kerkivad tööprobleemid lahendatud, määratleti pr Kuusega tema tööülesanded ja töötati välja vastavad lahendused.

- Kasutajagruppide õigused – raamatupidaja vastutab kõikide partnerfirmadega A–K seotud arvelduste läbitöötamise eest. Tööks vajalikud andmed asuvad andmebaasis, mis omakorda asub serveris PF1. Asenduse puhul on kolleegidel Kask ja Mänd oma kasutajanimede all võimalik kõnealuseid andmeid töödelda, kuna andmebaasis on määratud vastavad kasutajaõigused.
- Töö tulemused peavad kajastuma serveril – Osa pr Kuuse koostatud dokumentidest asub tema personaalarvutis. Eelnevalt tehti kokkulepe, et pr Kuusk tõstab kõik tööks vajalikud failid serveris olevatesse projektikaustadesse. Kui asenduse puhul on tarvis vastavatele andmetele ligi pääseda, on administraatoril võimalus neid õigusi välja jagada. Kõnealune tegevus tuleb kirjalikult fikseerida. Lisaks saab ka pr Kuusk toimunu kohta teavitava e-kirja.
- Klientide haldamiseks kasutab pr Kuusk ühte vana, kuid see-eest vägagi töökindlat IT-rakendust. Kuna vastava rakenduse tehniline lahendus ei võimalda asenduste puhuks juurdepääsuõiguseid muuta, saab asendaja pr Kask pr Kuuse juurdepääsu alt oma parooli. Niimoodi on asendajal võimalik muudatused süsteemi sisse viia.
- Teatud toimingud, mis puudutavad finantsidega ümberkäimist, vajavad digitaalallkirjaga kinnitamist. Selleks on kõikidele töötajatele välja jagatud isiklikud krüptovõtmega kiipkaardid, mille edasiandmine on keelatud. Asenduse puhul kinnitab asendaja kõik toimingud omaenda digitaalse allkirjaga.

Paroolide deponeerimine peab olema läbimõeldud

Igasugune paroolide deponeerimine on alati seotud suure organisatoorsete tööde mahuga. Paroolide deponeerimiseks peavad kõik töötajad toimetama oma vajaminevad kehtivad paroolid teatud kindlasse kohta (nt sulgema ümbrikusse ja andma üle sekretärile, kes paneb need seifi hoiule). Paroolide muutumisel tuleb ka deponeeritud paroolid vastavalt ära muuta. Mitte ühtki parooli ei tohi sealjuures

kahe silma vahele jätta. (Leidub olukordi, kus ühe arvuti rakendustele ligipääsemiseks läheb tarvis kuni viit erinevat parooli). Volitamata isikute juurdepääs deponeeritud paroolidele peab olema välistatud. Kui tekib olukord, kus mõnda deponeeritud parooli on tarvis kasutada, peaks see toimuma nn nelja silma printsiibil, st kahe inimese poolt korraga. Iga võimaliku deponeeritud parooli kasutamine tuleb dokumenteerida. Paroolide deponeerimist tuleks kasutada neil juhtudel, kui igasugused muud (tehnilised) võimalused selleks puuduvad. Samas tuleb silmas pidada, et paroolide deponeerimine edastab kasutajatele vale signaali paroolide turvalise kasutamise kohta. Paroole ei tohi „deponeerida" klaviatuuri alla või muudesse sarnastesse kohtadesse, samuti ei tohi neid kolleegidele edasi anda, tuues põhjuseks, et nii on võrreldes administraatorilt juurdepääsuõiguse taotlemisega palju lihtsam. Paroolid tuleks alati turvaliselt deponeerida juhul, kui see on ainuke IT-süsteemi või IT-rakenduse juurdepääsuvõimalus. Sellisteks juhtudeks on näiteks administraatori pääsuõigused või autonoomsed süsteemid. Seepärast peaks olema välja töötatud reeglid, kus on kirjas, millist liiki paroolide deponeerimine on kohustuslik ja millised raamtingimused tuleb selleks luua.

Kaugtöö tegijad

Kaugtöö tegijate puhul tuleb tagada, et kodutöökoha IT-süsteemide paroolid oleksid deponeeritud ka asutuse ruumides, et häda korral oleks asendavatel kolleegidel võimalik kaugtööarvutisse salvestatud andmetele juurde pääseda.

Administraatorid

Kõikide administraatorite hallatavate süsteemide, eriti võrguühendusega süsteemide puhul tuleb regulaarselt kontrollida, et deponeeritud oleks alati süsteemi administraatori kõige värskem parool.

Kontrollküsimused:

- Kas paroolide deponeerimise kohta on olemas reeglid?
- Kas kõik paroolid on deponeeritud ning kas see info on ajakohane?
- Kas deponeeritud parooli kasutamise kord on reguleeritud?
- Kas deponeeritud paroolide alusel kontrollitakse paroolivahetuse süsteemsust?
- Kas on uuritud, millised võiksid olla paroolide deponeerimise alternatiivid?

M 2.23z PC kasutamise juhised

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT- turvaosakond, IT-juht

Rakendamise eest vastutavad: IT-juht, kasutajad

Suure ettevõtte või ametiasutuse IT-süsteemide korrakohaseks kasutamiseks on tarvis koostada reeglid, mis määratlevad nii töötajate IT-kasutuse kohustuslikud raamtingimused kui ka vastavad IT- turvameetmed. Kõiki töötajaid tuleb kehtivatest reeglitest teavitada, näiteks elektroonilisel kujul intraneti serveris. Enne infotehnoloogiaga tööleasumist tuleb igalt kasutajalt võtta kinnitus, et ta on reeglitega tutvunud. Suuremate muudatuste korral või hiljemalt kahe aasta möödudes tuleb töötajatelt võtta uus kinnitus. Järgnevalt väike lihtsustatud ülevaade sellest, millega peaks vastavate reeglite koostamisel arvestama.

Eesmärgi püstitamine ja mõistete defineerimine

Kasutusreeglistiku esimene osa on mõeldud selleks, et kasutajaid IT- turvalisuse tagamisest teavitada ja neid selleks motiveerida. Samas toimub ka kõigi kasutatavate mõistete selgitamine, nt mis on PC (personaalarvuti), server, võrk, programmi kasutaja, seadmete kasutaja, kaitset vajavad objektid.

Reguleerimisala

Selles osas tuleb täpselt ära määrata, millisele ettevõtte või ametiasutuse osale käesolev reeglistik kehtib. Seadusest tulenevad ettekirjutused ja organisatsioonisisesed reeglid. Siinkohal tuleks tuua ülevaade olulisematest seadustest, nt isikuandmete kaitse seadus ja autoriõiguse seadus, millest tuleb kinni pidada. Näidete varal tuleks selgitada, milliseid tagajärgi need infotehnoloogia kasutamisel antud kasutuskeskkonnas kaasa võivad tuua. Lisaks tuleks käesolevat alalõiku kasutada kohustuslike organisatsiooniliste reeglite loetlemiseks.

Vastutuse jaotumine

Antud lõigus tuleks defineerida, millised on erinevaid tööülesandeid täitvate töötajate IT-kasutusest tulenevad vastutused. Eriti oluline on siinkohal vahet teha kasutaja, ülemuse, administraatori, auditi läbiviija, andmekaitse eest vastutava töötaja ja IT turvaosakonna meeskonna vastutusel.

Kontaktisikud

Reeglistikus peaksid olema loetletud kontaktisikud ja nende kontaktinfo (telefonid, e-post jne), kelle poole IT-kasutajad võiksid pöörduda IT- turvalisust puudutavate küsimustega, või ära näidatud kohad, kust vastavat infot võib leida. Siinkohal tuleks arvestada asjaoluga, et kui kasutajatele on loetletud liiga palju erinevaid kontaktisikuid, tekitab see ainult segadust. Tihti on parem, kui kasutajatele tuuakse ära vaid mõningad kontaktisikud, kes vajadusel suunavad kasutajad õige töötajani (Help-Desk -kontseptsioon).

Rakendatavad ja kohustuslikud IT-turvameetmed

Reeglistiku viimases osas tuleb IT-kasutuse kohta kindlaks määrata kasutajale kohustuslikud IT-turvameetmed. Vastavalt kaitsevajadusele võivad need IT etalonturbe raamidest isegi välja minna. Tüüpilisteks näideteks töökohal rakendatavate IT-turvameetmete kohta on näiteks turvaline arvutisse sisse- ja väljalogimine, paroolide korrakohane kasutamine ning Interneti kasutamise reeglid. Kui ettevõtte

või asutuse palgal on ka kaugtöö tegijaid, tuleks reeglistikku vastavalt kaugtöö spetsiifikale täiendada.

Kontrollküsimused:

- Kas IT-kasutamise kohta on olemas vastav reeglistik?
- Kas reeglistikust kinnipidamist kontrollitakse?
- Kas reeglistiku sisu, eriti kohustuslikke IT-turvameetmeid kontrollitakse võimaliku aegumise suhtes?
- Kas IT-kasutamise reeglistik on kõikidele töötajatele kättesaadav?
- Kas vastava reeglistikuga arvestatakse ka IT-turvameetmeid tutvustavatel koolitustel?

M 2.24z IT-passi juurutamine

Algatamise eest vastutavad: IT turvaosakond

Rakendamise eest vastutavad: IT turvaosakond, IT-juht

IT turvakontseptsiooni koostamisel tuleks esimese sammuna luua ülevaade olemasolevatest süsteemidest, rakendustest ja andmetest. Väikese asutuse puhul on üldjuhul kõige efektiivsem lahendus lähtuda olemasolevatest IT-süsteemidest. Seetõttu on väikese asutuse puhul suureks abiks, kui iga IT-süsteemi kohta on olemas oma IT-pass, millesse on koondatud kogu tähtsam info.

Kiire ülevaade väikse asutuse jaoks

IT-pass peaks andma IT eest vastutavale töötajale ülevaate asutuses leiduvatest arvutitest ja aitama kaasa probleemide kiirele ja efektiivsele lahendamisele. IT-passi juurutamine on eriti kasulik väikeste asutuste puhul, kus IT-süsteeme on vähe ning kus laialdasemad struktuurianalüüsid näivad mõttetud.

Iga IT-süsteemi kohta tuleb kokku koguda järgnev info:

- IT-süsteemi märgistus (inventariseerimisnumber);
- kontaktisik, kellele poole pöörduda probleemidega, nt teeninduse ja infoliini telefoninumbrid äralangemise tarbeks ning süsteemi hooldaja andmed;
- kasutatava operatsioonisüsteemi andmed;
- viirusetõrjeprogrammi andmed (kasutatav toode ning kord, kuidas laaditakse uuendusi ja paikasid);
- süsteemi asukoht (ruum);
- ülevaade tähtsamast infost, mis on süsteemi salvestatud ja rakendustest, mis süsteemis töötavad;
- kaitsevajadus lähtuvalt konfidentsiaalsusest, terviklusest ja kättesaadavusest;
- info süsteemi installeerimise ja konfiguratsiooni kohta;
- kasutuses olevad lisaseadmed;
- läbiviidud hooldus- ja parandustööd;
- läbiviidud andmevarunduse liik.

Teadmiseks: otse lõppseadmete külge ühendatud printereid ei loeta eraldi komponentideks, vaid lõppseadme osaks. IT-passides võib neid kajastada lisaseadmete või riistvara all.

Sarnased IT-süsteemid, nagu kasutajate PCd, võib koondada ka gruppidesse.

Juhul kui kasutatakse mobiiltelefone või pihuarvuteid, tuleks ka niisuguste seadmete kohta koostada üks kokkuvõtlik IT-pass, kusjuures vajalikud andmeväljad tuleb kohandada seadmetele vastavaks. Ka telefoniseadmete ja andmevõrkude ühenduste tähtsamad andmed tuleks IT-passi kujul dokumenteerida. IT-süsteemi kaitsevajaduse dokumenteerimiseks peaks IT-passis sisalduv info kajastama iga tähtsama rakenduse puhul ka seda, kas seal töödeldakse isikuandmetega seotud infot, samuti on tarvis üles märkida kaitsevajadus lähtuvalt põhiväärtustest, nagu konfidentsiaalsus, terviklus ja kättesaadavus. Lisainfona võib veel kirja panna IT-süsteemis rakendatud turvameetmed, et kahju korral oleks võimalik kiiresti reageerida.

IT-passide eest peaks hoolt kandma kas IT turvaosakond või administraator. Infot võivad passi kanda ka töötajad ise, kuid seejärel tuleb üle kontrollida, kas andmete sisu on õige ning kas kõik vajalikud andmed on üles loetletud. IT-passid tuleb kõik ühte kesksesse kohta kokku koguda. Kuna sarnaste IT-süsteemide, nagu nt PC-de puhul on infos väga palju kordusi, võiks IT-passe pidada elektroonilisel kujul.

Võimalike muudatuste korral tuleb uuenenud IT-süsteemi info kohe passi sisse viia, et dokumentatsioon oleks alati ajakohane. IT-passid lihtsustavad olulisel määral kontrollitegevuste läbiviimist, kuna kõikide olulisemate läbiviidud muudatuste ja rakendatud IT turvameetmeid puudutav info võetakse IT-passidest. Lisaks aitab niisuguste IT-passide pidamine kaasa regulaarsele IT hooldusele ja IT turvameetmete läbitöötamisele, nt andmevarundus ja kõik paroolide muutmisega seonduv. IT-passid toetavad ka hädaolukorraks valmisoleku plaani.

M 2.25 Süsteemi konfiguratsiooni dokumenteerimine

Algatamise eest vastutavad: IT turvaosakond, IT-juht

Rakendamise eest vastutavad: administraator

IT-kasutuse planeerimine, juhtimine, kontrollimine ja hädaolukorraks valmisoleku plaan toetuvad kõik ühisele alustalale – olemasoleva IT-süsteemi dokumentatsiooni ajakohasusele. Ainult värskele informatsioonile toetudes on võimalik hädaolukorras IT-süsteemi uuesti vajalikul moel töökorda seada.

Võrgu füüsikaline ja loogiline konfiguratsioon

Võrgu käitamisel tuleb dokumenteerida nii selle füüsiline struktuur (vt M 5.4 Kaabelduse dokumenteerimine ja märgistus) kui ka võrgu loogiline konfiguratsioon. Siia alla kuuluvad ka üksikute kasutajate kasutajaõigused (vt M 2.31 Volitatud kasutajate ja õiguste profiilide dokumenteerimine) ning andmevarunduse seis. Lisaks tuleb dokumenteerida ka kõikides IT-süsteemides kasutatavad rakendused ja kõikide IT-süsteemide failistruktuurid.

Dokumentatsiooni kättesaadavus

Koostatud dokumentatsioon peab olema üheselt mõistetav, et ka asendajatel oleks võimalik igal ajal vajalikku administreerimistööd jätkata. Süsteemi dokumentatsiooni tuleb hoida sellises kohas, kust seda on võimalik vajaduse korral alati kätte saada. Kui dokumentatsiooni hoitakse elektroonilisel kujul, tuleks see kas regulaarselt välja trükkida või salvestada mobiilsele andmekandjale. Dokumentatsioonile peaks olema juurdepääs ainult vastutavatel administraatoritel.

Sisse- ja väljalülitamise reeglid

Süsteemi dokumentatsiooni tuleb kirja panna kõik vajalikud sammud, mida tuleb järgida IT-süsteemide sisse- ja väljalülitamisel. Eriti oluline on see võrku ühendatud IT-süsteemide puhul. Näiteks tuleb draivide ühendamisel või võrguteenuste sisselülitamisel tihti kinni pidada teatud kindlatest järjekordadest.

Kontrollküsimused:

- Kas olemasolev dokumentatsioon on ajakohane?
- Kas olemasoleva dokumentatsiooni alusel on võimalik administreerimist jätkata?

M 2.26z Süsteemiülema ja ta asetäitja määramine

Algatamise eest vastutavad: IT-juht, IT turvaosakond, telekommunikatsiooniseadmete eest vastutav isik

IT-süsteemide korrakohase käitamise tagamiseks on kõikide IT-süsteemide ja võrkude jaoks tarvis määrata administraatorid. Nende töötajate õlule langevad nii üldised administreerimistööd kui ka kasutajate haldamine koos pääsuõiguste haldamisega. Lisaks vastutavad nad ka kõigi enda hallatavate IT-süsteemide turvaküsimuste eest.

Ülesannete jaotamisel tuleb vältida kattumisi ja kohustuste väljajätmist

Suurte ettevõtete ja asutuste puhul, kus on suur hulk erinevaid IT-süsteeme ja alamvõrkusid, tuleb lisaks eelnevale tagada, et tööülesanded oleks jaotatud erinevate administraatorite vahel selliselt, et vastutusala ei tekitaks probleeme, st et tööülesanded ei tohi teineteisega kattuda, samuti ei tohi ülesannete jaotamisel mitte midagi välja jääda. Lisaks tuleks hoolitseda, et erinevate administraatorite vaheline kommunikatsioon toimiks võimalikult sujuvalt. Selleks võib korraldada näiteks regulaarseid administraatorite koosolekuid, kus arutatakse igapäevatöös esinevaid tüüpilisi probleeme ja nende lahendusi.

Auditi ja administraatorite rollid peavad olema eraldatud

Protokollimisel tuleb arvestada asjaoluga, et auditit läbiviivate töötajate ja administraatorite rollid peavad olema üksteisest eraldatud. Siinkohal tuleks kontrollida, mil määral kasutatavad IT-süsteemid seda võimaldavad.

Eraldi administraatorite kasutajatunnused asenduste tarbeks

Iga administraatori kohta tuleb kindlaks määrata tema asendaja, kes peab vajaduse korral kõiki funktsioone töös hoidma. Siinkohal on tarvis jälgida, et asendajad saaksid isikliku administraatori kasutajatunnuse (vt M 2.38 Administraatorirollide jagamine). Parooli ei tohi mitte mingil juhul mugavusest lähtudes lihtsalt niisama asendajale edasi anda. Administraatori tööülesannete ülevõtmisel peab olema tagatud, et nii igale oma tavatööd tegevale kui ka asendusülesandeid täitvale administraatorile jääks tema tööülesannete täitmiseks piisavalt aega, mis laseks eeldada, et nad suudavad oma tööga korralikult toime tulla. Siinkohal tuleb arvestada ka erinevate koolituse ja täiendõppe vajadustega.

Kontrollküsimused:

- Kas kõik administraatorid ja nende asendajad on saanud piisava koolituse?
- Kas administraatorite vastutusala muutmisel algatati ka vajalikud koolitusprogrammid?

M 2.27z Kodukeskjaama (PBX) hooldus

Algatamise eest vastutavad: kodukeskjaama eest vastutav töötaja, infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator

Kodukeskjaamas on hooldusüksus, millega saab keskjaama konfigureerida ja hallata. Vanematel mudelitel võib selleks olla spetsiaalne riistvara, uuematel on selleks enamasti juhtimistarkvara.
Olenevalt keskjaamast on nimetatud üksusele võimalik juurde pääseda erinevatel viisidel, näiteks:

- süsteemitelefoni kaudu; sel juhul ei ole tegemist tavapärase lõppseadmega, vaid laiendatud funktsioonidega lõppseadmega,
- telefoniseadmega lokaalselt ühendatud arvuti kaudu (nt üle RS232, USB, Ethernet),
- arvuti kaudu, mis on ühendatud kohtvõrku (LAN), kuhu on paigaldatud spetsiaalne haldustarkvara; seda juhul, kui kodukeskjaam ei ole samuti kohtvõrku ühendatud,
- kohtvõrku ühendatud arvuti brauseri kaudu; seda juhul, kui kodukeskjaam ei ole samuti kohtvõrku ühendatud.

Institutsioonivälise teenusepakkuja puhul, kui kodukeskjaam on füüsiliselt IP-ühenduse kaudu liidetud, hallatakse keskjaama tavaliselt brauseri kaudu. Hooldusüksus peaks olema konfigureeritud nii, et juurdepääs oleks ainult hooldatavale arvutile. Näiteks nii, et IT-süsteemid saaksid suhelda hooldusüksusega ainult kindlate IP-aadresside kaudu. Teistest IT-süsteemidest tulevad ühenduskatsed peaksid olema tagasi lükatud. Samuti peaks olema piiratud juurdepääs hooldatavatele arvutitele. Selleks võiksid nad näiteks olla paigutatud eraldi turvaruumidesse, mis on kõrvalistele isikutele suletud. Üldjuhul võiks juurdepääs hooldusüksusele olla võimalik ainult pärast edukat autentimist. Võimalusel võiks hoolduseks kasutatavate seadmete ja hooldusüksuse vaheline andmeühendus olla krüpteeritud, välja arvatud juhul, kui on tegemist ainult sel eesmärgil kasutatava ühendusega (nt seeriakaabel). Seadmed, mida hooldatakse ja konfigureeritakse keskjaama kaudu, peaksid olema kaitstud paroolide ja PIN-idega. Samuti tuleb järgida moodulis M 2.11 Paroolide kasutamise reeglid toodud meetmeid. Mitte ainult majasisesed, vaid ka asutusevälised hooldustöötajad peavad end autentima.

Kodukeskjaama hoolduseks on vaja vastavaid teadmisi, seepärast peaksid töötajaid hooldustöid tegema näiteks koos koolitatud administraatoritega. Kui töötajatel puuduvad teadmised keskjaama optimaalseks hoolduseks ja haldamiseks, ning töötajaid ei ole võimalik kiiresti koolitada, tuleks kaaluda välisekspertide kasutamist. Sõltumata sellest, kes on kodukeskjaama hooldaja, tuleks järgida ka moodulis M 2.4 Hooldus- ja remonditööde reeglid toodud meetmeid.

Kaughooldus

Mõnel juhul on tarvis, et kodukeskjaama konfigureeriks ja hooldaks kolmas isik, näiteks välisekspert. Kui keskjaama hallatakse andmevõrgu kaudu, on vaja, et see oleks keskjaamaga ühendatud. Kui kodukeskjaam on ühendatud kohalikku kohtvõrku („majavõrku"), oleks ründajal võimalik rünnata nii keskjaama kui ka kohtvõrku. Seepärast peaksid juurdepääsud olema kindlustatud. Seda võib teha järgmistel viisidel. Kui hooldus- ja remonditöid teevad väliseksperdid, tuleb kehtestada kindlad reeglid. Näiteks selle kohta, kuidas väljastpoolt tulnud isikuid töö ajal jälgi-

takse ja kuidas käituda seadmetega, mis antakse remonditööde tegemiseks majast välja. Täpsemat infot leiate moodulist M 2.4 Hooldus- ja remonditööde reeglid . Üldiselt võib kaughooldus tekitada mitmeid turvaprobleeme. Nende vähendamiseks peab kaughooldusjuurdepääs olema kaitstud. Võimalikud turvafunktsioonid leiate moodulist M 5.33 Kaughoolduse turve . Avaliku võrgu kaudu IP-l põhinevad andmeühendused peavad olema kaitstud ja krüpteeritud, nt turvakestaga (secure shell, SSH) või virtuaalse privaatvõrgu kaudu.

Kontrollküsimused.

- Kas kodukeskjaama hooldusjuurdepääsud on tehniliste ja organisatoorsete meetmetega kõrvaliste isikute eest kaitstud?
- Kas kodukeskjaama hooldusüksusega saab suhelda vaid hooldusarvuti kaudu?
- Kas kodukeskjaam kaitseb seadmed hoolduse ja konfiguratsiooni ajal paroolide või PIN-idega?
- Kas IP-l põhineva kodukeskjaama juurdepääs andmeühendusele on krüpteeritud?

M 2.28z Väline sidealase konsultatsiooni teenus

Algatamise eest vastutavad: IT-juht, IT-turvaosakond, telekommunikatsiooniseadmete eest vastutav isik

Selleks, et probleemide korral kiiresti professionaalset abi saada, tuleks juba telefonikeskjaama ostmisel või rentimisel läbi mõelda vajaliku konsultatsiooniteenuste kasutamine. Siinkohal on oluline, et hädaolukorras toimuks abi saamine võimalikult kiiresti, kuna telefonikeskjaama väljalangemine mõjutab olulisel määral kogu asutuse tegutsemisvõimet ning sellist olukorda saab lubada vaid erandkorras ja lühikeseks ajaks.

Kontrollküsimused:

- Kui pikk on telefonikeskjaama väljalangemise lubatav aeg?
- Millise aja jooksul muutub kättesaadavaks tootjapoolne abi?
- Kui palju kulub andmevarunduse seisust lähtudes aega süsteemi täielikuks „restardiks“?

M 2.29 Kodukeskjaama (PBX) kasutamisjuhendid

Algatamise eest vastutavad: IT-juht, IT-turvaosakond, telekommunikatsiooniseadmete eest vastutav isik

Rakendamise eest vastutavad: administraator

Kodukeskjaama kasutajale tuleb kõik lõppseadmete kasutamiseks vajalikud dokumendid kättesaadavaks teha (nt telefoni kasutusjuhendid). Eelkõige peaksid töötajad oskama, lisaks telefoni tavapärasele kasutamisele, ka lugeda keskjaama hoiatussignaale (vt M 3.12 Töötajate teavitamine kodukeskjaama (PBX) signaalidest ja teadetest).

Kontrollküsimused:

- Kas kõikide lõppseadmete jaoks on olemas õiged kasutusjuhendid?
- Kas töötajad oskavad nende käsutuses olevaid funktsioone õigesti kasutada?
- Kas töötajad tunnevad hoiatavaid teateid ja helisignaale?

M 2.30 Kasutajate ja kasutajarühmade määramise protseduurid

Algatamise eest vastutavad: IT-juht, IT turvaosakond

Rakendamise eest vastutavad: administraator

Kasutajate ja kasutajarühmade määramise reeglid loovad aluse korrakohaseks pääsuõiguste jagamiseks ning on korrastatud ja ülevaatliku tööprotsessi eelduseks. Iga kasutaja või kasutajarühma kohta käiva info kogumiseks tuleks kasutada ühtset ankeeti,

mis sisaldab järgmist infot:

- perekonnanimi, eesnimi,
- ettepanek üksikkasutaja kasutajatunnuse või rühma kasutajatunnuse valiku kohta juhul, kui selle määramise põhimõtted pole ette antud,
- organisatsiooni allüksus,
- kättesaadavus (nt telefon, kabinet),
- vajaduse korral projektinimi,
- vajaduse korral info süsteemis läbiviidavate planeeritavate tegevuste ja vastavate õiguste kohta ning tegevustele kuluv aeg,
- vajaduse korral info erinevate piirangute kohta, nagu nt aeg, lõppseadmed, kõvaketta maht, pääsuõigused (teatud, kaustad, kaugpöörduse juurdepääsud jne), kasutajakeskkonna piirangud,
- vajaduse korral ülemuse nõusolek.

Juhul kui pääsuõiguste jagamisel ületatakse standardit, tuleb vastavate õiguste jagamist põhjendada. Seda võib teha ka elektroonilisel kujul, kasutades spetsiaalset sisselogimist, mille kasutajatunnus ja parool tehakse loodavatele kasutajatele eraldi teatavaks. Pärast sisselogimist töötatakse vastav programm läbi ja tegevus lõpeb väljalogimisega. Kogutud andmed võib ülemuse juures näidise jaoks välja printida. Esmakordseks sisselogimiseks kasutajale antud parool tuleb kohe peale esmast sisselogimist ära muuta. Süsteem peaks kohustama kasutajat seda tegema. Õiguste profiile tuleks määratleda vaid piiratud arv. Uus kasutaja liigitatakse sobiva profiili alla ja selle alusel saab töötaja täpselt oma tööde läbiviimiseks vajalikud õigused. Siinkohal tuleb silmas pidada süsteemide eripärasid kasutajate ja kasutajarühmade loomisel. Mõistlik oleks kindlaks määrata kasutajate ja kasutajarühmade nimeandmise põhimõtted (nt kasutaja ID = organisatsiooni allüksuse lühend || jooksev number).

Kasutajahalduse spetsiaalsed sisselogimised

Juurdepääsuõigusi erinevatele failidele tuleb piirata kasutajate või kasutajarühmade õigustatud huvi alusel. Juhul kui ühte faili peavad kasutama mitu inimest, tuleks selle jaoks moodustada kasutajarühm. Reeglina peaks igal kasutajal olema vaid üksainus kasutajatunnus. Sama kasutajatunnuse kasutamine mitme töötaja poolt peaks olema keelatud. Iga kasutaja kohta tuleb luua üheselt mõistatav isiklik kaust. Süsteemis tehtavate seadistustööde jaoks tuleks luua vastavate administreerimisõigustega kasutaja: kasutaja loomine peaks toimuma spetsiaalse sisselogimise abil, mille all käivitatakse vastav programm või kestaskript. Niimoodi saavad vastutavad administraatorid kasutajaid ja kasutajarühmasid sisse seada

üksnes eelnevalt määratud määratluste kohaselt ning puudub vajadus täiendavate administraatoritööde õiguste jagamiseks.

Spetsiaalsed Unixi meetmed

Seda meedet tuleb Unixi puhul täiendada järgmiste meetmetega:

- M 4.13 Identifikaatorite hoolikas jaotamine
- M 4.19 Unixi süsteemifailide ja -kataloogide atribuutide jaotuse piirangud
- M 4.20 Unixi kasutajafailide ja -kataloogide atribuutide jaotuse piirangud

Spetsiaalsed z/OS-i meetmed

Seda meedet tuleb z/OS-i puhul täiendada järgmise meetmega:

- M 4.211 z/OS turvasüsteemi RACF kasutamine

Muud operatsioonisüsteemid

Muude operatsioonisüsteemide puhul tuleb kirjeldatud meetmeid rakendada sarnasel moel (tutvuge lisaks ka erinevaid operatsioonisüsteeme kajastavate moodulitega).

Kontrollküsimused:

- Kas organisatsioon on kehtestanud reeglid kasutajate ja kasutajarühmade loomiseks?
- Kas kasutajate ja kasutajarühmade loomiseks on olemas vastav programm?

M 2.31 Volitatud kasutajate ja õiguste profiilide dokumenteerimine

Algatamise eest vastutavad: IT-juht, IT turvaosakond

Rakendamise eest vastutab: administraator

IT-süsteemi volitatud kasutajad, loodud kasutajarühmad ja õiguste profiilid peavad olema dokumenteeritud. Dokumentatsiooni loomiseks on erinevaid võimalusi, nt võib kasutada

- süsteemi etteantud administreerimisfaile,
- individuaalseid faile, mida haldavad vastutavad administraatorid,
- paberkandjaid.

Valik tuleks langetada ühe kindla variandi kasuks ja seda tuleks rakendada ühtemoodi kogu asutuse lõikes.

Dokumentatsiooni sisu

Väljajagatud õiguste, kasutajate ja kasutajarühmade kohta tuleks kirja panna eelkõige järgnev informatsioon:

Volitatud kasutajad:

- õiguste profiil (vajaduse korral märkida ära kõrvalekaldumised kasutatavast standardprofiilist),
- õiguste profiili valiku põhjendus (vajaduse korral märkida ära kõrvalekalded),
- kasutaja jaotumine organisatsiooni allüksuse, ruumi ja telefoninumbri lõikes,
- loomise aeg ja põhjus,
- ajalised piirangud.

Volitatud kasutajarühmad:

- volitatud kasutajad,
- loomise aeg ja põhjus,
- ajalised piirangud.

Spetsiaalsed soovitused z/OS-i tarbeks

Vastav dokumentatsioon, mis loetleb volitatud kasutajaid ja nende õiguste profiile, tuleks regulaarselt (vähemalt iga kuue kuu tagant) üle kontrollida, et välja selgitada, kas dokumentatsioon ja hetkel välja jagatud kasutajaõigused langevad kokku ning kas õiguste jagamine vastab turvanõuetele ja kasutajatele sel hetkel kohustuslikele tööülesannetele.

Korrektne dokumentatsioon kujutab endast väljajagatud kasutajaõiguste kontrollimise eeldust. Dokumentatsioon tuleb salvestada või hoiule panna selliselt, et volitamata isikutel puuduks sellele juurdepääs, samuti peab olema tagatud, et ka suurema IT turvaintsidendi või IT-süsteemi äralangemise korral oleks võimalik neid andmeid kasutada. Juhul kui dokumentatsiooni peetakse elektroonilisel kujul, tuleb need andmed kaasata andmevarunduse protsessi.

Kontrollküsimused:

- Kas volitatud kasutajad, loodud kasutajagrupid ja õiguste profiilid on dokumenteeritud?
- Kas volitatud kasutajate, loodud kasutajagruppide ja õiguste profiilide dokumentatsiooni ajakohasust kontrollitakse regulaarselt?
- Kas volitatud kasutajate, loodud kasutajagruppide ja õiguste profiilide dokumentatsioon on kaitstud volitamata ligipääsu eest?
- Kui volitatud kasutajate, loodud kasutajagruppide ja õiguste profiilide dokumenteerimine toimub elektroonilisel kujul, siis kas see on kaasatud andmevarunduse protsessi?

M 2.32z Piiratud kasutajakeskkonna loomine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

Kui kasutajad täidavad ainult kindlaid ülesandeid, pole neile alati tarvis anda kõiki iseseisva sisselogimisega kaasnevaid õigusi (mõningatel juhtudel isegi mitte süsteemiülema õigusi). Näitena võib tuua mõningad rutiinsed süsteemihaldusega seotud ülesanded, nt varukoopiate tegemine või uute kasutajakontode loomine, mille jaoks kasutatakse menüüjuhtimisega programmi, või tegevused, mille jaoks vajab kasutaja ainult ühte rakendust. Eriti just ajutiste töötajate puhul tuleb hoolikalt jälgida, et neil oleks võimalik kasutada ainult selliseid teenuseid ja andmeid, mida nad tõepoolest oma tööks vajavad. Pärast seda, kui ajutiste töötajate töökohustused on lõppenud, tuleb nende kasutajakontod desaktiveerida ja kõik pääsuõigused tühistada (vt M 4.17 Tarbetute kontode ja terminalide blokeerimine).

Sellistele kasutajatele tuleb luua piiratud kasutajakeskkond. Selle võib luua näiteks Unixis, kasutades Restricted Shelli (rsh) ja juurdepääsude piiramiseks Unixi käsku chroot. Kasutajate jaoks, kes vajavad oma tööks vaid ühte rakendusprogrammi, võib võtta kasutusele ka Login-Shelli, mis hoolitseb, et rakendus käivitataks juba sisselogimisel, ja tagab, et programmi sulgemisel saab kasutaja automaatselt süsteemist välja logitud. IT-süsteemis kättesaadavate funktsioonide arvukust võib üksikute kasutajate ja kasutajarühmade lõikes piirata. Kui kasutaja tööülesanded neid ette ei näe, tuleks piirata redaktorite ja kompilaatorite kasutusõigusi. Üksikrežiimis töötavate süsteemide puhul võib vastavad programmid eemaldada ning võrgus töötavate süsteemide puhul võib piirata nende kasutusõigusi.

Microsoft Windows

Järgnevalt tutvustatakse Microsoft Windowsi versioonide turbeomadusi ehk tehnilisi meetmeid, mille abil saab luua piiratud kasutajakeskkonna. Microsoft Windows pakub käivitusskriptide kasutamise võimalust, et piirata kasutajate juurdepääsu erinevatele rakendustele. Tuleb jälgida, et kasutaja ei saaks skriptide käivitamist katkestada ega muuta. Näiteks võivad sisselogiva kasutajaga seotud skriptid käivituda nähtamatult. Ka käivitatud rakendus ei tohi kasutajale pakkuda teiste programmide käivitamise võimalust. Windows 7 ja Windows 2008 R2 saab juurdepääsu blokeerida AppLockeriga ja administraator vajadusel lukustada (M 4.419z Rakenduste juhtimine AppLockeriga alates Windows 7-st).

Kasutajakontode haldamine peab piirama administraatoritena sisseloginud kasutajate liiga suurtest privileegidest tulenevat kuritarvitatavat juurdepääsu failidele ja programmidele. Enne kui kasutaja saab installida tarkvara või käivitada operatsioonisüsteemi seisukohast kriitilise tähtsusega programme või funktsioone, kontrollib kasutajakontode haldus, kas kasutajal on sellise tegevuse jaoks vajalikud privileegid. Kasutajatelt, kes kuuluvad rühma „Administraatorid”, küsitakse tavaliselt enne installimist või programmi käivitamist, kas nad annavad selleks oma nõusoleku. Vähemate õigustega kasutajad peavad sisestama administraatori autentimisandmed. Vastava GPO-poliitika (Group Policy Objects) „User Account Control: Behavior of the elevation prompt for standard users” konfiguratsioonis tuleks valida seadistus „Automatically deny elevation requests”. Selle tulemusel ei saa standardkasutajad, kes ei kuulu administraatorite rühma, oma õiguseid enam suurendada. Funktsiooniga Parental Controls saab administraator kasutajale seada Windows 2008 süsteemi kasutamise piiranguid.

Parental Controlsi abil saab piirata:

- aegu, millal kasutaja saab sisse logida;
- programme, mida kasutaja saab käivitada;
- veebilehti (internetiaadresse), mida kasutaja saab avada.

Parental Controls ei ole aga loodud professionaalseks kasutamiseks. Parental Controlsi piiravad funktsioonid tuleks professionaalses töökeskkonnas asendada asjakohaste alternatiivsete meetmetega.

Kontrollküsimused:

- Kas kasutajakeskkonna ja käivitusprotseduuri puhul arvestatakse iga kasutaja reaalsete tööülesannetega?
- Kas redaktorite ja kompilaatorite kasutamine on takistatud, kui need pole kasutajale tööülesannete täitmiseks vajalikud?
- Kas on tagatud, et kasutajal ei ole Windowsi käivitamisel võimalik muuta ega katkestada käivitusskripte?
- Kas ajutiste töötajate kasutajakeskkonna õigused on reguleeritud?
- Kas kasutajakeskkonna piiramiseks rakendatakse IT-süsteemis leiduvaid turvafunktsioone?

M 2.33z Unixi ülemarollide jagamine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator

Enamikes Unixi süsteemides eksisteerib vaid üksainus administraatori roll (Super-User nimega root , mille kasutaja-ID-ks on (UID) 0). Isikutel, kel on juurdepääs vastavale kasutajale, omavad kontrolli terve süsteemi üle. Oluline on siinkohal märkida, et vastav kasutajaõigus võimaldab juurdepääsu kõikidele failidele ning lubab neid muuta ja kustutada.

Nelja-silma-printsiip

Super-User-Password tohib teada olla vaid administraatoritele. Parooli edasiandmine peab olema reeglitega piiratud ning vastav toiming tuleb dokumenteerida. Super-User-Login root i võib täiendavalt kaitsta nelja-silma-printsiibi abil, kasutades näiteks organisatsioonilisi meetmeid nagu nt jagatud parool. Sealjuures on tähtis, et parooli miinimumpikkus oleks suurem (12 või rohkem kohta). Täiendavalt tuleb tagada, et süsteem kontrolliks parooli kogu selle miinimumpikkuse ulatuses.

Ülesannete eraldamine

Mitmed Unix -süsteemid võimaldavad ülesannete jagamiseks ära kasutada olemasolevaid administraatorirolle. Ülesannete eraldamisel peaks neid täitma erinevad töötajad. Terve rida administraatori ülesandeid ei nõua otseselt Login root juurdepääsu. Kui administraatorite tööülesannetes on tehtud spetsiaalsed jaotused, tuleks seda võimalust ära kasutada. Suurte süsteemide puhul, eriti seal, kus administraatoriülesandeid täidab korraga mitu isikut, on tööülesannete jaotamisega võimalik maandada riskifaktoreid.
Selleks on kaks võimalust:

- administratiivsete Logini de loomine: neil on küll UID 0, kui sisselogimisel käivitub vaid üks programm, millega hakatakse täitma oma administraatoriülesandeid ning tööde lõpetamine toimub Logout iga. Näited: uute kasutajate loomine, draivi ühendamine. UNIX V.4 saab näiteks administraatorite Login-nimed setup , sysadm , powerdown , checkfsys , mountfsys ning umountfsys sisse seada samanimeliste programmide abil.
- Login ide kasutamine, mille puudub UID 0: need Login -nimed (sys , bin , adm , uucp , nuucp , daemon ning lp) omavad programme ja faile, mis on süsteemi toimimiseks määrava tähtsusega ning seepärast kuuluvad nad erilise kaitse alla. Enamikes Unix -süsteemides on need määratud vastavate teenuste haldamiseks.

Abiprogrammide kasutamine

Selgitamaks välja, millised Login-id on administraatoriõigustega seotud, tuleks reeglipäraselt kasutada abiprogramme (nt cops, tiger), mis otsivad paroolikaustas UID 0 Logine.

Kontrollküsimused:

- Millistele isikutele on teada Super-User-Password ?
- Kas administraatorite töörollid on eraldatud?
- Millistel Loginidel on UID 0?
- Kas on olemas Login e, millel on UID 0 ja Shell -juurdepääs?

M 2.34 IT-süsteemi muutuste dokumenteerimine

Algatamise eest vastutavad: IT-juht, IT turvaosakond
Rakendamise eest vastutavad: administraator

Süsteemi ülevaade

Süsteemi sujuva töö tagamiseks peab administraatoril olema sellest ülevaade, st tal peab olema võimalik luua süsteemi ülevaade. Kui administraator peaks ootamatult oma tööst kõrvale jääma, peaks ka tema asendajal olema võimalik luua süsteemi ülevaade. Süsteemi ülevaade on lisaks ka süsteemi kontrollivõimaluse eelduseks (nt probleemsete seadistuste kontrollimine, muudatuste sisu kontrollimine). Seetõttu peaksid administraatorite tehtud süsteemimuudatused olema dokumenteeritud ja võimaluse korral peaks see toimuma automaatselt. Eriti oluline on see süsteemikaustade ja süsteemifailide muudatuste puhul.

Uued operatsioonisüsteemid või täiendid

Uute operatsioonisüsteemide või täiendite installeerimisel tuleb asetleidnud muudatused eriti hoolikalt kirja panna. Uute süsteemiparameetrite aktiveerimine ja olemasolevate parameetrite muutmine võib endaga kaasa tuua olulise muudatuse IT-süsteemi toimimises (eriti võib see puudutada turvafunktsioone).

Käitusfailide aktsepteerimine ja dokumenteerimine

Unixi all peab süsteemi administraator aktsepteerima ja dokumenteerima käitusfailid, millele on juurdepääs ka teistel kasutajatel peale omaniku või mille omanik on juurkasutaja (vt M 2.9 Aktsepteerimata riist- ja tarkvara kasutuse keeld). Eriti tähtis on koostada nimekirjad failide aktsepteeritud versioonide kohta, mis lisaks kõigele muule peaksid sisaldama ka infot vähemalt loomise kuupäeva, iga faili suuruse ning võimaluse korral ka rakendatud s-bittide kohta. Nimekirjad on regulaarse turvakontrolli ja tervikluse kao kontrolli läbiviimise eelduseks.

Kontrollküsimused:

- Kas süsteemi muudatuste kohta peetakse logiraamatuid?
- Kas dokumentatsiooni andmed on ajakohased ja täielikud?
- Kas olemasolevate üleskirjutuste alusel on võimalik administreerimist jätkata?
- Kas vastavad üleskirjutused on kaitstud volitamata isikute juurdepääsu eest?

M 2.35 Teabe hankimine turvaaukude kohta

Algatamise eest vastutavad: IT-juht, IT turvaosakond

Rakendamise eest vastutavad: IT turvaosakond, administraator

Tuvastatud ja avalikustatud turvaaukude vastu tuleb kasutusele võtta vajalikud organisatsioonilised ja administratiivsed meetmed. Vajaduse korral tuleb kasutatavasse riist- ja tarkvarasse paigaldada turvalisust mõjutavad paigad ja täiendid (vt M 2.273 Turvalisust mõjutavate paikade ja värskenduste kiire paigaldamine). Kui vastava juhtumi jaoks täiendeid ja paikasid ei ole, tuleb vajaduse korral rakendada täiendavaid turvariistvara ja turvatarkvara lahendusi. Seetõttu on väga oluline, et süsteemi administraatorid hoiaksid ennast pidevalt kursis uute tuvastatud nõrkade külgedega.

Infot on võimalik saada näiteks järgmistest allikatest:

- Programmide ja operatsioonisüsteemide tootjad ja edasimüüjad. Tihti informeerivad nad oma registreeritud kliente süsteemide võimalikest turvaaukudest ise ning teevad kättesaadavaks ka süsteemi uued parandatud versioonid või paigad.
- Arvutiavariide tõrje rühmad (computer emergency response teams, CERT), mis koondavad arvutisüsteemide turvaintsidentide ennetamise ja nendele reageerimise meetmeid. CERTid informeerivad nn nõuandmike (advisories) kaudu inimesi hetkel riist- ja tarkvaratoodetes leiduvatest nõrkadest külgedest ning jagavad soovitusi nende kõrvaldamiseks.
- CERT-EE (Computer Emergency Response Team of Estonia), Pärnu mnt 139a, Tallinn. Telefon: +372 663 0299 | | cert[at]cert.ee.
- Tootja- või süsteemispetsiifilised, samuti turvaprobleemidele keskenduvad uudistegrupid või meililistid. Vastavates foorumites toimuvad arutelud erinevates operatsioonisüsteemides ja muudes tarkvaratoodetes ilmsiks tulnud või kahtlustatavate turvaaukude ja vigade kohta. Kõige värskemat informatsiooni pakuvad enamasti ingliskeelsed meililistid, nagu näiteks Bugtraq, mille arhiivide jaoks on olemas paljusid avalikke juurdepääsupunkte, nt http://www.securityfocus.com.

Ideaalvariandis peaksid nii administraatorid kui ka IT turvalisuse eest vastutav töötaja kasutama turvaaukude kohta käiva informatsiooni kogumiseks vähemalt kahte infoallikat. Sealjuures on soovitatav, et lisaks tootja edastatavale informatsioonile kasutataks ka „sõltumatuid" infoallikaid. Administraatorid peaksid siiski igal juhul kasutama ka tootjate spetsiaalselt vastava toote kohta väljastatud infot, et olla nt kursis sellega, kas teatud tootele, juhul kui sellel peaks ilmnema turvaauke, üleüldse antakse välja täiendeid ja paikasid. Toodete puhul, millele tootjafirmad turvapaikasid enam ei väljasta, tuleb aegsasti kontrollida, kas niisugustes tingimustes saab toodet veel turvaliselt edasi kasutada ning milliseid lisameetmeid läheks tarvis kõnealuste süsteemide jätkuva turvalisuse tagamiseks.

Kontrollküsimused:

- Kas administraator kontakteerub regulaarselt enda hallatavate süsteemide tootjatega? Kas süsteemid on registreeritud?
- Milliseid informatsiooniallikaid kasutatakse turvaaukude väljaselgitamiseks?

- Kas otsitakse uusi informatsiooniallikaid turvapaikade leidmiseks?
- Kas on olemas protsess turvaintsidentide lahendamiseks?

M 2.36 Sülearvuti väljaandmise ja tagastamise reeglid

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator, kasutaja

Sülearvuteid ja teisi kaasaskantavaid IT-süsteeme kasutatakse korraga ühe töötaja poolt, nt töökohaarvutina, mida on võimalik kasutada ka mobiilselt. Samas on võimalik ka nende kasutamine mitme töötaja poolt, nt esitluste tarbeks. Sõltuvalt kasutusalast tuleb täita erinevaid turvanõudeid. Seetõttu tuleks juba enne seadmete kasutamist planeerida nende võimalik kasutusala ja kasutusviis. Töökohaarvutina kasutamisel tuleb näiteks arvestada, et seadmete kasutamine vaheldub pidevalt statsionaarse ja mobiilse kasutusviisi vahel. Sealjuures on võimalik, et seadmega kasutatakse erinevaid võrkusid. Selle tarbeks peavad sülearvutid olema ühelt poolt piisavalt kaitstud, et mobiilse kasutuse käigus oleks sülearvutis olevate andmete kompromiteerimise, manipuleerimise ja kaotsimineku võimalus välistatud. Teiselt poolt ei tohi sülearvutid ise muutuda ohuallikateks, mille tagajärjel võiksid sisevõrgud saada kannatada. Kui sülearvuteid kasutatakse vaheldumisi erinevate töötajate poolt, on ülimalt oluline, et seadme üleandmine oleks täpselt reguleeritud. Toimiva süsteemi tagamiseks tuleks luua sülearvutite ühisladustus (vt M 1.35 Kaasaskantavate IT-süsteemide ühisladustus).

Reguleeritud üleandmine ja tagasivõtt

Kaasaskantavate IT-süsteemide üleandmisel on oluline pöörata tähelepanu järgmistele punktidele:

Üleandmine:

- Seadme uuel kasutajal palutakse vahetult üleandmise käigus sülearvuti vana parool või standardparool ära muuta.
- Uuele kasutajale tuleb üle anda infoleht, kus on kirjas kaasaskantava IT-süsteemi turvalise kasutamise reeglid.
- Ülevaate säilimiseks tuleks üleandmise/tagasivõtmise päevikusse üles märkida iga kasutaja nimi, organisatsiooni allüksus, telefoninumber ja seadme kasutuseesmärk.

Tagasivõtmine ja edasiandmine:

- Kasutaja teeb teatavaks tema poolt viimati kasutatud parooli või määrab parooliks standardparooli, nt „LAPTOP“.
- Sülearvuti tuleb uuendatud viirusetõrjetarkvaraga üle kontrollida.
- Kasutaja peab veenduma, et enne seadme üleandmist saavad kõik talle vajalikud andmed tema jaoks ligipääsetavale andmekandjale ümber kopeeritud (nt tema PCIe). Sellele lisaks peab kasutaja hoolt kandma selle eest, et kõik tema poolt loodud failid ja andmed saaksid seadmest (võimalusel füüsiliselt) kustutatud. Selleks peavad olemas olema sobivad tööriistad (tools).
- Sülearvuti tagasiandmine ja viirusetõrjetarkvara skaneerimise tulemus tuleb dokumenteerida. Tuleb kindlaks teha, kas seade, seadme lisad ja dokumentatsioon on terviklikud.
- Tagamaks, et seadmele kindlaksmääratud turvaline aluskonfiguratsioon püsib muutmata kujul, ning et tundlikud andmed saavad seadmest eemaldatud, tuleks sülearvuti reinstalleerida, kasutades vastavat referentsinstallatsiooni (vt M 4.28 Sülearvuti tarkvara reinstalleerimine kasutaja vahetumisel).

- Tagastatud sülearvutid formaaditakse uuesti.

Sülearvutitele ette nähtud kasutusalad tuleb dokumenteerida.
Kontrollküsimused:

- Kas sülearvutite rakendamisvõimalustega tegeldi juba enne nende soetamist ja installeerimist?
- Milline dokumentatsioon eksisteerib sülearvutite kasutamise planeerimise kohta?
- Kas kaasaskantavate IT-süsteemide edasiandmist kolleegidele dokumenteeritakse?
- Kas sealjuures peetakse kinni kohustuslikest turvanõuetest?

M 2.37 Korrastatud töölaud

Algatamise eest vastutavad: organisatsiooni juht, IT turvaosakond

Rakendamise eest vastutavad: töötajad

Iga töötaja peaks olema kohustatud tagama töökohalt lahkudes selle korrastatud oleku. IT kasutaja ei pea hoolitsema mitte ainult selle eest, et töökohalt lahkudes oleks võetud kõik meetmed, mis välistavad kõrvaliste isikute juurdepääsu IT-rakendustele või andmetele. Kõik töötajad peavad olema ühtemoodi hoolsad oma töökoha kontrollimisel, et veenduda, et tundlik informatsioon ei oleks vabalt juurdepääsetav, ning et andmete kättesaadavus, nende konfidentsiaalsus ja terviklus ei kannataks. Ei tohi lubada olukordi, kus volitamata isikutel on võimalus ligi pääseda andmekandjatele (diskettidele, USB mälupulkadele või kõvaketastele) või dokumentidele (väljatrükkidele). Tööajal piisab lühiajalise ruumist eemaloleku puhul sellest, et töötaja paneb oma kabineti ukse võimaluse korral lukku. Töötaja planeeritud eemalviibimise korral (nt pikemad koosolekud, töölähetused, puhkus, täiendkoolitused) tuleb töökoht korrastada selliselt, et töökohale jäetavad kaitset vajavad andmekandjad ja dokumendid oleksid kindlalt suletud. Selle jaoks on loomulikult tarvis, et töötajate käsutuseks oleks piisavas koguses vajaliku suurusega suletavaid panipaiku, nt stabiilseid kappe. Ka paroole ei tohi mingil juhul hoida nähtaval kohal, nt paberikesega monitori külge kleepida või kergesti aimatavas kohas, nagu kirjutuslaua plaadi katte all või lukustamata sahtlis (vt M 2.2 Ressursside haldamine). Samuti tuleks paroolide puhul vältida üheselt mõistetavaid viiteid (nt perekonnaliikmete nimesid või niinimetatud triviaalseid paroole, nagu järjestikused numbrid või tähed), et parooli kiire väljanuputamine oleks välistatud (vt M 2.11 Paroolide kasutamise reeglid).

M 2.38 Administraatorirollide jagamine

Algatamise eest vastutavad: IT-juht, IT turvaosakond

Rakendamise eest vastutavad: administraator

Paljud võrgus kasutatavad operatsioonisüsteemid võimaldavad administraatorirollide jagamist mitme eri kasutaja vahel. Näiteks Novell Netware 3.11 all on võimalik sisse seada järgmised administraatorirollid: Workgroup Manager, User Account Manager, File Server Console Operator, Print Server Operator ja Print Queue Operator.

Kui administraatorite rollides on tehtud spetsiaalsed jaotused, tuleks seda võimalust ära kasutada. Eriti just suurte süsteemide puhul, kus administraatori ülesandeid täidab korraga mitu isikut, on tööülesannete jaotamisega võimalik maandada üleliia suurte volitustega kaasnevaid riske, st välistada, et administraatoritel oleks võimalik süsteemi kontrollimatult sisse viia kas kooskõlastamata või planeerimata muudatusi. Vaatamata administraatorirollide jagamisele loob süsteem enamasti ka veel ise automaatselt ühe administraatori kasutajakonto, millel ei ole piiranguid – järelevaataja (supervisor). Kui üldse, siis peaks järelevaataja parool olema teada ainult kitsale inimeste ringile. Mitte ükski alama astme administraator ei tohiks seda parooli teada, et välistada seeläbi õiguste omavoliline laiendamine. Parool tuleb turvaliselt hoiule panna (vt M 2.22z Paroolide deponeerimine). Järelevaataja sisselogimist võib täiendavalt kaitsta kahemehereegli abil, kasutades näiteks organisatsioonilisi meetmeid, nagu jagatud parool. Sealjuures on tähtis, et parooli miinimumpikkus oleks tõstetud (12 või rohkem kohta). Täiendavalt tuleb tagada, et süsteem kontrolliks parooli kogu selle miinimumpikkuse ulatuses.

Kontrollküsimused:

- Millistele isikutele on teada järelevaataja parool?
- Kas administraatorite töörollid on eraldatud?

M 2.39 Vastutus turvapoliitika rikkumise eest

Algatamise eest vastutavad: IT turvaosakond, IT-juht

Rakendamise eest vastutavad: IT turvaosakond

Turvapoliitika rikkumiste puhul on tarvis kindlaks määrata võimalikud tagajärjed, et rikkumistele reageerimine oleks selge ja kiire. Rikkumiste puhul tuleb läbi viia juurdlus, et selgitada välja, kuidas ja kus vastav rikkumine aset leidis. Selle lõppedes tuleb võtta vajaminevaid kahjusid kõrvaldavad või kahjusid pehmendavad meetmed. Vajaduse korral tuleb kasutusele võtta veel ka täiendavad kahjusid ennetavad meetmed. Läbiviidavad tegevused sõltuvad nii rikkumise liigist kui ka rikkujast. Kindlaks tuleb määrata isikud, kes vastutavad teiste organisatsioonidega suhtlemise eest, et hankida teavet ilmnenud turvaaukude kohta (vt M 2.35 Teabe hankimine turvaaukude kohta) või anda edasi infot leitud turvaaukude kohta. Hoolitseda tuleb selle eest, et asjassepuutuvaid üksuseid teavitataks asetleidnud turvaintsidentidest võimalikult kiiresti (vt B 1.8 Turvaintsidentide käsitlus).

Kontrollküsimused:

- Kas turvapoliitika rikkumiskahtluse korral on tegutsemine selgelt määratletud?

M 2.40z Töötajate esinduse õigeaegne kaasamine

Algatamise eest vastutavad: IT turvaosakond, IT-juht

Rakendamise eest vastutavad: IT turvaosakond

Kõikide meetmete puhul, mis võimaldavad jälgida töötajate käitumist või tööviljakust, nagu nt protokollimine, tuleb protsessi kaasata töötajate esindaja. Selle abil on võimalik ära hoida liigset ajakadu IT etalonturbe erinevatele meetmetele. Reaalse kahtluse korral, et mõni töötaja võib olla põhjustanud turvaintsidendi, mille tagajärjeks võivad olla erinevad sanktsioonid töötaja vastu, tuleb asjaolude väljaselgitamiseks algatatavas uurimises arvestada kindlasti töötajate esindaja osalemisõigustega.

Kontrollküsimused

- Kas töötajate esindust teavitatakse neid puudutavatest menetlustest ja projektidest õigel ajal?

M 2.41 Töötajate kaasamine andmevarundusse

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtorgan

Rakendamise eest vastutavad: IT-turvaosakond

Kuna andmevarundus on IT-turvalisuse üks olulisemaid meetmeid, peaksid töötajad olema kohustatud kinni pidama kehtivast andmevarunduspoliitikast, täpsemalt selle miinimumnõuetest. Töötajatele tuleb regulaarselt meelde tuletada andmevarunduse vajalikkust ja neid selleks motiveerida.

Kontrollküsimused:

- Kas töötajate andmevarunduse kohustus on kirjalikult fikseeritud?
- Kas andmevarunduskohustusest kinnipidamist kontrollitakse?

M 2.42 Võimalike suhtluspartnerite määramine

Algatamise eest vastutavad: organisatsiooni juht, IT-juht, IT turvaosakond, andmekaitse eest vastutav töötaja

Rakendamise eest vastutavad: IT turvaosakond

Juhul kui on tarvis edastada informatsiooni, peab olema kindlaks tehtud, et informatsiooni vastuvõtjal on vajaminevad volitused talle edastatud info edasitöötlemiseks. Kui informatsiooni vahetatakse mitme kommunikatsioonikoha vahel, peaks kõikidel osapooltel olema ülevaade sellest, kellele peale tema enda vastav informatsioon veel edastati või edastatakse. Äsja nimetatud kriteeriumite täitmiseks peab olema selgelt määratletud, millised kommunikatsioonipartnerid millist infot saada tohivad. Selleks on vaja, et organisatsiooni igasugune info oleks jagatud selle strateegilise sisu alusel eri klassidesse (vt M 2.217 Teabe, rakenduste ja süsteemide hoolikas liigitamine ja käitlus). Ka andmekaitsest lähtuvalt on tarvis luua kasutajatest ülevaade, märkides ära, milliseid andmeid, eriti just isikuandmeid, tohib andmekandjate vahelise kommunikatsiooniga kätte saada.

Kontrollküsimused:

- Kas võimalikud kommunikatsioonisuhted on reguleeritud?
- Kas mainitud ülevaateid uuendatakse regulaarselt?

M 2.43 Andmekandjate õige märgistus edasiandmiseks

Algatamise eest vastutavad: organisatsiooni juht, IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: kasutajad

Lisaks meetmes M 2.3 Andmekandjate haldus kirjeldatud juhtnööridele tuleb vahetatavate andmekandjate korrakohasel märgistamisel arvestada veel sellega, et nii saadetise saatja kui ka (kõik) adressaadid peavad olema üheselt väljaloetavad. Andmekandjate või nende pakendite märgistamine peab võimaldama adressaadil selgelt ära tunda, mis on saadetise sisuks. Samas on kaitset vajava informatsiooni puhul oluline see, et märgistamine ei võimaldaks volitamata isikutel teha liigseid järeldusi saadetises oleva info liigi ja sisu kohta. Konfidentsiaalsete materjalide puhul tuleb igal juhul kinni pidada kehtivatest saladuse hoidmist käsitlevatest eeskirjadest. Sellele lisaks tuleb andmekandjatele märkida neis kasutatud formaadid ehk vajalike parameetrite väljalugemiseks vajaliku info. Näiteks tuleb DVD edasiandmisel lisaks kõigele muule märkida, kas tegu on video-, audio- või andme-DVDga. Märgistamise puhul võib kasulikuks infoks osutuda ka saadetise edastamise kuupäev, võimalik versiooni number või asukoha tunnused.

Kontrollküsimused:

- Kas edasiantavate andmekandjate märgistamisreeglid on ette antud?
- Kas märgistamise reeglistikust kinnipidamist kontrollitakse pisteliselt?

M 2.44 Andmekandjate pakkimine edasiandmiseks

Algatamise eest vastutavad: IT-turvaosakond

Rakendamise eest vastutavad: kasutajad, postiosakond

Lisaks meetmes M 2.3 Andmekandjate haldus kirjeldatud rakendusjuhistele peaksid andmekandjate saadetiste pakendid olema sellised, et andmekandjate võimalik manipuleerimine oleks pakendi kaudu äratuntav.
Võimalikeks meetmeteks on kasutada:

- ümbrikute pitseerimist,
- saadetiste plommimist,
- ümbrikute ülekleepimist teibiga, mis seejärel vees mittelahustuva tindiga mitu korda ebakorrapäraselt üle sirgeldatakse.
- turvaetikette ümbrikute sulgemiseks.

Saladuste edastamise jaoks on välja töötatud spetsiaalsed ennast tõestanud turvaümbrikud, pitseerimisteibid ja turvaetiketid. Kui digitaalsed andmekandjad on varustatud ülekirjutuskaitsega (nt disketi nupukesed, lintide kirjutusrõngad), tuleks neid ka kasutada. Lähtudes andmekandjatele salvestatud andmete kaitsevajadusest, tuleks kontrollida, milliseid järgmisi turvameetmeid oleks mõttekas rakendada:

- Failide salvestamine andmekandjale peaks toimuma võimalikult suure kirjutuskaitse astmega. Selleks võib kasutada näiteks paljude Office -programmide poolt pakutavaid kasutamispiirangu funktsioone (vt M 4.30 Rakendusprogrammide turvavahendite kasutamine).
- Kui andmekandjatele salvestatud info manipuleerimist peab olema võimalik tuvastada, võib kasutada krüpteerimis- või kontrollsumma -funktsioone (vt M 4.34 Krüpteerimise, kontrollsummade ja digitaalallkirjade rakendamine).
- Volitamata lugemise vältimiseks tuleks krüpteerida kas terve andmekandja või siis selle üksikud failid.

Kontrollküsimused:

- Kas erinevate andmekandjate turvaliseks transportimiseks vajaminevad pakendid on organisatsiooni poolt kasutamiseks ette kirjutatud ning kas neid on piisavas koguses olemas?
- Kas transportimisel kasutatavad pakendid võimaldavad adressaadil kontrollida, et pakendi sisuga ei oleks manipuleeritud?

M 2.45 Andmekandjate üleandmine

Algatamise eest vastutavad: organisatsiooni juht, IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: kasutajad, postiosakond

Juhul kui andmekandjaid on tarvis saata kahe või rohkema kommunikatsiooni osapoole vahel, tuleb korrakohase üleandmise tagamiseks kinni pidada tervest reast asjakohastest soovitustest. Kindlaks tuleb määrata sobilik saatmisviis. Sealjuures on tarvis pöörata põhitähelepanu andmekandja liigile ja sellel olevate andmete kaitsevajadusele. Vale kättetoimetamise vältimiseks peavad adressaadid olema saadetise peale korrektselt märgitud. Seepärast peaks lisaks adressaadi nimele olema saadetise peale märgitud ka organisatsiooni allüksus ja vastava ettevõtte või ametiasutuse täpne nimi. Organisatsiooni sees tuleks pidada nimekirju enamkasutatavatest aadressidest, et saadetiste adressaatide andmed oleksid võimalikult värsked ja korrektsed. Ka saatjapoolne aadress peab olema saadetise peale selgelt ja täielikult märgitud. Institutsiooni sees tuleks väljastada sellekohane eeskiri, mis reguleerib täpselt ja üheselt saatja aadressi info ülesehitust ja selle ulatust.
Digitaalsetele andmekandjatele tuleks (soovi korral) lisada andmekandja infoleht, mis sisaldab järgnevat infot:

- saatja,
- adressaat,
- andmekandjate liik ja kogus,
- seerianumber (kui on olemas),
- identifitseerimistunnused andmekandja sisu kohta,
- saadetise saatmiskuupäev, vajadusel kuupäev, millal peaks adressaat saadetise hiljemalt kätte saama,
- info andmekandjale tehtud viiruste skaneerimise kohta,
- andmekandja lugemiseks vajalikud parameetrid, nt lindi lugemise kiirus.

Andmekandja infolehele ei tohi märkida:

- milline on võimalike kaitset vajavate andmete lugemiseks välja antud parool,
- milliseid võtmeid kasutati kaitset vajavate andmete krüpteerimiseks,
- andmekandja sisu.

Andmekandja saatmist võib (soovi korral) dokumenteerida. Isikuandmete või muude tundlike andmete saatmine peab olema dokumenteeritud. Kontrollimist vajab, kas adressaat on saadetise korrakohaselt kätte saanud. Saadetiste puhul, mille sisuks on ülikonfidentsiaalsed või kindlate tähtaegadega seotud materjalid, peaks adressaate teavitama saadetise teelepanekust ning valitud transpordi teekonnast. Kõrge kaitsevajaduse puhul on soovitav, et adressaadilt palutaks saadetise kättesaamise kinnitamist. Määrata tuleb nii saadetise väljasaatmise kui ka selle vastuvõtu eest vastutavad töötajad. Võimalike vihjete puhul saadetisega manipuleerimise või selle kadumise kohta tuleb sellest kohe turvaosakonnale teada anda.

Kontrollküsimused:

- Kas töötajaid on andmekandjate saatmise reeglistikust teavitatud?
- Kas andmekandjate saatmise eest vastutavaid töötajaid on piisavalt teavitatud võimalikest ohtudest?

M 2.46 Krüpteerimise õige korraldus

Algatamise eest vastutavad: IT turvaosakond

Rakendamise eest vastutavad: IT turvaosakond, IT rakendusmeetmete eest vastutav töötaja

Krüptograafiliste turvamehhanismide (nt krüpteerimise, digitaalkirjade) kasutamise eeldus on sobilike võtmete konfidentsiaalne, terviklik ja autentne loomine, jagamine ja installeerimine. Krüptovõtmed, mis on saanud teatavaks volitamata isikutele, mida on jagamisel võltsitud või mis pärinevad koguni kontrollimatust allikast (sama kehtib ka võtmete kokkuleppimisel sidepartnerite vahel) võivad krüptograafilist turvamehhanismi ohustada samamoodi nagu halva kvaliteediga ebasobival viisil koostatud võtmed. Hea kvaliteediga võtmeid luuakse reeglina sobilike võtmegeneraatorite abil (vt allpool).

Võtmete haldamise puhul tuleb pöörata tähelepanu alljärgnevale:

Võtmete loomine

Võtmete loomine peaks aset leidma turvalises keskkonnas, kasutades selleks sobilikke võtmegeneraatoreid. Krüptograafilisi võtmeid võib ühelt poolt luua nii otse kasutuskohas (vastavatel juhtudel enamasti kasutaja enda loodud) kui ka tsentraalselt. Võtmete kohapeal loomise puhul tuleb tihti teha mööndusi seoses turvalisusega, tsentraliseeritud võtmete loomise süsteemi korral peab seevastu olema tagatud, et võtmed jõuaksid nende kasutajateni autentsel ja kompromiteerimata kujul. Sobilikud võtmegeneraatorid peavad tootma kontrollitud, statistiliselt ühtlase jaotusega juhuslikke järjekordi, kasutades selleks ära kogu võimalikku võtmeruumi. Selleks toodab teatud generaator nt suvalised bitijärjekorrad, mida hakatakse loogika abil üle töötlema. Seejärel kontrollitakse erinevate testimismeetoditega eelnevalt loodud võtmete kvaliteeti. Mõningad krüptomoodulid, eriti need, millel ei ole integreeritud juhuarvude generaatorit, kasutavad võtmete loomisel kasutajate sisestatud infot. Näiteks palub süsteem sisestada parooli, millest omakorda tuletatakse krüptovõti, või palutakse kasutajal sisestada suvaline tekst, et luua võtme genereerimise jaoks vajalikud juhuslikud lähteväärtused. Niisugused paroolid peaksid olema hoolikalt valitud ning võimalikult pikad. Kui süsteem palub, et sisendid oleksid võimalikult „juhuslikud“, siis tuleb seda ka järgida, st sisendid ei tohi olla kergesti aimatavad.

Võtme funktsioonide eraldamine

Krüptograafilised võtmed peaksid olema võimaluse korral loodud võimalikult ühe kasutusala jaoks. Eriti oluline on, et alati kasutataks muudetud võtmeid pigem krüpteerimise kui allkirja loomise tarbeks, kuna

- võtme ilmsikstuleku puhul ei ole kõik protsessid sellest mõjutatud,
- mõnikord võib olla tarvis krüptovõtmeid teistele kasutajatele edasi anda (asendused),
- võtmete vahetamise jaoks võib eksisteerida erinevaid tsükleid.

Võtmete jagamine / võtmete väljavahetamine

Krüptograafiline side saab toimida ainult siis, kui sidepartnerite käsutuses on üksteisega kokku sobitatud krüptograafilised võtmed. Selleks tuleb kõik sides osalejad varustada selleks vajalike võtmetega. Võtmete jagamiseks ja võtmete väljavahetamiseks võib kasutada erinevaid protseduure. Erinevused tulenevad erine-

vate krüptograafiliste protseduuride ja mehhanismide kasutamisest ning nende omavahelisest kombineerimisest (vt M 2.164 Sobiva krüptoprotseduuri valimine). Võtmete jagamise all peetakse siinkohal silmas sidepartnerite varustamist baasvõtmetega. Enamasti toimub võtmete edastamine üksikutele sidepartneritele mõne tsentraalse koha kaudu (nt trust center'i kaudu). Võtmete jagamiseks tuleks kasutada selleks sobilikke andmekandjaid (nt kiipkaarte) või sideühendusi (nt LAN, WAN) ja see peaks toimuma konfidentsiaalselt (nt võtmekrüpteerimisvõtme krüpteeringuga – key encryption key, KEK), puutumatult (nt MAC-kaitsega) ja autentselt (nt seadusest tulenevatele nõuetele vastava digitaalallkirjaga). Võtme lubamatu ilmsikstulek ja võltsimine peab olema takistatud või siis peab vähemalt olema võimalik seda tuvastada. Võtme väljavahetamine toimub kahe sidepartneri vahel seansivõtme abil. Seansivõti on võti, mida kasutatakse ainult lühikese aja jooksul, nt sideühenduse kestuse ajal. Ajaline kestus peab olema kindlaks määratud, kuna sessioonid võivad venida väga pikaks. Aja kindlaksmääramine toimub nt teatud suhtelise aja möödumise defineerimise või paketiloenduri abil. Iga uue seansi jaoks luuakse sidepartnerite vahel uus seansivõti. Moodsad süsteemid kasutavad tänapäeval võtmete jagamiseks ja väljavahetamiseks asümmeetrilist krüpteerimismeetodit.

Avalike võtmete autentsuse kontrollimiseks on võimalik sisse seada usaldusväärne sertifitseerimisüksus. Kommunikatsioonis osalejad peavad ennast sertifitseerimisüksusele tuvastama ja laskma oma avaliku võtme sertifitseerimisüksuse digitaalallkirjaga kinnitada. Eelneva kirjelduse alusel loodud digitaalne sertifikaat peaks sisaldama informatsiooni vähemalt sides osaleja avaliku võtme, tema identifitseerimistunnuste, sertifikaadi kehtivusaja ning sertifitseerimisüksuse digitaalse allkirja kohta. Teades sertifitseerimisüksuse avalikku digitaalallkirja võtit, saab iga sides osaleja kontrollida oma sidepartneri avaliku võtme autentsust.

Võtme installeerimine ja salvestamine

Võtme installeerimise käigus tuleb kontrollida, kas selle päritolu on autentne ja kas selle andmed on terviklikud. Üldjuhul ei tohiks võtmeid salvestada kunagi süsteemi lahtisel kujul, vaid tuleb kasutada krüpteerimist. Tarkvaraliste krüpteerimistoodete puhul tuleb arvestada sellega, et võtmed peavad krüpteerimis- ja dekrüpteerimisprotsessi jaoks vähemalt lühikeseks ajaks PC-süsteemis originaalkujul olemas olema. Juhul kui IT-süsteemid, milles krüptotooteid kasutatakse, ei paku ise piisavalt kaitset võtmete turvaliseks hoidmiseks, ei tohiks võtmeid sellesse süsteemi salvestada. Niisugustel juhtudel võib olenevalt vajadusest kasutada võtme käsitsi sisestamist. Teine võimalus on hoida võtmeid välisel andmekandjal, kuid sellisel juhul tuleb seda hoida turvalises kohas, nagu kirjeldatakse võtme arhiveerimise all. Turvakaalutlustest lähtuvalt tuleks seetõttu eelistada riistvaralisi krüpteerimiskomponente, mille puhul laaditakse võtmed andmekandja (nt kiipkaardi) pealt krüpteeritud kujul otse krüpteerimiskomponentidesse ning sealt need enam krüpteerimata kujul ei lahku. Sõltumata konkreetsest olukorrast peab alati olema tagatud, et krüpteerimislahenduse installeerimise käigus tuleb eelnevalt seadistatud võtmed ära muuta.

Võtmete arhiveerimine

Arhiveerimise tarbeks peaks krüptograafilisi võtmeid saama salvestada krüpteeritud kujul ning vajaduse korral uuesti sisse lugeda ka väljaspool krüpteerimismoodulit. Selleks võib koondada mitu võtit, mis krüpteeritakse omakorda KEKi abil. KEKi tuleb hoida piisavalt turvalises kohas, nt kiipkaardi peale salvestatult ja

seifis luku taga. KEKi jagamisel kaheks osavõtmeks saab rakendada nelja silma printsiibi kasutamist: kaks eri töötajat omavad kumbki juurdepääsu ühele andmekandjale (nt kiipkaardile või disketile), millele on salvestatud vaid võtme üks pool. KEKi genereerimiseks tuleb mõlemad andmekandjad sisestada kas korraga või üksteise järel krüpteerimismooduli lugejasse.

Pääsu- ja asendusõigused

Pääsuõigusi ja töötajate asendusõigusi puudutavad küsimused peaksid olema lahendatud kehtiva turvapoliitika abil. Vajalikke meetmeid peavad toetama võtmete haldamine ja nende kasutatavad krüpteerimismoodulid/-seadmed (nt võtmete deponeerimise võimalus juhuks, kui mõni töötaja peaks ettevõttest lahkuma või kui töötaja jääb haiguse tõttu pikemaks ajaks eemale, vt lisaks võtmete arhiveerimine).

Võtmete vahetamine

Võttes aluseks kehtivad turvaeeskirjad, tuleb krüpteerimisprotsesside jaoks kindlaks määrata, millal ja kui sageli peab krüptovõtmeid vahetama. Mida suurem on krüpteeritud andmete hulk, mis võimaliku ründe puhul analüüsi alla võib langeda, seda suurem on tõenäosus, et mõningatel juhtudel võib kurjategijatel vastavate andmete lahtimuukimine isegi õnnestuda. Võtmete regulaarne vahetamine minimeerib krüpteeritud andmete kahjustamisvõimalusi. Vahetamise sagedus sõltub mitmetest teguritest. Siinkohal mängivad rolli nii krüpteeritud materjali andmekandja liik (nt pikaajaliseks andmete ladustamiseks või andmeedastuseks loodud andmekandja) kui ka krüptograafiline algoritm, rünnete tuvastamisvõimalus (nt võtme kaotsiminek või vargus) ning andmete konfidentsiaalsuse aste. Võtmete vahetamise intervalli täiendavad tegurid võivad olla võtmete kasutustihedus, sellega seotud ohupotentsiaal ja võtme kohapeal hoidmise turvalisus. Olenevalt kasutusel olevast meetodist, tuleb igale üksikule sideühendusele anda uus võti, st seansivõti. Kasutajate jaoks peaks see toimuma muidugi märkamatult, protsessi enda poolt juhituna. Võtmevahetuse all peetakse siinkohal silmas alusvõtme vahetamist, mis on seansivõtmete loomise aluseks ning otse loomulikult tuleb seda ka regulaarselt teha. Kahtluse korral, et mõni kasutusel olev võti on saanud avalikuks, tuleb selle kasutamine lõpetada ja olukorrast kõigile seotud osapooltele teada anda. Kahtluse all oleva võtmega seni krüpteeritud informatsioonilt tuleb krüpteering eemaldada ja see mõne muu võtmega uuesti krüpteerida.

Võtmete hävitamine

Võtmed, mida ei lähe enam tarvis (nt lõppenud kehtivusajaga võtmed) tuleb turvalisel moel kustutada või hävitada (mitmekordne kustutamine/ülekirjutamine ja/või mehaaniliselt purustada). Tooteid, mille võtmeid ei saa kontrollitud viisil deponeerida, tuleks üldjuhul vältida.

Kontrollküsimused:

- Kas mõni töötaja on määratud vastutama krüptovõtmete halduse eest?
- Kas kaitset vajav informatsioon edastatakse krüpteerimisel kasutatud võtmeid kajastavast infost eraldatult?
- Kas kasutatavaid krüptovõtmeid muudetakse piisavalt sageli?
- Kas võtmeid on kohapeal võimalik hoida turvaliselt?

M 2.47 Faksi eest vastutaja

Algatamise eest vastutavad: sisekommunikatsiooni juht, ülemused

Rakendamise eest vastutavad: sisekommunikatsiooni osakond

Iga faksiseadme kohta tuleb määrata vastutav isik, kelle tööülesannete hulka kuuluvad järgnevad tegevused:

- sissetulnud fakside edastamine nende adressaatidele,
- faksiseadmele vajaminevate kulumaterjalide varustamise koordineerimine,
- faksi kulumaterjalide korrakohane hävitamine,
- faksiseadme jääkinfo korrakohane kustutamine enne seadme hooldus- või remonditöid,
- kohalviibimine hooldus- ja remonditööde juures (vt M 2.4 Hooldus- ja remonditööde reeglid),
- süsteemi sisestatud adressaatide ja protokollide pisteline kontroll, eriti peale hooldus- ja remonditöid,
- kontaktisik faksi kasutamisel esinevate probleemide korral.

Kontrollküsimused:

- Kas faksi kasutamise eest vastutavale töötajale on selgitatud tema tööülesandeid?
- Kas faksi kasutamise eest vastutava töötaja usaldusväärsust kontrollitakse pisteliselt?

M 2.48z Faksioperaator

Algatamise eest vastutavad: IT-turvaosakond

Rakendamise eest vastutavad: sisekommunikatsiooni osakond

Faksiseadme kasutamine peaks olema antud ainult väljavalitud usaldusväärsete töötajate hoolde. Töötajatele tuleb õpetada korrektset faksiseadmega ümberkäimist ning koos sellega ka IT-turvameetmete järgimist. Igale volitatud faksioperaatorile peab olema teada, millised inimesed tohivad faksiseadet kasutada ning kes on vastava faksiseadme kasutamise eest vastutav töötaja. Lisaks sellele peaksid faksiseadmete juures olema selgelt mõistetavad kasutusjuhendid. Faksioperaatorite ringi piiramisega kuni töö tagamiseks vajaliku miinimumini saavutatakse olukord, kus sissetulevate fakside lugejate arv hoitakse võimalikult madalal.

Kontrollküsimused:

- Kas faksioperaatorite arv on piisav, et tööprotsessid kulgeksid sujuvalt?
- Kas iga kasutaja teab, kes on veel peale tema enda volitatud faksiaparaati kasutama.

M 2.49z Sobivate faksiaparaatide hankimine

Algatamise eest vastutavad: IT-turvaosakond
Rakendamise eest vastutavad: varustusosakond
Uute faksiseadmete ostmisel tuleks tähelepanu pöörata sellele, kas seadmetesse on integreeritud standardsed turvafunktsioonid nagu näiteks:

- terminali ID vahetamisvõimalus,
- saateraport,
- registrikirjete funktsioon.

Lisaks hinna ja kvaliteedi suhtele oleks tervitatav, kui arvestataks veel ka järgnevate täiendavate turvafunktsioonidega:

- paroolkaitsega kasutusõigus,
- paroolkaitsega puhversalvesti,
- suletud kasutajagrupi loomise võimalus,
- teatud faksiühenduse saatmis- ja vastuvõtuõiguste väljalülitamine.

Kontrollküsimused:

- Kas uute faksiaparaatide soetamisel arvestatakse valiku tegemisel ka seadme võimalike turvafunktsioonidega?
- Kas täiendavate turvafunktsioonidega faksiaparaatide soetamisel tehakse seadme sobilikkus ja majanduslikkus kindlaks eelkõige kaitsevajadustest lähtudes?

M 2.50 Faksimaterjalide ja varuosade õige hävitamine

Algatamise eest vastutavad: sisemise kommunikatsiooni juht, IT- turvaosakond

Rakendamise eest vastutavad: faksi kasutamise eest vastutav töötaja

Kõik faksi kuluvahendid, millest on võimalik saada informatsiooni fakside kohta, nagu nt fakside vahekopeerlindid või ebaõnnestunud väljatrükid tuleb enne kõrvaldamist kas ise hävitada või lasta infokaitseteenust pakkuvatel firmadel kõrvaldada. Sama kehtib ka informatsiooni sisaldavate varuosade vahetamisel, nagu nt fotoelektrilised trumlid. Hooldusfirmadele, kes faksiaparaate perioodiliselt hooldavad või parandavad, tuleb teha vastavad ettekirjutused ja kontrollida nende täitmist.

Kontrollküsimused:

- Mil moel toimub enam mittevajalike faksi kulumaterjalide hävitamine?
- Kas faksi kasutamise eest vastutavaid töötajaid on teavitatud hävitamisele kuuluvate materjalide kaitsevajadusest ning selleks sobilikest käitlemismeetoditest?

M 2.51z Sissetulnud fakside kopeerimine

Algatamise eest vastutavad: faksi kasutamise eest vastutav töötaja

Rakendamise eest vastutavad: kasutajad

Termopaberile väljatrükitud faks võib mõningase aja möödudes tugevasti heledamaks või tumedamaks muutuda. Seepärast tuleks termopaberile väljatrükitud faksidest, mille sisu on tarvis kasutada pikema aja jooksul, teha tavapaberitel koopiad.

Kontrollküsimused:

- Kas ettevõttes/ametiasutuses kasutatakse termopaberil töötavaid fakse?
- Kas sissetulevatest faksidest tehakse koopiad?

M 2.52 Faksimaterjalide varude jälgimine ja täiendamine

Algatamise eest vastutavad: IT-turvaosakond, sisekommunikatsiooni juht

Rakendamise eest vastutavad: sisekommunikatsiooni osakond, administraator, kasutajad

Paljude igapäevases bürootöös vajaminevate seadmete nagu fakside printerite jms kasutamine sõltub suuresti selleks vajaminevate kulumaterjalide (nt paber, tahmakassett, andmevarunduslindid) olemasolust. Seetõttu peab kohapeal olema tagatud, et seadmed oleksid alati varustatud vajalike kulumaterjalidega. Tarvis on selgeid ja üheselt mõistetavaid eeskirju, mis määravad, kes on milliste kulumaterjalide lisamise ja juurdetellimise eest vastutav. Teatud kulumaterjale tohivad lisada ja juurde tellida mitte kõik, vaid ainult selleks volitatud töötajad, nt kui tegu on kas väga kallite või tehniliselt keerukate toodetega.

Kõiki kasutajaid tuleb informeerida sellest, kes on vastutavad töötajad, kelle poole tuleb pöörduda juhul, kui kulumaterjale on tarvis lisada või juurde tellida. Iga kulumaterjali liigi kohta tuleks määrata vastutav töötaja, kelle ülesannete hulka kuulub varustamine ja olemasolevate koguste kontrollimine. Nimetatud vastutav töötaja peab hoolt kandma, et:

- regulaarselt kontrollitaks kulumaterjalide olemasolevaid koguseid ja lisataks neid vajadusel,
- varustusosakond saaks juurdetellimist puudutava info teada õigeaegselt,
- kulunud või tühjaks saanud kulumaterjalid saaksid korrakohaselt hävitatud, ning et
- kulumaterjalid saaksid seadmes välja vahetatud juhul, kui see ei ole otseselt kasutaja ülesanne.

Varustusosakond peab hoolitsema selle eest, et kulumaterjale oleks alati piisavas koguses.

Täiendavad kontrollküsimused:

- Kas kulumaterjalide juurdetellimise vastutus on kindlalt ära jaotatud?
- Kas kasutajatele on teada kontaktisikud, kes vastutavad kulumaterjalidega varustamise eest?

M 2.53z Faksi desaktiveerimine õhtul

Algatamise eest vastutavad: IT-turvaosakond, tuleohutusspetsialist

Rakendamise eest vastutavad: faksi kasutamise eest vastutav töötaja

Kõikide faksiaparaatide puhul eksisteerib tuleoht, mille minimeerimiseks tuleks vastavad seadmed, mida väljaspool tööaega ei kasutata (osakonna faksiaparaat, isiklik aparaat) peale tööpäeva lõppu välja lülitada. Muuhulgas on võimalik sellega saavutada, et sissetulevad faksid ei jääks kontrollimatult pikaks ajaks faksiseadmesse. Väljalülitamist on võimalik teostada väga lihtsalt, kasutades aegreleesid, mis piiravad aparaatide voolutarbimist väljaspool tavapärast tööaega. Pärast tööaega sissetulevate fakside vastuvõtuks võib määrata mõne muu (võimalusel regulaarselt kontrollitava) faksiühenduse ning moodsamad keskjaamad võimaldavad ka sissetuleva kõne suunamist. Faksiaparaadi väljalülitamine aitab vältida ka seadme ülekoormamist väljaspool tööaega, mis võib olla põhjustatud kas tehnilise defekti või ettekavatsetud massilise faksimise poolt. Aparaadi väljalülitamist tuleks vältida juhul, kui selle kättesaadavusele kehtivad kõrgendatud nõudmised, mille täitmist ei ole võimalik asenduslahendustega tagada.

Täiendavad kontrollküsimused:

- Millised faksiaparaadid peavad jääma peale tööpäeva lõppu sisselülitatuks?
- Kas ülejäänud seadmed lülitatakse välja?
- Kas sissetuleva kõne ümbersuunamine on võimalik?

M 2.59z Sobiva modemi valimine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: kasutaja, administraator, varustusosakond

Modemi valimise puhul tuleb pöörata tähelepanu järgnevale:

Modemi liik

- Arvutisse paigaldatud modemi eeliseks on see, et seda on võimalik konfigureerida vaid sellest arvutist, kuhu modem on paigaldatud. Juhul kui arvutis on olemas pääsuõiguste kontrollimise funktsioonid, saab neid rakendada ka modemi konfiguratsioonifailide kaitsmiseks. Samuti võib modemi kasutajate ringi piirata vaid selleks volitatud isikutega. Arvutitesse paigaldatud modemite manipuleerimisvõimalused on raskendatud. Võrku ühendatud süsteemide puhul, kus vastavad turvamehhanismid puuduvad (nt Peer-to-Peer võrgud), on modemi kasutamise puuduseks tõsiasi, et seda saavad kasutada kontrollimatult kõik töökohad.
- Välist modemit seevastu on võimalik pärast selle kasutamist lukku panna. Lisaks on välise modemi eeliseks selle kõikvõimalikud näidud, isegi kõlarid, mille kaudu edastatakse infot modemi hetkeseisundi kohta. Modemi kõlarite kaudu on võimalik kuulda, kas väliselt toimub mõne ühenduse loomine või kas mõni rakendusprogramm püüab, ilma selleks luba taotlemata, installeerimist ja süsteemi konfiguratsiooni puudutavat informatsiooni tootjafirmale edasi saata. Välise modemi täiendavaks eeliseks on selle sõltumatus IT-süsteemist, st võimalus seda sisse lülitada vaid vajaliku andmeedastuse tarbeks, mille abil saab näiteks tagada, et viimane ühendus kindlasti katkestatakse, ning et teiste ühenduste loomine väljastpoolt ei ole võimalik. Puudusteks on välise modemi puhul on tõsiasi, et seda on võimalik kergesti mittekaitstud IT-süsteemi külge ühendada, mis võimaldab manipuleerida konfiguratsiooni andmetega ja lugeda sinna salvestatud paroole. PCMCIA-modemite eeliseks on nende konstruktsiooni mõõtmed, mistõttu on neid kerge peale kasutamist turvaliselt hoiule panna. Turvaline hoiulepanek välistab modemite kasutamise mittekaitstud arvutite manipuleerimiseks.

Andmeedastuskiirus

- Mida suurem on modemi andmeedastuskiirus, seda odavam on suuri andmehulki edastada, kuna tekib aja kokkuhoid.
- Esmalt tuleks välja selgitada, milliseid andmeedastuskiirusi soovitud kasutusalas tarvis läheb. Näiteks ASCII-terminaliemuleeringu jaoks piisab kiirusest 2400 bit/s, faksidele 9600 bit/s, Datex-J jaoks (T-Online) hetkel 14400 bit/s. Suurte andmehulkade edastamise jaoks tuleks kasutada suurimaid hetkel saadaolevaid edastuskiirusi. Andmeedastuskiirused, mis on suuremad kui 2400 bit/s, raskendavad muuhulgas oluliselt ka pealtkuulamise võimalusi.
- Kiiruste puhul, mis on suuremad kui 9600 bit/s, tuleks kontrollida, kas IT-süsteemide liidesed, mille külge modemit soovitakse ühendada, üleüldse toetavad suuremaid kiirusi.
- Modemi valimisel tuleks jälgida, et jõudluse näitajad, mis määravad reaalselt saavutatava andmeedastuskiiruse, oleksid normeeritud. Siia alla kuuluvad üheltpoolt andmeedastuskiiruse normid nagu nt V.32bis kiirusele 14400

bit/s ning teiselt poolt andmeedastusprotokollid andmete kompressiooniks ja vigade korrektuuriks nagu nt MNP 5 või V.24bis.

Eritingimused

- Suurem osa tänapäeva modemitest töötab firma Hayes poolt loodud standardil (nimetatakse ka AT-standardiks). Kuna eelnimetatud standard on laialt levinud, võib selle standardiga modemi kasutamisel eeldada, et vastava seadme ja teiste modemite vaheline kommunikatsioon toimib ilma probleemideta. Uuemasse generatsiooni kuuluvate modemite soetamisel tuleb arvestada tõsiasjaga, et tootja poolt lubatud suur andmeedastuskiirus eeldab tihti seda, et mõlemas otsas tuleb kasutada sama tootja poolt valmistatud seadmeid.

Käsiraamat

- Kergesti loetav ja põhjalikku informatsiooni sisaldav käsiraamat on modemi installeerimiseks ja optimaalseks konfigureerimiseks väga oluline.

Turvamehhanismid

- Modemitesse võib olla integreeritud terve rida erinevaid turvamehhanisme nagu nt paroolkaitse või Callback funktsioon. Mõningad modemid pakuvad isegi edastatavate andmete krüpteerimisvõimalust.
- Krüpteerimisfunktsiooniga modemi soetamine pakub eeliseid näiteks juhul, kui ühe organisatsiooni sees on tarvis liigutada suuri andmemahtusid erinevate sihtkohtade vahel, mis asuvad eri kinnistutel. Niisugune online -krüpteering on seotud väiksema organisatoorse vaevaga kui andmete krüpteerimine võimalike lisatoodete abil. Kasutatavate algoritmide kohta üldistusi välja tuua ei ole võimalik. IT-etalonturbe seisukohast võib öelda, et DES-algoritm koos sobiva võtmete haldamisega pakub piisavat kaitset.
- Paljudes toodetes reklaamitava Callback -funktsiooniga on võimalik lihtsal moel volitamata helistajaid kindlaks teha (vt M 5.30 Olemasoleva tagasihelistusfunktsiooni aktiveerimine).

Täiendav kontrollküsimus:

- Kas IT kasutajad või varustusosakond on antud nõuannetest teadlikud?

M 2.60 Modemi turvaline haldus

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: kasutaja, administraator

Modemi turvaline haldus nõuab teatud administratiivsete meetmete tarvituselevõtmist:

- Volitamata sisenemiskatsete vältimiseks tohivad modemi juurdepääsu telefoninumbrit teada vaid õigustatud kommunikatsioonipartnerid. Organisatsiooni telefoninumbrite loetellu ei tohi lisada modemi juurdepääsu telefoninumbrit.
- Võrguserverisse integreeritud modemit saavad kasutada kõik töötajad oma isiklike töökohaarvutite kaudu. Niisugustel juhtudel peaks kommunikatsioonitarkvara kasutajaõigused olema antud vaid neile töötajatele, kellel on volitused andmete edastamiseks (vt M 2.42 Võimalike suhtluspartnerite määramine).
- Sellele lisaks tuleb regulaarselt kontrollida nii modemi kui ka kommunikatsioonitarkvara seadistust, samuti tuleb kontrollida, et kõik andmeedastused saaksid protokollitud.
- Peab olema tagatud, et niipea kui kasutaja ennast süsteemist välja logib, katkestab modem ka vastava telefoniühenduse. Üksikrežiimis töötavate süsteemide korral on seda võimalik realiseerida seeläbi, et modem jääb vaid nii kauaks telefoniliiniga ühendatuks kuni toimub andmete edastamine ning seejärel lülitatakse modem välja või ühendus katkestatakse. Võrguserverisse integreeritud modemi puhul tuleb sama tagada modemi vastava konfigureerimise abil. Välist modemit on võimalik lihtsalt välja lülitada. Lisaks tuleb kõiki kasutajaid informeerida sellest, et peale andmete edastamist on tarvis vastav kommunikatsiooniprogramm välja lülitada.
- Täiendava meetmena peab olema tagatud, et modemiühenduse äralangemise korral toimuks automaatselt välise kasutaja IT-süsteemist väljalogimine. Vastasel korral saab järgmine sissehelistaja sama kasutajatunnuse all edasi töötada, ilma et peaks ennast eraldi sisse logima.

Täiendavad kontrollküsimused:

- Kas on testitud, kas modemi senine seadistus suudab ära hoida selle volitamata kasutamise?
- Kas modemiühendus katkestatakse, kui kasutaja end välja logib?
- Kas kasutaja logitakse välja, kui modemiühendus katkestatakse?

M 2.61 Modemi kasutamise reeglid

Algatamise eest vastutavad: IT-turvaosakond
Rakendamise eest vastutavad: IT-turvaosakond
Kindlaks tuleb määrata:

- modemi turvalise kasutamise eest vastutav töötaja (nt üksikrežiimis töötava süsteemi puhul IT-kasutaja, võrguühendusega süsteemide puhul administraator),
- isikud, kellel on õigus modemit kasutada,
- erinevad olukorrad, millal on kohustuslik konfidentsiaalse info edastamine krüpteeritud kujul,
- millistel juhtudel tuleb andmete edastamine protokollida (nt isikuandmete edastamine). Juhul kui kommunikatsioonitarkvaras on protokollimisfunktsioon olemas, tuleks seda mõistlikes piirides kasutada.

Eranditult kõik login -protsessid, ükskõik, kas edukad või mitteedukad, tuleb protokollida. Korrektselt sisestatud paroole ei tuleks protokollimisse kaasata, kuid paroolide muukimiskatsete avastamiseks tuleks kaaluda ebaõnnestunud sisselogimiskatsetel sisestatud paroolide fikseerimist. Paroolide muukimise tunnusteks võivad olla: ühe kasutaja sagedased ebaõnnestunud sisselogimiskatsed, mis tulevad alati sama liini alt, katsed ühe ja sama kestva ühenduse või sama liini alt ennast erinevate kasutajanimedega sisse logida. Pärast ühenduse loomist peab sissehelistaja saama süsteemiteate oma sisselogimise kohta. Siinjuures tuleb silmas pidada, et sisselogimise käigus, enne selle edukat lõpuleviimist, ei tohiks sissehelistajale edastada liiga palju informatsiooni tema poolt sisenemiseks valitud IT-süsteemi kohta. Poolelioleva sisselogimisprotsessi käigus ei tohi siseneja teada saada ei kasutatavat riistvara ega ka operatsioonisüsteemi. Sisselogimisele järgnev süsteemiteade peaks sisaldama endas IT-süsteemi ja/või organisatsiooni nime, viidet, et kõiki ühendusi protokollitakse ning palvet sisestada oma kasutajatunnus ja parool. Ebaõnnestunud sisselogimiskatse puhul ei tohi sisenejale edastada infot võimaliku eksimuse kohta (vale kasutajatunnus, vale parool).

Dial-In/ Dial-Out katkestamine

Sisenevate ja väljuvate ühenduste jaoks tuleks kasutada eraldi liine ja eraldi modemeid. Sissehelistajal ei tohi olla võimalik ennast sisselogitud IT-süsteemi kaudu uuesti väljapoole ühendada. (Juhul kui palju ringiliikuvate töötajate jaoks on see ilmtingimata vajalik, tuleb luua tugev autentimisprotsess, nt kiipkaardi abil.) Muudel juhtudel kujutab see endast vaid ohtu, kuna kräkkerid võivad niisugust juurdepääsu kuritarvitada ning luua kas ühendusi kallite tariifidega kaugkõnede jaoks või kasutada seda oma jälgede segamiseks. Callback funktsiooni puhul tuleks tagasihelistamise jaoks kasutada mõnda teist modemit või modemiliini, mitte sissehelistamist vahendanud modemi liini (vt M 5.44 Ühesuunaline ühenduse loomine).

Täiendav kontrollküsimus:

- Kas kõikidele töötajatele, kes on volitatud kommunikatsioonis osalema, on selgitatud sellekohaseid reegleid?

M 2.62 Tarkvara vastuvõtuprotseduurid

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: IT-juht

IT kasutamine erinevate tööülesannete täitmiseks eeldab, et masinate teostatav andmetöötlus toimib võimalikult vigadeta, kuna paljudel juhtudel ei ole võimalik üksikuid tulemusi enam eraldi kontrollida. Tarkvara vastuvõtuprotseduuride käigus uuritakse seetõttu, kas vaadeldav tarkvara töötab vigadeta, st kontrollitakse, kas tarkvara täidab oma funktsiooni laitmatult, ning kas tarkvaral puuduvad ebasoovitavad kõrvalefektid. Protsessi lõpus väljastatakse tarkvarale vastutava ametiasutuse luba selle kasutamiseks. Ühtlasi võtab kontrolliasutus enda kanda ka vastutuse IT-rakenduse toimimise kohta, milles vastavat tarkvara kasutama hakatakse. Tarkvara vastuvõtu käigus tehakse vahet ise või tellimuse alusel valmistatud tarkvara ning tüüptarkvara vahel, mida mugandatakse ainult selle plaanitud rakendusala kohaselt.

Omaalgatusliku või tellimuse alusel valminud tarkvara vastuvõtmine

Enne kui organisatsioon esitab enda sees või ka endast väljapoole tellimuse tarkvara arendamiseks, peab olema koostatud sellekohane nõudmiste loetelu, mille alusel töötatakse välja realiseerimist vajava toote üldine ja detailne kontseptsioon. Vastava dokumentatsiooni alusel koostab erialaselt vastutav, kuid mitte tarkvara arendamise eest vastutav asutus üldise tarkvara vastuvõtu plaani. Üldjuhul töötatakse siinkohal välja testimisprotsessid ja sõnastatakse ootused, millele loodav tarkvara peab vastama. Testimisprotsesside alusel toimub tarkvara testimine ja selle tulemust võrreldakse eelnevalt toote kohta sõnastatud ootustega, mille alusel antakse hinnang tarkvara sobivuse kohta.

Testimisprotsesside väljatöötamisel ja testide läbiviimisel tuleks arvestada alljärgnevaga:

- testimisprotsessid peaks välja töötama selle valdkonna eest vastutav asutus,
- testimiseks ei tohiks kasutada reaalse töö käigus kasutatavaid andmeid,
- testimisandmed, eriti kui need luuakse reaalsete tööandmete kopeerimise teel, ei tohi sisaldada konfidentsiaalset infot; isikuandmed tuleb kas anonüümseks muuta või simuleerida,
- testimise läbiviimine ei tohi mõjutada süsteemi igapäevast kasutamist ning võimaluse korral tuleks testimine läbi viia kas loogiliselt või füüsiliselt eraldiseisvatel testimisarvutitel.

Vastuvõtust tuleks keelduda juhul, kui

- tarkvaras tuvastatakse raskeid vigu,
- testimise käigus saadakse tulemusi, mis ei vasta ootustele,
- puuduvad käsiraamatud või kasutusjuhendid või kui nende kvaliteet ei ole piisav ning
- kui tarkvara juurde kuuluv dokumentatsioon kas puudub või on ebatäielik.

Vastuvõtmisprotseduuri tulemused tuleb kirjalikult fikseerida. Vastuvõtmist kajastav **dokumentatsioon peaks sisaldama järgmisi andmeid:**

- tarkvara, vajaduse korral ka IT-rakenduse nimetus ja versiooni number,

- testimiskeskkonna kirjeldus,
- testimised ja testimiste tulemused ning
- vastuvõtu kinnitus.

Tüüptarkvara vastuvõtmine

Ka tüüptarkavara hankimine peaks olema seotud vastuvõtu ja kasutamise aktsepteerimise protsessidega. Vastuvõtmise käigus tuleb kontrollida, kas

- tarkvara on viirustest vaba,
- tarkvara ühildub teiste kasutuses olevate toodetega,
- tarkvara on tema jaoks plaanitud rakenduskeskkonnas kasutuskõlblik ning millised on kohustuslikud parameetrid,
- tarkvara on edasi antud täies mahus koos vajaminevate käsiraamatutega ning kas
- nõutud funktsionaalsus on täidetud.

Kasutuse aktsepteerimise protsess

Pärast tarkvara vastuvõtmist tuleb välja anda luba selle kasutamise kohta. Selle tarvis tuleb esmalt kindlaks määrata isikud, kes on volitatud tarkvarale kasutamisluba väljastama. Tarkvarale kasutusloa andmine tuleb fikseerida kirjalikult ning dokumendid tuleb panna hoiule. **Kasutuse aktsepteerimise tõend peaks sisaldama järgmist infot:**

- tarkvara, vajaduse korral ka IT-rakenduse nimetus ja versiooni number,
- kinnitus selle kohta, et vastuvõtuprotsess toimus korrakohaselt,
- kasutuspiirangud (parameetrite seadistused, kasutajate ring jne).
- kasutusloa saamise kuupäev, alates millest tohib vastavat tarkvara kasutada ning
- kasutusloa väljastamise tõend.

Kui kasutatav IT-tehnoloogia seda võimaldab, tuleks tagada, et peale kasutusloa saamist ei oleks võimalik tarkvara muuta ega sellega manipuleerida. Vastasel juhul tuleb kehtestada täiendavad reeglid. Ka pärast intensiivset testimist tarkvara vastuvõtuprotsessis võib juhtuda, et tarkvara kasutamise käigus avastatakse selles ikka veel vigu. Sellisteks juhtudeks tuleb kindlaks määrata, kuidas vigadele reageerida (kontaktisikud, vigade kõrvaldamise protsessi kulg, erialaselt vastutava asutuse kaasamine, vastuvõtuprotsessi ja kasutusloa andmise kordamine, versiooni kontrollimine). Täiendavad selgitused leiate moodulist B 1.10 Tüüptarkvara .

Täiendavad kontrollküsimused:

- Kas kõikidel kasutatavatel riist- ja tarkvaralahendustel on olemas vastuvõtmise ja kasutusloa saamise kinnitus?
- Kas vigasid kõrvaldatakse ka ilma erialaselt vastutavat asutust protsessi kaasamata?
- Kas rakendatava tarkvaraga on võimalik manipuleerida nii, et seda ei ole võimalik tuvastada?

M 2.63 Pääsuvolituste kehtestamine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: üksikute IT-rakenduste eest vastutavad töötajad, administraator

Kui ühe IT-süsteemiga töötab mitu kasutajat, tuleb korrakohase pääsuvolituste haldusega tagada, et igal kasutajal oleks võimalik IT-süsteemi kasutada ainult vastavalt tema töökohustustele. Eelduseks on, et pääsuõigused on üksikute tööülesannete lõikes vastutava töötaja poolt juba kindlaks määratud (vt M 2.7 Süsteemi ja võrgu pääsuõiguste andmine ja M 2.8 IT-rakendustele ja andmetele pääsuõiguste andmine). Seejärel toimub IT-süsteemi kasutavate töötajate liigitamine nende üksikute tööülesannete alusel. Jaotamise tulemused tuleb kirja panna. Seejärel peab administraator konfigureerima IT-süsteemi selliselt, et kõik kasutajad saavad oma juurdepääsu, mille kasutajaõigused võimaldavad neil IT-süsteemi kasutada ainult vastavalt oma tööülesannetele. Juhul kui süsteem ei toeta igale kasutajale erinevate kasutajaõiguste määramist, (nt mitme kasutajaga DOS-PC), tuleb selle võimaldamiseks abi otsida lisatoodetest (vt M 4.41 Sobivate IT-süsteemide turvatoodete valimine). Kui süsteem seda võimaldab, tuleks administraatoril aktiveerida protokollifunktsioonid, mille abil on võimalik tõestada erinevaid asetleidnud protsesse. Siia alla kuuluvad näiteks nii edukad kui ka ebaedukad sisse- ja väljalogimised, süsteemi veateated ja volitamata juurdepääsu loomise katsed. Töötajate asenduste puhul peab administraator juba ette kontrollima, kas asendaja on saanud vastutava töötaja käest vajalikud volitused. Alles seejärel tohib administraator ootamatu asenduse korral vajaminevad pääsuõigused asendaja jaoks sisse seada.

Täiendavad kontrollküsimused:

- Kas administraatori poolt sisseseatud pääsuõiguseid kontrollitakse pisteliselt?
- Kas on olemas dokumentatsioon, mis kirjeldab IT-süsteemis kehtivate õiguste struktuuri?

M 2.64 Logifailide kontroll

Algatamise eest vastutavad: IT-juht, IT turvaosakond

Rakendamise eest vastutavad: üksikute IT-rakenduste eest vastutavad töötajad, audiitor

Turvalisust mõjutavate juhtumite protokollimine on turvameetmena tõhus vaid siis, kui administraator või mõni automaatne süsteem vastavaid logidesse kogutud andmeid ka kontrollib. Kindlasti tuleb logisid kontrollida arvutivõrkudes toimunud mistahes intsidentide esinemisel! Kuna logifailid sisaldavad paljudel juhtudel isikuandmeid, tuleb tagada, et vastavaid andmeid saab kasutada ainult andmekaitse kontrollimise, andmevarunduse või süsteemi korrakohase töö tagamise eesmärgil (vt M 2.110 Andmeprivaatsuse suunised logimisprotseduurides).

Logimisse kaasatavate andmete ulatus ja nende kontrollimise kriteeriumid tuleks dokumenteerida ja organisatsioonisiseselt kokku leppida. Logimisele kuuluvate andmete säilitamiskohustuse ajalised miinimum- ja maksimumnõuded on erinevate seadusesätetega ette antud. Samuti tuleb arvestada asutusesiseseid nõudeid logifailide säilitamise tähtaegadele. Teatud logiandmete säilitamisele võivad olla kehtestatud kindlad ajalised miinimumnõuded, nt kui andmed sisaldavad infot majanduslike tegemiste kohta. Enne logiandmete kustutamist tuleb seega hoolikalt kontrollida, kas andmetele kehtivad seadustest tulenevad ettekirjutused ning kui pikk on vastavate andmete säilitamiskohustus. Kohustuste väljaselgitamisse tuleks kaasata organisatsiooni juristid.

Alljärgnevad hindamiskriteeriumid on toodud näidetena, kuidas võimalikke turvaaukusid, manipuleerimiskatseid ja ebakorrapärasusi ära tunda:

- Kas sisse- ja väljalogimise aeg jääb väljapoole tööaega? (Vihje võimalikule manipuleerimiskatsele).
- Kas on esinenud korduvaid ebaõnnestunud sisselogimiskatseid? (Vihje võimalikule paroolide muukimisele).
- Kas on esinenud korduvaid volitamata juurdepääsu loomise katseid? (Vihje võimalikule manipuleerimiskatsele).
- kas on esinenud silmatorkavalt suuri ajavahemikke, mil logifaile ei salvestatud? (Vihje võimalikule logifailide volitamata kustutamisele).
- Kas logifailide maht on liiga suur? (Liiga suured failid raskendavad ebakorrapärasuste ülesleidmist).
- Kas on esinenud silmatorkavalt suuri ajavahemikke, mil kasutaja vahetust pole toimunud? (Vihje sellele, et tööpäeva lõpus jäetakse kohustuslik süsteemist väljalogimine tegemata).
- Kas avalike võrkudega loodud ühendused on silmatorkavalt pikad? (Vt G 4.25 Lahutamata ühendused).
- Kas võrgu üksikutes osades või terves võrgus on täheldatud silmatorkavalt suurt võrgukoormust või võrgukatkestusi? (Vihje võimalikule katsele takistada või mõjutada võrguteenuseid või võrgu ebasobivale kontseptsioonile ja konfiguratsioonile).

Logifailide kontrollimisel tuleks kriitilise pilguga üle vaadata ka kõik administraatori kasutajatunnuse all läbiviidud toimingud. Kui on tarvis regulaarselt läbi vaadata

suure mahuga logifaile, on mõttekas kasutada kontrollimiseks mõnda programmi. Vastav programm peaks võimaldama valida erinevate hindamiskriteeriumite vahel ja tõstma esile kriitilised logikanded (nt korduvad ebaõnnestunud sisselogimiskatsed).

Kontrollküsimused:

- Kas asutuses tegeletakse logifailide kontrollimisega? Kas rakendatakse kahemehereeglit või on kasutusel automaatne logide seiramise süsteem?
- Kas ja kuidas toimub logifailide kontroll/ülevaatus intsidentide puhul?
- Kas administraatori tegevusi on võimalik kontrollida?
- Kas avastatud juhtumitele reageeritakse?

M 2.65 IT-süsteemi kasutajate eraldatuse kontroll

Algatamise eest vastutavad: IT-juht, IT turvaosakond

Rakendamise eest vastutavad: audiitor, administraator, IT turvaosakond

Mõistliku aja tagant tuleks logiprotokollide hindamise või pistelise kontrolli abil välja selgitada, kas IT-süsteemi kasutajad peavad peale tööülesannete täitmist regulaarselt kinni oma väljalogimiskohustusest, ning ega ühe ja sama kasutajatunnuse all ei tööta mitut kasutajat. Kui kontrolli käigus peaks selguma, et ühe kasutajatunnuse all töötab tõepoolest mitu erinevat kasutajat, tuleb töötajatele selgitada, et pärast tööülesannete täitmist on nad kohustatud ennast süsteemist välja logima. Ühtlasi tuleks töötajatele selgitada selle kohustuse tagamaid, st miks on see iga töötaja enda huvides, et ta ennast välja logiks. Kui peaks selguma, et sisse- ja väljalogimise protseduurid on liiga ajamahukad ja töötajad ei aktsepteeri nimetatud kohustust hoolimata sellekohastest üleskutsetest,

tuleks kaaluda järgmiste alternatiivsete meetmete rakendamist:

- IT-süsteemi kasutajaõigused on võimalik siduda kindla ajavahemiku ja ühe kindla töötajaga nii, et teistel töötajatel on samal ajal vastava IT-süsteemi kasutamine keelatud. See eeldab, et töögraafikud on sobiva ajalise nihkega.
- IT-süsteemi niinimetatud paralleelse kasutamise vältimiseks võib juurde hankida täiendavaid IT-süsteeme. Tuleb silmas pidada, et uute süsteemide hankimisega on seotud vastavad kulutused, kuid samas jäävad seeläbi ära võimalikud kulutused PC turvatoodete hankimiseks.
- Juhul kui töödeldavaid andmeid on võimalik töötajate vahel ära jagada (näiteks töötaja A tegeleb andmetega A–L, töötaja B andmetega M–Z), võib selle tarbeks sisse seada erinevad pääsuõigused. Kui töötaja tahab oma andmetele ligi pääseda, peab ta ennast eelnevalt süsteemi sisse logima, kuna tema kolleegidel puudub juurdepääs vastavatele andmetele.
- Ajamahukate mitmeastmeliste autentimisprotseduuride asemel võiks kasutada automaatseid autentimisprotseduure, nagu näiteks RFID-l põhinevad load või biomeetrilised protseduurid.
- Kui korrakohaste kasutajavahetustega esinevad aktsepteerimisprobleeme, siis kas uuritakse alternatiivseid meetmeid?

Kontrollküsimused:

- Kui tihti kontrollitakse kasutaja vahetumisnõuetest kinnipidamist?
- Kas töötajad aktsepteerivad kasutaja vahetumiskohustust?
- Kas andmeid on võimalik jagada eri gruppidesse?

M 2.66z Sertifikaatidega arvestamine IT soetamisel

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtorgan

Rakendamise eest vastutavad: varustusosakond

IT-toodete ja IT-süsteemide hankimisel peab olema juba võimalikult vara kindlaks määratud, kas tootja või edasimüüja antud kinnitusi seadmetesse paigaldatud turvafunktsioonide kohta saab lugeda piisavalt usutavaks tõendiks või mitte. Kõrgete kaitsevajaduste puhul saab toodete tagatava IT-turbe usaldusväärsuses veenduda ainult nii, et tooted edastatakse sõltumatule osapoolele, kes teostab vastavad kontrollid ja annab toodete kohta oma hinnangu. Üldtunnustatud aluse annavad niisugustele hindamisaktidele aastast 1991 Euroopas ühtlustatud „Infotehnoloogia turvalisuse hindamiskriteeriumid (ITSEC)" ja hindamise käsiraamat ITSEM ning aastast 1998 ülemaailmselt tunnustatud „Infotehnoloogia turvalisuse kontrollimise ja hindamise üldkriteeriumid" (Common Criteria (CC)). Vastavaid hindamisi teevad maailmas mitmed akrediteeritud asutused – täpsemat infot leiate veebiaadressilt http://www.commoncriteriaportal.org. Positiivsete hindamistulemuste korral ning ITSECi, ITSEMi ja Common Criteria raamtingimustest kinnipidamisel väljastab vastav sertifitseerimiskeskus uuritud tootele või süsteemile turvasertifikaadi. Sertifikaadi juurde kuulub aruanne, millest saab välja lugeda, millist funktsiooni kui põhjalikult kontrolliti ning milline oli läbiviidud hindamine. ITSECi kontrollimise põhjalikkusastmed liigituvad hindamisklassi E1 (madalaim kontrolliaste) kuni E6 (kõrgeim kontrolliaste) ning CC usaldusväärsuse klassid liigituvad vastavalt EAL 1 (madalaim kontrolliaste) kuni EAL 7 (kõrgeim kontrolliaste). ITSECi hindamisklass E1 vastab enam-vähem CC usaldusväärsuse klassile EAL 2 jne. Lisaks tuuakse välja ka rakendatud turvamehhanismide kontrollitud tugevus, mis kajastab seda, kui palju tuleb näha vaeva, et rakendatud turvafunktsioonidest mööda pääseda.

ITSEC ja CC liigitavad turvamehhanismide tugevusklassid madalaks, keskmiseks ja kõrgeks. Sellele lisaks antakse juhtnööre, milliste raamtingimustega tuleks vastava toote kasutamisel arvestada. Kui IT soetamisel on valida mitme sarnase hinna- ja kvaliteedisuhtega toote vahel, võib positiivse valikukriteeriumina arvestada võimaliku turvasertifikaadi olemasolu. Siinkohal tuleks turvasertifikaatide olemasoluga arvestada eriti nendel juhtudel, kus sertifikaat tõendab, et kontrollitud funktsioonid täidavad (suurema osa) funktsioonidele esitatud miinimumnõuetest ning mehhanismide tugevus vastab nõutud kaitsevajadustele (vt M 4.41z Sobivate IT-süsteemide turvatoodete valimine). Mida põhjalikumat kontrolliastet olemasolev sertifikaat tõendab, seda kindlam saab olla vastava toote turvafunktsioonide toimimises ja korrektsuses.

Täiendavad kontrollküsimused:

- Kas ettevõtte/organisatsiooni varustusosakonnad on toodete hindamise/sertifitseerimise tähtsusest teadlikud?
- Kas ettevõtte/organisatsiooni varustusosakondadel on olemas sertifitseeritud toodete kohta koostatud ülevaated?
- Kas varustusosakonnad tellivad endale vajalikke sertifitseerimisaruandeid?

M 2.69 Tüüpsete tööjaamade rajamine

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: administraator, IT-juht

Tüüpseid tööjaamu iseloomustab ühtmoodi riist- ja tarkvara ning nende ühesugune konfiguratsioon. Planeerimisel ja sisseseadmisel lähtutakse üldjuhul erinevatest aspektidest nagu tööülesannete iseloom, töökindlus, ergonoomilisus, töökiirus ja hooldamise lihtsus. Planeerimist ja juurutamist teostavad spetsialistid. Tüüpsete tööjaamade rajamine toob endaga kaasa mitmeid eeliseid:

IT-turvalisus:

- tüüpseid tööjaamasid on lihtne kaasata turvakontseptsioonidesse .
- IT-varade dokumenteerimisele kuluv töö maht väheneb.

IT haldus:

- suurtes kogustes samasuguste komponentide ostmine võimaldab paremaid hinnakokkuleppeid.
- aktsepteerimata tarkvara kasutamise tuvastamine muutub lihtsamaks.
- sarnase IT-varustuse puhul ei teki üksikute kasutajate vahel kadedust.

IT kasutajad:

- Seadmete vahetamisel ei ole tarvis kasutajat IT-konfiguratsiooni suhtes ümber koolitada ning seetõttu on võimalikud tööseisakud minimaalsed.
- Riistvara ja tarkvara puudutavate küsimuste puhul saavad töötajad üksteist aidata.

Süsteemi administreerimine installeerimise ja hoolduse käigus:

- Täpselt planeeritud ja testitud installatsiooni on võimalik installeerida ilma vigadeta ja selleks kulub vähem tööd.
- Ühtemoodi kasutajakeskkond lihtsustab kasutajate nõustamist (hooldus, tugi ja korrashoid).

Koolitus:

- Koolitusel kasutatav keskkond ja töökeskkond on samad.

Täiendavad kontrollküsimused:

- Kas tüüpsetest tööjaamadest kõrvalekaldumised on põhjendatud?
- Kas põhjendusi kontrollitakse regulaarselt?
- Milliste asjaoludega arvestatakse tüüpsete tööjaamade planeerimisel ja rajamisel?

M 2.70 Turvalüüsi (tulemüüri) kontseptsiooni väljatöötamine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: IT-turvaosakond

Kohtvõrkude ühendamine globaalvõrkudega nagu nt Internet, loob informatsiooni kättesaadavusele uued võimalused. Arvutite ühendamine lokaalvõrku hoolitseb selle eest, et iga töökohaarvutist oleks võimalik erinevale informatsioonile juurde pääseda. Niisuguse võrguühendusega tekivad samas ka uued ohuallikad, kuna lisaks sellele, et väljastpoolt tulevad andmed võivad liikuda kaitstavasse võrku, on põhimõtteliselt võimalik ka andmete liikumine vastupidises suunas. Sellele lisaks kahjustab võimalus, et kusagil kaugelasuvast arvutist, nt Interneti kaudu, on võimalik kohtvõrgus olevatele arvutitele töökäske jagada, kohtvõrgus olevate arvutite terviklust ja kättesaadavust ning seetõttu on kaudselt kahjustatud ka kohtvõrgus olevate andmete konfidentsiaalsus.

Kaitstavat allvõrku tuleks seetõttu ebakindlasse võrku ühendada ainult neil juhtudel, kus see on tõesti ilmtingimata vajalik. Eriti kehtib see Interneti kohta, mis on tänu oma suurele kasutajate arvule ilmselt kõige väiksema usaldusväärsusega võrk üldse. Siinjuures vajab kontrollimist, millises ulatuses tuleb kaitstavat võrku allvõrkudeks jaotada selle pärast, et teatud arvuteid või kaitstava võrgu osasid ei tohiks kas üldse või tohiks ainult piiratult Internetti ühendada ning kas interneti-ühenduse kasutamiseks piisaks üksnes autonoomselt töötavast süsteemist (vt M 5.46 Autonoomsüsteemide installeerimine interneti kasutamiseks
B 3.208 Interneti-PC). Kaitstava võrgu turvalisuse tagamiseks tuleb kasutusele võtta sobilik tulemüür. Selleks, et tulemüür suudaks pakkuda efektiivset kaitset, peavad olema täidetud järgmised põhinõudmised tulemüürile:

- lähtuma laiapõhjalisest turvaeeskirjast,
- olema kaasatud organisatsiooni IT-turvakontseptsiooni,
- olema korrektselt installeeritud ning
- korrektselt administreeritud.

Ühendus ebausaldusväärsesse võrku võib aset leida alles siis, kui eelnevalt on kontrollitud, kas väljavalitud tulemüüri kontseptsioon ja töötajate poolt täidetavad ning organisatsioonilised raamtingimused on piisavad, et tulla toime kõikvõimalike ohtudega. Tulemüüride kasutamiseks on olemas erinevaid võimalusi. Selgitamaks, milline kontseptsioon on vastavale rakendusalale kõige sobilikum, tuleb esmalt kindlaks teha, milliseid turvaeesmärke peaks tulemüür täitma. **Turvaeesmärkide näited:**

- usaldusväärse (sisemise) võrgu kaitse ebausaldusväärsest võrgust tulevate volitamata juurdepääsukatsete vastu,
- lokaalsel tasandil edastatud ja salvestatud andmete kaitsmine rünnete vastu, eesmärgiga säilitada nende terviklus või konfidentsiaalsus,
- kohtvõrgu komponentide kaitse selle kättesaadavusele tehtud rünnete vastu (eriti kehtib see ka infoserverite kohta, mis teevad sisekeskkonna info üldsusele kättesaadavaks),
- välisvõrgu informatsiooni kättesaadavus kaitstavas sisevõrgus (vastava info kättesaadavus on oma tähtsuse järjekorras alles teine, esmatähtis on siiski lokaalsete arvutite ja informatsiooni kaitse!),
- kaitse IP-Spoofingul põhinevate rünnete ning Source-Routing funktsiooni, ICMP protokolli või Routing -protokollide väärkasutamise vastu,

- kaitse uute võimalike tarkvara turvaaukude vasta. (Kuna potentsiaalsete ründajate ja nende teadmiste taset tuleb tänu internetiühendusele hinnata väga kõrgeks, on käesolev turvaeesmärk eriti tähtis).
- kaitse mittesoovitud andmeliikumise vastu.

Lähtudes turvaeesmärkidest, tuleb välja töötada turvapoliitika, kus määratakse ära tulemüüri tööülesanded ja nende täitmiseks tulemüürile seatud nõudmised. Vastav turvapoliitika tuleb organisatsiooni IT-turvastrateegiasse sisse töötada ning seetõttu peab see olema IT-turvaosakonnaga kooskõlastatud.

Otsused tuleb dokumenteerida

Turvaeeskirja väljatöötamisel tulemüüri kohta vastu võetud otsused tuleks, sarnaselt otsuste aluseks olnud põhjendustega, selgelt kirja panna. Tulemüüri puudutava turvaeeskirja ellurakendamine toimub tulemüüri juurutamise läbi, mis tähendab sobilike riistvarakomponentide, paketifiltrite ja Application-Level-Gateway väljavalimist ning hoolikat filtrireeglite määramist ja ellurakendamist. Kuna mõisted paketifilter ning Application-Level-Gateway on järgnevate lõikude mõistmiseks väga olulised, toome vääritimõistmise vältimiseks siinkohal ära nende mõistete lühikese sisuseletuse.

Paketifilter

- Paketifiltrid on spetsiaalse tarkvaraga IT-süsteemid, mis filtreerivad tuginedes OSI-mudeli alumiste kihtide (transpordikihi või ühenduskihi) päise andmetele ning saadavad paketid spetsiaalsete reeglite alusel edasi või hülgavad need (vt M 2.74 Sobiva paketifiltri valimine). Paketifiltrid langetavad otsuseid näiteks paketi allika või sihtkoha aadresside või portide alusel, ilma selle sisu puudutamata.

Application-Level-Gateway

- Application-Level-Gateway ehk rakenduslüüs on IT-süsteem, mis filtreerib kas ühe või mitme kokkukuuluva paketi kasutuskihi infot (st reaalset sisu ehk kasulikke andmeid) ning spetsiaalsete reeglite alusel võib see ühendusi või ka teatud käske lubada ja tühistada (vt M 2.75 Sobiva rakenduslüüsi valimine). Kui paketifiltrid töötavad OSI-mudeli kihtides nr 3 ja 4, siis rakenduslüüsid töötavad kihis nr 7. Application-Level-Gateway ehk rakenduslüüs on reeglina paigaldatud mõnda IT-süsteemi, mida kasutatakse vaid selle kindla ülesande täitmiseks ning mille käskude ulatus on piiratud miinimumini.

Selleks, et turvalüüs suudaks edukalt täita oma ülesannet ja kaitsta võrku väljast tulevate rünnete eest, peavad olema täidetud teatud põhjapanevad eeldused:

- Kogu kommunikatsioon, mis erinevate võrkude vahel aset leiab, peab toimuma läbi turvalüüsi. Selle tagamiseks peab olema kindlustatud, et ainukeseks liideseks kahe võrgu vahel oleks turvalüüs. Vastu tuleb võtta eeskirjad, mis sätestavad, et täiendavad välised ühendused tuleb luua läbi turvalüüsi, ning et turvalüüsist möödaminek on keelatud.
- Turvalüüsi tohib kasutada eranditult vaid kui sisemist võrku kaitsvat üleminekut. Seetõttu tohivad turvalüüsis endas saadaval olla vaid hädavajalikud teenused ning täiendavate teenuste (nt veebiserveri) pakkumisest tuleb loobuda. Seda, kuidas infoservereid ja teisi oma süsteemi all töötavaid komponente sobival moel turvalüüsi alla integreerida, selgitavad tere rida eri

süsteeme kirjeldavad meetmeid, vt M 4.223 Proksiserverite integreerimine turvalüüsi koostisesse või M 5.115 Veebiserveri integreerimine turvalüüsi koostisse .

- Turvalüüsi komponentide administreerimine tohib olla võimalik vaid ühe turvalise juurdepääsu kaudu, seega näiteks turvalise konsooli, krüpteeritud ühenduse või eraldi võrgu (administraatori võrgu) kaudu. Vastav konsool peaks olema üles seatud serveriruumi (vt B 2.4 Serveriruum).
- Turvalüüs peab arvestama kaitstava võrgu jaoks väljatöötatud turvaeeskirja nõudeid ja lubama ainult neid ühendusi, mis on turvaeeskirjaga lubatud. Vajadusel peab saama neid ühendusi defineerida väga detailselt (kuni individuaalse IP-aadressi, teenuse, aja, suuna ja erinevate kasutajateni välja).
- Turvalüüsi kontseptsiooni loomisel ja kasutamisel peab olema võimalik kasutada selleks sobiva personali abi. Turvalüüsi kasutamisega seotud aja kulu ei tohi alahinnata. Juba ainuüksi süsteemi poolt loodavate logiandmete analüüs võtab tihti küllaltki palju aega. Administraatoril peavad olema põhjalikud teadmised kasutatavatest IT-komponentidest ja ta peab saama asjakohase koolituse.
- Kohtvõrkude kasutajatele ei tohiks turvalüüsi kasutamine kaasa tuua liigseid kitsendusi.

Turvalüüside piirid

Turvalüüs suudab sisemist võrku Internetti ühendamise puhul küll paljude ohtude eest kaitsta, kuid see ei paku kaitset kõikide ohtude vastu. Seetõttu tuleks turvalüüsi ülesehitamisel ja turvaeeskirja väljatöötamisel ennast kurssi viia turvalüüsi võimaluste piiridega:

- Kontrollitakse logisid, mitte edastatud informatsiooni. Logi kontrollimine kinnitab näiteks, et teatud e-post saadeti õigete käskudega, kuid selle alusel ei saa teha mitte mingisuguseid järeldusi e-posti tegeliku sisu kohta.
- Aktiivse sisu filtreerimine õnnestub olenevalt olukorrast vaid mõningatel juhtudel, kuna on võimalik, et kõiki erinevaid meetodeid aktiivse sisu varjamiseks ei suudeta ära tunda.
- Niipea kui mõnel kasutajal on õigus luua turvalüüsi kaudu kommunikatsiooniühendusi, on tal võimalik kasutatava kommunikatsiooniprotokolli abil suvalisi teisi protokolle tunneldada. Seega võib organisatsiooni sees tulev pahatahtlik võimaldada juurdepääsu siseringi arvutitele või ise keelatud protokolle kasutada. Volitamata tunneldamist on tihti vaid väga raske kindlaks teha.
- Internetikasutuse piiramine kindlate veebiserveritega on praktiliselt võimatu, kuna paljud veebiserverid on kasutatavad ka prokside kaudu. Seetõttu on võimalik teatud IP-aadresside sulgemisest kergesti mööda minna.
- Veebiaadresside filtreerimist võimaldav tarkvara (URL-idel põhinev) ei ole tihti veel piisavalt välja arendatud. Näiteks võib juhtuda, et programm ei hõlma kõiki adresseerimisviise. Järgnev näide BSI-veebiserveri kohta peaks selgitama erinevaid adresseerimiseks kasutatavaid võimalusi. Toodud loetelu ei ole kaugeltki täielik, kuna tähti on võimalik kuvada ka Escape -jadade abil.

www.bsi.bund.de
www.bsi.de
194.95.176.226

- Lisaks on võimalik URLi filtritest nn anonümiseerijate abil mööda minna.
- Spam-meilide filtreerimine ei ole hetkel veel piisavalt välja töötatud. Mitte ükski SMTP-Proxy ei suuda vaieldamatult kindlaks teha, kas teatud e-post on kliendi poolt soovitud või mitte. Spam-maile tohib kõrvaldada alles siis, kui e-posti saatjad on vaieldamatult tuvastatud. Tavalise SMTP- protokolliga üksi ei ole seda võimalik teostada.
- Turvalüüsid ei suuda kaitset pakkuda kõikide teenuse tõkestus rünnete (Denial-of-Service) vastu. Kui ründe läbiviija tõkestab nt ühenduse Provider iga, pole ka kõige paremast turvalüüsist mitte mingisugust kasu. Lisaks esineb alati vigu protokollide juurutamisel lõppseadmetesse, mida turvaproksid ei suuda tuvastada.
- Turvalüüs võib küll võrgu üleminekut turvata, kuid võrgu sees toimuva kommunikatsiooni turvalisust ei mõjuta see mitte kuidagi!
- Ka spetsiaalsetes turvalüüside jaoks välja töötatud komponentides, mille puhul on arvestatud kõikide turvaaspektidega, võib hoolikale tööle vaatamata siiski vigasid esineda.
- Kaitstavate klientide või serverite ettekavatsetud või kogemata vääralt teostatud konfiguratsiooni vastu suudavad turvalüüsid vaid vähe aidata.
- Kasutatavasse tarkvarasse sisseehitatud tagauste kaudu võib funktsioonide kasutusvõimalus säilida ka läbi turvalüüsi. Ekstreemsematel juhtudel võib isegi turvalüüsi enda tarkavara sisaldada tagauksi.
- Turvalüüsi komponentide korrektne konfigureerimine on tihti väga raske. Konfiguratsiooni vead võivad viia turvaaukude tekkimise või avariideni.
- Kui turvalüüsi tootjafirma poolt kaasa pandud tehniline dokumentatsioon on puudulik, soodustab see vigade tekkimist konfigureerimise ja administreerimise käigus.
- Kui turvalüüsi komponendid on valesti dimensioneeritud, võib see mõjutada süsteemi kättesaadavust. Kui näiteks arvuti, mille all töötab HTTP-turvaproksi, on dimensioneeritud liiga nõrgalt (liiga vähe töömälu, liiga aeglane protsessor), võib see oluliselt mõjutada Interneti kasutamise kiirust .
- Ründe planeerijaid ei ole võimalik takistada, kui nad on võtnud nõuks turvalüüside komponentide skaneerimise ja sellel abil turvaaugud välja peilida.
- Turvalüüs ei suuda pakkuda kaitset kasutajapoolse teadliku või mitteteadliku turvaeeskirjade ja turvakontseptsioonide eiramise vastu.
- Turvalüüs ei suuda kaitsta ühiskasutusse antud kommunikatsioonivõimaluste väärkasutamise vastu, kui see tuleb organisatsiooni seest (nn Insider - ründed).
- Turvalüüs ei paku kaitset Social Engineeringu (inimestega manipuleerimise) vastu.
- Kui sisevõrku ühendatakse töötajate mobiilseid lõppseadmeid (sülearvuteid, pihuarvuteid), mida kasutatakse ka sisevõrgust väljas, eksisteerib oht kahjulike komponentide (viiruste, ussviiruste, Trooja hobuste) sissetoomiseks.
- Turvalüüs ei suuda kaitset pakkuda ka selle vastu, kui kahjulikke programme püütakse usaldusväärsesse võrku sisse tuua vahetatavate andmekandjate kaudu (nt CD-ROMid, disketid, USB-mälupulgad).

Täiendavad kontrollküsimused:

- Kas turvalüüsi turvaeesmärgid on dokumenteeritud?
- Kas turvalüüsi turvapoliitika on üldise turvastrateegiaga kooskõlas?

M 2.71 Turvalüüsi (tulemüüri) turvapoliitika

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: IT-turvaosakond, administraator

Tulemüüri turvapoliitika määrab ära tulemüüride käitumise. See defineerib tulemüüri käitumise erineva informatsiooni, teenuste ja protokollide suhtes ning määrab, kellel on õigus neid kasutada. Turvapoliitikat ei tohi segi ajada tulemüüri turvaeeskirjaga, mille eesmärgiks on tulemüüri enda turvalise kasutamise reeglite kindlaksmääramine.

Kommunikatsiooninõuded

Turvapoliitika loomiseks tuleb esmalt välja selgitada, millist erinevat liiki kommunikatsiooni tahetakse välise võrguga lubada. Kommunikatsiooninõuete kindlaksmääramisel tuleb leida vastused järgnevatele küsimustele:

- Milline informatsioon tohib läbi tulemüüri välja liikuda ning millisel informatsioonil lubatakse väljast sisse liikuda?
- Mis liiki informatsiooni peaks tulemüür varjama (nt sisevõrgu struktuuri või kasutajanimesid)?
- Milliseid autentimisprotsesse tuleks kasutada kaitstava võrgu sees, st tulemüüri jaoks (nt ühekordseid paroole või kiipkaarte)?
- Milliseid juurdepääse läheb tarvis (nt kas ainult mõne internetiteenuse pakkuja omi või ka Modem-Pool lahendusi)?
- Kui suur on oodatav andmete liikuvuse maht?

Teenuste valimine

Väljaselgitatud kommunikatsiooninõuete alusel tuletatakse teenused, mille kasutamist soovitakse kaitstavas võrgus lubada. Siinkohal tuleb vahet teha nende teenuste vahel, mis on mõeldud siseringi kasutajatele kaitstava võrgu sees ja nende teenuste vahel, mis tehakse kättesaadavaks väljastpoolt tulevatele kasutajatele. Kui kasutusfunktsioonide hulka kuulub näiteks e-posti vastuvõtmise võimalus, (mis kuulub üldjuhul miinimumnõuete alla), peab tulemüür lubama SMTP-protokolli kasutamist. Turvapoliitikas peab olema selgelt kindlaks määratud, milliseid teenuseid erinevad kasutajad ja/või arvutid tohivad kasutada ning millistele teenustele tuleb tagada konfidentsiaalsus ja/või terviklus. Kasutusse tuleks lubada ainult need teenused, mis on tõepoolest hädavajalikud. Kõikide ülejäänud teenuste kasutamine tuleb ära keelata. Selline peab olema ka eelseadistus: nende teenuste kasutamist, mille kohta ei ole selgeid kasutusreegleid kehtestatud, ei tohi lubada. Iga lubatud teenuse kohta tuleb kindlaks määrata, milliseid rakendatava protokolli funktsioone tohib kasutada ning milliste funktsioonide kasutamist tuleks takistada (nt FTP käsk “PORT” aktiivse FTP tõkestamiseks) ning milliseid edastatud võrdlusandmeid tuleks filtreerida (nt arvutiviiruste tuvastamiseks). Tuleb kindlaks määrata millistel nädalapäevadel ja millistel kellaaegadel võib lubatud teenuseid kasutada. Lühiajaliste muudatuste tegemiseks (nt testimise ajaks) või uute teenuste tarbeks tuleb välja töötada erijuhtumite reeglid. Filtritele tuleb kehtestada oma nõuded, st nii paketifiltrile, mis kasutab OSI-kihimudeli 3. ja 4. kihi (IP, ICMP, ARP, TCP ja UDP) päise informatsiooni kui ka turvaproksidele, mis kasutavad kasutuskihi teenuste (nt. Telnet, FTP, SMTP, DNS, NNTP, HTTP) informatsiooni. Ülevaate selle kohta, mida tuleb erinevate protokollide ja teenuste turvaliseks kasutuseks järgida, leiate M 5.39 Protokollide ja teenuste ohutu kasutamine . Sellest lähtuvalt tuleb sõnastada filtreerimisreeglid (vt M 2.76 Sobivate filtreerimisreeglite valimine ja kehtestamine).

Organisatoorse töö reeglid

Lisaks filtreerimisreeglite hoolikale väljatöötamisele ja elluviimisele tuleb vastu võtta järgnevad organisatoorset tööd puudutavad otsused:

- Kindlaks tuleb määrata nii filtreerimisreeglite väljatöötamise kui ka nende ellurakendamise ja testimise eest vastutavad töötajad. Kindlaks tuleb määrata isikud, kellele antakse volitused filtreerimisreeglite muutmiseks, nt uute teenuste testimise tarbeks.
- Tuleb kindlaks määrata, mis liiki informatsiooni tuleks koguda logidesse ning kes peaks vastavaid logiandmeid analüüsima. Logi peab hõlmama nii korrektselt loodud kui ka tõkestatud ühenduste kohta käivaid andmeid. Andmete logimine peab vastama andmekaitse kohta kehtivatele eeskirjadele.
- Kasutajaid tuleb teavitada piisavalt nende õigustest, eriti kasutajaandmete filtreerimise ulatusest.
- Kasutajatele on soovitav välja jagada vastav dokumentatsioon, millest saab välja lugeda, millist teenust millises mahus kasutada tohib ning kas selle juures on tarvis järgida teatud iseärasusi.
- Tulemüüri vastu suunatud ründeid peab olema võimalik mitte ainult edukalt ära hoida vaid ka kiiresti tuvastada. Ründeid on võimalik avastada logiandmete analüüsimise läbi. Siiski peaks ka tulemüür ise suutma eelnevalt defineeritud sündmuste põhjal, nt kui mõnel Application-Level-Gatewayl ebaõnnestub parooli sisestamine liiga tihti või kui püütakse luua keelatud ühendusi, väljastada sellekohaseid hoiatusi või koguni astuda teatud samme .
- Kindlaks tuleb määrata funktsioonid, mida võimaliku ründe korral rakendada, nt kas ründajat hakatakse jälitama või kas süsteemist välja viiv võrguühendus tuleks katkestada. Kuna selline tegevus võib tugevasti mõjutada võrgu tööd, peavad olema määratud kindlad isikud, kes otsustavad, kas asetleidnud sündmuse näol on tegemist ründega ning kas on tarvis selle vastu midagi ette võtta. Vastavate töötajate ülesanded, nende teadmistele esitatavad nõuded ning nende funktsioonid peavad olema selgelt määratletud.

Turvapoliitika kehtestamisel peavad olema lahendatud järgmised küsimused:

- Milliseid kahjusid võib endaga kaasa tuua olukord, kus kaitstava võrgu tulemüürist on suudetud läbi tungida? Kuna absoluutset turvalisust ei ole olemas, tuleb otsustada, kas maksimaalse võimaliku kahju tagajärgedega suudetakse toime tulla, või on tarvis rakendada täiendavaid meetmeid.
- Millised on tulemüüri korrakohase kasutamise jääkohud? Näiteks võivad selle alla kuuluda kasutatavate seadmete ja operatsioonisüsteemide kitsaskohad.
- Kui ruttu suudetakse tulemüüri vastu sooritatud rünnet tuvastada?
- Millised logiandmed on kättesaadavad ka pärast edukaks osutunud rünnet?
- Kas kasutajad on valmis tulemüürist tingitud kitsendusi aktsepteerima?

Otsused ja põhjendused tuleb dokumenteerida

Turvapoliitika kohta vastuvõetud otsused tuleb dokumenteerida. Sellele lisaks on tähtis, et kirja saaks pandud ka otsuste langetamisel oluliseks osutunud info ja

otsuste langetamise põhjused, et neid oleks võimalik hiljem (nt turvapoliitika auditeerimise käigus) mõista. Taustainformatsiooni ei ole ilmtingimata tarvis turvapoliitika enda dokumentide hulka lisada, pigem on soovitatav koostada selle kohata eraldi dokument.

Täiendavad kontrollküsimused:

- Milliseid teenuseid ja protokolle tahetakse läbi tulemüüri kasutama hakata?
- Kas väljavalitud kasutatavate teenuste valikukriteeriumid on dokumenteeritud?
- Kas tulemüüri tööd ja järelvalvet puudutavad volitused on kindlalt määratletud?

M 2.73 Sobiva turvalüüsi (tulemüüri) põhistruktuuri väljavalimine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: IT-turvaosakond, administraator

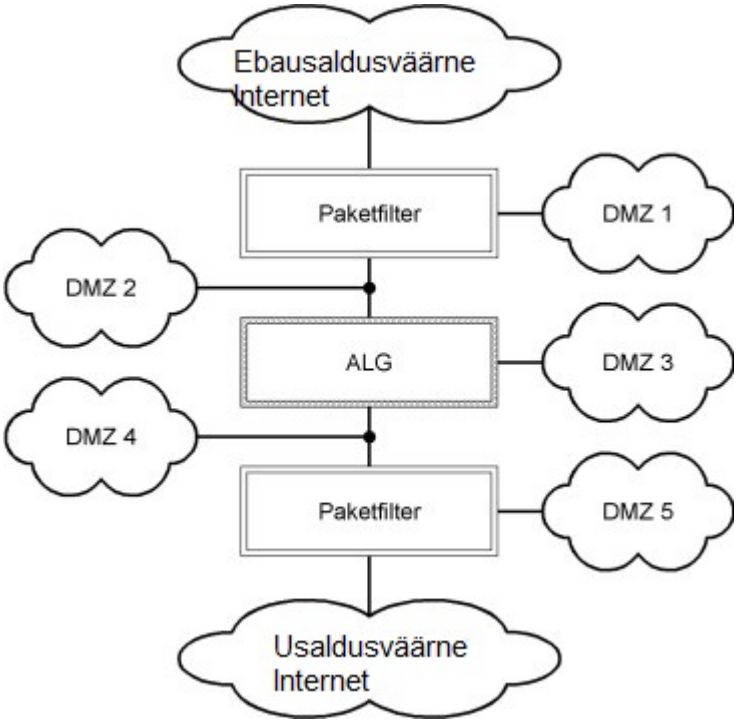
Peale tulemüüri turvapoliitika kehtestamist tuleb otsustada, milliste komponentide abil soovitakse tulemüüri ellu rakendada. Selle jaoks tuleb välja valida sobilik paigutus.

Tulemüüride alusstruktuurid

Üldiselt on olemas kaks mõistlikku alusstruktuuri, mida võib kasutada näidistena tulemüüri ülesehitamiseks. Alusstruktuure selgitatakse järgnevate punktide abil.

1. Paketifilter - Application-Level-Gateway - Paketifilter (P-A-P)

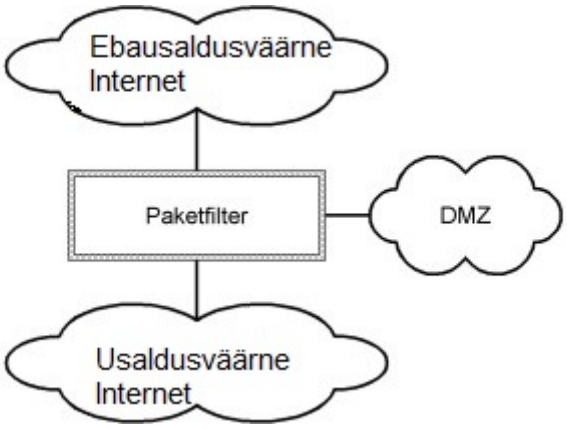
Selle alusstruktuuri puhul lülitatakse paketifilter, Application-Level-Gateway (ALG) ja veel üks paketifilter „üksteise järele“ nii, et igasugune andmete liikumine peab oma teel läbima kõik kolm nimetatud komponenti. Järgneval joonisel on näidatud mõningaid võimalusi nn demilitariseeritud tsoonide (DMZ) loomiseks, kus tulemüüri täiendavaid komponente on võimalik kasutada kaitstud keskkonnas. Sellise skeemi järgi ülesehitatud tulemüüride kasutusalaks on eelkõige võrkude lahutamine juhtudel, kus kahe võrgu usaldusväärsus erineb teineteisest märgatavalt (nt Interneti lahutamine intranetist), või sisevõrgu kahe allvõru lahutamine, kui nende turvanõuded on teineteisest märgatavalt erinevad. Mõlema paketifiltri puhul ei pea ilmtingimata tegu olema spetsiaalselt selleks otstarbeks kasutatavate IT-süsteemidega (arvutite või masinatega). Juhul kui kasutatavatesse marsruuteritesse on integreeritud paketifiltri funktsioonid, võivad marsruuterid ka tulemüüri paketifiltri funktsioonid enda kanda võtta. Samas on paketifiltrite funktsioonid marsruuterite puhul tihti küllaltki piiratud, mistõttu võib teatud kasutusvaldkondades siiski ka vaja minna spetsiaalseid paketifiltreid.



Joonis 1: Mitmeastmeline ülesehitus, mis koosneb P-A-P-ist

2. Ainult paketifilter

Tulemüüri kõige lihtsam alusstruktuur koosneb ühest ainsast paketifiltrist. Peamine probleem kogu kommunikatsiooni filtreerimisel ühe ainsa paketifiltriga seisneb selles, et otsus, kas teatud juurdepääsu lubada või keelata, langetatakse erinevatel IP-del põhinevate protokollide päise andmete analüüsimisel, mille andmeid on kerge võltsida.



Joonis 2: üheastmeline ülesehitus, mis koosneb ainult ühest paketifiltrist

Seetõttu on kasutusalaks eelkõige:

1. Kahe võrgu teineteisest lahutamine juhtudel, kus võrkude usaldusväärsus erineb teineteisest vaid vähesel määral (nt Interneti eraldamine intranetist, mille kaitsevajadus on väike).
2. Kahe organisatsioonisisese võrgu teineteisest lahutamine.
3. Kodukasutajad (koduarvuti internetijuurdepääsu kaitsmine).

Usaldusväärse võrgu IP päise kohta käiva informatsiooni väljumist, nt IP-ID või TTL („Time-To-Live“) kohta suudab ära hoida täiendava IP-proksi kasutamine. IP-ID abil saab vaatamata NAT-funktsioonile määrata usaldusväärsesse võrku ühendatud arvutite arvu ning TTL võimaldab teha järeldusi kasutatavate operatsioonisüsteemide kohta. Paketifiltri reeglite või sobiliku marsruutimise abil tuleb tagada, et IP-proksist ei oleks võimalik mööda minna.

Alusstruktuuride eelised ja puudused

Üldjuhul võib soovitada, et kõikides rakendusvaldkondades, kus on tarvis saavutada kõrgemat turbeastet, võiks kasutada P-A-P struktuuri. Struktuuri erinevatest komponentidest loobumine toob alati endaga kaasa turvalisuse nõrgenemise. Järgnev tabel on toodud võrdluseks P-A-P struktuuri ja ühest ainsast paketifiltrist koosneva struktuurikasutuskeskkonna eelistest ja puudustest.

- Saab võtta aluseks kõrgete turvanõuete täitmisel. - Tänu erinevate moodulite kasutamisele on süsteem piisavalt keerukas. - Ei saa kasutada kõikides rakenduskeskkondades. Näiteks IPSEC-andmesidet ei saa läbi TCP/IP-Proxy juhtida. - Lihtsad laiendamisvõimalused, nt viiruseskaneerijat ja spämmifiltrit on võimalik ilma suurema vaevata ALG külge ühendada. - Klientide tarkvaras esinevate turvaaukude ärakasutamist on võimalik osaliselt tõkestada. - Laialdased võimalused andmete logimiseks.	- Ei paku kõrget turbeastet, parimal juhul piisav, et tagada tavakasutuse turve. - Võrreldes P-A-P struktuuriga on administreerimine suhteliselt lihtne. - Madalad investeerimiskulud (tarkvara on tasuta, st paljudes operatsiooni-süsteemides juba olemas). - Kitsendused maksimaalsele andmete läbilaskevõimele võrgu ülemineku juures peaaegu et puuduvad. - Lihtne, põhjapanev turve. - Integreerimine kaitstavasse arvutisse on teoreetiliselt mõeldav (nt on võimalik veebiserverit samaaegselt ka paketifiltrina kasutada). Uute teenuste lisamine P-A-P struktuuriga võrreldes tugevalt lihtsustatud.

Tabel 1: P-A-P ja üksiku paketifiltri struktuuri eelised ja puudused

Rakenduslüüsi ehk Application-Level-Gateway peal töötavad niinimetatud Proxy-protsessid (nimetatakse tihti ka Proxy-Serveriks), mis pärast kasutaja autentimisprotsessi loovad ühenduse sihtkoha arvuti ning filtreerivad andmeid vastavalt kasutuskihis olemasolevale informatsioonile. Ühendusi, mille jaoks Proxy-protsesse ei eksisteeri, ei ole võimalik luua. Arvutid, millel soovitakse rakendada tulemüüri üksikkomponente, peavad olema seadistatud selliselt, et neil töötaksid vaid hädavalikud programmid (minimaalne süsteem). Kasutatavad programmid peavad olema õigesti konfigureeritud ning kõik teadaolevad turvaaugud peavad olema kõrvaldatud. Juhul kui kõrge turbeastme saavutamiseks soovitakse üksteisega ühendada mitu süsteemi, on ülimalt soovitatav, et vastavad süsteemid pandaks tööle erinevate süsteemide all (nt erinevate operatsioonisüsteemide abil). Niimoodi välistatakse olukord, kus ründajal oleks tulemüürist jagusaamine liiga lihtne, kuna kõikides süsteemides saaks ära kasutada täpselt samasuguseid turvaauke.

Nõuandeid alusstruktuuri valimiseks

Küsimus, millist tüüpi struktuuriga tulemüüri tuleks parasjagu kasutada, sõltub ühelt poolt sellest, kui palju erineb teineteisest lahutatavate võrkude usaldusväärsus (st kui ebausaldusväärne on vähem usaldatav võrk) ning teiselt poolt ka sellest, kui kõrget turbeastet on vaja saavutada tulemüüriga kaitstava võrgu jaoks.

Erijuhtum Internet

Antud kontekstis on kõige väiksema usaldusväärusega võrguks Internet. Kui oma võrku tahetakse ühendada Internetiga, tuleks üldjuhul langetada oma valik mitmeastmelise P-A-P struktuuri kasuks. Sellest soovitusest võib kõrvale kalduda ainult erijuhtumite korral, näiteks kui võrgud on väga väikesed ning nende kaitsmine mitmeastmelise tulemüüriga oleks liiga tülikas või kui kaitstava võrgu turbevajadused on madalad. Ka sellistel juhtudel tuleb kasutada vähemalt ühte pake-

tifiltrit, mis peab olema eriti hoolikalt konfigureeritud. Juhul kui vähem usaldatava võrgu usaldusväärsus on ainult natuke madalam, pole võrkude teineteisest eraldamiseks tarvis mitmeastmelist tulemüüri. Niisugustel juhtudel on hoolikalt konfigureeritud paketifilter üldjuhul täiesti piisav. Ainult vähesel määral teineteisest erineva usaldusväärsusega võrgud võivad esineda näiteks järgnevate võrgutüüpide korral:

- Teised (organisatsiooni-) sisesed võrgud
- Internetiühendusteta võrgud
- Internetiühendusega võrgud, mis on Internetist eraldatud spetsiaalsete turvameetmete abil (nt oma tulemüüriga).

Järgnev tabel võtab kokku erinevad soovitused:

Kasutusala	Soovituslik ülesehitus
Sisevõrgu kahe samade turbevajadustega allvõrgu lahutamine teineteisest	Paketifilter. Tavalise turbevajaduse katmiseks piisab ühest integreeritud paketifiltri funktsiooniga marsruuterist.
Sisevõrgu kahe erinevate turbevajadustega allvõrgu lahutamine teineteisest (eriti siis, kui kõrge kaitsevajadusega võrk tuleb lahutada tavalise kaitsevajadusega võrgust).	Vähemalt paketifilter. Juhul kui vähemusaldusväärsest võrgu läbi on tarvis juurde pääseda kõrge turbeastmega võrgu mõnele teenusele, on soovitav see juurdepääs ALG abil kindlustada.
Spetsiaalsete turvanõuetega allvõrgu eraldamine mõnest teisest sisevõrgust.	Mitmeastmeline ülesehitus, mille koostiseks on paketifilter - ALG - paketifilter. Lisaks on turvalisust tarvis siinkohal vaadelda veidi täpsemalt. Mitmeastmelisse struktuuri tuleb siinkohal suhtuda kui alusesse, mille peale on võimalik kõrgemat turbeastet üles ehitada. Enamjaolt tuleb rakendada täiendavaid meetmeid, kuid üldkehtivaid reegleid pole siinkohal välja tuua võimalik.

Oma võrgu eraldamine Internetist	Üldjuhul mitmeastmeline ülesehitus, st paketifilter - ALG - paketifilter. Erandjuhtumitel (väga väiksed võrgud, madal kaitsevajadus) võib piisata paketifiltrist (nt kui see on ühenduses NAT-Routeriga). Vähemalt e-posti ja HTTP teenuste tarbeks on ülimalt soovitav kasutada vastavat proksiserverit. Tavalise kaitsevajaduse korral võib sõltuvalt olukorrast sisemisest paketifiltrist ka loobuda. Kui otsustatakse P-A-P struktuuri kasuks, on ülimalt soovitatav, et läbi viidaks täiendav riskide hindamine.

Tabel 2: alusstruktuuride soovitused

Muud struktuurid

Lisaks senikirjeldatud struktuuridele võib kasutada ka teisi ülesehitusi, mis tekivad tihti P-A-P struktuuri komponentide loobumisest. Sellise tegevus on kahjuks alati seotud järeleandmistega turvalisuses.

Paketifiltritest loobumine ei ole mõttekas

Aeg-ajalt loobutakse näiteks „sisemisest“ paketifiltrist, mis eraldab ALG-d usaldusväärsest võrgust (st sisevõrgust). Kuna paljud marsruuterid on juba saadaval integreeritud paketifiltri funktsioonidega ning kulutused vastavate arvutite varustusele ei ole suured, ei ole olemas loogilist põhjendust, miks mõnest paketifiltrist peaks loobuma.

Eraldiseisvad seadmed (Appliances)

Paljud erinevad tootjad pakuvad tulemüüre eraldiseisvate seadmetena. Tegu on eelkonfigureeritud seadmetega, mis on osaliselt kokku pandud täiesti tavapärastest arvutikomponentidest ja töötavad mõne tavalise, selle jaoks kohandatud operatsioonisüsteemi all, kuid nende tootmisel ja konfigureerimisel on arvestatud täpselt piiritletud kasutusalaga (paketifilter või ALG). Tooteid on saada väga laias valikus, alates puhtast paketifiltri funktsioonist kuni mitmeastmeliste lahendusteni välja, kus ühte seadmesse võib olla kokku koondatud tulemüüri mitu erinevat komponenti. Võrreldes nende tulemüüridega, mis on üles ehitatud „tavalistest“ arvutitest ning mida tuleb kas ise või mõnel teenusepakkujal vastavalt konfigureerida lasta, on eraldiseisvate seadmete eeliseks tihti just nende konfigureerimise lihtsus. Sellele eelisele vastandub aga jällegi tõsiasi, et niisugused konfiguratsioonid on vähem paindlikumad ning spetsiaalsete nõudmiste täitmiseks pakuvad nad vähem võimalusi. Lisaks on eraldiseisva seadme, kus ühe installeeritud operatsioonisüsteemi all töötavad mitu funktsiooni korraga (nt paketifilter ja ALG) puuduseks võrreldes tulemüüriga, mis on kokku pandud kolmest eraldi süsteemist, tõsiasi, et tulemüüri täielikuks kompromiteerimiseks on ründajal tarvis vaid ühe operatsioonisüsteemi turvamehhanismidest jagu saada. Tulemüüri planeerimise käigus tuleb selle asjaoluga arvestada. Kui otsustatakse siiski vastava seadme kasuks, võib soovitud turbeastme tagamiseks tarvis minna täiendavaid turvameetmeid.

Dokumenteerimine

Otsuse langetamine teatud kindla struktuuri kasuks tuleb koos otsuse langetamisel määravaks saanud põhjendustega arusaadavalt kirja panna.

Täiendav kontrollküsimus:

- Milline on tulemüüri jaoks väljavalitud struktuur? Kas otsuse langetamise põhjendused on dokumenteeritud?

M 2.74 Sobiva paketifiltri valimine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator

Transportimise ja võrgu tasandil võtavad tulemüüri funktsioonid enda kanda niinimetatud paketifiltrid. Paketifiltri ülesandeks on andmepakettide töötlemine UDP/IP- ja TCP/IP-kihi päises sisalduvate andmete põhjal (nt IP-aadress ja pordi number). Vastavad otsused teeb paketifilter vastavalt administraatori poolt ette antud filtreerimisreeglitele. Paljudel juhtudel pakuvad paketifiltrid ka „ Network Address Translation “ (NAT) võimalust, mille puhul asendatakse IP-pakettide saatja aadressid paketifiltri IP-aadressiga. Niimoodi varjatakse kaitstava võrgu struktuuri. Filtreerimisreeglite läbitöötamine toimub sisenevate andmepakettide kaupa järjestikku. Tavaliselt katkestatakse kontrollimine niipea kui avastatakse, et mõni pakett vastab teatud reeglile ning seejärel hakatakse vastavat reeglit paketi peal rakendama. Paketifiltreid saab nende filtreerimisvõimaluste alusel jaotada erinevatesse klassidesse.

Staatilised paketifiltrid

Paketifiltreid, mis teevad oma otsuse UDP/IP- ja TCP/IP-kihtide päise andmete (nt IP-allika aadressi, IP-sihtaadressi ja TCP-Flag-ide) põhjal, nimetatakse staatilisteks paketifiltriteks.

Dünaamilised paketifiltrid / Stateful Inspection

Dünaamilise paketifiltri näol (nimetatakse ka „Stateful Inspection“ funktsiooniga paketifiltriks) on tegemist staatilise paketifiltri funktsioonide laiendusega, mis võimaldab vaadelda ka kommunikatsiooni konteksti. Dünaamilised paketifiltrid suudavad ka ühendusevabade protokollide (nt UDP) puhul otsustada, kas sissetuleva andmepaketi puhul on tegemist vastusega teatud päringule või kuulub see pakett hoopis loodava kommunikatsiooniühenduse juurde. Lisaks on võimalik turvaliselt tagada ka nende teenuste kasutamine, mis ei ole seotud kindlate pordinumbritega, kuna ka siin suunatakse paketid edasi pordinumbritest sõltumata ning ainult siis, kui eelnevalt on usaldusväärsest võrgust tulnud sobilik päring. Dünaamiline paketifilter salvestab teatud ajaks väljuvate pakettide IP-allikate aadressid ning allikate portide numbrid. Sissetulevad IP-paketid saadetakse edasi vaid juhul, kui nende sihtkoha IP-aadress ja pordi number on mälus veel alles, st kui usaldusväärsest võrgust algatati eelnevalt mõni päring ning kui kindlaksmääratud ooteaega ei ole ületatud. Stateful Inspection funktsiooniga paketifiltrid võimaldavad edastatavaid andmeid jälgida tihti lisaks ka veel kasutaja tasandilt.

Paketifiltrite ellurakendamise võimalused

1. Arvuti seadistamine paketifiltriks, kasutades selleks operatsioonisüsteemi, milles on hädavajalikud funktsioonid olemas.

Eelised	Puudused

Sõltuvalt kasutatavast operatsioonisüsteemist võivad kulutused olla suhtelised väiksed.	- Pikad seisakud võimalike defektide tõttu, kuna väljavahetatava riistvara puhul tuleb vajadusel kogu operatsioonisüsteem uuesti installeerida ja konfigureerida. - Minimaalse süsteemi konfigureeri-mine nõuab suhteliselt palju tööd (paketifiltri funktsiooniga marsruuteriga võrreldes). - Minimaalse süsteemi konfigureeri-mine eeldab ülesehituse kohta käiva oskusteabe olemasolu. - PC-süsteemide riistvara on kahjustustele tihti palju vastuvõtlikum kui eraldiseisvad seadmed, kuna viimastel puuduvad tihti kõvakettad või ventilaatorid. - Administreerimiskulud on reeglina suuremad kui eraldiseisvate süsteemide puhul, kuna konfigureerimisliidesed ei ole tihti enam kättesaadavad. - Tihti on need keerulisemad kui eraldiseisvad seadmed.

Tabel 1: arvuti seadistamine paketifiltri funktsiooni täitmiseks

2. Marsruuteri filtreerimisreeglite seadistamine

Eelised	Puudused
- Kui marsruuter on juba olemas, siis täiendavaid kulutusi pole tarvis. - Võrreldes arvutitel põhinevate paketi-filtritega on avarii tekkimise võimalus väike, kuna üldjuhul on marsruuterite poolt pakutav kättesaadavus parem.	- Marsruuterite laiendamisvõimalused on tihti piiratud. - Konfigureerimine võib olla keerulisem kui eraldiseisvate seadmete või arvutitel põhinevate paketifiltrite puhul. - Juhul kui marsruuter seatakse üles teenusepakkuja juures ning kui teenusepakkuja seda ka administreerib, siis organisatsiooni enda personal ei saa kontrollida marsruuteri turvafunktsioone .

Tabel 2: marsruuteri filtreerimisreeglite seadistamisega seotud eelised ja puudused

3. Eraldiseisva seadme kasutamine

Eelised	Puudused

- Kasutuselevõtmiseks kulub vähe aega. - Kasutatavate funktsioonide konfigureerimine on tehtud lihtsaks (nt veebipõhise kasutajaliidese abil). - Lihtne konfigureerida, kuna eraldiseisvatel seadmetel on tihti oma administreerimisliidesed. - Eraldiseisvatel seadmetel on tihti automaatsete täiendite laadimise tugi. - Võrreldes arvutitel põhinevate paketifiltritega on avarii tekkevõimalus pigem väike, kuna eraldiseisvad seadmed sisaldavad tihti vähem „liikuvaid masinaosi“ (nt kõvakettaid või ventilaatoreid) kui tavapärased arvutid.	- Tootjapoolse riist- ja tarkvara laiendamisvõimalused on piiratud. - Kui seadet tuleb vigade korral tihti tootja juurde tagasi saata, kuna vastavaid hooldelepinguid ei ole sõlmitud, võib seisakuaeg muutuda pikaks. Seetõttu tuleks vajadusel muretseda asendusseade, mida hoitakse „Cold Standby“ režiimis. - Spetsiaalsete toodete turvalise konfigureerimise ja kasutamise kohta on vähe informatsiooni saada (täiendavat infot lisaks tootjainfole). Eriti problemaatiliseks muutuvad need juhud, kus tootja lõpetab omapoolse toe. - Teatud eraldiseisvad süsteemid võivad olla vähe levinud. Niisugustel juhtudel on väga vähe nõustajaid või teenusepakkujaid.

Tabel 3: eraldiseisva seadme kasutamine

Paketifiltrile esitatavad nõuded

Kõigi kolme valiku puhul on sõltuvalt olukorrast võimalik paketifiltri konfiguratsiooni tuletada olemasolevast ALG-st automaatselt (kui ALG on olemas). Ühelt poolt pakub see küll eeliseid konfigureerimisel, kuna vaeva on vähem, kuid teiselt poolt jällegi kaasneb sellega madalam turvalisus, kuna ALG väär konfiguratsioon tekitab automaatselt ka paketifiltri väära konfiguratsiooni. Enne soetamist tuleks kontrollida, milliseid järgnevatest tingimustest vastav ALG täita suudab. Vastavalt rakendustingimustele võib mõnedest nõudmistest sealjuures loobuda, st loetletud nõudmisi tuleb hinnata vastavalt rakenduskeskkonna kontekstile.

Paketifilter võiks toetada järgmiste funktsioonide kasutamist:

1. Pakettide edasisaatmine või sellest loobumine, lähtudes

   - üksikute arvutite või võrkude allika IPst ja sihtkoha aadressist,
   - allika ja sihtkoha portidest,
   - ICMP-tüübist,
   - kõikidest TCP-Flag-idest (URG, ACK, PSH, RST, SYN, FIN). Näiteks ACK-Biti abil on võimalik eristada ühenduse loomise pakettide ja juba loodud ühenduste raames liikuvate pakettide vahel. Kontrollides teisi Bitte, on võimalik ebamõistlike TCP-Flagide kombinatsioone sisaldavaid IP-pakette keelata.
   - IP-valikutest.

2. Erinevate tegevuste tugi

   - Paketi edasisaatmine („allow“).
   - Paketi keelamine („deny & drop“).
   - Paketi keelamine ja teade selle saatjale („deny & reject“).

3. Filtreerimisreeglite loomise võimalus eraldi iga paketifiltri ühendusliidese kohta.

4. Saabuvate ja väljuvate pakettide eraldi filtreerimine.

5. Võimalus filtreerimisreeglite läbitöötamise järjekorda määrata nii, et seda ei saa muuta.

6. Iga paketi IP-aadressi, teenuse, aja, kuupäeva logimisvõimalus ning võimalus seda valikut piirata ka teatud kindlate pakettide jaoks.

7. Neil juhtudel, kus marsruuterit kasutatakse ka paketifiltrina, peab dünaamiline marsruutimine olema konfigureeritud selliselt, et kaitstavat võrku puudutavad marsruutimise paketid (nt RIP) oleks lubatud ainult selle liidese kaudu, mis on ka ise kaitstava võrguga ühenduses.

8. Kaitse IP-spuufingu vastu.

9. Kui tulemüürina kasutatakse ainult ühte paketifiltrit ilma ALGta, peab sellel olema järgnevate täiendavate funktsioonide tugi:

- Port-Forwarding (nimetatakse ka „Destination NAT“)
- Network Address Translation (NAT). Samuti järgnev tugi:
- IP-ID asendamine
- TLL-i asendamine
- Stateful Inspection.

Paketifiltrile esitatavad nõuded ja valiku tegemisel oluliseks saanud põhjused tuleb arusaadavalt dokumenteerida.

Täiendavad kontrollküsimused:

- Millised nõudmised on kehtestatud paketifiltrile?
- Mis liiki paketifiltreid (arvuteid, marsruutereid, eraldiseisvaid seadmeid) kasutatakse? Kas valiku tegemise põhjused on dokumenteeritud?

M 2.75 Sobiva rakenduslüüsi valimine

Algatamise eest vastutavad: IT juht, IT turvaosakond

Rakendamise eest vastutavad: IT-turvaosakond, administraator

Kasutaja tasandil võtavad tulemüüri funktsioonid enda kanda niinimetatud Application-Level-Gateways (ALG-d) ehk rakenduslüüsid. Kaudselt täidavad ALGd ka 1-3. kihi funktsioone. ALGsid nimetatakse ka tihti turvaproksideks, järgnevas tekstis on kasutatud mõiste lühendatud versiooni „Proxy“. Proksid katkestavad otsese andmevoo allika ja selle sihtkoha vahel. Kliendi ja serveri vahelises kommunikatsioonis, mis toimub üle Proxy, võtab Proxy kliendi päringud vastu ja saadab need serverile edasi. Proxy toimib analoogselt ka siis, kui ühenduse loomine toimub vastupidises järjekorras, st serverilt kliendi suunas. Kõik kommunikatsioonisuhted kahe arvuti vahel kulgevad sellisel juhul otseselt Proxy kaudu. Järgnevas loetelus on püütud kokku võtta turvaprokside mõningaid eeliseid ja puudusi.

Prokside eelised

- Võrreldes Proxy poolt kaitstavate klientide ja serverite teenuseprogrammidega esineb programmeerimisvigu tihti vähem.
- Üksikute protokollikäskude filtreerimist (nt HTTP puhul käsk POST) on võimalik teha kooskõlas käskude, aja ja kasutajate parameetrite määramisega.
- Edastatavatest andmetest on võimalik eemaldada soovimatu sisu.
- Kaitse rünnete vastu, mis põhinevad vigastel päise andemetel .
- Edasisaadetava IP-paketi saatja-aadressi asendamine võrguliidese IP-aadressiga, läbi mille pakett vastavast proksist lahkub. Seeläbi suudetakse kaitstava võrgu IP-aadresse varjata. Lisaks tuleb DNS-i sellisel juhul sisestada ainult üks IP-aadress.
- Võimaldab kohustada tugeva autentimisprotsessi läbimist.
- Laialdased võimalused andmete logimiseks. Kasutajakihi iga ühenduse kohta on võimalik logida järgmisi andmeid:
- kasutaja identifitseerimistunnus
- allika ja sihtkoha arvuti IP-aadressid
- portide numbrid
- kellaaeg ja kuupäev.
- Sõltuvalt teenusest on võimalik logida ka täiendavat informatsiooni (nt HTTP puhul URLi).

Prokside puudused

- Andmete maksimaalse läbilaskevõime kahanemine.
- Pikemad vastuse ootamise ajad (latentsusajad) andmepäringute esitamisel.
- Võivad kaasneda mõningate klientprogrammide funktsioonide piirangud (nt aktiivse sisu filtreerimise tõttu).

Läbipaistvad ja mitteläbipaistvad proksid

Proksid võivad töötada kahes erinevas töörežiimis, nn läbipaistvas ja mitteläbipaistvas režiimis. Läbipaistvas režiimis töötava proksi kohta ei ole kliente tarvis eraldi teavitada. See loeb kõiki võrgus olevaid IP-pakette ja otsustab IP-aadresside ja portide numbrite alusel, millised pakette tohib teise võrku edasi saata ja milliseid mitte. Mitteläbipaistva proksi kasutamse puhul tuleb proksi kaudu toimiva ühenduse võimaldamiseks selle IP-aadress ja pordi number kliendi tarkvarasse sisse kanda (nt veebibrauserisse). Enne soetamist tuleks kontrollida, milliseid järgnevatest tingimustest vastav ALG täita suudab. Sõltuvalt kasutusvaldkonnast võib sealjuures teatud nõuetest ka loobuda. Loetletud nõudmisi tuleb hinnata vastavalt kasutuskeskkonna kontekstile. Kui mõnda teatud protokolli ei kasutata, ei pea ALG-l ilmtingimata vastava protokolli tuge olema. Kui ALG-l on siiski ka nende protokollide tugi, mille kasutamist ei planeerita, peaks ALG-l funktsioonide valikus olema võimalus nende protokollide desaktiveerimiseks. Juhul kui tulemüüri turvapoliitikaga on paika pandud, et teatud järgnevalt loetletud protokollide kasutamine on keelatud, ei pea seade loomulikult nende kasutamist toetama.

Hindamiskriteeriumid ja vastuvõetud otsused tuleb arusaadavalt dokumenteerida.

Üldnõuded

- Tähtsamate kasutatavate protokollide tugi (näiteks Telnet, FTP, SMTP, NNTP, HTTP ja HTTPS) kasutaja tasandil. Teiste teenuste kasutamiseks peaksid TCP ja UDP jaoks olemas olema geneerilised proksid.
- Application-Level-Gateway proksisid peab saama kasutada läbipaistvalt.
- ALG-le peaks saama integreerida oma MTA-d, et vajadusel olema võimalik erinevaid usaldusväärsete võrkude meiliedastusagente kasutada.
- Kahjuliku tarkvara tuvastamiseks peaks olema väliste analüüsiprogrammide ühendusliides (nt viirusetõrjeprogrammide kasutamiseks).
- Kasutajate autentimiseks peaks olema Directory -teenusega kommunikatsiooni astumise tugi
- Igat toetatavat protokolli peab saama filtreerida vastavalt M 2.76 Sobivate filtreerimisreeglite valimine ja kehtestamine kirjeldatud nõudmistele. Eriti oluline on, et filtreerimisreegleid saaks defineerida kasutajatest lähtuvalt, samuti peab olema võimalik kasutajaid kasutajarühmadesse kokku grupeerida.
- Sisust sõltuva filtreerimise tugi, et viirusetõrje käivitamist ja aktiivset materjali blokeerimist saaks teostada tsentraalselt (vt G 5.23 Viirused ja G 5.88 Aktiivsisu väärkasutus).
- Application-Level-Gateway kasutamisel ei tohiks olla vajadust muuta ei kaitstava võrgu ega ka välimise võrgu tarkvara.
- Iga kasutuskihis loodud ja seejärel keelatud ühendus peab kajastuma logis, mis annab infot asetleidnud sündmuses osalenud allika ja sihtkoha arvutite IP-aadresside, portide numbrite, kellaaja, kuupäeva ja asjassepuutuva reegli kohta, samuti peab olema võimalik kehtestada teatud ühendustele piiranguid.
- Logiandmetesse peaks saama kaasata edastatud andmete hulka.
- Logiandmetesse peaks saama kaasata ühenduse loomise ja sulgemise kellaaegasid.

Järgnevalt on kokku võetud spetsiaalsed nõudmised enamkasutatavate protokollide kohta:

HTTP:

- filtreerimisvõimalus Request -meetodi alusel, nt GET, HEAD, PUT või CONNECT
- veebisaitide kasutamise tõkestamine nende URLi alusel
- MIME-Types filtreerimine
- aktiivsisu ja küpsiste eemaldamine veebisaitidelt
- filtreerimine HTTP päise andmete põhjal
- võimalik peaks olema järgnevate päise väljade filtreerimine: Referrer, Via, From, Server
- „Web-Bugs“ filtreerimine
- kohustus tugeva autentimisprotsessi läbimiseks Proxy juures
- Accounting funktsioon kasutaja poolt edastatud andmepäringu andmekoguse määramiseks
- signatuuride kontrollimise tugi aktiivsisu signatuuride kontrollimiseks
- külastatud veebisaitide logimisfunktsioon
- keelatud Request -meetodite kasutamise logimisfunktsioon

HTTPS:

- andmeside ajutine dekrüpteerimine, et HTTPS-i kaudu kasutatavate veebisaitide aktiivsisu oleks võimalik eemaldada. Ajutine dekrüpteerimine tähendab, et edastatud andmed esmalt dekrüpteeritakse ning pärast aktiivsisu filtreerimist krüpteeritakse uuesti.
- külastatud veebisaitide logimisfunktsioon
- administraatori teavitamine automaatse Update-i raames ilmnenud aegunud või kehtetutest sertifikaatidest

SMTP:

- aktiivsisu eemaldamine HTML-E-postist
- MIME-Types filtreerimine
- filtreerimine saatja ja sihtkoha aadresside põhjal
- filtreerimine MTA IP-aadressi põhjal
- Mail-Relaying kontrollimine Domain-Name põhjal
- e-posti kohaletoimetamisvõimaluse kontrollimine domeeni nime põhjal
- kahtlaste e-posti lisade eemaldamine nende failinime lõppude põhjal. Blokeeritavaid lisasid peab saama vabalt määrata.
- Spämm-meilide tuvastamine erinevate filtreerimisprotsesside kombinatsioonina.
- Tuvastatud spämm-mailid tuleks kas kustutada, isoleerida (“Quarantine”) või markeerida.
- Tuvastatud e-mailid, mille päised ei vasta spetsifikatsioonidele („Bad Mails“) kas kustutada, isoleerida (”Quarantine") või markeerida.
- liides, mis võimaldaks spämmifiltri külgeühendamist.
- väljuvate e-posti blokeerimine võtmesõnade tuvastamise põhjal
- saatja ja adressaadi e-posti aadresside logimine
- e-posti edasisaatmise õnnestunud ja ebaõnnestunud toimingute logimine
- võimalus seadistada

- Mail-Relay (usaldusvääre võrgu MTA edasisaatmine ebausaldusväärse võrgu MTA juurde)
- Mail-Server (võimalus kasutada POP3 või IMAP protokolli ja edastada SMTP abil)

FTP (passiivne ja aktiivne):

- filtreerimine FTP-käskudega (nt GET, PUT, PASV, PORT)
- FTP-käskude kasutajapõhine lubamine ja keelamine
- piirangute kehtestamine failinimede põhjal (nt *.exe keelamine)
- kohustus tugeva autentimisprotsessi läbimiseks Proksi juures
- keelatud Request -meetodite kasutamise logimisfunktsioon
- autentimisel kasutatud kasutajanime logimine ja faili nime logimine

NNTP:

- filtreerimisvõimalus Request -meetodi alusel, nt ARTICLE, BODY, HEAD ja STAT
- keelatud Request -meetodite kasutamise logimisfunktsioon
- aktiivsisu ja küpsiste eemaldamine veebisaitidelt
- kohustus tugeva autentimisprotsessi läbimiseks Proxy juures
- üksikute foorumite sihipärane sulgemisvõimalus

Telnet:

- kohustus tugeva autentimisprotsessi läbimiseks Proxy juures
- autentimisel kasutatud kasutajanime logimine

POP:
- filtreerimisvõimalus Request -meetodi alusel, nt STAT, LIST, RETR või DELE
- aktiivsisu ja küpsiste eemaldamine HTML-E-postist
- keelatud Request -meetodite kasutamise logimisfunktsioon

UDP- ja TCP-Relays:

- kohustus tugeva autentimisprotsessi läbimiseks Proksi juures
- autentimisel kasutatud kasutajanime logimine

IP-Relay:

- VPNide loomisel läbi Application-Level-Gateway peaks olema IP-Relays tugi.

DNS:

- valmisolek integreeritud lahenduseks, mis koosneb avalikust ja privaatsest DNS-serverist
- DNS-prokside turvaline varjamine muust ALG operatsioonisüsteemist

Muutmata tekstiga protokollide nagu Telnet ja FTP kasutamist tuleks avalikes võrkudes vältida ning need tuleks asendada turvalisemate alternatiividega (SSH / SCP). Kas sisevõrkudes tuleks neid kasutada vaid juhul, kui olude sunnil ei ole üleminek SSH või mõne teise turvalisema protokolli kasutamisele võimalik. Ka POP protokolli tuleks rakendada äärmisel juhul vaid sisekasutuses. Kui e-postile on tarvis ligi pääseda mõne välise meiliserveri kaudu (nt mõne Provider i juures), tuleks eelistada varianti „POP SSL-i kaudu“. Vastaval juhul läheb tarvis SSL-proksit (analoogselt HTTPS-proksiga), mis katkestab krüpteeritud ühenduse tulemüüri juures ja võimaldab seeläbi e-poste tsentraalsel moel võimalike viiruste ja muu kahjuliku sisu suhtes kontrollida.

Täiendavad kontrollküsimused:

- Milliste protokollide kasutamist väljavalitud ALG toetab? Kas kasutusest väljajäävaid protokolle on võimalik desaktiveerida?
- Kas ALG-le esitatud nõudmiste valik ja nende hindamine on dokumenteeritud?
- Kas rakendatavad proksid suudavad täita neile pandud ülesandeid?

M 2.76 Sobivate filtreerimisreeglite valimine ja kehtestamine

Algatamise eest vastutavad: IT juht, IT turvaosakond

Rakendamise eest vastutavad: administraator

Tulemüüri filtreerimisreeglite kehtestamine ja selle hädavajalike täiendite laadimine ei kuulu just kõige kergemate ülesannete hulka. Administraatoril peavad olema põhjalikud teadmised kasutatavate protokollide kohta ja ta peab saama asjakohase koolituse. Filtreerimisreeglite kehtestamisel tuleks arvestada järgmiste punktidega:

- üldjuhul tuleks rakendada „Whitelist“ strateegiat, mis tähendab, et kõik reeglid tuleks sõnastada nõnda, et kõik juurdepääsud, mis ei ole otseselt lubatud, on keelatud.
- Juhul kui tekib vajadus kasutajapõhise autentimisprotsessi järele, tuleb eelnevalt selgitada, milliseid teenuseid erinevad sisevõrgu kasutajad kasutada tohivad ning milline peaks olema selle tarbeks rakendatav autentimisprotsess.
- Arvestada tuleb kõikide sisevõrgus olevate arvutitega.

Ajalised piirangud

Tuleb kindlaks määrata, millises ajavahemikus peaksid erinevad teenused olema kättesaadavad. Kui organisatsioon töötab ainult kindlatel kellaaegadel, näiteks kui töötajad saavad kohal viibida ainult kella 7.00 ja 19.00 vahel, ei tohiks võimaldada ühenduste loomist väljaspool tavapärast tööaega. Filtreerimisreeglid tuleks tabelisse kokku koguda, kus ühele poolele on üles loetletud adressaatide IP-aadressid ning teisel poolele lähtekoha IP-aadressid. Sissekanded peavad sisaldama lubatud portide numbreid, kusjuures ülemine peab olema lähtekoha ja alumine sihtkoha port. Paketifiltrid võivad pakettide kontrollimisega tegeleda muuhulgas ka vahetult pärast nende vastuvõtmist või vahetult enne nende edasisuunamist. Üldjuhul tuleks otsus langetada esimese variandi kasuks. Lisaks peavad paketifiltrid olema konfigureeritud selliselt, et saatja aadressina oleks lubatud kasutada vaid liidese külge ühendatud arvuti numbreid („Ingress-Filtering“) . Teiste liidestega (Interface) ühendatud aadresse ei tohi läbi lubada. Niimoodi vähendatakse IP-spuufingul põhinevate rünnete ohtu.

Näide

Järgnevas tabelis on ära toodud sisevõrgu ja vahepealese võrgu vahel oleva paketifiltri sisemise liidese filtreerimisreeglid, st liides asub sisemise ja välimise paketifiltri vahel ja kontrollib nendevahelisi ühendusi.

Sissekanded sisaldavad lubatud ühendusi, millest ülemine tähistab lähtekoha ja alumine sihtkoha porti.

Lähtesüsteem	Sihtsüsteem	Lähteport	Sihtport
Sisemine meiliserver	Vahevõrgus olev väline meiliserver	TCP > 1023	TCP: 25

Sisemine DNS-server	Vahevõrgus olev väline DNS-sever	UDP : 53	UDP : 53
IT-süsteem, mille IP-aadress on 192.168.0.5	Vahevõrgus olev Application-Level-Gateway	TCP > 1023	TCP: 20,21
IT-süsteem, mille IP-aadress on 192.168.0.7	Vahevõrgus olev Application-Level-Gateway	TCP > 1023	TCP: 23
IT-süsteem, mille IP-aadresside vahemik on 192.168.0.*	Vahevõrgus olev Application-Level-Gateway	TCP > 1023	TCP: 22,80
IT-süsteem, mille IP-aadresside vahemik on 192.168.1.*	Vahevõrgus olev Application-Level-Gateway	TCP > 1023	TCP: 80

Tabel 1: paketifiltri sisemise liidese filtreerimisreeglid

Ühenduste loomise katseid ülesloetlemata süsteemide vahel, näiteks sisemise meiliserveri ja välimise DNS-serveri vahel, tuleb takistada. Kõikide ülesloetlemata portide numbrid tuleb blokeerida. Kui on tarvis kasutada täiendavaid kommunikatsiooniteenuseid, tuleb tabelit nr 1 vastavalt täiendada. Näiteks tähendab see seda, et sisemine meiliserver võib TCP abil pordist, mille pordi numbrid jäävad vahemikku > 1023 juurde pääseda vahepealses võrgus asuva välise meiliserveri pordile 25 (SMTP). Porte, mille numbrid jäävad vahemikku > 1023 nimetatakse ka mitteprivilegeeritud portideks vastupidiselt madalamate numbritega portidele, mida nimetatakse privilegeeritud või „ well-known -portideks“, kuna nende portide numbrite taga olevad teenused on ära jaotatud „Internet Assigned Numbers Authority“ (IANA) poolt. Vastava tabeli alusel tuleb välja töötada sobilikud filtreerimisreeglid. Antud tegevus ei kuulu just kõige kergemate hulka ning seetõttu tuleb seda väga täpselt kontrollida. Filtreerimisreeglite koostamisel võib mõnikord kasutada ka abiprogramme, mille kasutajaliidese abil on võrgu modelleerimine ja sinna juurde kuuluvate filtreerimisreeglite loomine veidi lihtsam. Regulaarse testimisega tuleb kontrollida, kas kõiki filtreerimisreegleid on rakendatud korrektselt. Eriti oluline on kontrollida, et lubatud oleks vaid nende teenuste kasutamine, mis on turvapoliitikaga ette nähtud. Analoogsed tabelid tuleb koostada Application-Level-Gateways reeglite kohta ja seejärel välja töötada vastavad filtreerimisreeglid.

Näide

Kasutajanimi	Teenus	Käsk	Autentimine
Proua Kuusk	FTP	. . . , RETR, STOR	ühekordne parool
Härra Lepp	FTP	. . . , RETR	kiipkaart

Tabel 2: Application-Level-Gateway reeglite tabel

Kasutaja, proua Kuusk, võib (muuhulgas) kasutada FTP teenuse käske RETR

ja STOR, mis tähendab, et tal on õigus FTP abil faile laadida ja välja saata, kuid härra Lepal on õigus faile ainult laadida.

Täiendavad kontrollküsimused:

- Kas administraatoritel on vajalikud teadmised filtreerimisreeglite formuleerimiseks?
- Kas lubatud IP- ja pordikombinatsioonide kohta koostatakse vastavad tabelid?
- Kas tabeli alusel välja töötatud filtreerimisreeglite kehtestamist on kontrollitud? Kas loodud filtreerimisreeglid vastavad tabelis sõnastatud nõudmistele?
- Kas Application-Level-Gateway jaoks koostatud reeglid on korrektselt välja töötatud ja rakendatud?

M 2.77 Serverite integreerimine tulemüüri

Algatamise eest vastutavad: IT juht, IT turvaosakond

Rakendamise eest vastutavad: IT-turvaosakond, administraator

Lisaks tulemüüride installeerimisele ja kasutamisele tuleb tihti tegeleda lisaks ka serverite turvalise paigutamisega. Siia alla kuuluvad näiteks infoserverid, mis peavad tagama info kättesaadavuse sisemistele ja välimistele kasutajatele, meiliserverid ning DNS-serverid. Serverite paigutuse puhul tuleb vahet teha, kas neid tahetakse ühendada kaitstavasse võrku, kahe paketifiltri vahel olevasse võrku (edaspidi „vahevõrku“) või tulemüüri välimise poole külge.

Välimised juurdepääsud

Usaldusväärsesse võrku viivaid välimisi juurdepääse, nt SSH abil läbi ModemPool-i, tuleks käsitleda kui ebausaldusväärsest võrgust tulevaid juurdepääse. Seda on võimalik ellu viia seeläbi, et tulemüüri välimise külje külge ühendatakse modemiühendusega terminaliserver, et sealt edasi oleks juurdepääs sisemisele arvutile võimalik ainult SSH kaudu.

Juurdepääsud ei tohi tulemüürist mööda minna

Vastu tuleb võtta selged eeskirjad, mis sätestavad, et väliste ühenduste loomisel on tulemüürist möödaminek keelatud. Vastavatest eeskirjadest tuleb teavitada kõiki töötajaid. IT-turvakontseptsiooni ja tulemüüri turvaeeskirjaga arvestamiseks tuleb tagada, et vastavatest plaanidest teavitataks õigeaegselt ka IT-turvaosakonda ja tulemüüri haldavat administraatorit. Täiendavat informatsiooni väliste juurdepääsudega ümberkäimiseks leiate B 4.4 Virtuaalne privaatvõrk (VPN) .

Infoserverite paigutamine

Serverid, mis peavad tagama informatsiooni kättesaadavuse väliste kasutajate jaoks, peaks üldjuhul asuma ebausaldusväärsele võrgule „võimalikult lähedal“ (nt välimise paketifiltri taga) ning nendega tuleks käituda nagu kõikide teiste ebausaldusväärses võrgus leiduvate serveritega. Kui nende asukoht jääb „võimalikult kaugele välja“, raskendab see infoserveri ründe puhul juurdepääsu usaldusväärsele võrgule, kuna ründe läbiviijal tuleb juurdepääsuks jagu saada mitmest teisest tulemüüri komponendist. Nende haldamine peaks toimuma kas ainult lokaalselt või siis usaldusväärsest võrgust loodud, spetsiaalselt turvatud ja vajadusel koguni ajaliselt piiratud juurdepääsuude abil. Kuna infoservereid, mille ülesandeks on välistele kasutajatele info kättesaadavuse tagamine, tuleb käsitleda nagu ebausaldusväärses võrgus olevaid arvuteid, tuleks filtreerimisreeglite ning vajadusel lisaks ka serveri vastava konfiguratsiooni abil tagada, et sellisest serverist ei oleks võimalik luua ühendusi usaldusväärse võrguga, vaid et ainuke ühenduse loomise suund oleks usaldusväärsest võrgust serverisse. Näiteks tuleks usaldusväärse võrgu kaudu SSH ühenduse abil hallatava veebiserveri puhul keelata serverist alguse saavad SSH ühendused ning lubada tuleks ainult neid ühendusi, mis saavad alguse usaldusväärsest võrgust ja liiguvad edasi serverisse.

Eraldi serverid intraneti ja välise võrgu tarbeks

Kui mõningad andmed peaksid olema kättesaadavad ainult usaldusväärse võrgu kasutajatele (nt intranet-veebiserver), tuleks võimalusel vältida nende andmete salvestamist sellisele serverile, mis pakub oma teenuseid muuhulgas ka välistele kasutajatele. Niisugustel juhtudel soovitatakse vahevõrku lisada täiendavaid infoservereid, mis ei ole väljastpoolt ligipääsetavad ning võimalike seest tulevate rünnete vastu kaitseb neid paketifilter. Juhul kui andmetele, mis peavad ainult siseringi kasutajatele kättesaadavad olema, kehtib suur kaitsevajadus nende konfidentsiaalsuse osas, ei tohi vastavat serverit paigutada samasse vahevõrku väliste

kasutajate jaoks mõeldud infoserveriga. Niisugusel juhul tuleb vastavate serverite jaos luua oma demilitariseeritud tsoon. Erinevate informatsiooniserverite turvalüüsi integreerimisest räägivad järgnevad eraldi meetmed:

- veebiserver (vt M 5.115 Veebiserveri integreerimine turvalüüsi koostisse
- meiliserver (vt M 5.116 Meiliserveri integreerimine turvalüüsi koostisse)
- andmebaasiserver (vt M 5.117 Andmebaasiserveri integreerimine turvalüüsi koostisse)
- DNS-server (vt M 5.118 DNS-serveri integreerimine turvalüüsi koostisse)
- veebi-, rakendus- ja andmebaasiserveritega veebirakendus (vt M 5.119 Veebi-, rakendus- ja andmebaasiserveritega veebirakenduse integreerimine turvalüüsi koostisesse)

Täiendavad kontrollküsimused:

- Kas andmed, mis peavad olema kättesaadavad ainult siseringi kasutajatele, on väliste kasutajate jaoks mõeldud andmetest eraldatud?
- Kas konfidentsiaalseid andmeid sisaldavad serverid, mis peaksid olema ligipääsetavad ainult sisekasutajatele, on paigutatud eraldi demilitariseeritud tsooni?

M 2.78 Turvalüüsi (tulemüüri) turvaline kasutamine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: IT-turvaosakond, administraator

Tulemüüri turvaline kasutamine eeldab regulaarset kontrollimist, kas rakendatud turvameetmed töötavad korrektselt. Eriti oluline on tulemüüri kasutamise juures regulaarselt/pisteliselt kontrollida seda, kas tulemüüri kasutuse kohta vastu võetud organisatoorsetest reeglitest peetakse kinni või mitte. Regulaarselt tuleks kontrollida, kas on loodud uusi ühendusi, mille käigus on tulemüürist mööda mindud.

Filtreerimisreegleid tuleb testida

Regulaarse testimisega tuleb muuhulgas kontrollida, kas kõiki filtreerimisreegleid on rakendatud korrektselt. Eriti oluline on sealjuures kontrollida, et lubatud oleks vaid nende teenuste kasutamine, mis on tulemüürile kehtestatud turvapoliitikaga ette nähtud. Kui turvapoliitikasse on tarvis tagantjärele muudatusi sisse viia, tuleb need täpselt üle kontrollida ning erilist tähelepanu tuleb sealjuures pöörata võimalike kõrvalefektide tekkimisele. Paketifiltri ja Application-Level-Gateway soetamise käigus neile seatud nõudmised peavad saama korrektselt ellu rakendatud. Neile tuleb regulaarselt täiendeid laadida ja kontrollida nende terviklust. Filtreerimisreeglite vaikehäälestus ja komponentide paigutus peavad tagama, et kõik ühendused, mida ei ole konkreetselt lubatud, oleksid keelatud. See peab kehtima ka tulemüüri komponentide täieliku avarii korral. Kõik peab toimima reegli järgi: „kõik, mis ei ole otseselt lubatud, on keelatud“ . Näiteks töötajal, kes ei ole Access-List -i kantud, ei tohi olla Interneti kasutamise võimalust. Sellele lisaks tuleb arvestada järgmiste punktidega:

Komponentide konfiguratsioon tuleb teha eriti hoolikalt - Kõik tulemüüri koostisesse kuuluvad seadmed (arvutid, marsruuterid, eraldiseisvad seadmed) peavad olema konfigureeritud eriti hoolikalt ja turvaliselt. Kasutatavates komponentides tohib olla ainult selliseid programme, mis on tulemüüri funktsioneerimiseks vajalikud. Vastavate programmide rakendamine peab olema piisavalt dokumenteeritud ja põhjendatud. Näiteks tuleb enam mittevajalikud teenused desaktiveerida ja draiverid eemaldada. Võimalusel tuleks draiverid eemaldada ka operatsioonisüsteemi tuumast. Tarkvara edasine saatus dokumenteerida ja põhjendada.

Turvaline juurdepääs - Autentimist puudutava informatsiooni lugemise ja muutmise vältimiseks tohivad administraatorid ja auditi läbiviijad kasutada tulemüüriga suhtlemiseks ainult turvalist pöördusteed (path), nt otse konsooli abil, kasutades kas krüpteeritud ühendust või eraldiseisvat administraatorivõrku (Out-of-Band Management).

Värsked paigad - Tulemüüri komponentides kasutatavate operatsioonisüsteemide ja programmide turvalisuse tagamisel tuleb hoolitseda selle eest, nende kõige värskemad paigad oleksid alati alla laetud. Seetõttu peavad süsteemi administraatorid ennast regulaarselt kursis hoidma võimalike avastatud turvaaukudega ning installeerima turvapaigad võimalikult operatiivselt (vt M 2.35 Teabe hankimine turvaaukude kohta , M 2.273 Turvalisust mõjutavate paikade ja värskenduste kiire paigaldamine ja M 4.177 Tarkvarapakettide tervikluse ja autentsuse tagamine).

Regulaarne tervikluse testimine

- Rakendatava tarkvara puhul tuleb regulaarselt kontrollida selle terviklust (vt M 4.93 Regulaarne tervikluse kontroll). Vigade ilmnemisel tuleb tulemüür välja lülitada.
- Testimisega tuleb välja selgitada, kuidas käitub tulemüür süsteemi avarii korral. Oluline on, et tulemüür ei lubaks automaatset taaskäivitust ning et seade

võimaldaks Access-List - e salvestada mõne kirjutuskaitsega salvestusvahendi peale.

- Tulemüüri Access-List - id on ühed olulisemad andmed tulemüüri kasutamisel. Seepärast peab olema tagatud nende andmete piisav kaitse ka sellisteks juhtudeks, kus mõnel ründajal on õnnestunud algatada tulemüüri või selle üksikute komponentide taaskäivitus, et ka selliste juhtumite korral ei tuleks kasutada vanu või vigaseid Access-List -e.
- Tulemüüri avarii korral peab olema tagatud, et avarii jooksul ei oleks võimalik luua ühendusi kaitstava võrgu seest väljapoole ega ka väljastpoolt, kaitstava võrgu enda suunas (vt M 2.302 Turvalüüside kõrge käideldavuse tagamine ja M 6.94 Turvalüüside hädaolukorraks valmisoleku plaan).
- Eelnevalt turvaliselt hoiule pandud andmete taassisestamisel tuleb tähelepanu pöörata sellele, et tulemüüri turvaliseks kasutamiseks vajalikud failid nagu Access-List -id, paroolifailid ja filtreerimisreeglid oleksid värsked.

Täiendavad kontrollküsimused:

- Kas tulemüüri komponentide konfiguratsioon on turvaline?
- Kas on tagatud, et tulemüüri komponentides kasutatavate operatsioonisüsteemide ja programmide kõige värskemad paigad saavad alati alla laetud?
- Millist kanalit pidi astuvad administraatorid ja auditi läbiviijad ühendusse tulemüüri ja selle komponentidega?
- Kui pika aja tagant toimub tervikluse kontrollimine?
- Mis juhtub tulemüüri avarii või taaskäivitamise korral?

M 2.79 Vastutuste määramine tüüptarkvara alal

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtorgan

Rakendamise eest vastutavad: IT-juht, organisatsiooni juht

Enne tüüptarkvara kasutuselevõttu tuleb määrata mitmeid vastutusalasid. Näitena erinevatest vastutusaladest võib siinkohal nimetada nõudmisi kajastava kataloogi koostamist, toodete eelvaliku tegemist, testimist, kasutusloa andmist ja installeerimist. Alljärgnevalt püüame näidete varal selgitada, kuidas on vastavaid kohustusi kõige mõttekam töötajate vahel ära jagada. Kuna alluvussuhted on organisatsioonide lõikes küllaltki erinevad, lähtutakse erinevate instantside defineerimisel nende ülesannetest, mille alusel saab neile hiljem erinevaid vastutusalasid määrata:

- Tüüptarkvara kasutajateks on spetsialistid. Selle osakonna töötajad avaldavad soovi uue tarkvara kasutamiseks ja annavad seeläbi esimese tõuke uue tarkvara soetamiseks. Spetsialistidest töötajad kaasatakse eelvaliku tegemisse ja testimisse, et kasutajate nõudmistega oleks arvestatud.
- Ametiasutuse/ettevõtte juhtkond vastutab tüüptarkvara kasutamise aktsepteerimise eest, st väljastab omapoolse kasutusloa. Nimetatud vastutus delegeeritakse üldjuhul spetsialistide osakonna juhatajale, mis tähendab et pärast organisatsioonisisese kasutusloa saamist jääb vastutus tüüptarkvara korrektse kasutamise eest vastava osakonna kanda.
- Organisatsiooni IT-osakonna ülesanne on varustada spetsialiste nende tööks vajalike IT-lahendustega ning kindlustada nende süsteemide turvaline ja tõrgeteta kasutamine.
- Varustusosakonna ülesanne on vastutada soetatava tüüptarkvara koostalitlusvõime ja ühilduvuse eest, samuti kuulub nende ülesannete hulka majasiseste standardite ning seadustest tulenevate ettekirjutuste järgimise kontrollimine. Tihti on erinevatel osakondadel olemas oma IT koordinaatorid, kes võivad tegeleda osaliselt ka varustusosakonna ülesannetega, nt spetsialistide nõustamise ning eelarveosakonna ja spetsialistide vahelise koostöö koordineerimisega.
- Eelarveosakond vastutab raamatupidamise, IT-eelarve haldamise ja vajaminevate eelarvevahendite olemasolu eest.
- IT turvaspetsialist peab kontrollima, kas kasutusele võetud ja soetatavad tooted suudavad tagada IT piisava turbeastme. Tema ülesanne on tagada jooksvalt IT turvalisuse haldamise raames IT turvalisus (vt B 1.0 Infoturbe haldus).
- Andmekaitsespetsialist peab valvama seadusest tulenevate andmekaitsenõuete järgimise ja isikuandmete piisava kaitsmise üle.
- Uue tüüptarkvara valimisse tuleb tihti kaasata ka töötajate esindus, eriti neil juhtudel, kui sellega kaasnevad suuremad muudatused tööprotsessis või kui soetatav tarkvara võimaldab hinnata tööpanust (vt M 2.40z Töötajate esinduse õigeaegne kaasamine).

Tüüptarkvaraga tegelemiseks peab iga üksiku läbitava sammu jaoks olema kindlaks määratud, milline eespool kirjeldatud instantsidest selle läbiviimise eest vastutab ja milliseid instantse tuleb vastavasse protsessi kaasata. Näitena vastutuse jaotumise ühe võimaliku variandi kohta, mida orientiiriks võtta, on koostatud järgnev tabel:

	on vastutav	tuleb kaasata
nõudmisi koondava kataloogi koostamine	spetsialistide osakond, IT-valdkond	varustusosakond, majapidaja, IT-turvaspetsialist, andmekaitsespetsialist, töötajate esindus
sobiva toote eelvaliku tegemine	varustusosakond	IT-valdkond, spetsialistide osakond
testimine	spetsialistide osakond ja IT-valdkond	IT-turvaspetsialist, andmekaitsespetsialist, töötajate esindus
kasutuse aktsepteerimine	ametiasutuse/ettevõtte juhtkond, võib olla delegeeritud ka spetsialistide osakonna juhatajale	-
Soetamine	varustusosakond	eelarveosakond
tarkvara tervikluse tagamine	IT-valdkond	-
installeerimine ja konfigureerimine	IT-valdkond	-
versiooni kontrollimine ja litsentside haldus	IT-valdkond	-
deinstalleerimine	IT-valdkond	-
IT-töö kontrollimine	IT-turvaspetsialist	-

Jaotatud vastutusalad tuleb kirjalikult fikseerida ja kohustuslikuks teha ning nende järgimist tuleb teatud aja tagant kontrollida.

Täiendavad kontrollküsimused:

- Millised eeskirjad on hetkel jõus?
- Kas kõiki töötajaid on teavitatud kehtivatest eeskirjadest ja nende kontrollimisest?
- Kas asjasse puutuvad instantsid (nt töötajate esindus, eelarveosakond, andmekaitsespetsialist jne) kaastakse nende funktsiooni kohaselt?

M 2.80 Tüüptarkvara nõuete kataloogi koostamine

Algatamise eest vastutavad: spetsialistide osakonna juhataja

Rakendamise eest vastutavad: spetsialistide osakond, IT-juht

IT kasutamisega seotud ülesannete täitmiseks pakub turg tavaliselt suurel hulgal sarnase tüüptarkvaraga tooteid. Tooted on oma põhifunktsioonidelt küll sarnased, kuid soetamise ja kasutamisega seotud kulude, lisafunktsioonide, ühilduvuse, administreerimise, ergonoomilisuse ja IT-turbe seisukohast on need siiski erinevad. Tüüptarkvara, juhul kui selles kasutatakse krüptograafilisi algoritme, peab võimaldama seadistada igas funktsioonis vähemalt kahe erineva krüptograafilise algoritmi kasutamist, et kogu tarkvaratoote ümbervahetamise asemel saaks õigel ajal asendada nõrgeneva krüptograafilise algoritmi.

Nõudmiste kataloog

Sobiva toote väljavalimiseks tuleks esmalt koostada nõudmiste kataloog. See peaks muu hulgas sisaldama ka informatsiooni järgmiste punktide kohta:

- Funktsioonide nõuded, st milliseid funktsioone peab toode sisaldama, et spetsialistide osakond saaks oma tööülesandeid täita. Eri valdkondade jaoks olulised üksikud funktsioonid tuleks eraldi esile tõsta.

Lühendatud näited

- Tekstitöötlus koos lisafunktsioonidega, nagu nt graafika lisamine, makrode programmeerimine, õigekirja kontroll ja silbitamine. Makrode programmeerimist peab olema võimalik välja lülitada, õigekirja kontrolli tugi peab olema inglise ja eesti keele jaoks. Spetsiaalseid tekstiformaate peab olema võimalik importida ja eksportida.
- Mitme kasutajaga kasutusrežiimi andmebaas (ees- ja tagakomponent) koos standardse päringukeele SQL toe ja graafilise kasutajaliidesega.
- Märkmiku funktsioon osakonna töötajate tähtsate kohtumiste koordineerimiseks ja kontrollimiseks, kuhu on integreeritud kokkusaamiste kokkuleppimise funktsioon, automaatne ülesannete ja prioriteetide nimekirja saatmine ning kasutajaliides majasisese e-posti programmi kasutamiseks.
- IT rakenduskeskkond, mida kirjeldatakse ühelt poolt kas juba olemasoleva või plaanitava kasutuskesskonna etteantud raamtingimustega ja teiselt poolt toote enda jõudlusele esitatavate nõudmistega, mis on toote kasutuskeskkonnas vajalikud.

Lühendatud näited

- Olemasolev IT rakenduskeskkond: Novell 3.11 all võrku ühendatud PC, 80486-protsessor, 8 MB põhimälu, 500 MB kõvaketta ruumi, disketiseade, CD-ROM-seade, MS-DOS 6.0, kõvaketta mahust tohib toode enda alla võtta maksimaalselt 50 MB, see peab töötama Windows 3.11 all ja seda peab saama võrgus kasutada.
- Jõudlusele esitatavad nõuded: tekstitöötlusprogramm X vajab 16 MB kõvaketta ruumi, töötab PC-l alates protsessorist 80386, 8 MB põhimälu, Windows 3.11.

- Ühilduvuse nõuded teiste programmide või IT-süsteemidega, st üleviimise tugi, ühilduvus uuemate ja vanemate süsteemidega.

Lühendatud näited

- Olemasoleva andmebaasi XYZ andmeid peab olema võimalik üle viia.
- Funktsioonid A, B, C peavad versiooni vahetamise käigus alles jääma.
- Süsteem peab toetama andmevahetust Unixi all töötava XYZ süsteemiga.
- Jõudluse nõuded kirjeldavad vajaminevaid jõudlusi andmete läbilaskevõime ja talitlusele kuluva aja osas. Vajaminevate funktsioonide kohta tuleks võimalikult täpselt kindlaks määrata maksimaalne aeg, mis millegi töötlemiseks võib kuluda.

Lühendatud näited

- Kasutades funktsiooni X, ei tohi vastuse saamiseks kuluda rohkem aega kui 2 sekundit.
- Krüpteerimise kiirus peaks 486 DX 33 puhul olema vähemalt 60 KB/sek.
- Teised samal ajal töötavad protsessid tohivad toote kiirust alandada maksimaalselt 30% võrra
- Koostalitlusvõime nõuded, st teiste toodetega koos töötamine peab olema võimalik ka väljasool platvormi piire.

Lühendatud näited

- Tekstitöötlusprogrammi versioonid peaksid olemas olema nii Windowsi, Unixi kui ka Macintoshi platvormi jaoks. Ühe kindla operatsioonisüsteemi all loodud dokumente peab olema võimalik teiste operatsioonisüsteemide all edasi töödelda.
- Tekstitöötlusprogrammi peab saama kasutada koos e-posti programmiga.
- Töökindluse nõuded puudutavad toote stabiilsust, st vigade tuvastamist ja tolerantse ning avarii- ja töökindlust.

Lühendatud näited

- Süsteem peab tuvastama kasutajate vigased sisestused ja need ei tohi viia programmi töö katkemiseni ega põhjustada avariid.
- Andmebaasil peavad olema mehhanismid mis võimaldavad süsteemi avarii tõttu hävinud andmebaasi kõik transaktsioonid rekonstrueerida (edasipööre).
- Vastavus standarditele, nt rahvusvahelised normid, de facto standardid või majasisesed standardid.

Lühendatud näited

- Toode peab vastama EL-i kuvariga töötamise direktiivile 90/270/EMÜ.
- Token-ring-LAN-i juurutamine peab olema kooskõlas standardiga ENV 41110.

- Toode peab vastama standardile X/Open.
- Organisatsioonisiseste reeglite ja seadustest tulenevate kohustuste järgimine (nt piisava andmekaitse tagamine isikuandmete töötlemisel).

Lühendatud näited

- Toode peab vastama andmetöötluse toega varustatud raamatupidamissüsteemidele esitatud nõudmistele.
- Kuna töödeldakse isikuandmeid, peavad rakendatavad funktsioonid vastama riikliku andmekaitseseaduse ettekirjutustele.
- Kasutajasõbralikkuse nõuded hõlmavad kasutamise lihtsust, arusaadavust, kerget omandamist ning eriti kasutajaliidese sobilikkust, kasutaja dokumentatsiooni kvaliteeti ja abifunktsioonide kvaliteeti.

Lühendatud näited

- Tootel peab olema võrgu-abifunktsioon.
- Kasutajaliides peab olema loodud selliselt, et töötajaid, kes ei ole saanud spetsiaalset koolitust, oleks võimalik kahe tunni jooksul asjaga kurssi viia.
- Kasutaja dokumentatsioon ja kasutajaliides peaksid olema riigikeeles.
- Hoolduse nõuded tekivad kasutaja jaoks peamiselt sellest, kuidas tuleb toote võimalike vigadega ümber käia.

Lühendatud näited

- Administreerimine ei tohi olla ülemäära töömahukas.
- Tarnijal peab olema küsimustele vastamiseks sisse seatud oma telefoni infoliin.
- Toodet peab saama lihtsalt installeerida ja konfigureerida.
- Toodet peab saama lihtsalt desinstalleerida.
- Hinna ülempiir tähendab toote soetamiseks vajaminevaid maksimaalseid kulutusi. Siia alla ei kuulu mitte ainult toote soetamisega seotud kulutused, vaid ka soetamisele järgnevad kulutused, nt riistavara täiendamisega tehtavad kulutused, personalikulu ja koolituste kulud.

Lühendatud näited

- Toote hind võib olla maksimaalselt 15 000 eurot.
- Koolituskulud peavad jääma 2000 euro piiridesse.
- Dokumentatsiooni nõuded peavad kajastama seda, milliseid dokumente on tarvis ning kui põhjalikud need peavad olema (sisu ulatus ja arusaadavus).

Lühendatud näited

- Kasutaja dokumentatsioon peab olema kergesti mõistetav ja sobima iseseisvaks tutvumiseks. Kirjeldada tuleb toote kõiki funktsioone.

- Süsteemihaldaja dokumentatsioon peab sisaldama juhiseid võimalike vigadega ümberkäimiseks.
- Tarkvara kvaliteedinõuded võivad ulatuda tootjapoolsest kinnitusest, kasutatavatest kvaliteeditagamiseprotsessidest, ISO 9000 jt sertifikaatidest kuni sõltumatu, ISO 12119 normile vastava kontrollini välja.

Lühendatud näited

- Tootja kasutatav tarkvara loomise protsess peab vastama ISO 9000 sertifikaadile.
- Toote funktsioonid peavad olema normi ISO 12119 kohaselt kontrollitud sõltumatu osapoole poolt.
- Juhul kui toode peab täitma IT-turbe funktsioone, tuleb need sõnastada turvanõuetes (vt M 4.42z Turvafunktsioonide rakendamine IT-rakenduses).

Turvanõuded

Olenevalt sellest, kas toode peab võimaldama turbefunktsioone või mitte, võib turvafunktsioonid üles loetleda ka nõudmiste kataloogi koostades. Alljärgnevalt anname lühikese ülevaate võimalikest tüüpilistest turbefunktsioonidest. Täiendavat informatsiooni pakub kõnealuse teema kohta ITSEC.

Identifitseerimine ja autentimine

Paljude toodete puhul võib esineda nõudmisi, et toote kontrollitavatele töövahenditele juurdepääsu omavad kasutajad tuleb identifitseerida ja kontrollida. Selle tagamiseks on lisaks töötaja identifitseerimisele tarvis veel ka üle kontrollida, kas kasutaja näol on tegemist tõepoolest selle isikuga, kellena ta ennast esitleb. Kontrollimiseks edastab kasutaja vastavale tootele informatsiooni, mis on kindlalt seotud tema kasutajaga.

Juurdepääsu kontroll

Paljude toodete kasutamisel on vajadus tagada, et kasutaja ja tema algatatud protsessid oleksid takistatud, kui kasutajal puudub õigus vastavatele andmetele või töövahenditele ligi pääseda või kui juurdepääs ei ole tema töö jaoks hädavajalik. Sarnaselt eelnevaga tuleb rakendada ka nõudeid, mida tuleb täita informatsiooni volitamata koostamise või muutmise (kaasa arvatud kustutamise) tõkestamiseks.

Tõendite säilitamine

Paljude toodete puhul on tarvis tagada, et kasutajate või teatud protsesside poolt kellegi kasutajanime alt algatatud toimingud saaksid fikseeritud, st toimuks informatsiooni salvestamine, mille alusel oleks hiljem võimalik seostada tegevuste tagajärgi kindlate kasutajatega ning ja kasutajaid vastutama oma tegude eest.

Logiandmete läbitöötamine

Tihti on nii, et paljud tooted salvestavad logidesse piisavalt palju informatsiooni nii tavapäraste sündmuste kui ka tavajuhtumistest kõrvalekaldumiste kohta, mille hilisemal läbitöötamisel on võimalik kindlaks teha, kas sündmuste näol oli tegu turvalisust pärssivate juhtumitega või mitte ning milline informatsioon või töövahendid olid sellest puudutatud.

Võltsimiskindlus

Paljude toodete puhul on tarvis tagada, et säiliksid erinevate andmete korrektsed seosed ja et andmete liikumine mitmete protsesside vahel ei tooks endaga kaasa muudatusi andmete sisus. Lisaks peaksid olemas olema funktsioonid, mis võimaldaksid tuvastada ja takistada erinevate protsesside, kasutajate ja objektide vahel andmeedastuse käigus tekkida võivaid kadusid, täiendusi või muudatusi, samuti funktsioonid, mis teeksid andmeedastuse näilise või tegeliku algus- ja sihtkoha muutmise võimatuks.

Usaldusväärsus

Paljude toodete rakendamise puhul on vajadus tagada, et kindlate kellaaegadega seotud ülesanded toimuksid just sellel ajahetkel, mis on nende läbiviimiseks määratud, mitte varem ega hiljem, samuti on tarvis kindel olla, et ajaga mitteseotud ülesandeid ei oleks võimalik muuta kindla ajalise määratlusega ülesanneteks. Samuti on tarvis paljude toodete puhul tagada, et vajalikul ajahetkel oleks kindlustatud vajaminev juurdepääs ning et töövahendeid ei saaks tarbetult kasutada ega nende kasutamist kinni hoida.

Andmeedastuse turvalisus

See mõiste hõlmab kõiki funktsioone, mis on vajalikud kommunikatsioonikanaleid pidi liikuvate andmete kaitsmiseks:

- autentimine,
- juurdepääsu kontroll,
- andmete konfidentsiaalsus,
- andmete terviklus,
- saatmise ja vastuvõtu kinnitus.

Osad loetletud funktsioonid tagatakse krüptograafiliste lahenduste abil.

Lisaks ITSEC-ile võib tüüptarkvara kasutuse jaoks sõnasta veel ka täiendavaid turvanõudeid.

Andmevarundus

Toote abil töödeldavatele andmetele esitatakse tavaliselt suuri nõudmisi andmete kättesaadavuses. Selle punkti alla kuuluvad tootesse integreeritud funktsioonid, mis ennetavad andmekadu, salvestavad automaatselt vahepealseid tulemusi või koostavad automaatselt turvakoopiaid enne suuremate muudatuste läbiviimist.

Krüpteerimine

Krüpteerimise eesmärk on andmete konfidentsiaalsuse säilitamine. Paljude toodete puhul on tarvis kasutajaandmeid enne nende edastamist või peale nende töötlemist krüpteerida ja pärast vastuvõtmist või enne edasist töötlemist dekrüpteerida. Selleks tuleb kasutada tunnustatud krüpteerimismeetodit. Krüpteerimiseks vajalike parameetrite (nt võtmete) puhul peab olema tagatud piisav kaitse, et volitamata isikutel ei oleks võimalik vastavatele andmetele ligi pääseda.

Andmeterviklust kindlustavad funktsioonid

Andmete puhul, mille tervikluse kadu võib põhjustada kahjusid, tuleb kasutada funktsioone, mis võimaldavad vigu tuvastada või koguni korrigeerida, kasutades selleks eelnevalt varutud andmeid. Tervikluse kontrollimisel rakendatakse tihti meetodeid, mille abil on võimalik üheselt tuvastada sihilikku, toote või tootega loodud andmetega manipuleerimist ja andmete volitamata uuesti importimist. Kõik

need põhinevad krüptograafilisel meetodil (vt M 4.34z Krüpteerimise, kontrollsummade ja digitaalallkirjade rakendamine).

Seadustest tulenevad andmekaitsenõuded

Kui tootega plaanitakse töödelda isikuandmeid, tuleb seadustest tulenevate andmekaitsenõuete täitmiseks kehtestada lisaks loetletud turvafunktsioonidele veel täiendavaid spetsiaalseid tehnilisi nõudmisi.

Mehhanismide tugevus

Turvafunktsioone rakendatakse turvamehhanismide abil. Olenevalt kasutusalast peavad mehhanismid olema erineva tugevusega, et võimalikele rünnetele vastu pidada. Vajaminevad turvamehhanismid tuleb nõuete kataloogis üles loetleda. ITSECi klassifikatsioon eristab mehhanismidel kolme erinevat tugevusastet:

- **madal**: pakub kaitset juhuslike ettekavatsemata rünnete, nt kasutajavigade vastu.
- **keskmine**: pakub kaitset väheste ründevõimaluste või väheste töövahenditega ründajate vastu.
- **kõrge**: pakub kaitset, millest jagu saamiseks peavad ründajal olema väga head erialateadmised, töövahendid ja soodsad võimalused, kusjuures niisugust edukaks õnnestunud rünnet hinnatakse tavaolukorras mitteteostatavaks.

Turvaomaduste nõuete näited

Alljärgnevalt esitatakse mõningad näited tähtsamate turvafunktsioonide kohta, mis aitavad mõista tüüpilisi turvalisusele esitatavaid nõudeid. Kui tootel peaksid olema identifitseerimise ja autentimise mehhanismid, võiks tootele seada näiteks järgnevad nõudmised:

- Juurdepääs tohib olla võimalik ainult kindlalt määratletud ühenduskoha kaudu. Sealjuures võib kasutada näiteks sisselogimise protsessi, mis nõuab kasutajalt kindla kasutajatunnuse ja parooli sisestamist. Kui IT-süsteemi enda kasutamisele eelneb kasutaja tuvastamine, piisab ka anonüümsest parooli sisestustest. Teiste variantidena tulevad kõne alla teatud sorti lubade (volitustõend) kasutamine, milleks võivad olla näiteks kiipkaardid.
- Ka juurdepääsu protsess ise peab suutma turvalisust mõjutavaid parameetreid (parooli, kasutajatunnust jne) turvaliselt hallata. Näiteks ei tohi kunagi hetkel kasutuses olevaid paroole salvestada IT-süsteemidesse krüpteerimata kujul.
- Juurdepääsu protsess peab reageerima sisestustel tehtud vigadele nii, nagu see on eelnevalt defineeritud. Kui autentimine on näiteks kolm korda järjest ebaõnnestunud, tuleb toote juurdepääs kas tõkestada või ajavahemikke, mille möödumisel on võimalik juurdepääsu loomist uuesti proovida, sammsammult suurendada.
- Juurdepääsu protsess peab võimaldama turvaparameetritele teatud miinimumnõuete kehtestamist. Näiteks peaks parooli minimaalne pikkus olema kuus kohta, PIN-i minimaalne pikkus kolm kohta ja vajadusekorral tuleb ette anda ka paroolide süntaks.

Kui tootel peaks olema juurdepääsu kontrollimehhanism, võiks tootele seada näiteks järgnevad nõudmised:

- Toode peab suutma erinevaid kasutajaid üksteisest eristada.
- Toode peab suutma tagada, et volitatud kasutajad saaksid seadistuse kohaselt ressursse kasutada ja et volitamata isikutele oleksid juurdepääsud tõkestatud.
- Juurdepääsu tagamisel kasutatav õiguste struktuur peaks sisaldama erinevaid astmeid (lugemine, kirjutamine, käivitamine, muutmine jne). Õiguste haldamisega seotud andmeid peab toode suutma hoida selliselt, et nendega ei oleks võimalik manipuleerida.

Kui tootel peaks olema logimehhanism, võiks tootele seada näiteks järgnevad nõudmised:

- Toote poolt logisse lülitatavate andmete minimaalset ulatust peab saama ise määrata. Näiteks peaks logimisse olema võimalik kaasata järgmisi funktsioone:

1. **autentimine:** kasutajatunnus, kuupäev ja kellaaeg, edukas toiming jne,
2. **juurdepääsu kontroll:** kasutajatunnus, kuupäev ja kellaaeg, edukas toiming, juurdepääsu liik, mida kuidas muudeti, loeti, kirjutati jne,
3. **administraatori tegevuste läbiviimine**,
4. **funktsionaalsete vigade esinemine**.

- Volitamata isikutel ei tohi olla võimalik logifunktsiooni välja lülitada. Volitamata isikute jaoks ei tohi logiandmed olla ei loetavad ega ka muudetavad.
- Logimine peab olema ülevaatlik, terviklik ja korrektne.

Kui tootel peaks olema logiandmete kontrollimise mehhanism, võiks tootele seada näiteks järgnevad nõudmised:

- Logiandmete kontrollimise funktsioon peab suutma logimisel kasutatavaid andmeid liigiti eristada (nt filtreerimine, leidmaks kõik volitamata juurdepääsud kõikide ressursside puhul ühes kindlas etteantud ajavahemikus).

Kontrollifunktsioon peab suutma väljastada kontrollitavaid („loetavaid") kontrolliaruandeid, et ükski turvalisust mõjutanud sündmus ei jääks märkamata. Kui tootel peaks olema võltsimiskindlust tagavad funktsioonid, võiks tootele seada näiteks järgnevad nõudmised:

- Andmebaaside haldamissüsteem peab suutma kirjeldada, milliste reeglite alusel on erinevad salvestatud andmed omavahel seotud (nt viiteterviklus).

Lisaks on tarvis ka sobilikke mehhanisme, mis suudaks tagada, et andmete muutmise käigus ei eksitaks eelnimetatud reeglite vastu. Kui tootel peaks olema andmevarundust tagavad funktsioonid, võiks tootele seada näiteks järgnevad nõudmised:

- Konfiguratsiooniga peab saama määrata, milliseid andmeid millal varundatakse.

- Peab olema võimalus igasuguste varundatud andmete importimiseks.
- Funktsioon peaks suutma varundada mitut generatsiooni.
- Varundada peab saama ka töös olevate protsesside vahepealseid tulemusi.

Kui tootel peaksid olema krüpteerimist võimaldavad komponendid, oleks mõttekas seada tootele järgnevad nõudmised:

Rakendatav krüpteerimisalgoritm peaks olema vastavate ametiasutuste tunnustatud.

Võtmete haldamine peab olema toote funktsioonidega kooskõlas. Siinjuures on oluline teha vahet algoritmide põhiliste erinevuste vahel:

1. sümmeetrilised algoritmid kasutavad krüpteerimiseks ja dekrüpteerimiseks võtit, mida tuleb saladuses hoida,
2. asümmeetrilised algoritmid kasutavad krüpteerimiseks avalikku võtit ja dekrüpteerimiseks privaatset võtit (tuleb saladuses hoida).

Turbe seisukohalt olulisi parameetreid, nagu võtmeid, peab toode suutma turvaliselt hallata. Näiteks ei tohi vastavates IT-süsteemides hoida võtmeid (ka neid, mida parasjagu ei kasutata) kunagi kaitsmata kujul, st loetavalt.

Kui tootel peaksid olema tervikluse kontrolli mehhanismid, oleks mõttekas seada tootele järgnevad nõudmised:

- Toode peab tegema iga kord, kui programm käivitatakse, tervikluse kontrolli.
- Andmeedastuse tarbeks peavad tootel olema mehhanismid, mille abil oleks võimalik tuvastada tahtlikku aadressiväljade ja kasutajaandmetega manipuleerimist.

Sellele lisaks ei tohi eelnimetatud andmetega saada märkamatult manipuleerida ainult seeläbi, et teatakse rakendatavaid algoritme, st kasutus peab olema seotud spetsiaalsete lisateadmistega.

Kui tootega soovitakse töödelda isikuandmeid, võib tootele seada näiteks järgmised andmekaitse nõuded:

- Toode ei tohi võimaldada vaba päringut andmete hindamiseks. Andmehulkade analüüsimist peab saama erinevate kriteeriumite alusel piiritleda.
- Tootel peab olema funktsioon, mis teeb teatud failide muutmise, kustutamise või isikuandmete väljatrüki võimalikuks ainult kahemehereegli alusel.
- Logifunktsiooni peab saama seadistada selliselt, et oleks võimalik fikseerida, kes, millal ja millist isikuandmeid puudutavat infot kuidas muutis.
- Isikuandmete andmeedastust peab olema võimalik pistelise kontrolli meetodi abil kindlaks teha ja kontrollida. Pistelise kontrolli teostuse aega peab saama ise määrata.
- Toode peab võimaldama isikuandmetega seotud info kustutamist. Alternatiivina peaks olema võimalik piirata ja tõkestada isikuandmetega seotud andmete kasutamist ja levikut.

Hindamisskaala

Erinevate toodete kasutusväärtuse hindamiseks peavad olemas olema kriteeriumid, mille alusel üksikute nõudmise täitmist hinnata. Selleks on tarvis juba

eelnevalt paika panna tööks vajalike IT-lahenduste vastavate nõuete kvalitatiivne ja kvantitatiivne tähtsus. Tähtsuse hindamist võib näiteks läbi viia kolme astme kaupa. Esimeses hindamisetapis määratakse, millised nõuete kataloogis loetletud tooteomadused on hädavajalikud ja milliste olemasolu on soovitav. Juhul kui üks hädavajalikest tingimustest ei ole täidetud, jäetakse vastav toode valikust kõrvale. Soovitusliku omaduse puudumist hinnatakse küll negatiivselt, kuid selle alusel ei pea toodet veel ilmtingimata kõrvale heitma. Teises hindamisetapis määratakse tootelt nõutud soovitusliku omaduse tähtsus tööülesannete täitmisel.

Vastava hinnangu andmiseks võib kasutada näiteks punktiskaalat, kus 1 tähistab kõrget ja 5 madalat hinnangut. Hädavajalikke tooteomadusi ei ole tarvis kvantitatiivselt hinnata, kuid kui see on arvutuslikel põhjustel vajalik, tuleb neid igal juhul kõrgemalt hinnata kui ükskõik millist soovituslikku omadust (hädavajaliku tooteomaduse esiletõstmiseks võib seda hinnata nt 10ga). Kolmandas hindamisetapis määratakse toote usaldusväärsus, st kui korrektselt suudab toode temalt nõutud ülesandeid täita (nt väärtuseskaala abil, 1 madal ja 5 kõrge). Usaldusväärsusele antud hinnangust lähtudes tuleb hiljem otsustada, kui põhjalikult on tarvis vastavat omadust testida. Turvamehhanismide usaldusväärsust tuleb hinnata mehhanismide tugevuse alusel, kombineerides näiteks:

- mehhanismi tugevus madal: usaldusväärsus 1
- mehhanismi tugevus keskmine: usaldusväärsus 3
- mehhanismi tugevus kõrge: usaldusväärsus 5

Orienteeruvad hinnangud tuleb eraldi üle kontrollida.

Näited:

Valikuliselt tuleb kontrollida tüüpilise tüüptarkvara turvanõudeid:

- Tekstitöötlusprogramm

Hädavajalikud turvaomadused:

- automaatne jooksva töö käigus tekkivate vahepealsete andmete varundamine.

Soovituslikud turvaomadused:

- üksikute failide paroolkaitse,
- üksikute failide krüpteerimisvõimalus,
- makrode programmeerimist peab saama välja lülitada.
- Andmepakkimisprogramm

Hädavajalikud turvaomadused:

- andmevarunduse seisukohast tohib pakkimisprogramm pärast pakkimist vastavaid faile kustutada ainult siis, kui pakkimine toimus ilma vigadeta;

- enne mõne faili lahtipakkimist tuleb kontrollida selle terviklust, nt et pakitud andmetes oleks võimalik tuvastada bitivigasid.

Soovituslikud turvaomadused:

- kokkupakitud failide paroolkaitse.
- Kalender:

Hädavajalikud turvaomadused:

- Üksikute kasutajate kindlat identifitseerimist ja autentimist peab saama teha kohustuslikuks, nt paroolide abil.
- Toode peab võimaldama kontrollida üksikute kasutajate märkmiku kasutamise juurdepääsusid.
- Juurdepääsuõiguste jagamisel peab saama eristada üksikut töötajat, kasutajarühma ja ülemusi.
- Toode peab võimaldama eristada lugemisõigust ja kirjutamisõigust.

Soovituslikud turvaomadused:

- Automaatne andmete varundamine krüpteeritud kujul.
- Töölähetuskulude arveldussüsteem

Hädavajalikud turvaomadused:

- Üksikute kasutajate kindlat identifitseerimist ja autentimist peab saama teha kohustuslikuks, nt paroolide abil.
- Vajalik on juurdepääsu kontroll ning seda peab saama rakendada ka üksikute failide peal.
- Juurdepääsuõigusi peab saama jagada eraldi kasutajale, administraatorile, auditeerijale ja andmekaitsespetsialistile. Administraatori ja auditeerija töörolle peab olema võimalik teineteisest lahutada.
- Andmete varundamist peab saama reguleerida selliselt, et andmed pannakse hoiule krüpteeritud kujul ja et nende importimine oleks võimalik ainult volitatud töötajatele.
- Tootel peab olema detailidesse laskuv logimisfunktsioon.

Soovituslikud turvaomadused:

- Tootel võiks olla valikuline funktsioon maksete seisukohalt oluliste andmete tervikluse kontrollimiseks.

Näide võimaliku hindamisskaala kohta

Teatud spetsialistide osakond soovib andmevarunduse jaoks soetada andmepakkimisprogrammi. Pärast nõuete kataloogi koostamist võib hakata tegelema seal ülesloetletud spetsiifiliste kriteeriumite hindamisega:

Omadus	hädavajalik	soovituslik	tähendus	usaldusväärsus
korrektselt toimiv kokku- ja lahtipakkimine	X		10	5
bitivigade tuvastamine kokkupakitud failis	X		10	2
failide kustutamine ainult pärast edukat kokkupakkimist	X		10	3
DOS-PC, 80486, 8 MB	X		10	5
sobib Windowsiga		X	2	1
läbilaskevõime 50 MHz juures suurem kui 1 MB/s		X	4	3
programmi XYZ tekstifailide kokkupakkimise aste suurem kui 40 %		X	4	3
Online-abifunktsioon		X	3	1
maksimaalsed kulud 50.- eurot litsentsi kohta	X		10	5
kokkupakitud failide paroolkaitse (turvamehhanismi tugevus kõrge		X	2	5

Täiendavad kontrollküsimused:

- Kes kaasatakse nõuete kataloogi koostamisse?

- Kas otsustab, kas tootel peavad või ei pea olema turvafunktsioonid?
- Kas on olemas ühtlustatud reeglid, kuidas kasutusväärtuse hindamist üles ehitada?

M 2.81 Sobiva tüüptarkvaratoote eelvalimine

Algatamise eest vastutavad: varustusosakond

Rakendamise eest vastutavad: varustusosakond, IT juht, spetsialistide osakond

Tüüptarkvaratoote eelvaliku tegemisel tuleb lähtuda spetsialistide osakonna ja IT-valdkonna töötajate koostatud nõuete kataloogist. Esmalt peaks eelvaliku langetamise eest vastutav osakond tegema turu-uuringu, koostades nõuete kataloogist lähtuvalt saadaolevate toodete kohta ülevaatliku tabeli. Vastavasse tabelisse tuleks kõne alla tulevate toodete kohta üles märkida informatsioon nõuete kataloogis loetletud punktide lõikes. Turuülevaate peaks koostama IT-valdkonna töötajad ning selle koostamiseks võib kasutada tootekirjeldusi, tootjainfot, ajakirju või edasimüüjate väljastatavat infot. Alternatiivse lahendusena võib välja kuulutada hanke, mis võib mõningatel juhtudel olla ka kohutuslik. Hanke väljakuulutamise aluseks on nõuete kataloog, et laekuvate pakkumiste alusel oleks võimalik koostada võrdlev turuülevaade. Seejärel tuleb turuülevaatesse lülitatud tooteid hinnata nõuete kataloogi alusel. Selleks võib kasutada meetmes M 2.80 Tüüptarkvara nõuete kataloogi koostamine välja töötatud hindamisskaalat. Kokkukogutud informatsiooni kohaselt tehakse kindlaks, millised nõutud omadused on tootel olemas. Kui tootel on hädavajalikke omadusi puudu, heidetakse see kõrvale. Iga toote üksikute tooteomaduste hindamise käigus võib kokku arvutada hinnangu kogusumma. Selle summa alusel võib eelvalikusse kaasatud tooted reastada pingeritta.

Näide

Kokkupakkimisprogrammi kohta nõuete kataloogis loetletud nõudmisi hinnati alljärgnevalt:

Omadus	hädavajalik/ soovituslik	tähendus	toode nr 1	toode nr 2	toode nr 3	toode nr 4
korrektselt toimiv kokku- ja lahtipakkimine	H	10	jah	jah	jah	jah
bitivigade tuvastamine kokkupakitud failis	H	10	jah	jah	K.O.	jah

failide kustutamine ainult pärast edukat kokkupakkimist
H
10
jah
jah
jah
jah
DOS-PC, 80486, 8 MB
H
10
jah
jah
jah
jah
sobib Windowsiga
S
2
ei
jah
jah
jah
läbilaskevõime 50 MHz juures suurem kui 1 MB/s
S
4
jah
jah
jah
ei
programmi XYZ tekstifailide kokkupakkimise aste suurem kui 40 %
S
4
jah
jah
ei
ei
Online-abifunktsioon
S
3
ei
ei
ei
jah
maksimaalsed kulud 50.- eurot litsentsi kohta
H
10
jah
jah
jah
jah
kokkupakitud failide paroolkaitse (turvamehhanismi tugevus kõrge

S
2
jah
jah
ei
jah
Hinnang
65 (=maksimum)
60
62
K.O.
57

Tulemusena selgus, et toode nr 3 langeb valikust välja, kuna sellel puudub üks hädavajalik tooteomadus. Pingerida juhib toode nr 2, sellel järgnevad tooted nr 1 ja nr 4. Koosatud pingerida ja turuülevaade tuleks esitada varustusosakonnale, et see saaks kontrollida, mil määral vastavad loetletud tooted organisatsiooni sisereeglitele ja seadustest tulenevatele nõuetele. Kontrollimisel peab varustusosakond arvestama lisaks ka sellega, et kõik ülejäänud osapooled, nagu nt andmekaitsespetsialist, IT turvaspetsialist ja töötajate esindus oleksid õigel ajal protsessi kaasatud. Tuleb otsustada, kui paljusid ja milliseid pingereas olevaid tooteid hakatakse testima. Mõttekas oleks testida pingerea kahte või kolme esimest toodet. Testimise käigus selgitatakse välja, kas tooted täidavad nõuete kataloogis loetletud tähtsamaid valikukriteeriume. Eriti oluline on välja selgitada hädavajalike tooteomaduste olemasolu. Selleks tuleks muretseda testimislitsentsid ning viia läbi testimine meetmetes M 2.82 Tüüptarkvara testimisplaani väljatöötamine ja M 2.83 Tüüptarkvara testimine .

Lisaks nõuete kataloogis loetletud kriteeriumitele võib täiendavalt arvestada ka järgnevate punktidega:

- Soovitused – kas tootjal või edasimüüjal on nimetada kontakte, kus vastav toode on installeeritud, et küsida, millised on kasutuskohas tootega seotud kogemused ning kuidas seal vastavat toodet hinnatakse. Kui testitava tarkvaratoote kohta on olemas testitulemusi või kvaliteedile antud hinnanguid (ajakirjade testitulemused, tootjapoolse standardi testimistulemused, kontrollid ja sertifikaadid, mis vastavad asjakohastele normidele, nagu ISO 12119), tuleks ka neid eelvaliku tegemisel arvestada.
- Toote levik – vigade kõrvaldamine ja täiendavate funktsioonide lisamine on laialt levinud toodete puhul valdkonnad, kus üksikul kasutajal on kas vähe või puuduvad peaaegu üldse igasugused võimalused tootja mõjutamiseks. Kasutaja võib eeldada, et toodet arendatakse edasi. Tihti leidub kolmandate osapoolte läbiviidud teste, mille on algatanud kas tootjad ise või mõned ajakirjad. Laiemalt levinud toodete puhul on nende nõrgad kohad üldjuhul paremini teada ja kasutaja võib eeldada, et põhilised puudused on kas juba tuvastatud või tuvastamisel ning vastav info, mille abil ilmsiks tulnud probleeme likvideerida, levib suhteliselt kiiresti. Vähem levinud toote puhul on kasutajal rohkem võimalusi tootja mõjutamiseks. Üldjuhul puuduvad niisugustel toodetel kolmandate osapoolte läbiviidud testid, kuna väikeste tootja-

te jaoks on need liiga töömahukad ja kallid. Vähem levinud toodetel ei esine tavaliselt ei rohkem ega ka vähem nõrku kohti kui laialt levinud toodetel. Puuduseks võib olla tõsiasi, et kitsaskohti ei avastata võibolla nii ruttu ning seega ei saa neid ka kiiresti kõrvaldada. Kui tegemist on turvaauguga, siis tõenäoliselt ei tea neid ka potentsiaalsed ründajad, st ründe objekti ei peeta piisavalt atraktiivseks.
- Majanduslikkus, st soetamise, töö, hoolduse ja koolitusega seotud kulud – enne mõne toote kasuks otsustamist tuleks alati küsida, kas tootega kaasnevad kulutused ja tootega saavutatav kasutegur on omavahel kooskõlas. Lisaks soetamiskuludele tuleb kokku arvestada ka järgnevad kulud, mis on seotud toote kasutamise, hooldamise ning töötajate koolitamisega. Selleks tuleb nt välja selgitada, kas olemasolevat riistvaraplatvormi on tarvis täiendada või kas toote installeerimiseks ja kasutamiseks läheb tarvis täiendavat koolitust.

Kui toote soetamine on otsustatud, tuleks ost teha loomulikult kõige soodsama pakkuja juures. Soodsaim hind võib olla leitud juba turuanalüüsi käigus.

Täiendavad kontrollküsimused:

- Millised eeskirjad on hetkel jõus?
- Kas välja valitud tarkvaratoode sisaldab kõiki nõuete kataloogis loetletud funktsioone?
- Kas toode sobib kokku praegu kasutatava IT-infrastruktuuriga?
- Milliseid täiendavaid kulusid võib oodata nt koolituse ja programmi hoolduse näol?
- Kas toote installeerimine ja kasutamine on võimalik ära teha olemasolevate töötajate abil või on tarvis suurendada personalikulusid või tuleb spetsialistid tellida väljastpoolt?

M 2.82 Tüüptarkvara testimisplaani väljatöötamine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond

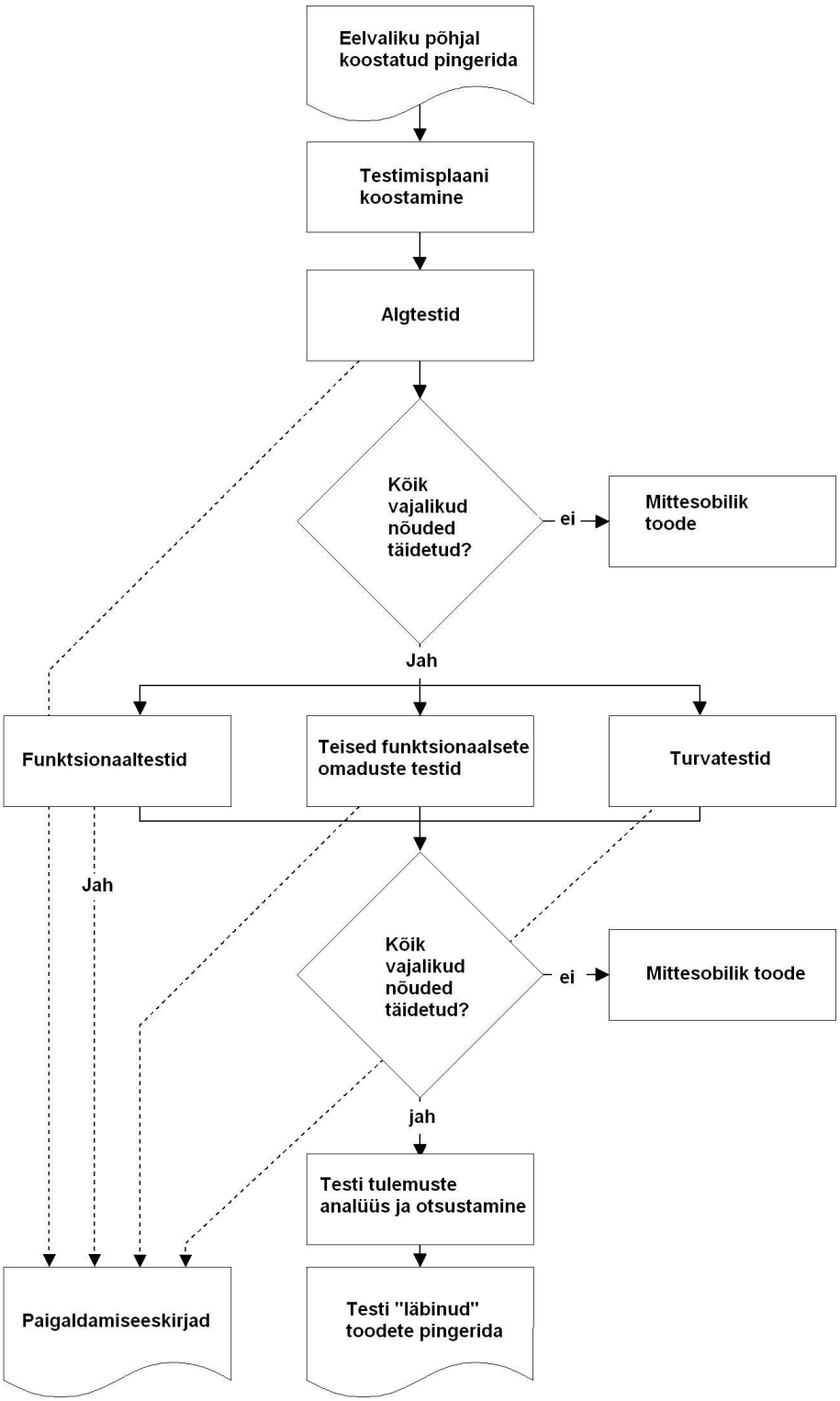
Rakendamise eest vastutavad: erialavaldkonna juhataja, IT-juht

Alljärgnevalt kirjeldatav testimine lähtub standardist ISO/IEC 25051 „Tarkvaratooted, kvaliteedinõuded ja kontrollmehhanismid“, IT-projekti planeerimise ja läbiviimise toimimismudelist (V-mudel) ja informatsioonitehnika süsteemide turvalisuse määramise käsiraamatust (ITSEM). Kõigist eespool nimetatud dokumentidest on võimalik leida põhjalikumat informatsiooni. Enne otsuse langetamist, milline tüüptarkvaratoode soetada, tuleb eelvaliku (vt M 2.81 Sobiva tüüptarkvaratoote eelvalimine) käigus väljavalitud tooteid testimislitsentside abil põhjalikult testida. Juhul kui enne toote soetamist ei olnud seda kas ajaliste piirangute või institutsionaalsete soovituste (kinnipidamine asutusesisestest standarditest) tõttu või mõnel muul põhjusel võimalik teha, tuleb toodet enne selle lõplikku kasutuselevõttu alati testida. Testide tulemused on aluseks paigaldamis- ja kasutuseeskirjade koostamisele. Kuigi juba eelvaliku käigus selgitati välja, kas tootele esitatavad nõuded vastavad tootja lubatutele, ei saa eeldada, et need nõuded oleksid soovitud ulatuses ka tegelikult täidetud. Pigem tuleks enne lõpliku otsuse langetamist viia nõudmiste kataloogile tuginedes läbi süstemaatiline testimine, eesmärgiga määratleda toote sobilikkus ja usaldusväärsus.

Testimine on võimalik neljas valdkonnas:

- algtestid (arvutiviiruste kontroll, töövõime soovitud IT-rakenduskeskkonnas),
- funktsionaaltestid (funktsionaalnõuetele vastavuse kontroll),
- teiste funktsionaalsete omaduste testid (ühilduvus, jõudlus, koostalitlusvõime, seaduslikkus, kasutajasõbralikkus, hooldatavus, dokumentatsioon) ja
- turvatestid (turvanõuetele vastavuse kontroll).

Järgneval joonisel kujutatakse tüüptarkvara üldist testimise käiku.



Testimist vajavad tooted valitakse välja eelvaliku käigus valminud pingereast. Seejärel tuleb koostada testimisplaan, mis peaks sisaldama alljärgnevat:

- testi sisu määratlemine nõuete kataloogi alusel,
- soovituste kontrollimine,
- summaarse testimisaja määratlemine,
- ajakava koostamine, sh igale testile kuluva aja määratlemine,
- testimise eest vastutajate määratlemine,
- testimiskeskkonna määratlemine,
- testimisdokumendi sisu määratlemine,
- otsustuskriteeriumide kindlaksmääramine.

Alljärgnevalt selgitatakse nimetatud punktide sisu.

Nõuete kataloogi alusel testi sisu määratlemine

Nõuete kataloogist valitakse välja testimist vajavad nõuded. Esmajoones peaks siinkohal tegemist olema omadustega, millel on oluline tähtsus või mille usaldusväärsus peaks olema tagatud.

Soovituste kontroll

Esialgsed soovitused testitavate toodete kohta saadi juba eelvaliku käigus. Neid soovitusi võib järgida vaid juhul, kui välistestijad on olnud piisavalt usaldusväärsed. Kui tootele on informatsioonitehnika süsteemide turvalisuse määramise (ITSEM) või Common Criteria (CC) kriteeriumide kohaselt väljastatud sertifikaat, tuleb sertifitseerimisaruande põhjal kindlaks teha, kuivõrd saab sertifikaadis sisalduvaid testi tulemusi usaldada. Kui tegemist on usaldusväärsete tulemustega, ei ole vaja kõiki teste läbi viia või võib seda teha väiksemas ulatuses. Vabaksjäävaid ressursse võib kasutada muudeks testimisteks.

Summaarse testimisaja määratlemine

Selleks, et testimisaega mitte liialt pikaks venitada, tuleks kohe algul kindlaks määrata testimisele kulutatav aeg, näiteks piiritleda see kindlate päevade või tähtajaga.

Ajakava koostamine, sh igale testile kuluva aja määratlemine

Mitme toote testimisel on soovitatav testida neid võrreldavalt. See tähendab, et kõikide toodete ühte kindlat omadust või nende vastavust nõuete kataloogi ühele kindlale nõudele testitakse korraga. Testimisele kulutatav aeg on sel juhul piiritletud nõuete kataloogi ühe kindla nõudega ja on seega jagatud automaatselt võrdselt kõigi testitavate toodete vahel. Seejuures tuletatakse testimisele kulutatav aeg testimise läbiviimise põhjalikkusest ja omaduse komplekssusest. Iga omaduse testimise põhjalikkus sõltub sellest, kuivõrd usaldusväärne iga omadus peaks olema. Samas tuleb silmas pidada ka iga omaduse vastuvõtlikkust vigadele ja selle kasutamissagedust. Põhjalikumat informatsiooni leiate ISO-standardist 25051.

Soovitused:

- Spetsiifiliste turvanõuete puhul võib testimise põhjalikkus lisaks olla tuletatud ka vajalike mehhanismide tugevusest.
- Algtestide läbiviimisele tuleks võrreldes teiste testidega kulutada vähem aega.

Lõpuks tuleb summaarne testimisaeg jagada iga vastava omaduse testimiseks kulutatavaks ajaks.

Testimise eest vastutajate määratlemine

Iga üksiku testi puhul tuleb kindlaks määrata teostamist vajavad ülesanded ja määrata nende eest vastutajad. Kindlasti tuleks silmas pidada, et mõne testi läbiviimisesse on vaja kaasata ka personali või ettevõtte nõukogu esindajad ja andmeturbe ning IT-turbe eest vastutavad töötajad.

Testimiskeskkonna määratlemine

Testimine on alati destruktiivne, kuna selle eesmärk on otsida vigu. Seepärast peab testimine toimuma alati isoleeritud keskkonnas. Võimaluse korral peaks testimiskeskkond olema töökeskkonna täpne jäljend. Majanduslikult ei ole aga tavaliselt võimalik töökeskkonda täies mahus jäljendada. Selleks, et väljavalitud tooteid saaks testida võimalikult sarnastes tingimustes, tuleb defineerida soovituslik keskkond. Üksikute testide läbiviimiseks võib seda vajaduse korral sobitada või piiritleda. Tuleb kindlaks määrata üksikute testide läbiviimiseks vajalikud ressursid (vahendid, IT infrastruktuur) ning kirjeldada detailselt, millal ja millises ulatuses neid kasutada. Oluline on, et testimiskeskkonnas oleksid kättesaadavad kõik vajalikud rakendussüsteemid kõigis kasutatavates versioonides. See aitab avastada töökeskkonna süsteemist tulenevate komponentide nõrku kohti, mis pääsevad mõjule koos paigaldatava tüüptarkvaraga. Juhul kui erinevaid aspekte on võimalik üldistada, võib erandkorras üksikutest komponentidest loobuda.

Kindla ja sobiliku testimiskeskkonna loomiseks tuleb kindlasti arvestada ka järgnevaga:

- Viirustevaba testimiskeskkonna kindlustamiseks tuleks rakendada uusimat viirusetõrjeprogrammi.
- Kõrvalmõjudeta testimiskeskkonna kindlustamiseks on soovitatav kohe alguses paigaldada spetsiaalsed IT-süsteemid.
- Ligipääsuõigused peavad testimiskeskkonnas olema konfigureeritud nii, et nad vastaksid töökeskkonnale.
- Ligi- ja juurdepääs testimiskeskkonnale peab olema reglementeeritud.
- Tuleb tagada, et toode rakendatakse töösse täpselt selles konfiguratsioonis, milles teda testimiskeskkonnas katsetati. Seepärast on testimiskeskkond sobilik tervikluse kaitse nõude rakendamiseks (digitaalsed allkirjad, kontrollsummad).
- Testimiskeskkonna loomiseks tehtavad kulutused peavad olema mõõdukad.

Pärast kõikide plaanis olnud testimiste lõpetamist tuleb otsustada, kas testimiskeskkond tuleb likvideerida või jätta alles. Võimalik, et pärast toote soetamist on vaja läbi viia veel mõningaid teste, seepärast on majanduslikult ilmselt õigem testimiskeskkond säilitada. Enne testimiskeskkonna likvideerimist tuleb kõik testimisandmed kustutada, seda juhul, kui neid hiljem enam vaja pole (näiteks hilisemal paigaldamisel). Väljatrükid tuleb eeskirjade kohaselt hävitada, programmid desinstalleerida. Valituks mitteosutunud toodete testimislitsentsid tuleb tagastada.

Testimisdokumendi sisu määratlemine

Testimisplaanis peab olema kindlaks määratud, millise põhjalikkusega tuleb testimisdokument koostada. Dokument peaks olema koostatud nii, et sellele oleks

hiljem võimalik tugineda, samuti peaks olema täidetud täielikkuse nõue. Testimisdokument peab sisaldama testimisplaane, -eesmärke, -meetodeid ja -tulemusi, samuti peaks seal olema kirjeldatud, kuivõrd on testid ja spetsiifilised nõuded üksteisega kooskõlas. Kõik testimisega seotud toimingud, samuti testi tulemused (koos tehtud otsuste põhjendusega) peaksid olema kirjalikult fikseeritud. Dokument peaks seega sisaldama alljärgnevat:

- toote nimetus ja selle kirjeldus,
- testi algus- ja lõpuaeg ning kogukestus,
- testi eest vastutaja,
- testimiskeskkonna konfiguratsioon,
- testimisjuhtumite kirjeldus,
- otsustuskriteeriumid, testi tulemused ja argumentatsioon,
- täitmata nõuded lähtuvalt nõuete kataloogist.

Testijatele peab võimaldama testimisdokumendi nõuetekohase täitmise ja testimisega seotud toimingute ja testimise tulemuste protokollimise (vastav protokollimisprogramm, ankeedid jne). Kui kasutati automatiseeritud testimist, tuleb testidokumendis seda võimalikult täpselt kirjeldada, et hiljem oleks võimalik mõista, miks langetati just selline otsus.

Otsustuskriteeriumite kindlaksmääramine

Igat läbiviidavat testi võib hinnata näiteks järgmise kolmeastmelise skaala abil:

Hinne

Otsustuskriteerium

0

-

Nõuded ei ole täidetud.

või

-

Avastati olulised vead, mida ei ole võimalik kõrvaldada.

1

-

Nõuded on mõningaste mööndustega täidetud (nt funktsioon on sobilik vaid piiratult).

või

-

Avastati väikesed vead. Need ei mängi olulist rolli, kuna nende mõju töökeskkonnas ei ole märkimisväärne või nende ilmnemine on vähetõenäoline.

2

-

Nõuded on täies ulatuses täidetud.

või

-

Avastatud vead on kõrvaldatavad või neil ei ole töökeskkonnas mingit tähendust.

Tabel. Väärtusskaala

Kui testija avastas vea, mida ei saa uuesti esile kutsuda, peab ta otsustama, millisesse kategooriasse ta vea liigitab (millise hinde annab). Kui avastati viga,

mida oli testimise käigus võimalik kõrvaldada, tuleb pärast vea kõrvaldamist sama omadust vajalikus ulatuses uuesti testida.

Näide:

Jätkates punktis M 2.81 Sobiva tüüptarkvaratoote eelvalimine toodud kokkupakkimisprogrammi näidet, kirjeldatakse allpool võimalust, kuidas määratleda nõuete kataloogis kirjeldatavate üksikute nõuete testimiseks kuluvat aega. Testimisaeg sõltub seejuures testimise põhjalikkusest ja komplekssusest. Usaldusväärsuse nõue tähistab omadusele esitatavat usaldatavuse määra. Ühe omaduse esinemissagedust, vastuvõtlikkust vigadele ja komplekssust hinnatakse alljärgnevalt:

1 – madal,
2 – keskmine,
3 – kõrge.

Kui toote omadus jääb muutumatuks ega sõltu ei selle vastuvõtlikkusest vigadele ega ka kasutamissagedusest, on tegemist erandjuhtumiga. Sel juhul hinnatakse seda 0ga. Kokkupakkimisprogrammi näidet kasutades saab koostada järgneva tabeli:

%des
Ajakulu
Komplekssus
Põhjalikkus
Kasutamissagedus
Vastuvõtlikus vigadele
Usaldusväärsus
korrektne kokku- ja lahtipakkimine
5
2
3
10
2
20
23
bitivigade avastamine kokkupakitud failis
2
2
1
5
2
10
11
failide kustutamine ainult pärast edukat kokkupakkimist
3
2
1
6
1
6
7
DOS-PC, 80486, 8 MB

5
0
0
5
1
5
6
sobib Windowsiga
1
0
0
1
1
1
1
läbilaskevõime 50 MHz juures suurem kui 1 MB/s
3
1
2
6
1
6
7
programmi XYZ tekstifailide kokkupakkimise aste suurem kui 40%
3
2
2
7
1
7
8
online-abifunktsioon
1
1
2
4
1
4
5
maksimaalsed kulud 50.- DM litsentsi kohta
5
0
0
5
1
5
5
kokkupakitud failide paroolkaitse (turvamehhanismi tugevus kõrge)
5
1

2
8
3
24
27

Tabel. Kokkupakkimisprogrammi näide

Kõnealuse näite puhul määratleti testimise ajakulu järgmiselt:

testimiseks vajalik aeg = komplekssus * põhjalikkus,

kus

põhjalikkus = usaldusväärsus + vastuvõtlikkus vigadele + kasutamissagedus

(Tabeli viimases veerus esitatud ajakulu protsentides tuleneb kontrollitavatele väärtustele kulutatud ajast, jagades selle nende väärtuste summaga.)

Näide teisest meetodist, kuidas arvestada ajakulu ja hinnata testi tulemusi, sisaldub ISO-standardis 25051. Siin toimub hindamine järgmiselt:

iga üksiku testi hindamine = (komplekssus + vastuvõtlikkus vigadele) * (kasutamissagedus + olulisus).

Sobiliku hindamismeetodi lõpliku valiku peab testi eest vastutaja igal konkreetsel juhul ise tegema, arvestades toodet ja institutsiooni. Kui testimisplaan on valmis, tehakse kõigile plaanis määratud testite eest vastutavatele isikutele või isikute grupile ülesandeks viia läbi testimine. Igale testimisgrupi liikmele antakse testimisplaan ja tehakse teatavaks üksikute testide läbiviimise ajad.

Täiendavad kontrollküsimused:

- Kas kõik testi läbiviimiseks vajalikud ankeedid ja nimekirjad on koostatud?
- Kas kõik testimise läbiviimiseks vajalikud ülesanded on jagatud?
- Kas kõik testimist vajavad aspektid on määratletud?

M 2.83 Tüüptarkvara testimine

Algatamise eest vastutavad: erialavaldkonna juhataja, IT-juht

Rakendamise eest vastutavad: testija

Tüüptarkvara testimise saab jaotada ettevalmistus-, teostamis- ja hindamisetapiks. Iga etapp sisaldab kindlaid ülesandeid.

Testi ettevalmistamine

- Üksikute testimismeetodite määratlemine (testiliigid, -meetodid ja -vahendid)
- Testi andmete ja testijuhtumite genereerimine
- Vajaliku testimiskeskkonna loomine

Testi teostamine

- Algtestid
- Funktsionaalsed testid
- Teiste funktsionaalsete omaduste testid
- Turvatestid
- Pilootrakendus

Testimise hindamine

Alljärgnevalt kirjeldatakse üksikuid ülesandeid.

Testi ettevalmistamine

Testide läbiviimise meetodid on näiteks staatiline analüüs, simulatsioon, veatuse tõestus, sümboolne programmiteostus, ülevaade, inspektsioon, tõrkeanalüüs. Siinjuures tuleb aga silmas pidada, et mõned nimetatud meetodeist on läbiviidavad vaid allikteksti olemasolu korral. Ettevalmistusetapis tuleb välja valida ja määratleda sobivad testimismeetodid. Tuleb selgitada, milliseid meetodeid ja vahendeid programmide testimiseks ja dokumentide kontrollimiseks kasutada. Tüüpilisemad meetodid programmide testimiseks on nt funktsionaaltestimine, strukturaaltestimine või penetratsioonitest. Dokumente on võimalik kontrollida nt informaalse kontrolli, ülevaate või kontrollnimekirja abil. Funktsionaaltest on funktsioonivõime kontroll arvestamata sisemist programmikulgu, mille käigus kontrollitakse nt programmi kõiki andmeliike veatöötluse ja vastuvõetavuskontrolli seisukohast. Strukturaaltesti puhul on tegemist funktsioonivõime kontrolliga, kusjuures avalikustatakse sisemine programmikulg, nt allikteksti kontrollimise või jälituse kasutamise teel. Strukturaaltestid ületavad tavaliselt etalonturbe piirid ning neid ei saa kasutada tüüptarkvara testimiseks, kuna tootja ei avalikusta allikteksti. Funktsioonivõime testide puhul tuleb tõendada, et iga test vastab spetsifikatsioonile. Penetratsioonitesti abil määratakse kindlaks, kas teadaolevaid ja oletatavaid haavatavaid kohti saab toote praktilisel töölerakendamisel ära kasutada, nt turvamehhanismidega manipuleerimise või neist hoidumise teel, manipuleerides rakendussüsteemi tasandit. Samuti tuleb kindlaks määrata tulemuste kindlustamise ja nende hindamise viis, arvestades eriti kontrollimiste kordumist, ja see, millised andmed tuleb testi toimumise ajal ja pärast testi läbiviimist säilitada.

Testi andmete ja testijuhtumite genereerimine

Testiks ettevalmistamine hõlmab ka testiandmete genereerimist. Vastavad meetodid ja toimingud peavad olema varem kindlaks määratud ja kirjeldatud. Iga üksiku testi jaoks tuleb genereerida sobiv arv testijuhtumeid, mis oleksid vastavuses testi ajakuluga. Juhtumeid tuleks genereerida iga järgmise kategooria tarvis:

- Tüüpjuhtumid on juhtumid, mille abil saab kontrollida kindlate funktsioonide töötlemise korrektsust. Sisestatavaid andmeid nimetatakse normaalväärtusteks või piirväärtusteks. Normaalväärtused on keskmise väärtusega andmed, piirväärtused on iga kehtiva andmesisestusvaldkonna piirandmed.
- Veajuhtumid on juhtumid, mis provotseerivad programmi vastama veateatega. Neid sisendväärtusi, millele programm peaks etteantud veateatega reageerima, nimetatakse valeväärtusteks.
- Erandjuhtumid on juhtumid, mille puhul programm peaks erandkorras reageerima teisiti kui tüüpjuhtumite korral. Tuleb kontrollida, kas programm tuvastab taolised juhtumid ja kohandub neile õigesti.

Näited:

Kui sisendparameetrid oleksid vahemikus 1 kuni 365, tuleb testid läbi viia valeväärtusega (nt 0 või 1000), piirväärtustega 1 ja 365 ning normaalväärtusega, mis asub vahemikus 1 kuni 365. Kui testiandmete genereerimine on liialt töömahukas või keeruline, võib testi jaoks kasutada ka tõeseid, kuid anonüümseid andmeid. Usaldusväärsuse kaitse seisukohalt peavad tõesed andmed olema tõepoolest anonüümsed. Tuleks jälgida, et anonüümsed tõesed andmed ei kataks mitte kõiki piirväärtusi ja erandjuhtumeid, mis tuleks luua eraldi. Lisaks testi andmetele tuleks vaadelda ka kõikvõimalikke kasutajapoolseid vigu. Siinjuures on probleemiks kasutaja võimalikud reaktsioonid, mida programm ei oska näha ja mida seetõttu ei ole võimalik korrektselt tõrjuda.

Vajaliku testimiskeskkonna ülesehitamine

Testimise läbiviimiseks tuleb sisse seada testimisplaanis kirjeldatud testimiskeskkond ja installeerida sellele testitavad tooted. Rakendatavad komponendid tuleb märgistada, samuti tuleb kirjeldada nende konfiguratsiooni. Kui toote installeerimise käigus tekib kirjeldatud konfiguratsiooni suhtes kõrvalekaldeid, tuleb need kirja panna.

Testide läbiviimine

Teste tuleb läbi viia testimisplaani alusel. Kõik tegevused koos testide tulemustega tuleb piisava täpsusega üles kirjutada ja läbi analüüsida. Eriti oluline on vigade põhjalik dokumenteerimine, et neid oleks võimalik hiljem uuesti esile kutsuda. Välja tuleb selgitada tulevase tavakasutuse jaoks vajalikud kasutusparameetrid ja need kirja panna, et neid oleks võimalik hiljem installeerimisjuhendi koostamisel arvesse võtta. Kui tootel tuvastatakse lisafunktsioone, mis ei ole nõuete kataloogis üles loetletud, kuid võivad siiski kasulikuks osutuda, tuleb nende kontrollimiseks läbi viia vähemalt üks lühitest. Juhul kui funktsioonidel on tulevase kasutuse jaoks suurem tähtsus, tuleb neid põhjalikumalt testida. Täiendavate testimisega seotud tegevuste jaoks tuleb olenevalt olukorrast taotleda vastutavate töötajate käest testimistähtaja pikendamist. Testide tulemused tuleb kaasata lõpphinnangusse. Kui üksikute testitulemuste läbitöötamisel peaks selguma, et nõuete kataloogi üks või

mitu kriteeriumit ei ole olnud piisavalt konkreetselt sõnastatud, tuleb neid vajaduse korral täpsustada.

Näide:
Nõuete kataloog toob konfidentsiaalsuskaitse kriteeriumina välja nõude, et töödeldavaid andmeid peab olema võimalik krüpteerida. Testimiste käigus on selgunud, et krüpteering vallasprotseduurina ei ole selle kasutusvaldkonna jaoks sobilik. Seetõttu tuleks nõuete kataloogi vallasprotseduurina krüpteerimise puhul täiendada. (Vallasprotseduurina krüpteeringut kasutades peab kasutaja ise selle käivitama ja määrama ise ka krüpteerimisele kuuluvad elemendid; sidusprotseduurina krüpteerimine töötab kasutaja jaoks seevastu läbipaistvalt, kasutades eelseadistatud parameetreid).

Sissejuhatavad kontrollid
Enne kõikide muude testide läbiviimist tuleb kontrollida järgmisi põhiaspekte, sest kontrollide ebaõnnestumine toob endaga kaasa kas kindlad reaktsioonid või testi ebaõnnestumise:

- Viiruste välistamiseks tuleb testitav toode kõige värskema viirusetõrjetarkvaraga üle kontrollida.
- Installeerimistestiga tuleb kindlaks teha, kas toodet on võimalik tulevase kasutamise eesmärgil lihtsalt, täies mahus ja arusaadavalt installeerida. Samuti tuleb välja selgitada, kuidas toimub toote täielik desinstalleerimine.
- Toote rakendatavust tuleb testida selle planeeritavas kasutuskeskkonnas; eriti vajavad kontrollimist toote graafiline kasutajaliides, printimisfunktsioon, hiire kasutamise tugi, võrguvalmidus jne.
- Tuleb kontrollida, kas vastav toode on terviklik (kas kõik programmid ja käsiraamatud on olemas), nt võib võrrelda omavahel toodet ja toote koostisosade nimekirja, tootekirjeldust vms.
- Lühidalt tuleks testida programmi neid funktsioone, mis ei olnud nõuetena eraldi välja toodud (funktsioon, usaldusväärsus, rikkekindlus jne).

Funktsionaalsed testid
Nõuete kataloogis ülesloetletud funktsionaalseid nõudeid tuleks kontrollida järgmiste kriteeriumite suhtes:

- Funktsiooni olemasolu – funktsiooni käivitamine programmis ja programmi dokumentatsiooni analüüsimine.
- Funktsiooni rikkekindlus ehk korrektsus – funktsiooni rikkekindluse ehk korrektsuse väljaselgitamiseks tuleb olenevalt testimise põhjalikkusest kasutada erinevaid testimisprotseduure, nagu nt funktsionaal- või strukturaalteste või tavakasutuse simuleeritud kasutuskeskkonda.

Sissejuhatavas testimisfaasis saadud testimisandmeid ja testimisjuhtumeid kasutatakse funktsionaalsete testide läbiviimisel. Funktsionaalseid teste läbi viies on hädavajalik, et testide tulemusi kõrvutataks ka etteantud nõuetega. Lisaks tuleb kontrollida, kuidas töötab programm vigaste sisestusparameetrite või väära käsitsemise puhul. Funktsiooni tuleb testida ka sisestusparameetrite piirväärtuste intervallide piires, samuti erandlikes olukordades. Viimased tuleb õigesti tuvastada ja vastavalt ka käidelda.

Funktsiooni sobilikkus

Funktsiooni sobilikkust saab hinnata selle alusel, kas funktsioon

- täidab talle seatud ülesande ka reaalselt täies mahus ja efektiivselt ning
- kas seda on lihtne muude protsesside hulka integreerida.

Kui funktsiooni sobilikkus ei ole üheselt arusaadav, tuleks seda testida kasutuskeskkonna simulatsioonis, kuid ilmtingimata siiski testimiskeskkonnas.

Vastuolude välistamine

Funktsioone tuleb kontrollida ka võimalike vastuolude suhtes, st omavahel tuleb võrrelda nõuete kataloogi, dokumentatsiooni ja programmi. Võimalikud vastuolud tuleb kirja panna. Dokumentatsiooni ja programmi erinevused tuleb dokumenteerida sellise täpsusega, et toote hilisema kasutamise korral oleks võimalik lisada neid täiendustena programmi dokumentatsiooni.

Muude funktsionaalsete omaduste testimine

Lisaks funktsionaalsetele ja spetsiaalselt turvalisust puudutavatele nõuetele tuleb nõuete kataloogis testida ka muid funktsionaalseid omadusi:

- Jõudlus – kõikide toote jaoks planeeritud konfiguratsioonide kohta tuleb välja selgitada nende talitlusaeg. Jõudluse põhjalikuks testimiseks on üldjuhul mõttekas kasutada testimisprotseduure, mis simuleerivad kasutuskeskkonda või siis anda see väljavalitud töötajatele katse korras kasutada. Testimisega tuleb välja selgitada, kas jõudlusele seatud nõuded on täidetud või mitte.
- Usaldusväärsus – testida tuleks toote käitumist juhuslike või ka tahtlike süsteemi avariide (nn krahh-testid) puhul ning analüüside käigus tuvastada, millised võivad olla niisuguste olukordadega kaasnevad kahjud. Testi tulemusel tuleb kirja panna, kas pärast süsteemi avariid on toote korrapärane ja korrektne taaskäivitamine võimalik või mitte. Samuti tuleb kontrollida, kas andmetele on võimalik otse ligi pääseda ka tavapärasest programmifunktsioonist sõltumata. Paljudel juhtudel võib niisuguse juurdepääsu võimaldamine viia andmekadudeni ning toode peaks suutma seda takistada. Samuti tuleb üles märkida, kas programm toetab funktsioone, mis võimaldavad ennistada „kriitilisi tegevusi” (nt kustutamist ja formaatimist).
- Kasutajasõbralikkus – toote kasutajasõbralikkuse hindamine sõltub suuresti testi läbi viiva isiku isiklikest hinnangutest. Sellele vaatamata saab kasutajasõbralikkuse hindamisel lähtuda järgmistest abistavatest punktidest, nagu menüüde tehnilised lahendused (rippmenüüd, kerimine, lohistamine jne), menüüde disain (nt terviklus, arusaadavus, menüüde vahel liikumine), nuppude kasutamine, veateated, probleemivaba liidestega suhtlemine (pakkrežiim, kommunikatsioon jne), kasutaja dokumentatsiooni loetavus ja abifunktsioonid. Toote kasutajasõbralikkuse analüüs peab kirjeldama erinevaid töörežiime, samuti toote käitumist võimalike käitus- või kasutusvigade korral koos nende võimalike tagajärgede ning järelduste väljatoomisega turvalise kasutuse tagamisel.
- Hooldamine – testimise käigus tuleb välja selgitada, kui palju personali- ja finantsressursse kulub toote hooldamiseks ja korrashoiuks. Seda võib hinnata nt soovituste või erialases kirjanduses väljatoodud nõuannete ja võrdluseks tehtud installeerimiste põhjal või testimise käigus tuvastatud installeerimisele kulunud ressursside põhjal. Selleks tuleb täpselt kirja panna, kui

palju kordi oli tarvis installeerimistöö käigus protsessi käsitsi sekkuda, et jõuda konfiguratsiooniga soovitud lõpptulemuseni. Kui testitava toote eelmiste versioonidega on juba saadud kogemusi, tuleks meelde tuletada, kui suurt vaeva tuli näha eelnevate versioonide hooldamisega. Tuleks välja selgitada, kas tootele saab tootja või edasimüüja käest tellida ka tuge ning millised on selle tingimused. Kui tootja või edasimüüja pakub tootele infoliini teenust, tuleks kontrollida selle kättesaadavust ja kvaliteeti.

- Dokumentatsioon – tootega kaasasoleva dokumentatsiooni puhul tuleb kontrollida, kas see on täielik, korrektne ja ega see ei sisalda vastuolusid. Sellele lisaks peaks toote dokumentatsioon olema arusaadav, veatu ja ülevaatlik. Täiendavalt tuleb kontrollida, kas dokumentatsioon on toote turvaliseks kasutamiseks ja konfigureerimiseks piisav. Dokumentatsioonis peavad olema kirjeldatud kõik turbealased funktsioonid.

Lisaks eelnevale tuleb nõuete kataloogis kontrollida järgmisi punkte:

- ühilduvusele seatud nõuded,
- koostalitlusvõime,
- vastavus standarditele,
- sisereeglite ja test tulenevate nõuete järgimine,
- tarkvara kvaliteet.

Turbealased testid

Kui tootele on seatud turbealaseid nõudeid, tuleb lisaks eespool loetletud testidele läbi viia ka järgmised turbealased testid, mille käigus kontrollitakse

- turbefunktsioonide tõhusust ja nende toimimise korrektsust,
- turvamehhanismide tugevust ning
- turvamehhanismide eiramis- ja vältimisvõimalusi.

Turbealaste testide abimaterjalina võib kasutada näiteks IT-süsteemide turvalisuse hindamise käsiraamatut (ITSEM – Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik), kust võib leida ka paljusid alljärgnevalt väljatoodud lähenemisviise. Täiendavaid kirjeldusi võib kasutada näidetena ja teemaga tutvumiseks. Alustuseks peab olema funktsionaalsete testidega kindlaks tehtud, et tootel on olemas vajalikud turbealased funktsioonid. Seejärel tuleb kontrollida, kas kõik vajalikud turvamehhanismid on nõuete kataloogis üles loetletud ja kui mitte, tuleb kataloogi vastavalt täiendada. Mehhanismide miinimumtugevuse kinnitamiseks või ümberlükkamiseks tuleb läbi viia penetratsioonitestid. Vastavad penetratsioonitestid tuleb läbi teha kõikide muude testimisliikide järel, sest need testid võivad anda vihjeid võimalike turvaaukude kohta. Penetratsioonitest võib testitavat objekti ja testimiskeskkonda tugevalt mõjutada või koguni kahjustada. Seetõttu tuleks halbade tagajärgede vältimiseks teha andmetest enne penetratsioonitestide läbiviimist varukoopiad. Penetratsioonitestide läbiviimist võib toetada turvakonfiguratsiooni- ja logimistööriistadega. Vastavad tööriistad analüüsivad süsteemi konfiguratsiooni ja otsivad ühiseid turvaauke, nagu nt avalikult loetavaid faile ja paroolide puudumist. Penetratsioonitestidega tuleks välja selgitada programmi konstruktsiooni nõrgad kohad ja testimise käigus tuleks kasutada täpselt samu meetodeid, mida võiks võimalike turvaaukude ärakasutamise korral püüda rakendada ka potentsiaalne ründe toimepanija.

Näiteks:

- eelseadistatud käsujärjekorra muutmine,
- täiendava funktsiooni käivitamine,
- sisefailide otsene või kaudne lugemine, kirjutamine või muutmine,
- andmete töötlemine, mille puhul ei ole töötlemist ette nähtud,
- funktsiooni kasutamine ootamatus kontekstis või ootamatul otstarbel,
- vigade ignoreerimise sisselülitamine,
- kontrollimise ja kasutuse vahel tekkiva ajalise viivituse ärakasutamine,
- järjekorra katkestamine katkestustega või
- funktsiooni jaoks ootamatu sisendi genereerimine.

Mehhanismide tugevust hinnatakse erialateadmiste, võimaluste ja töövahendite kriteeriumitele toetudes, mille täpsemad kirjeldused leiate ITSEM-ist.

Näiteks võib mehhanismide tugevuse hindamisel kasutada alljärgnevaid reegleid:

- kui isegi võhik suudab mehhanismist mõne minuti jooksul jagu saada, ei saa selle mehhanismi turbeastet liigitada isegi mitte madalate hulka.
- kui rünne osutub minutite jooksul edukaks, ja selle on läbi viinud ükskõik kes peale mõne võhiku, võib mehhanismi turbeastme liigitada madalate hulka.
- kui ründe õnnestumiseks läheb vaja ekspertteadmisi ja ründe läbiviimiseks tuleb olemasoleva tehnikaga kulutada mitmeid päevi, võib mehhanismi turbeastme liigitada keskmiste hulka.
- kui mehhanismist suudavad jagu saada ainult eksperdid, kes saavad kasutada spetsiaalset varustust ja protsess võtab aega mitu kuud, eeldades veel ka salakokkulepet süsteemi haldajaga, võib vastava mehhanismi turbeastme liigitada kõrgete hulka.

Testide läbiviimisel peab olema tagatud, et kõik turbespetsiifikaga seotud funktsioonid saaksid läbi kontrollitud. Siinkohal on tähtis meeles pidada, et testimistega selgitatakse alati välja ainult vead või kõrvalekalded toote spetsifikatsioonist, kuid see ei tähenda veel sugugi, et toode on veatu. Alljärgnevalt on toodud mõningad näited tüüpiliste uurimisteemade kohta:

Paroolikaitse:

- Kas toode on varustatud tootja eelseadistatud paroolidega? Tüüpilised näited niisuguste paroolide kohta on tootenimi, tootjafirma nimi, „SUPERVISOR”, „ADMINISTRATOR”, „USER”, „GUEST”.
- Millises failis toimub muutus pärast seda, kui parooli on muudetud? Kas vastavat faili on võimalik varukoopiast võetava vanema versiooniga asendada, et vanu paroole uuesti sisse lülitada? Kas paroolid salvestatakse krüpteeritud kujul või on need vabalt loetavad? Kas vastava faili sees on võimalik teha muudatusi, et uusi paroole sisse lülitada?
- Kas pärast korduvaid vale parooli sisestamise katseid suletakse juurdepääs ka reaalselt?

- Kas ajakirjades või e-kirjades reklaamitakse tooteid, mis suudavad testitava toote paroole välja nuhkida? Mõningate standardsete rakenduste jaoks on sellised programmid saadaval.
- Kui failid on paroolidega kaitstud, siis kas faili võrdlemisega enne ja pärast parooli muutmist on võimalik kindlaks teha asukoht, kuhu vastav parool salvestatakse? Kas vastavas asukohas on võimalik sisse viia muudatusi või vanu väärtusi, et lülitada tööle teadaolevate paroolide kasutamine? Kas paroolid salvestatakse krüpteeritud kujul? Kuidas on see asukoht kaitstud siis, kui paroolkaitse on välja lülitaud?
- Kas parooli kontrollimise standardprotseduuri on võimalik katkestada? Kas on olemas klahvikombinatsioonid, mille abil on võimalik parooli kontrollimisest mööda minna?

Pääsuõigused:

- Millistesse failidesse salvestatakse pääsuõigused ja kuidas neid kaitstakse?
- Kas volitamata isikutel on võimalik muuta pääsuõigusi?
- Kas vanade pääsuõigustega faile on võimalik uuesti tööle lülitada ning milliseid õigusi on selle jaoks tarvis?
- Kas administraatori õigusi on võimalik piirata selliselt, et administraator ei pääse ligi kasutaja- või logiandmetele?

Andmevarundus:

- Kas andmeid on võimalik probleemivabalt varukoopiate abil taastada?
- Kas varundatud andmeid on võimalik paroolide abil kaitsta? Kui jah, siis saab paroolide testimiseks kasutada eespool välja toodud lähenemisviise.

Krüpteering:

- Kas tootel on olemas failide või andmete varukoopiate krüpteerimise tugi?
- Kas saab kasutada mitmeid erinevaid krüpteerimisalgoritme? Siinkohal tuleb üldjuhul lähtuda järgmisest rusikareeglist: mida kiiremini töötab tarkvara krüpteerimisalgoritm, seda madalam on sellega saavutatav turbeaste.
- Kuhu salvestatakse krüpteerimiseks ja dekrüpteerimiseks kasutatavad võtmed? Kui võtmed salvestatakse kohapeal, tuleb kontrollida, kas vastavaid võtmeid kaitstakse paroolidega või mõne muu võtmega ülekrüpteeritud kujul. Kui kasutatakse paroolkaitset, tuleb arvestada eespool väljatoodud punktidega. Ülekrüpteerimise puhul tuleb jälgida, kuidas kaitstakse sinna juurde kuuluvat võtit. Selleks võib läbi töötada järgmised punktid: millises failis toimub muutus pärast seda, kui võtit on muudetud? Võrreldes vastavat faili enne ja pärast võtmevahetust, saab kindlaks määrata asukoha, kuhu võti salvestatakse. Kas vastavas asukohas on võimalik sisse viia muudatusi, et lülitada uusi võtmeid sisse selliselt, et kasutaja hakkab neid kasutama ja ei pruugi märgata nende kompromiteerimist?
- Kas toode on varustatud tootjapoolsete eelseadistatud paroolidega, mis tuleb enne programmi esmakordset kasutamist ära muuta?

- Mis juhtub siis, kui krüpteerimise käigus sisestatakse vale võti?
- Kas pärast faili krüpteerimist kustutatakse selle krüpteerimata versioon? Kui jah, siis kas fail saab turvaliselt üle kirjutatud? Kas enne kustutamist kontrollitakse, kas krüpteerimine õnnetus?

Logimine:

- Kas logifailid on volitamata isikute juurdepääsu eest kaitstud?
- Kas logimiskohustuse alla kuuluvad protsessid logitakse lünkadeta?
- Kas administraatoril on oma privilegeeritud õiguste tõttu võimalik märkamatult logifailidele juurde pääseda või logimisfunktsiooni märkamatult välja lülitada?
- Kuidas käitub programm logimiseks ettenähtud mälumahu täissaamise korral?

Lisaks eelnevale tuleb välja selgitada, kas uue toote rakendamisega kaasneb turvaomaduste muutumine mõnes teises kohas. Näide: testitaval tootel on olemas liides operatsioonisüsteemi keskkonda ühendamiseks, kuid IT-süsteem oli eelnevalt konfigureeritud selliselt, et niisuguseid liideseid ei eksisteerinud.

Proovikasutus

Pärast kõikide testide läbiviimist võib tekkida vajadus toote proovikasutuseks ehk toote testimiseks reaalsetes töötingimustes. Kui proovikasutus toimub reaalses töökeskkonnas koos reaalsete andmetega, peab töökeskkonna käideldavuse ja tervikluse tagamiseks olema eelnevate, piisaval arvul läbiviidud testidega tõestatud, et programm töötab korrektselt ja vigadeta. Toote testimiseks reaalsetes tööprotsessides võib selle installeerida näiteks väljavalitud töötajate IT-süsteemidele ja kohustada töötajaid seda teatud aja jooksul kasutama.

Testitulemuste hindamine

Testide tulemusi tuleb hinnata eelnevalt kindlaksmääratud hindamiskriteeriumite alusel. Kõikide testide tulemused tuleb kokku koguda ja esitada koos teste kajastavate dokumentidega kas varumisosakonnale või muudele testi eest vastutavatele töötajatele. Testitulemustele toetudes tuleks soetatavale tootele anda lõplik hinnang. Kui ükski toode ei suutnud testimist edukalt läbida, tuleb kaaluda, kas oleks tarvis algatada uus turu-uuring, kas seatud nõuded olid võib-olla liiga kõrged ja vajavad muutmist või tuleb toote soetamisest hetkel üldse loobuda.

Näide:

Pakkimisprogrammi näitel on välja toodud olukord, kuidas võiks toimuda testitulemuste hindamine. Testide käigus uuriti kolme erinevat toodet, mida hinnati meetmes M 2.82 Tüüptarkvara testimisplaani väljatöötamine .

Omadus	Hädavajalik/ soovituslik	Tähendus	Toode nr 1	Toode nr 2	Toode nr 3	Toode nr 4

Korrektselt toimiv kokku- ja lahtipak-kimine	H	10	2	2	jah	0
Bitivigade tuvasta-mine kokkupa-kitud failis	H	10	2	2	ei	2
Failide kustuta-mine ainult pärast edukat kokku-pakkimist	H	10	2	2	jah	2
DOS-PC, 80486, 8 MB	H	10	2	2	jah	2
Sobib Window-siga	S	2	0	2	jah	2
Läbilaskevõime 50 MHz juures suurem kui 1 MB/s	S	4	2	2	jah	2
Tihendustegur üle 40%	S	4	2	1	ei	0
Online - abifunktsioon	S	3	0	0	ei	2
Pakitud failide pa-roolkaitse funkt-sioon	S	2	2	1	ei	2
Hinnang			100	98	K.O.	K.O.

Hind (maksimaalsed kulud 50.- eurot litsentsi kohta)	49,- €	25,- €	39,- €

Tabel. Tüüptarkvara testimisplaan

Toode nr 3 langes välja juba eelvalikuid tehes ning seetõttu seda ei testitud. Toode nr 4 põrus testimislõigus „Korrektselt toimiv kokku- ja lahtipakkimine", kuna seda omadust hinnati 0ga ning tegu oli hädavajaliku tooteomadusega. Toote nr 1 ja nr 2 lõpphinde saamiseks korrutati tootele antud punktid läbi hindamiskriteeriumi osatähtsusega ja liideti need omavahel kokku:

Toode nr 1: 10 * 2 + 10 * 2 + 10 * 2 + 10 * 2 + 2 * 0 + 4 * 2 + 4 * 2 + 2 * 2 = 120

Toode nr 2: 10 * 2 + 10 * 2 + 10 * 2 + 10 * 2 + 2 * 2 + 4 * 2 + 4 * 1 + 2 * 1 = 118

Testitulemuste hindamise järel on esimesel kohal toode nr 1, kohe selle kannul on aga ka toode nr 2. Lõpliku otsuse, kumma toote kasuks otsustada, peab testitulemuste alusel tegema varumisosakond, võttes sealjuures arvesse ka testidest selgunud hinna ja kvaliteedi suhet.

Täiendavad kontrollküsimused:

- Kas kasutatud riist- ja tarkvara konfiguratsioon vastab nõuete kataloogile?
- Kas tootja või edasimüüja pakub tootele ka tuge või hooldusteenust?
- Kas kasutajale mõeldud dokumentatsioonis on kõik kasutaja jaoks olulised funktsioonid täies mahus ja arusaadavalt lahti seletatud?
- Kas olemasolev dokumentatsioon sisaldab ka sisukorda, märksõnade registrit ja viiteid lehekülgedele?
- Kas kõiki nõutud funktsioone saab kasutada ning kas nad töötavad korrektselt?
- Kas toode on oma kasutuskeskkonnas piisavalt usaldusväärne ja tugev?
- Kas toote käitamisega piirvõimsusel või toote väärkasutamisega on võimalik andmeid võltsida või hävitada?
- Kas toode töötleb lubamatuid ja defineerimata sisestusi samamoodi nagu lubatud sisestusi?
- Kas testide dokumentatsioon on koostatud etteantud nõuete kohaselt?

M 2.84 Tüüptarkvara installeerimisjuhendite otsustamine ja koostamine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtorgan

Rakendamise eest vastutavad: IT-juht, spetsialistide osakond, varustusosakond

Pärast kõikide testide läbiviimist tuleb tulemused esitada varustusosakonnale. Ostuotsuse peab tegema varustusosakond koos spetsialistide ja IT-osakonna toega, võttes arvesse testitulemusi ja nendest tulenevaid hinna ja kvaliteedi suhteid. Eriti oluline on siinkohal võrrelda, kui suures osas suudavad erinevad tooted täita nõuete kataloogis seatud tingimusi ja milline toode on sealjuures kõige soodsama hinnaga. Otsuse langetamisel tuleks arvestada ka lisafunktsioonidega, mida pole küll nõuete kataloogis loetletud, kuid mis võivad kasutamise käigus siiski kasulikuks osutuda.

Installeerimisjuhendi koostamine

Pärast teatud kindla toote kasuks otsustamist tuleb väljavalitud toote jaoks koostada ka vastav installeerimisjuhend. Testimise käigus on välja selgitatud konfiguratsioon, mis peab tagama toote turvalise ja efektiivse kasutuse. Vastav konfiguratsioon peab tagama toote kasutamise parimal kasutajasõbralikul, korrektsel ja turvalisel moel. Sobiva konfiguratsiooni tagamiseks tuleb kehtestada teatud kohustuslikud parameetrid. Osaliselt tuleb nende rakendamist toetada ka organisatoorsete meetmetega. Järgnevas näites on püütud välja tuua kohustuslikud aspektid, mida installeerimisjuhend peab käsitlema.

Näide:

Kasutajasõbralikkus

- Kasutaja jaoks vastuvõetava kasutuskeskkonna loomiseks (et pilt ei virvendaks ja printeri lahutusvõime oleks piisav jne), tuleb koos tootega installeerida ka draiverid X, Y ja Z (monitor, printer, hiir).
- Nende seadistuste tegemine, kus üksikutel funktsioonidel on tarvis kõige suuremat töötlemiskiirust, tuleb kindlaks määrata. Seda tuleb teha eeldusel, et muud kriteeriumid, nagu nt turvalisus, ei sea sellele piiranguid (saalimisfailide suurus tuleb tõsta vähemalt 10 MBni, andmete varukoopiate loomise puhul tuleb sisse lülitada verifitseerimine ja seda vaatamata tõsiasjale, et verifitseerimine nõuab täiendavat ajalist ressurssi).

Turvalisus

- Turvafunktsioonide parameetrid tuleb eelseadistusega kindlaks määrata (näiteks tuleb kindlaks määrata paroolide miinimumpikkus (vt M 2.11 Paroolide kasutamise reeglid), andmete varukoopiaid tuleb luua iga päev, logimine tuleb sisse lülitada täies mahus, isikuandmetega seotud logifailide pääsuõigused tuleb anda ainult andmekaitse eest vastutavale töötajale jne).
- Kui toode toetab mitme erineva turvaprotseduuri (nt krüpteerimisalgoritmi, räsifunktsioonide) kasutamist, tuleb nende hulgast välja valida need funktsioonid, mis aitavad saavutada soovitud turbeastet (valikute M 2.164 Sobiva krüptoprotseduuri valimine).

Funktsioonid

- Sisse tuleb lülitada ainult X, Y ja Z funktsioonid. Sellised funktsioonid, mida ei soovita või mis ei ole vajalikud, tuleb välja lülitada.
- Andmete automaatse varukoopia loomise funktsioon peaks käivituma iga 10 min järel.

Organisatoorne külg

- Installeerimistöö peab tegema administraator.
- Toote kasutamise kohta tuleb koostada kasutusreeglid (nt andmete varukoopiate tegemise eest vastutab töötaja ise, paroole tuleb muuta iga 30 päeva tagant).

Raamtingimused

- Juhul kui platvormil, mille peal tüüptarkvara käitama hakatakse, esineb süsteemist tingitud kitsaskohti, mida tahetakse konfigureerimise abil kõrvaldada, tuleb konfigureerimist põhjalikult kirjeldada ja ette anda täpsed konfigureerimisjuhised.

Täiendavad kontrollküsimused:

- Kas installeerimisjuhendis on välja toodud kõik edukaks installeerimiseks vajalikud juhtnöörid?
- Kas on olemas informatsioon vastava toote desinstalleerimise kohta?

M 2.85 Tüüptarkvara kinnitamine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtorgan

Rakendamise eest vastutavad: osakonna juht, IT-juht

Enne tüüptarkvara kasutuselevõttu peab see läbima formaalse kinnitamisprotseduuri. Toote kasutuselevõtu kinnitamise eest vastutab ametiasutuse või ettevõtte juhtkond, kuid nad võivad selle delegeerida ka osakondade juhatajatele või IT-osakonna juhile. Osakond võib asutuse või ettevõtte juhtkonna kehtestatud kinnitamisprotseduuri täiendada omapoolsete piirangutega. Kinnitamata tarkvara kasutamine tuleb keelata (vt M 2.9 Aktsepteerimata riist- ja tarkvara kasutuse keeld). Enne tüüptarkvara kasutamise kinnitamist peab see olema edukalt läbinud vajalikud testid (vt M 2.83 Tüüptarkvara testimine). Kui testide käigus on tüüptarkvaras ilmnenud lubamatuid vigu, nt märgatavaid puudusi turvalisuses, siis ei tohi kasutuse kinnitust väljastada.

Kinnitamisprotseduuri tarbeks on tarvis luua installeerimis- ja konfigureerimiseeskirjad, mille detailsus sõltub sellest, kas vastava installeerimistöö peab tegema süsteemi administraator või kasutaja. Installeerimis- ja konfigureerimiseeskirjad peegeldavad soetamisprotsessi raames läbiviidud testide tulemusi. Juhul kui tootele on lubatud erinevad konfiguratsioonid, tuleb välja tuua erinevate konfiguratsioonide mõju turvalisusele. Eriti oluline on kindlaks määrata, kas toote erinevate funktsioonide ja pääsuõiguste piiranguid kehtestatakse kõikide või ainult mõningate kasutajate suhtes. Vastavate raamtingimuste kehtestamisprotsessi tuleb õigel ajal kaasata töötajate esindus, andmekaitse eest vastutav töötaja ja IT-turbe eest vastutav töötaja.

Tüüptarkvara kinnitamise protseduur peaks toimuma kirjaliku kasutuselevõtu kinnituse abil. Kirjalikus kinnituses peaks kajastuma informatsioon järgmiste punktide kohta:

- programmi nimi ja versiooni number,
- IT-protseduuri nimetus, mille raames hakatakse toodet kasutama,
- kinnitus, et kasutatavad IT-komponendid vastavad valdkonna nõuetele,
- kinnituse väljastamise kuupäev, kinnituse väljastanud isiku allkiri,
- IT turbespetsialisti, andmekaitsespetsialisti, töötajate esinduse kinnitus, et toode on ohutu,
- igapäevatöös kasutamiseks ettenähtud kellaajad,
- loetelu kasutajatest, kelle jaoks on tootele kasutuskinnitus väljastatud,
- installeerimisjuhised, eriti selle kohta, millistele töökohtadele tohib millist konfiguratsiooni installeerida,
- töötajad, kellel on õigus toodet installeerida,
- kellel on juurdepääs installeerimiseks vajalikele andmekandjatele,
- info koolituste kohta, mis tuleb enne toote kasutamist läbida.

Kasutuselevõtu kinnitusest tuleb kõigile osapooltele teada anda ning kinnituse väljastanud allüksusel, IT-osakonnal, spetsialistide osakonnal ja vajaduse korral ka IT-kasutajatel peaks olema selle koopia. Lisaks tuleb organisatoorsete meetmete abil tagada, et toote muutumise korral, eriti kui on tegu versiooni muutumise või täienditega, millel on suur mõju turvafunktsioonidele, väljastataks tootele uus kasutuse kinnitus ning korrataks vajaduse korral ka testimisprotsessi. Nimetatud liiki muudatustest tuleb teavitada toote kasutuselevõtu kinnitamise eest vastutavat töötajat. Lisaks võib kehtestada suunised, mis sätestavad, milliseid tüüptarkvara

tooteid tohib olenevalt kasutusvaldkonnast ja kasutuse otstarbest kinnitada. Kinnitamine eeldab, et tooted peavad olema vähemalt arvutiviiruste suhtes üle kontrollitud, litsentsides ei tohi olla küsitavusi ning need peavad olema registreeritud.

Mõned näited:

- testimisotstarbel rakendatavad demo-versioonid, mida kasutatakse spetsiaalsetel arvutitel,
- avalik tarkvara, mis installeeritakse spetsiaalsetele serveritele,
- mänguprogrammid spetsiaalsetele arvutitele, mis seatakse üles puhkeruumidesse.

Täiendavad kontrollküsimused:

- Kus toimub kasutuselevõtu kinnituste haldamine ja kus neid hoitakse?
- Kas toodetel on olemas installeerimisjuhendid?
- Kas on tagatud, et kogu kasutatav tarkvara läbib kasutuselevõtu kinnitamise protseduuri?

M 2.86 Tarkvara tervikluse tagamine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtorgan

Rakendamise eest vastutavad: IT-juht

Kasutuselevõtu kinnituse saanud tüüptarkvara puhul tuleb tagada, et see installeeritaks ilma muudatusteta. Eesmärk on ära hoida soovitud ja soovimatute muudatuste tegemine, mis võib olla põhjustatud nt arvutiviirustest, tehniliste vigade tõttu esinevatest bitivigadest või konfiguratsioonifailide manipuleerimisest. Seetõttu tohib installeerimisel kasutada ainult originaal-andmekandjaid või originaalandmekandjate nummerdatud koopiaid. Lokaalse installeerimise ja andmekandjate kasutamise alternatiivina võib installeerimist läbi viia ka kohtvõrgu abil, kasutades selle jaoks vastava kasutusloaga versiooni. Siinjuures peab olema tagatud, et sellele pääsevad ligi ainult volitatud isikud. Kui andmehulgad seda võimaldavad (nt CD-ROM-id), tuleks originaalandmekandjatest varukoopiad. Andmekandjate originaale ja varukoopiaid tuleb hoida kohas, kus need on kaitstud volitamata isikute juurdepääsu eest (vt M 6.21 Kasutatava tarkvara varukoopia). Varukoopiad tuleb nummerdada ja kanda inventari loeteludesse. Koopiad, mida rohkem ei vajata, tuleb kustutada. Enne installeerimist tuleb läbi viia viirusetõrje. Andmekandjate originaalide või testimise käigus installeeritud kontrollversiooni abil võib luua kontrollsumma (vt M 4.34z Krüpteerimise, kontrollsummade ja digitaalallkirjade rakendamine), mida saab kasutada enne installeerimist andmekandjatele või kohtvõrku salvestud versioonide tervikluse või läbiviidud installeerimise korrektsuse kontrollimiseks. Lisaks eelnevale võib installeeritud programme volitamata muudatuste eest kaitsta ka seeläbi, et kasutuselevõtu kinnituse saanud konfiguratsioon varustatakse kontrollsummadega. Sellisel moel on võimalik tuvastada ka nakatumisi seni veel tundmatutesse arvutiviirustesse. Lisaks on niimoodi võimalik tuvastada, kas arvutiviirusega nakatumine leidis aset enne või pärast installeerimist.

Täiendavad kontrollküsimused:

- Kuidas tagatakse tüüptarkvara terviklus?
- Kas perioodiliselt viiakse läbi ka kontrolle installeeritud tarkvara tervikluse väljaselgitamiseks?
- Kas programmide ja andmete manipuleerimiskatseid suudetakse tuvastada?

M 2.87 Tüüptarkvara installeerimine ja konfigureerimine

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: IT-juht, administraator

Kasutuselevõtu kinnituse saanud tüüptarkvara installeeritakse selleks ettenähtud IT-süsteemidele installeerimisjuhiste kohaselt. Installeerimisjuhend sisaldab lisaks installeeritavate programmide loetelule veel ka konfiguratsiooni parameetreid ning juhiseid sobiva riistvaralise ja tarkvaralise programmikeskkonna loomiseks. Kõrvalekalded installeerimisjuhendi nõuetest tuleb kooskõlastada kasutuse kinnitust väljastava osapoolega. Juhul kui tarkvara peavad installeerima kasutajad ise, peavad nad saama installeerimisjuhendi, mis võimaldaks installeerimisega iseseisvalt hakkama saada. Installeerimisjuhendi arusaadavuse kontrollimiseks tuleks läbi viia vähemalt üks katsetuslik installeerimine ühe väljavalitud tüüpkasutajaga, mis toimub IT-osakonna ja kasutaja koostöös. Kuna tüüptarkvara arendamisel lähtutakse paljudest erinevatest kasutusvaldkondadest, sisaldab see tihti paljusid funktsioone, mis ei ole tavaülesannete täitmiseks vajalikud. Vältimaks võimalikke probleeme ja vigu seoses vastava tarkvara kasutamisega, tuleks installeerida ainult tööülesannete täitmiseks vajalikud funktsioonid. Funktsioonidele, mis võivad põhjustada turvaprobleeme, ei tohi väljastada kasutuselevõtu kinnitust. Andmete täielikud varukoopiad tuleb luua nii enne kui ka pärast tarkvara installeerimist. Enne installeerimist loodud varukoopiat saab kasutada installeerimise käigus tekkivate probleemide lahendamiseks ehk konsolideeritud lähtepunkti taastamiseks. Samuti tuleks teha andmetest pärast õnnestunud installeerimist täielik varukoopia, et hilisemate probleemide korral oleks võimalik süsteemi seisundit taastada, võttes lähtepunktiks edukalt teostatud toote installeerimise. Õnnestunud installeerimise kohta tuleb kasutuselevõtu eest vastutavale osakonnale edastada kirjalik teade. Installeerimisprotsessi käigus võib kasutada ka niinimetatud deltatool tööriistade abi, mis dokumenteerivad kindlaksmääratud ajavahemikus kõik IT-keskkonnas asetleidnud muudatused. Vastav muudatusi kajastav dokumentatsioon on eriti kasulik tarkvara desinstalleerimisel. Uute toodete kasutuselevõtul võib juhtuda, et toote vanema versiooniga loodud andmed tuleb uude üle võtta. Kui testid on näidanud, et andmete ülevõtmisel võib esineda probleeme, tuleb töötajate jaoks luua kas vastavad abimaterjalid või korraldada andmete ülevõtmine tsentraliseeritult, vastava koolituse saanud töötajate abil.

Täiendavad kontrollküsimused:

- Millised eeskirjad on hetkel kehtivad?
- Millised reeglid on kehtestatud installeerimisjuhendist kõrvalekaldumiste kohta?
- Kuidas kontrollitakse installeerimise õnnestumist?

M 2.88 Tüüptarkvara litsentsi- ja versioonihaldus

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtorgan

Rakendamise eest vastutavad: IT-juht, organisatsiooni juht

Kogemustele toetudes võib väita, et ilma sobiva versiooni- ja litsentsikontrollita tekib kiiresti olukord, kus ühe ja sama IT-süsteemi peal või ka mõne allüksuse lõikes hakatakse korraga kasutama erinevaid versioone ning võib juhtuda, et mõnda isegi ilma vastava litsentsita. Kogu tarkvaral, mida kasutatakse institutsiooni kõikides IT-süsteemides, peavad olema kasutuslitsentsid. Sellest nõudest tuleb teavitada kõiki töötajaid ja erinevate IT-süsteemide administraatorid peavad tagama, et töötajad kasutaks ainult sellist tarkvara, mille jaoks olemas kasutuslitsentsid. Selleks peavad nad olema varustatud sobivate, litsentside kontrollimist võimaldavate tööriistadega. Tihti leidub olukordi, kus institutsiooni raames kasutatakse korraga ühe tüüptarkvara erinevaid versioone. Litsentside kontrollimise käigus peab olema võimalik saada ülevaadet kõikide kasutuses olevate versioonide kohta. Sellega on võimalik tagada vanade versioonide asendamine esimesel vajadusel ja kõikide versioonide kustutamine pärast kasutuslitsentside lõppemist.

Lisaks eelnevale tuleb dokumenteerida ka installeeritud tarkvara erinevad konfiguratsioonid. Seeläbi peab olema võimalik luua ülevaadeerinevates IT-süsteemides kasutatavate tüüptarkvaratoodete kehtivatest turvaseadistustest, mis on kehtestatud kasutuselevõtu kinnitusega ning sellest, millised neist on ka reaalselt installeeritud. Näiteks saab vastava dokumentatsiooni abil kiiresti välja selgitada, millistes arvutites on installeeritud toote XYZ makrode programmeerimine ja millistes mitte.

Täiendavad kontrollküsimused:

- Millised eeskirjad on hetkel kehtivad?
- Kas tüüptarkvaratoote puhul kasutatakse korraga selle erinevaid versioone?

M 2.89 Tüüptarkvara deinstalleerimine

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: administraator, IT-juht

Tarkvara desinstalleerimise käigus tuleb kustutada kõik failid, mis olid vajalikud vastava tarkvara käitamiseks IT-süsteemis, samuti kõik sissekanded süsteemikaustades, mis on seotud vastava tootega. Paljude tarkvaratoodete puhul luuakse tootega seotud kaustasid IT-süsteemi erinevatesse kataloogidesse või muudetakse olemasolevate kaustade sisu. Tihti ei informeerita kasutajat ka kõikidest installeerimise käigus asetleidnud IT-süsteemi muudatustest. Täielikuks desinstalleerimiseks on seega väga kasulik, kui installeerimise käigus tehtud süsteemimuudatused fikseeritakse kas käsitsi või spetsiaalseid tööriistu kasutades. Kogemused näitavad, et kui muudatusi kirja ei panda, viiakse desinstalleerimine läbi kas väga algeliselt või jäetakse hoopis tegemata, kartes, et selle käigus võivad olulised failid kaduma minna.

Täiendav kontrollküsimus:

- Kas pärast versiooni vahetumist tehakse pistelisi kontrolle, et välja selgitada, kas vanad versioonid on täielikult desinstalleeritud?

M 2.90 Kohaletoimetuse kontroll

Algatamise eest vastutavad: IT-juht, organisatsiooni juht
Rakendamise eest vastutavad: varustusosakond
Sissetulnud saadetise puhul tuleb olemasolevate dokumentide alusel kontrollida:

- kas keegi on kõnealuse saadetise tellinud,
- kellele on saadetis adresseeritud,
- kas saadetisel on näha transpordikahjustusi,
- kas saadetis on terviklik, nt kas kõik tellitud komponendid on olemas ja kas kõik tootekirjelduse järgi tarnepakendisse kuuluvad komponendid on saadetises olemas.

Saadetise kontrolli tulemused tuleb kanda kauba sissetuleku nimekirja koos järgmiste andmetega:

- toote nimi ja versioon,
- toote liik, nt tekstitöötlus,
- tarnitud kaup, st üksikute komponentide kirjeldus koos tükiarvu ja kujuga (raamat, diskett, CD-ROM, jne),
- saadetise kuupäev,
- saadetise liik,
- kes saadetise vastu võttis,
- hoiukoht ja
- kellele see edasi anti.

Saadetistes olnud tooted tuleb edastada IT-osakonnale, kes peab hakkama tegelema nende funktsioonide testimise ja sellele järgneva formaalse kasutusloa andmise ning installeerimise ja konfigureerimisega. Kui tooteid kasutatakse või tehakse need kättesaadavaks vaid ajutiselt, nt testide läbiviimiseks, tuleb inventari loetellu üles märkida vähemalt toodete seerianumbrid ja muud toote spetsiifikat iseloomustavad tunnused. Kui saadetises olnud tooted on mõeldud püsikasutuseks, tuleb need märgistada selgete ID-tunnustega (nt grupeeritud järjestikuste inventarinumbritega). Seejärel tuleb tooted kanda inventari loetellu.

Muu hulgas peab seal olema kajastatud järgnev informatsioon:

- identifitseerimistunnused,
- hankimise koht, tarne saabumise aeg,
- hoidmine,
- kasutusloa väljastamise kuupäev,
- installeerimise kuupäev ja konfiguratsiooni eripärad ning
- hooldusleping, hooldusvälbad.

Täiendavad kontrollküsimused:

- Millised IT-tooteid sisaldavate saadetistega ümberkäimist reguleerivad eeskirjad on hetkel jõus?

- Kuidas toimitakse, kui avastatakse, et saadetisest on midagi puudu?
- Kas saadetistes on tihti koostisosi puudu?

M 2.95 Sobivate kaitsekappide soetamine

Algatamise eest vastutavad: IT-osakond

Rakendamise eest vastutavad: varustusosakond

Kaitsekapid kaitsevad nendes hoitavaid materjale tulekahju ja soovimatu juurdepääsu eest. Olenevalt taotletavast kaitsest tuleb sobivate kaitsekappide valimisel järgida alljärgnevaid soovitusi:

- Kaitse tule kahjustava mõju eest: Vastavalt standardile EN 1047-1 eristatakse vastavalt kaitsele tule eest andmekaitsekappide kvaliteediklasse S 60 ja S 120.

Nimetatud kvaliteediklassi kuuluvaid kappe kontrollitakse, kas 60 kuni 120 minutilise tulekahju korral jääb kaitstavate andmekandjate temperatuur lubatud piiridesse. Kaitstavate andmekandjate klassifitseerimisel kasutatakse kindlaid tähistusi.

Lühendite tähendused

P	=	Paberdokumendid
D	=	Andmekandjad piirkoormusega on kuni 70°C (nt magnetlindid, filmid)
DIS	=	Andmekandjad piirkoormusega kuni 50°C (nt disketid, magnetlintkassetid koos kõigi teiste andmekandjatega)

- Erinevused klasside vahel seisnevad isoleerimisvõimes, mis DIS-kappidel on kõige kõrgem.
- infosüsteemide etalonturbe jaoks peaks kaitseks tule eest piisama S60 kvaliteediklassiga andmekaitsekappidest. Serverikappidena kasutamiseks pakutakse kliimaseadmega andmekaitsekappe vastavalt standardile EN 1047-1 või andmekaitsekonteinereid vastavalt standardile EN 1047-2.
- Kaitsekappidel, mis on ette nähtud kaitseks tule ja suitsu eest, peaks olema ette nähtud seade, mis tagaks tulekahju korral uste automaatse sulgumise. Sulgumisprotsessi peaks olema võimalik käivitada lokaalselt suitsuanduri ja/või väljastpoolt tulekahjusignaali (kui on olemas) kaudu.

Kaitse volitamata juurdepääsu eest:

- Kaitsekapi kaitsevõimet volitamata juurdepääsu eest mõjutab lisaks kapi mehaanilisele tugevusele ka luku kvaliteediklass. Infosüsteemide etalonturbes on võimalik kasutada seife vastavalt standardile EN 1143-1 või turvakappe vastavalt standardile EN 14450. Turvakapid jäävad vastupidavuse poolest seifidele alla.

- Kui on vajalik kombineerida omavahel juurdepääsukaitse ja tulekaitse, võib kasutada andmekaitsekappe, mis peaksid vastama nii standardi EN 1143-1 kui ka EN 1047-1 nõuetele (nn kaheotstarbelised kapid).

Erinevate kaitsekappide vastupidavuse määramisel on abiks standard VDMA-24990, milles kirjeldatakse lühidalt kaitsekappide turvaomadusi. Kaitsekappide valikul tuleb tähelepanu pöörata ka lubatud laekoormusele montaažikohas. Nimetatud valikukriteeriumide järgi kaitsekappide kaitseväärtuse kindlaksmääramisel tuleb järgmisena kindlaks määrata kapi sisu vastavalt vajadustele. Selleks tuleks enne kaitsekapi soetamist kindlaks määrata, milliseid seadmeid või mis liiki andmekandjaid selles soovitakse säilitada. Vastavalt vajadusele tuleb kindlaks määrata ka kaitsekapi sisekujundus. Hilisem ümberkujundamine on tavaliselt raske, kuna kapi kaitsevõime ja selle spetsiifiline kasutusluba võivad saada kahjustatud.

Edaspidisteks täiendusteks tuleks samuti ruumi planeerida. Serverikappides peaks peale serveri ja klaviatuuri olema ruumi ka monitorile ja teistele perifeeriaseadmetele nagu nt lindidraividele, et administraatori töid saaks teostada kohapeal. Seejuures tuleb arvestada, et valitaks ergonoomiline sisustus, et serveri juures oleks võimalik administraatori töid takistusteta läbi viia. Nii näiteks on soovitav väljatõmmatav alus klaviatuuri jaoks, mis on paigutatud sellisele kõrgusele, et administraator saaks teostada oma töid istudes. Olenevalt kapi kasutusotstarbest võivad vajalikuks osutuda ka kliimaseade ja/või puhvertoiteallikas. Vastavad seadmed tuleks samuti paigutada kappi. Vastasel korral peaks olemas olema vähemalt ventilatsioon. Soovitav on kapi varustamine lokaalse süsteemiga põlengu varajaseks avastamiseks, mis katkestab tulekahju korral seadmete vooluga varustamise (puhvertoiteallika voolu sisenemis- ja väljumiskohas, kui see on olemas). Samasse kappi ei tohiks paigutada varu-andmekandjat ja logiprinterit. Varu-andmekandja saaks serveri kahjustuse korral ka kahjustada. Toimingute logimine serveris aitab samuti kaasa administraatorite tegevuse kontrollile. Niisiis ei ole otstarbekas, võibolla isegi ainsana, võimaldada juurdepääsu logide väljatrükile.

Täiendavad kontrollküsimused:

- Milliseid kaitsefunktsioone peab kapp täitma?
- Kas valitud kapp täidab vastavaid kaitsefunktsioone?
- Millisele nimetatud kvaliteediklassidest kaitsekapp vastab?
- Kas serveri konsool on juurdepääsetav vaid administraatorile?
- Kas kaitsekapp on küllaldaselt dimensioneeritud?
- Kas kapi juures on läbi viidud volitamata muutusi?

M 2.96 Kaitsekappide lukustamine

Algatamise eest vastutavad: IT-osakond

Rakendamise eest vastutavad: kasutaja

Kaitsekapid, mida ei kasutata, peavad olema lukustatud. Kui katkestatakse töö avatud kaitsekapi juures, tuleb ka lühiajalise lahkumise korral ruumist kaitsekapp lukustada. Koodlukkude kasutamisel tuleb koodid igakordselt tühistada.

Täiendav kontrollküsimus:

- Kas aeg-ajalt kontrollitakse, et kaitsekapid, mida ei kasutata, on suletud?

M 2.97 Õige koodlukuprotseduur

Algatamise eest vastutavad: IT-osakond

Rakendamise eest vastutavad: kasutaja

Kui kasutatakse mehaaniliste või elektrooniliste koodlukkudega kaitsekappe, tuleb nende lukkude koodi muuta:

- pärast soetamist,
- kasutaja vahetumisel,
- pärast avamist kasutaja äraolekul,
- kui on kahtlus, et kood on saanud teatavaks volitamata isikule ning
- vähemalt iga 12 kuu möödudes.

Kood ei tohi koosneda kergesti aimatavatest numbritest (nt isikuandmed, aritmeetilised jadad). Kehtivad koodilukkude koodid tuleb üles kirjutada ja turvaliselt deponeerida (vt M 2.22z Paroolide deponeerimine). Tähelepanu tuleb pöörata asjaolule, et deponeerimine samas kaitsekapis on mõttetu. Kui kaitsekapil on lisaks koodilukule veel teine lukk, tuleb mõelda, kas deponeerida kood ja võti koos, mis tagaks hädaolukorras kiirema juurdepääsu, või eraldi, nii et ründaja jaoks oleks juurdepääs raskem.

Täiendavad kontrollküsimused:

- Kas ülalnimetatud sündmuste järgselt vahetatakse luku koodi?
- Millal vahetati viimati luku kood?
- Kas koodilukkude kood deponeeritakse?
- Kuhu ja kuidas see deponeeritakse?
- Kus hoitakse võimalikke olemasolevaid kapi varuvõtmeid?

M 2.105w Kodukeskjaama soetamine

Algatamise eest vastutavad: asutuse/ettevõtte juhtkond

Rakendamise eest vastutavad: asutuse/ettevõtte tehniline töötaja, hanketalitus

Kodukeskjaama või selle seadistamiseks vajalike komponentide (nt tavapärase keskjaama seadistamine VoIP-ile) soetamisel tuleks muu hulgas järgida ka nõudlusanalüüsi ja seadme planeerimise tulemusi. Erinevate funktsioonide ja nende võimalike rakenduste arv teeb kodukeskjaama väljavalimise suhteliselt keerukaks ja aeganõudvaks. Soetamisel tuleks silmas pidada ka ettevõtte olemasolevaid kommunikatsioonisüsteeme ja -komponente. Kui ei ole plaanis soetada täiesti uut keskjaama, tuleks jälgida, et uued ja vanad osad oleksid omavahel ühildatavad. Uue keskjaama soetamisel tuleks jälgida, et selle hilisem kasutamine ei nõuaks väga palju inimressursse ega tööd, kuid samas oleks kindlustatud selle turvalisus. Esmajoones tuleks jälgida, et keskjaamal oleksid:

- vajalikud funktsioonid selle haldamiseks,
- piisavalt logimehhanisme ja analüüsivõimalusi;
- revisjonide läbiviimise võimalus.

Tavapärase kodukeskjaama soetamisel tuleks selgeks teha, kas sel peaks olema lisaks digitaalsele ka analoogühenduse võimalus. Analoogühendusi on vaja analoogsete lõppseadmete kasutamisel, nagu nt faksiaparaadid, automaatvastajad, traadita telefonid, andmekasutusmodemid, signalisatsiooniseadmed või helistamine hädaabinumbritele. Olenevalt soovitud rakendustest võib valida analoogsete või digitaalsete seadmete vahel. Hübriidseadme puhul on tavapärast kodukeskjaama täiendatud IP-funktsiooniga ja see võimaldab IP-lõppseadmed keskjaamaga ühendada. Lisaks kodukeskjaamale tuleb soetada ka tavapärased või IP-funktsiooniga lõppseadmed. Kui lõppseadmena kasutatakse arvutit, peavad sel olema võrguliidesed, telefonitarkvara, helikaart, mikrofon ja soovitavalt ka vabakäesüsteem. VoIP-il põhineva lahenduse puhul tuleb silmas pidada järgmisi elemente: VoIP-keskjaama, VoIP-telefone, tarkvaratelefone, VoIP-serveritarkvara ja muid võrguelemente. Neile lisanduvad veel ka traadita lahenduste ja lisaväärtusteenuste integreerimine, nagu nt unified communications, mille hulka kuuluvad CTI (arvuti- ja telefonitehnika integratsioon), unified messaging ja kõnepostid, aga ka vahenduskoht või arveldussüsteemid.

M 2.107 ISDN-liideste konfiguratsiooni dokumenteerimine

Dokumentatsioon peab sisaldama vähemalt järgmist infot:

1. Tüüp ja sarjanumber
2. Helistusnumbrid sidelülide loomiseks ja autentimiseks
3. Kasutatav D-kanali protokoll (1TR6, EDSS-1. . . .)
4. Kasutatav B-kanali protokoll (X.25, PPP, TCP/IP, bitt-transparentne,..),
5. Kasutatav CAPI versioon
6. Kasutatav draiveri tarkvara versioon
7. Kasutatav andmetihenduse tüüp
8. Autentimise tüüp (nt PAP/CHAP)

M 2.109 Kaugpääsuõiguste määramine

Algatamise eest vastutavad: IT-juht, infoturbespetsialist

Rakendamise eest vastutab: administraator

Väline juurdepääs ametiasutuse või ettevõtte võrgule peab olema piisavalt piiratud, s.t vastama töötajale antud õigustele. Meetmes M 2.8 IT-rakendustele ja andmetele pääsuõiguste andmine kirjeldatud nõuete kõrval peab arvestama ka sellega, et kaugpääsuõiguste andmisele tuleb kehtestada tavapärasest suuremad piirangud.

Näiteks pole kaugtöökohale ilmtingimata alati tarvis anda pääsuõigusi, mis tagavad juurdepääsu tarkvara sisaldavatele kataloogidele.

Kaugpöördumise kasutamise volitusi tuleb regulaarselt kontrollida, et veenduda nende vajalikkuses ja ajakohasuses.

Kontrollküsimused

- Kas kaugjuurdepääs sisevõrgule on piisavalt piiratud?

M 2.110 Andmeprivaatsuse suunised logimisprotseduurides

Algatamise eest vastutavad: IT-juht, andmekaitse eest vastutav töötaja

Rakendamise eest vastutavad: administraator, andmekaitse eest vastutav töötaja

IT-süsteemide kasutamisel tuleb andmekaitsealases mõttes logimisprotseduuride all mõista manuaalsete ja automatiseeritud salvestuste loomist, mille põhjal on võimalik vastata alljärgnevatele küsimustele:

- Kes, millal ja milliste vahenditega midagi põhjustas või mingeid andmeid kasutas?

Lisaks sellele peab olema võimalik teha järeldusi süsteemi seisukorra kohta:

- Kellel olid mingil perioodil millised pääsuõigused?

Logimisprotseduuride liigid ja ulatus sõltuvad üldisest andmekaitseõigusest ning ka valdkonnaspetsiifilistest reeglitest. Haldustoimingute logimine vastab süsteemi monitooringule, samal ajal kui kasutaja toimingute logimine aitab oluliselt kaasa protseduuride monitooringule. Selle alusel on võimalik leida nõudeid süsteemile orienteeritud logimise viisile ja ulatusele enamasti andmekaitseseadusest, samal ajal kui protseduuridele orienteeritud logimist määratletakse tihti valdkonnaspetsiifiliste reeglitega. Näidetena protseduuridele orienteeritud logimise kohta võib muu hulgas välja tuua registreerimisseadused, politseiseadused ja põhiseaduse kaitseseadused.

Minimaalsed nõuded logimisprotseduuridele

IT-süsteemide haldamisel tuleb täielikult logida alljärgnevad toimingud:

- Süsteemi genereerimine ja süsteemi parameetrite muutmine. Kuna nimetatud tasandil ei toodeta reeglina süsteemi juhitud logifaile, on selleks vaja vastavaid detailseid käsitsi tehtud salvestusi, mis peavad olema vastavuses süsteemi dokumentatsiooniga.
- Kasutajate konfigureerimine. Täielikult tuleb logida andmed selle kohta, kellele ja milliseks ajavahemikuks on antud õigus vastava IT-süsteemi kasutamiseks ja kes selle andis. Nimetatud logifailidele tuleks ette näha pikemaajalised säilitusajad, kuna need on praktiliselt iga auditi aluseks.
- Õigusprofiilide koostamine. Kasutajahalduse logimise käigus on väga oluline, et salvestataks, kes on andnud korralduse teatud kasutajaõiguste kehtestamiseks (vt M 2.31 Volitatud kasutajate ja õiguste profiilide dokumenteerimine)
- Rakendustarkvara installeerimine ja muutmine. Logifailid esitavad programmide ja protseduuride kinnitamise tulemust.
- Failikorraldusemuudatused. Arvestades erinevate manipuleerimisvõimalustega, mis ilmnevad juba standard-failihaldussüsteemide kasutamisel, tuleb erilist tähelepanu pöörata täielikule logimisele.
- Andmevarunduse läbiviimine. Kuna sellelaadsed meetmed (varundus, taaste) on seotud koopiate või andmevaramu ülekirjutamisega ja nimetatud toimingud viiakse sageli läbi erandkorras, tekib kõrgendatud vajadus logimiseks.

- Haldusinstrumentide kasutamine. Kõikide haldusinstrumentide kasutamine tuleb protokollida, et oleks võimalik tuvastada, ega volitamata isikud pole pettuse teel omandanud süsteemiadministraatori õiguseid.
- Volitamata sisselogimise katsed ja õiguste rikkumine. Kui lähtutakse efektiivsest autentimise protseduurist ja asjakohasest õiguste kehtestamisest, tuleb pöörata suurt tähelepanu kõikide silmatorkavate kõrvalekallete täielikule protokollimisele sisselogimisel ning riist- ja tarkvarakomponentide kasutamisel. Selles mõttes on kasutaja ka süsteemi administraator.

Isiklike andmete töötlemisel tuleb alljärgnevad kasutajatoimingud olenevalt protseduuride või andmete tundlikkusest täielikult või valikuliselt logida:

- Andmete sisestamine. Niinimetatud sisestuskontroll toimub põhiliselt protseduuri alusel (nt logimine toimikutes, kui need on olemas, logimine otse andmebaasis), kui ei kasutata toimikuid. Kui lähtutakse asjaolust, et võimupiiride ületamise juhtude logimine toimub mujal, peaks täielik andmete sisestamise logimine olema kohustuslik.
- Andmete edastamine. Valikulist logimist võib pidada piisavaks vaid juhul, kui täielikku logimist ei ole seadusega ette nähtud.
- Automatiseeritud käivitusprotseduuride kasutamine. Üldjuhul peaks toimuma käivitusprotseduuride ja nende põhjuste (protseduur, toimiku kohaviit jms) täielik logimine, et oleks võimalik paljastada volitamata isikute juurdepääs kaustadele.
- Andmete kustutamine. Andmete kustutamine tuleb logida.
- Programmide käivitamine. See on vajalik vaid eriti tundlike programmide korral, mida tohib kasutada näiteks ainult kindlatel aegadel või teatud olukordades. Logimine on vajalik ka volitatud kasutajate töökoormuse vähendamiseks (ainult programmide volitatud käivitamise tõestuseks).

Logiandmete sihtotstarbeline kasutamine

Logiandmeid tohib kasutada vaid otstarbel, mille alusel need salvestati, näiteks turvakontseptsioonis kindlaks määratud üldine kontroll, enamikes andmekaitseseadustes nõutud „monitooring isikuandmete töötlemiseks kasutatavate andmetöötlusprogrammide nõuetele vastava kasutamise üle” ning kontroll oma asutuse ja väliste andmekaitse eest vastutavate töötajate poolt. Vaid erandjuhtudel lubavad valdkonnaspetsiifilised eeskirjad nende andmete kasutamist mõnel muul otstarbel, näiteks kriminaaljälitustegevuses.

Säilitusaeg

Logifailide säilitamisaja aluseks võetakse valdkonnaspetsiifilised eeskirjad, näiteks:

- tõenäolisus, et ilmsiks võivad tulla kõrvalekalded ning
- võimalus kõrvalekallete põhjuste paljastamiseks logide ja teiste dokumentide abil.

Kogemuste kohaselt ei tohiks ületada üheaastast tähtaega. Juhul kui logifailid luuakse sihtkontrolli eesmärgil, peab rakendama lühemaid salvestusaegu. Reeglina jätkub nende säilitamisest tegeliku kontrollini. Ka siinkohal tuleb järgida valdkonnaspetsiifilisi eeskirju.

Tehnilised ja organisatsioonilised raamtingimused

Logitegevuse efektiivsus ja selle kasutamine kontrolli läbiviimise käigus sõltub suurel määral tehnilistest ja organisatsioonilistest raamtingimustest.

Seetõttu tuleb tähelepanu pöörata alljärgnevatele aspektidele:

- Logimise eesmärk, logiandmete kontrollimine ning töötajate ja muude logimisest puudutatud isikute kaitseks võetavad meetmed peavad olema eraldi kontseptsioonina selgelt määratletud ja sõnastatud (vt ka B 5.22 Logimine).
- Logimisprotseduuride puhul tuleb ühelt poolt tagada nende kohustuslik ja täiemahuline teostus ning teisalt ka logiandmete piisav kaitse kõikvõimalike manipulatsioonide eest.
- Olenevalt andmete kogumise otstarbest tuleb andmehulkade suhtes rakendada tugevaid juurdepääsupiiranguid.
- Logide struktuur peab võimaldama neid efektiivselt kontrollida. Selle hulka kuulub ka logide analüüsimine asjakohaste IT-lahendustega.
- Logide analüüsimisvõimalused peavad olema kooskõlastatud ja kindlaks määratud.
- Kontrolle tuleks teha ilma viivitusteta, et rikkumiste tuvastamisel oleks võimalik kahjusid ka ennetada ja vigadest õppida. Kontrolle tuleb teha õigel ajal enne logiandmete säilitamiskohustuse aegumist.
- Kontrollimisel tuleks rakendada kahemehereeglit.
- Töötajaid tuleb teavitada, et institutsioonis tehakse vastavaid kontrolle, mis võivad toimuda ka ilma ette teatamata.
- Rutiinsete kontrollide tegemiseks tuleks kasutada automaatprotsesse, nt valvekoeri (watch dogs).
- Logimiskontseptsiooni väljatöötamisse ja logidele kehtestatavate analüüsimisnõuete määratlemise protsessi tuleb kaasata ka töötajate esindus.

Kontrollküsimused

- Kas institutsioonil on olemas eraldi kontseptsioon, milles kirjeldatakse logimist, logide analüüsimist ning töötajate ja muude puudutatud isikute kaitseks võetavaid meetmeid?
- Kas logiandmete puhul järgitakse nende kogumise ostarvet, eriti mis puudutab juurdepääsukaitset?
- Kas logide struktuur võimaldab neid efektiivselt analüüsida?
- Kas logide analüüsimise nõuded on kooskõlastatud andmekaitsespetsialisti ja töötajate esindusega?

M 2.111 Juhendite käepärast hoidmine

Algatamise eest vastutavad: IT-juht, IT-osakond

Algatamise eest vastutavad: IT-juht, IT-osakond

Informatsioonitehnika soetamisel, ükskõik, kas tegu on riist- või tarkvaraga, tuleb soetada piisavas koguses ka selle juurde kuuluvaid juhendeid ja tehnilisi infolehti.

Järjest enam tuleb ette olukordi, kus IT-toodete tarnemahu hulka ei kuulu täiendatavat dokumentatsiooni ja lisaks võrgupõhisele abile tarnitakse koos toodetega vaid installeerimisjuhendid ja sissejuhatavad tekstid. Piiratud mahus abidokumentatsioonist ei piisa eriti just tõrgete tekkimisel. Seepärast tuleb pöörata tähelepanu sellele, et soetataks lisaks ka vajalikud juhendid, tehnilised infomaterjalid ja tõrgete kataloogid. Seejuures ei pea piirduma vaid tootja pakutava kirjandusega. Kõik IT-toote juurde kuuluvad juhendid peavad olema alati käepärast toote kasutuskohas. Näiteks tuleb serveri operatsioonisüsteemi juhendeid hoida serveri vahetus läheduses, mitte aga näiteks suletud raamatukogus. Avariiprotseduuride planeerimisel tuleb planeerida juurdepääs nimetatud kirjandusele.

Täiendavad kontrollküsimused:

- Millised juhendid kuuluvad kasutatavate IT-toodete juurde?
- Kus neid juhendeid hoitakse? Kas need on kogu aeg käepärast?

M 2.112 Kodutööjaamade ja asutuse vahelise dokumentide ja andmekandjate transportimise reguleerimine

Algatamise eest vastutavad: IT-osakond, IT-juht

Rakendamise eest vastutavad: töötajad

Et dokumentide ja andmekandjate transport kodutööjaamade ja asutuse vahel võiks kulgeda turvaliselt, tuleb koostada selle toimumise viisi reguleerivad eeskirjad. **Selles peaks olema vaatluse alla võetud või reguleeritud vähemalt alljärgnevad aspektid:**

Milliste dokumentide/andmekandjate edastamiseks tohib kasutada millist edastusviisi (posti-, kulleri-, pakiteenuse kasutamine, vt M 5.23 Andmekandjate sobivate edastusviiside valimine).Milliseid turvameetmeid tuleb transportimisel järgida.

Näiteks:

- suletud mahuti,
- transpordikott,
- tähtkiri,
- väärtkiri,
- kaaskiri ning pitseerimine
- milliseid dokumente/andmekandjaid võib ainult isiklikult transportida.

Kuna ametlikud paberid, dokumendid ja toimikud on tihti ainueksemplarid, tuleb sobiva edastamisviisi valimisel arvestada asjaoluga, millist kahju tekitaks nende kaotus. Selle vältimiseks võib andmete edastamisele eelneda nende varundamine.

Täiendav kontrollküsimus:

- Kas vastavaid töötajaid on informeeritud, kuidas peab toimuma dokumentide ja andmekandjate transportimine?

M 2.113 Kaugtöö reeglid

Algatamise eest vastutavad: asutuse/ettevõtte juhatus, personalijuht

Rakendamise eest vastutavad: personaliosakond, juhataja

Mõningaid aspekte selgitades tuleks võtta aluseks tariifilepingud, kollektiivlepingud või lisaks töölepingut puudutavad individuaalsed kokkulepped kaugtöötaja ja tööandja vahel. Selles tuleks selgitada, täpsemalt öeldes reguleerida muu hulgas alljärgnevad aspektid: “Kaugtöö tegemine vabatahtlikkuse alusel”, “Ületunnitöö ja lisatasud”, “Transpordikulud sõiduks asutuse ja kodu vahel”, “Kulutused nt elektrivoolule ja küttele”, “Vastutus (IT-seadmete varguse või kahjustamise, aga ka tööõnnetuse või kutsehaigusesse haigestumise korral)” ning “Kaugtöölepingu lõpetamine”.

Infoturbe seisukohalt tuleks lisaks tähelepanu pöörata alljärgnevatele aspektidele:

- Tööaja reguleerimine: Tööaja jaotamine tegevustele asutuses ja kodutöökohas peab olema reguleeritud, samuti peavad olema kindlaks määratud kindlad ajad töötaja kättesaamiseks kodutöökohas.
- Reageerimisajad: Peaks olema reguleeritud, millise perioodi järel peaks toimuma aktuaalse informatsiooni hankimine (nt kui tihti tuleks lugeda meile ning kui kiiresti tuleks neile reageerida.
- Töövahendid: Võib kindlaks määrata, milliseid töövahendeid kaugtöötaja kasutada tohib ning milliseid mitte (nt mitte aktsepteeritud tarkvara). Näiteks võib olla lubatud meiliühendus, kuid teiste Internetiteenuste kasutamine aga keelatud. Lisaks sellele võib olla keelatud diskettide kasutamine (arvutiviiruste oht), kui kaugtöötaja seda just ei nõua.
- Andmevarundus: Kaugtöötajat tuleb kohustada regulaarseks andmevarunduse läbiviimiseks. Lisaks sellele tuleks kokku leppida, et üks andmete varukoopia jääks asutusse hoiule, et tagada andmete käideldavus.
- Infoturbemeetmed: Kaugtöötajat tuleb kohustada järgima kaugtööks vajalikke infoturbe meetmeid ning neid rakendama. Rakendatavad infoturbe meetmed tuleb kaugtöötajale edastada kirjalikult.
- Andmekaitse: Kaugtöötaja on kohustatud kinni pidama vastavasisulistest andmekaitse eeskirjadest ning vajalikest meetmetest isikuandmete töötlemisel kodutöökohas.
- Andmeside: Tuleb kindlaks määrata, milliseid andmeid millisel viisil tohib edastada, täpsemalt öeldes, milliseid andmeid ei tohi elektrooniliselt edastada või milliseid tohib elektrooniliselt edastada, kuid ainult krüpteeritult.
- Dokumentide transport: Reguleerida tuleb dokumentide transpordi viis ja turvalisuse tagamine kodutöökoha ja asutuse vahel.
- Teatamisprotseduurid: Kaugtöötaja on kohustatud infoturbe seisukohalt tähtsatest juhtumitest koheselt teatama asutuses kindlaks määratud kohta.
- Kodutööjaama pääsuõigused: Kontrolli teostamiseks ning dokumentide ja andmete käideldavuse tagamiseks töötaja asendamisel võib anda kodutöökohale (või eelneva teatamise korral) lihtsustatud pääsuõiguse.

Täiendavad kontrollküsimused:

- Kas kaugtöötaja on teadlik oma tegevuse suhtes kokkulepitud piiridest?
- Kas kaugtöötaja saab sellekohase infolehe?
- Kas kaugtöötajale antakse infoleht, milles on üksikasjaliselt lahti seletatud infoturbe meetmed, mida ta on kohustatud täitma? Millal infolehte viimati uuendati?

M 2.114 Infovool kaugtöötaja ja asutuse vahel

Algatamise eest vastutavad: ülemus, kaugtöötaja

Rakendamise eest vastutavad: ülemus, kaugtöötaja

Et kaugtöötaja oleks ettevõttes toimuvaga kursis, peaks ülemus võimaldama regulaarset infovahetust kaugtöötaja ja kolleegide vahel. See on vajalik hoidmaks kaugtöötajat kursis ka tulevikus tema töölõiku puudutavate plaanide ja sihtidega, et vältida frustratsiooni ning luua ja säilitada positiivset kaugtöökliimat. Reguleerimist vajab kaugtöötajate kursishoidmine asutusesiseste kirjalikult teatavaks tehtavate otsustega, nii et teated, asjakohane info ja ajakirjad jõuaks ka kaugtöötajateni See on probleemiks, kui kaugtöötaja töötab eranditult kodus. Üheks lahenduseks oleks ehk tähtsate dokumentide sisseskaneerimine, et neid kaugtöötajale meili teel saata. Lisaks sellele tuleb kaugtöötajaid kursis hoida muutustega infoturbe meetmete osas. Kolleege tuleks informeerida aegadest, mil kaugtöötaja on kohal või kättesaadav ning teha neile teatavaks kaugtöötaja meiliaadress või telefoninumber.

Lisaks sellele tuleb kaugtöö korral selgeks teha alljärgnevad aspektid:

- Kes on kontaktisikuks kaugtöö tegemisel tekkivate tehniliste ja/või organisatsiooniliste probleemide korral?
- Keda tuleb teavitada turvaprobleemidest?
- Kuidas toimub ülesannete jaotamine?
- Kuidas toimub töötulemuste edastamine?

Tehnilis-organisatsiooniliste probleemide esinemisel peab kaugtöötaja nendest viivitamata asutusele teatama.

Täiendavad kontrollküsimused:

- Kuidas jõuab kaugtöötajani tööalane informatsioon?
- Keda teavitab kaugtöötaja turvaprobleemidest?
- Kas kaugtöötajate jaoks on olemas kontaktisik (ülemusest sõltumatu).

M 2.115 Kodutööjaama hooldus

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: IT-juht, administraator, kaugtöötaja

Kaugtööjaama teeninduseks ja hoolduseks tuleb koostada spetsiaalne kontseptsioon, mis hõlmab alljärgnevaid aspekte:

- Kontaktisikute nimetamine kasutajate nõustamiseks probleemide korral: käesolevate isikute poole pöördub kaugtöötaja tark- ja riistvaraga seotud probleemide korral. Kasutajate nõustamiskeskuse loomise eesmärgiks on pakkuda ajutist abi (ka telefoni teel), see tähendab juhatada sisse hooldus- ja parandustööd.
- Hooldustööde teostamise tähtajad: Kohapeal läbiviidavate hooldustööde tähtajad peaksid olema varakult teada, et kodutöötajad saaksid selleks ajaks tagada juurdepääsu kodutööjaamale.
- Standardarvutite kasutamine kodutööjaamades: Ühe ettevõtte kõik kaugtöötajad peaksid kasutama standardarvutit, et teha kasutajate nõustamiskeskusele probleemide lahendamine kergemaks. See vähendab ka turvalise kaugtööjaama installeerimiseks tehtavaid kontseptuaalseid ja administratiivseid kulutusi.
- Kaughooldus: Kui kaugtööarvuti haldamine ja hooldus on võimalik kaughoolduse teel, tuleb leppida kokku vajalikes turvameetmetes ning nõutavates online -aegades. Erilist tähtsust omab turvaprotseduuride kindlaksmääramine, et vältida kaughooldeportide väärkasutust (M 5.33 Kaughoolduse turve).
- IT-seadmete transport: Vastutuse seisukohalt on tähtis kindlaks määrata, kes on volitatud transportima IT-seadmeid ettevõtte ja kodutööjaama vahel. Teisi aspekte puudutavad eeskirjad on ära toodud M 2.4 Hooldus- ja remonditööde reeglid .

Täiendavad kontrollküsimused:

- Kas kaugtöötaja on teadlik, kelle poole pöörduda tark- ja riistvaraga seotud probleemide korral?
- Kas kasutajate nõustamiskeskuses ollakse tuttav standardkodutöökohaarvuti konfiguratsiooniga?
- Kas kasutajate nõustamiskeskusele on teada kaugtöötaja aadress, et oleks võimalik pakkuda kohapeal kiiret abi?

M 2.116 Sidevahendite kasutamise reguleerimine

Algatamise eest vastutavad: infoturbe osakond

Rakendamise eest vastutavad: administraator, kaugtöötaja

Kaugtööarvuti on põhimõtteliselt varustatud elektrooniliste sidevahenditega. Infoturbe seisukohalt tuleb kokku leppida nõuetes olevate sidevahendite kasutamiseks. Põhimõtteliselt peaks olema keelatud sidevahendite kasutamine isiklikuks otstarbeks. **Selgitamist nõuavad vähemalt alljärgnevad aspektid:**

Andmevoogude kontroll

- Milliseid teenuseid tohib kasutada andmete edastamiseks?
- Milliseid teenuseid ei tohi mitte mingil juhul kasutada?
- Millist informatsiooni ja kellele tohib edastada?
- Millist kirjavahetust tohib meili teel pidada?
- Kui kaugtööarvutil on faksimodem või kui kaugtööjaamas on olemas faksiaparaat, tuleb selgeks teha, millist informatsiooni ja kellele tohib faksi teel edastada.
- Millise informatsiooni elektrooniliseks edastamiseks on vajalik ettevõtte eelnev nõusolek?

Informatsiooni hankimine

- Milliseid elektroonilisi teenuseid (andmebaasipäringud, elektroonilised otsingud) tohib kaugtööarvutil kasutada? Näiteks saab tehtud päringute laadi järgi teatud juhtudel teha järeldusi ettevõtte strateegia kohta.
- Milline eelarve on ette nähtud elektrooniliste teenuste kasutamiseks?

Infoturbe meetmed

- Milliste andmete kaitseks milliseid krüpteerimismeetodeid peaks kasutama?
- Milliste andmete edukalt toimunud edastamisele peab järgnema nende kustutamine? See võib kehtida näiteks isikuandmete kohta.
- Millistest andmetest peab vaatamata nende edukalt toimunud edastamisele jääma koopia kaugtööarvutile?
- Kas enne andmete edastamist või pärast saamist viiakse läbi kontroll arvutiviiruste suhtes?
- Milliste andmete edastamisel peab toimuma logimine? Kui automaatne logimine ei ole võimalik, tuleb kindlaks määrata, kas ja millisel määral on ette nähtud käsitsi logimine.

Interneti kasutamine

- Kas Internetiteenuste kasutamine on põhimõtteliselt keelatud?
- Millist liiki andmeid tohib Internetist alla laadida? Andmete laadimine võõrastelt serveritelt kätkeb endas arvutiviiruste ohtu.
- Milliseid Internetibrauseri funktsioone on lubatud aktiveerida?

- Millised Internetibrauseri turvafunktsioonid tuleb aktiveerida?
- Kas on vajalik asutuse nõusolek, kui kaugtöötaja tahab osaleda informatsiooni vahetamises uudisegruppide kaudu? Teatud olukordades on nõutav anonüümne kasutamine.

Allkirjastamise eeskirjad

- Kas side pidamiseks on ette nähtud allkirjastamise eeskirjad?
- Kas kasutatakse seadusele vastavaid digitaalallkirju?
- Kas kirjavahetusel kasutatakse teisi autentimismeetodeid?

Täiendavad kontrollküsimused:

- Kas kaugtöötaja on teadlik sidepidamisvahendite kasutamise reeglitest?
- Kas kaugtöötaja kinnitab instrueerimise sidevahendite kasutamise kohta oma allkirjaga?

M 2.117 Kaugtöötajate pääsu reguleerimine

Algatamise eest vastutavad: infoturbe osakond, IT-juht

Rakendamise eest vastutavad: administraator, ülemus

Kui kaugtöö teostamiseks on vajalik juurdepääs ettevõtte IT-süsteemile (näiteks serverile), tuleb eelnevalt kindlaks määrata, milliseid objekte (andmed, IT) kaugtöötaja tõepoolest oma tööülesannete täitmiseks vajab. Vastavalt sellele tuleb kehtestada vajalikud lugemis- ja kirjutusõigused nende objektide suhtes. Objektidele, mida kaugtöötaja oma tööülesannete täitmisel ei vaja, ei tohiks tal ka juurdepääsu olla. Öeldu kehtib nii andmete kui ka ettevõtte käsutuses oleva IT kohta. See on vajalik võimaliku häkkerite ründe tõttu sidearvutile tekitatava kahju minimeerimiseks. Pääsuõiguste andmisel tuleb järgida M 2.7 Süsteemi ja võrgu pääsuõiguste andmine ja M 2.8 IT-rakendustele ja andmetele pääsuõiguste andmine .

Täiendavad kontrollküsimused:

- Kas administraator on teadlik, millistele objektidele tohib kaugtöötaja omada juurdepääsu?
- Millised eeldused peavad olema täidetud enne pääsuõiguste andmist või muutmist?
- Kas serveri haldamine tagab kaugtöötaja juurdepääsu vaid lubatud objektidele?

M 2.122z Meiliaadresside standard

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator, kasutaja

Meiliaadresside skeemi kindlaksmääramine

Meiliaadressid tuleb määrata kindlate tavade alusel. Oluline on, et meiliaadressis ei kasutataks mitte -ASCII-märke nagu täpitähed. Rünnakute raskendamiseks, rämpsposti ja reklaammeilide vältimiseks ning võimalikult vähese teabe väljapoole saatmiseks võib olla mõttekas võtta kasutaja ja organisatsiooniga seoses kasutusele raskemini äraarvatavad meiliaadressid, mis asendaksid selliseid aadresse nagu perekonnanimi@organisatsioon.ee. See muudab aga aadresside edastamise ebamugavamaks ja võib tekitada suhtlemisraskusi. Meiliaadressi muutmise või tühistamise puhul tuleb jälgida, et vähemalt üleminekuaja jooksul suunataks veel neile aadressidele suunatud meilid uutele aadressidele edasi.

Funktsioonipõhiste meiliaadresside sisseseadmine

Paljudes olukordades toimub äritegevus täielikult või osaliselt meilitsi, kusjuures oluline on, et sõnumid õigeks ajaks adressaadini jõuaksid. Puhkuste, komandeeringute, haiguse või muude isiklike põhjuste tõttu võivad aga meilitöötluse eest vastutada erinevad isikud. Seetõttu tuleb isikutest sõltumatu organisatsioonilise ühtsuse tagamiseks seada teatud funktsioonide jaoks sisse organisatsiooni- või funktsioonipõhised meiliaadressid. Selline lähenemine on eriti oluline kesksete teenuste puhul ning selle eelised on allpool välja toodud:

- Funktsioonipõhiste aadressidega meilid saab vajadusel suunata otse asendajale , tagades sujuva töötluse ka kontaktisiku äraolekul. Kui funktsioonipõhistele aadressidele suunatud meilid suunatakse mitte otse vastavatele kontaktisikute le, vaid eraldi postkasti, annab see eelise ka andmekaitse seisukohast, sest sel juhul ei ole tegeliku saaja ootamatu äraoleku puhul (näiteks õnnetuse või haiguse tõttu) vaja tema isiklikku postkasti avadagi.
- Vastutuse muutumise korral pole vaja kõiki suhtluspartnereid informeerida. K õik funktsioonipõhistele aadressidele saadetud meilid suunatakse lihtsalt edasi uutele kontaktisikutele.
- F unktioonipõhistel meiliaadressidel võivad olla ilmekad nimetused nagu nouanne@. . . , veebihaldur@. . . , turundus@. . . ja nad on sageli paremini märgatavad kui isikuga seotud aadressid .
- Funktsiooniga seotud meiliaadressile saabunud kirja puhul saavad vastuvõtjad ka teemast (Subject) olenemata kindlaks teha, millest meilis juttu võib olla.
- Mitmesuguste funktsioonide puhul, mis on seotud otse internetidomeeni kasutamisega, soovitatakse tungivalt asjaomaste de-facto -standardite (IETF RFC, siin konkreetselt RFC 822 ja RFC 2142) puhul võtta täiendavalt kasutusele teatud funktsiooniga seotud meiliaadresse (näiteks postmaster) (vt M 2.256 Infoturbe planeerimine ja käigushoidmine väljasttellimise tegevuste ajal).

Organisatsiooni- ja funktsioonipõhise meili puhul tuleb dokumenteerida, millised organisatsiooni ja funktsiooniga seotud aadressid on olemas ja millist eesmärki nad teenivad.

Täiendavad kontrollküsimused :

- Kas asutuse meiliaadresside puhul on välja töötatud selged nimetamistavad ?
- Kas kõigi organisatsiooni ja funktsiooniga seotud meiliaadresside puhul on olemas esinduseeskirjad ?

M 2.123z Rühmatarkvara või meiliteenuse pakkuja valimine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: IT-juht

Enne rühmatarkvara või meiliteenuse pakkuja valimist tuleb endale selgeks teha pakkuja eeskirjadest tulenev vastutus, näiteks kas ja kui kaua protsesse ja suhtlusandmeid arhiveeritakse, kas vastuvõtmisel või saatmisel on meili suurus piiratud, kas meile filtreeritakse ja kui, siis milliste reeglite järgi. Kui asutused tahavad oma süsteemide ülesehitamisest ja hooldamisest loobuda või süsteeme paindlikumaks muuta, kasutavad nad rühmatarkvara või meiliteenuse pakkujate teenuseid. Lisaks rühmatarkvarateenuste täielikule sisseostmisele on meeskonnatöö hõlbustamiseks või reisil viibides võimalik kasutada ka internetis pakutavaid üksikteenuseid nagu veebimeiliteenused ja rühmakalendrid . Paljud töötajad kasutavad neid teenuseid ka isiklikel eesmärkidel, mistõttu tuleb endale selgeks teha, et teenistuslikult võib kasutada ainult asutuses lubatud väliseid rühmatarkvarateenuseid . Üldiselt peab kõigi töötajate puhul olema selgelt reguleeritud, millele väliste rühmatarkvarateenuste kasutamisel tähelepanu pöörata .

Asutuses tuleb välja selgitada, milliseid turvamehhanisme rühmatarkvara või meiliteenuse pakkuja puhul rakendatakse ja kas sellega täidetakse sisemisi turbenõudeid. Turbespetsialistid peavad veenduma, et rühmatarkvara või meiliteenuse pakkujate puhul töötab nende server turvaliselt, nii et M 5.56 Meiliserveri turvaline kasutamine kirjeldatud nõuded oleksid täidetud. Teenusepakkujate juures salvestatakse arveldamise huvides kasutajaandmed (nimi, aadress, kasutajatunnus, pangaandmed) ja kontaktandmeid ning olenevalt teenusepakkujast lühemaks või pikemaks ajaks ka edastatav sisu. Kasutajad peavad rühmatarkvara või meiliteenuse pakkuja käest välja uurima , milliseid andmeid ja kui kauaks salvestatakse. Meilide puhul saavad kasutajad krüpteerimise abil teenusepakkujat takistada, nii et viimane ei saa ülekantavat info lugeda. Teiste rühmatarkvarateenuste puhul nagu aadressiraamatud või kalendrid pole see enamasti võimalik, mistõttu kasutajad peaksid enne selliste teenuste kasutuselevõttu välja selgitama, kuidas andmeid volitamata juurdepääsu eest varjata. Suurtel ulatusliku eravõrguga teenusepakkujatel on see e elis, et ainult võrgu piires liikuvad meilid või muu info on manipuleerimise eest rohkem kaitstud kui internetis liikuv teave. Välismaal asuva peakontoriga teenusepakkujate puhul kulgevad ka kõik meilid ja muu info sageli selle riigi kaudu. Seda punkti tuleb silmas pidada. Arvesse tuleb võtta, mitmest lüüsist teave läbi liigub ja kes seda seejuures lugeda võib.

Täiendavad kontrollküsimused:

- Kas on tagatud, et rühmatarkvara- ja meiliteenuse pakkujate puhul on rakendatud kõiki turvamehhanisme?
- Kas kõiki töötajaid on teavitatud, millele pöörata tähelepanu väliste rühmatarkvarateenuste, nt veebimeili puhul?

M 2.124 Sobiva andmebaasitarkvara valimine

Algatamise eest vastutavad: IT-juht, IT-osakond

Algatamise eest vastutavad: IT-osakond, administraator

Uue andmebaasitarkvara soetamisel on võimalik see algusest peale nii välja valida, et selle hilisema kasutamise käigus on võimalik saavutada kõrge turvalisuse tase vaid väikeste lisakulutustega personalile ja organisatoorsele tegevusele. Alustuseks tuleb välja selgitada andmebaasisüsteemi kasutusala ja -otstarve, et oleks võimailik formuleerida nõuded käideldavuse, tervikluse ja konfidentsiaalsuse osas. Lisaks sellele on vaja kvantifitseerida nõuded töödeldavate andmete hulga, töötlemiskiiruse ning jõudluse osas. Nimetatud aspektidest tulenevad omadused, mis peaks soetataval tarkvaral olemas olema, nt käideldavus kindlate riistvaraplatvormide või operatsioonisüsteemide jaoks või vajalike turvamehhanismide hulk. Käesolevas planeerimisfaasis on juba võimalik aru saada, kas ja millisel määral on andmebaasisüsteemi hilisemaks tööks vajalik riistvara uuendamine või täiendamine.

Käideldavusele esitatud nõudeid arvestades tuleb määratleda ka vajaminevad võimalused monitooringu läbiviimiseks, s.t et tuleb kindlaks määrata, millised andmebaasi seisundid millisel kujul peaksid olema kindlaks määratavad (nt logimise kaudu ühes failis), samuti vastutavate isikute või isikugruppide teavitamine andmebaasi kriitilisest seisundist (nt sõnum konsoolile).

Andmebaasitarkvara soetamisel tuleks erilist tähelepanu pöörata alljärgnevatele aspektidele:

- Andmebaasitarkvara peab olema varustatud sobiva mehhanismiga kasutajate identifitseerimiseks ja autentimiseks (vt M 2.128 Andmebaasisüsteemi pääsu reguleerimine).
- Andmebaasitarkvaral peavad olema mehhanismid ressursside piiramiseks (vt M 4.73 Valitavate andmehulkade ülempiiride määramine).
- Kui andmebaasis hallatakse konfidentsiaalseid andmeid, peab olema võimalik vältida volitama isikute juurdepääsu. Nimetatud juhul peab soetatav andmebaasitarkvara olema varustatud vastavate pääsu reguleerimise mehhanismidega (vt M 2.129 Andmebaasiinfo pääsu reguleerimine). Võimalik peaks olema ka ühesuguste pääsuõigustega kasutajate koondamine gruppidesse. Kohustuslik on seejuures administraatorite ja kasutajate grupi lahutamine. Lisaks sellele peaks tarkvara pakkuma abi erinevate administraatorirollide lahutamiseks (vt M 2.131 Haldusülesannete lahusus andmebaasisüsteemides).
- On olemas andmebaase, millel on erineva tugevusega pääsu reguleerimise mehhanismid. Seejuures võib sarnaseid turvamehhanisme pakkuda ka erinevaid meetodeid kasutades. Eelnevalt on vaja selgeks teha, millist pääsuõiguste kaitset vajatakse ning milline andmebaasitarkvara vastab määratletud turvanõuetele. Määravaks on siinkohal võimalused ise piirata pääsuõigusi andebaasi objektidele ja andmetele.

Näited:

- Kasutajalt võib olla võetud õigus andmebaasiobjektide (nt tabelid) kujundamiseks ja muutmiseks.

- Kasutajad võivad saada küll tabeli lugemisõiguse, samal ajal võivad olla aga välistatud õigused selles sisalduvate andmete muutmiseks.
- Teatud tabelitele või tabeli teatud ridadele võib pääs olenevalt kasutajast olla keelatud.
- Kasutajad ei saa mingeid pääsuõigusi teatud tunnustega andmekogudele (nt referent Bonnist ei saa juurdepääsuõigust Kölni referendi andmetele).
- Mõned tootjad pakuvad võimalust nii gruppide kui ka rollide määratlemiseks. Sellega on võimalik pääsukontrolli andmebaasi objektidele rohkem diferentseerida. Eelnevalt tuleb sellele esitatavad nõuded välja selgitada ning võrrelda neid olemasolevate andmebaasitarkvara toodetega.
- Kontrollida tuleb ka andmebaasitarkvara monitooringu- ja kontrollimehhanismid.

Vastavad nõuded tuleb määratleda ning toodete jõudlusprofiilidega võrrelda (näiteks M 2.126 Andmebaasi turvakontseptsioon ja M 2.133 Andmebaasisüsteemi logifailide kontroll).

- Kontrollida tuleb, kas andmebaasitarkvaral on administraatori ja revidendi rollide lahutamist toetav funktsioon. Võimalik peab olema seada sisse revidendi roll, kes on ainsana võimeline analüüsima ja kustutama logifaile. See takistab administraatoril potentsiaalset manipuleerimist andmebaasiga.
- Andmebaasi tervikluse tagamiseks peab andmebaasitarkvaral olema täielik transaktsiooniline süsteem, mis vastab ACID printsiibi nõuetele. Nimetatud nõudeid täidavad tänapäeval kõik relatsioonilised andmebaasi haldussüsteemid.
- Olemas peavad olema mehhanismid andmevarunduseks andmebaasis (vt M 6.49 Andmebaasi varundamine).

Sellega seoses tuleb eelnevalt välja selgitada, milliseid andmevarunduse võimalusi andmebaasitarkvara peab pakkuma. Näiteks ei ole kõikidel turul pakutavatel toodetel osalise andmevarunduse funktsiooni. Konkreetsel juhul on niisiis vaja kontrollida, kas koostatud andmevarunduse kontseptsiooni on võimalik käsutuses olevate mehhanismidega realiseerida. Nimetatud kriteeriumide järgi tuleb turul saadaolevaid andmebaasisüsteeme kontrollida ning neile vastav hinnang anda. Valida tuleb tarkvara, mis vastab kõige paremini spetsiifilistele nõudmistele. Lisanõuete rahuldamiseks tuleb kasutada kas lisatooteid või omaarendusi. Enne tarkvara soetamist peaks olema välja selgitatud, milliseid lisatooteid saab koos andmebaasitarkvaraga, et ei tuleks otsida abi kallitest omaarendustest. Turul on reeglina saadaval enamike andmebaasitarkvarasüsteemide mitmed erinevad versioonid. Seejuures erinevad ka ühe andmebaasisüsteemi üksikud versioonid oma funktsionaalsuse ja ka turvalisuse tagamise poolest. Tugev konkurents viib selleni, et mõned tootjad tarnivad ka veel mittedetailselt väljatöötatud tarkvara, mille soetamise korral tuleb arvestada vigade ja piiratud funktsionaalsusega.

Testimisfaasis tuleks seepärast kontrollida, kas valitud andmebaasi tarkvaral on olemas nõutavad funktsioonid vastava kasutuskeskkonna jaoks. Seda peab eriti arvestama jõudlusele esitatavate nõuete ning vajalike mehhanismide olemasolu kohta, mis tagavad valmisoleku hädaolukorras. Enne soetamist tuleks arvestada ka kogemusi võrreldavate installatsioonidega.

Täiendavad kontrollküsimused:

- Kas nõudmised andmebaasitarkvarale on formuleeritud ja dokumenteeritud?
- Kas vastavate nõuete alusel viidi läbi oluliste andmebaasisüsteemide hindamine?

M 2.125 Andmebaasi installeerimine ja konfigureerimine

Algatamise eest vastutavad: IT-juht, IT-osakond

Rakendamise eest vastutavad: administraator

Põhimõtteliselt tuleb vahet teha andmebaasisüsteemi esmase installeerimise ja olemasolevatele andmebaasisüsteemidele installeerimise vahel. Kuna andmebaasitarkvara esmakordsel installeerimisel ei taha kasutajad veel andmebaasile juurde pääseda ning pole ka olemas vanu andmeid (kui, siis ainult teistes andmebaasisüsteemides), toimub see suhteliselt probleemideta ning ei sega IT-süsteemi normaalset talitlust. Olemasolevatele süsteemidele installeerimine peaks võimalusel toimuna väljaspool regulaarset tööaega, et hoida IT-süsteemide normaalset talitlust takistavad asjaolud minimaalsetena. Igal juhul peaksid kasutajad olema eelseisvatest töödest informeeritud, et nad oleksid valmis võimalikeks tõrgeteks või pikemateks vastamisaegadeks.

Andmebaasi installeerimine ja konfigureerimine jaguneb alljärgnevateks toiminguteks:

1. Andmebaasitarkvara installeerimine

Enne andmebaasitarkvara installeerimist tuleb kontrollida, kas IT-süsteem on plaanipäraselt ette valmistatud, nt kas on küllaldaselt salvestusruumi ning kas operatsioonisüsteem on vajadustekohaselt seadistatud. Andmebaasitarkvara installeerimisel tuleb järgida tootja juhiseid. Kui võimalik, tuleks üle võtta tootja poolt etteantud vaikseaded. See kehtib eriti tehniliste parameetrite kohta, mis nt juhivad erinevate andmebaasihaldurisiseste tabelite suurust. Turvalisuse seisukohalt tähtsate näitajate suhtes võib olenevalt olukorrast lubada kõrvalekaldeid ettenähtud väärtustest. Andmebaasitarkvara installeerimine tuleb nõuetekohaselt dokumenteerida. Eriti kehtib see kõrvalekallete kohta tootja poolt ettenähtud vaikseadete osas, mis tuleb üksikasjaliselt põhjendada. Kui kasutatakse tootja poolt pakutud lisafunktsioone, tuleb installeerimise käigus pöörata tähelepanu ka nende seadistamisele. Kõik nimetatud etapi toimingud viib läbi süsteemiadministraator.

2. Andmebaasi loomine

Juba andmebaasi loomisel tuleb ette anda parameetrid, mida hiljem andmebaasisüsteemi kasutamisel ei saa enam muuta. Kõne all olevate parameetrite ja nende sobivate väärtuste valimist selgitatakse põhjalikult tootja installeerimisdokumentides ja juhendites ning neid on nimetatud materjalidest võimalik ka hiljem järele vaadata. Installeerimis- või haldusjuhendist on lisaks sellele võimalik saada informatsiooni ka pärast andmebaasi loomist teostatavate tööde kohta. Ka nimetatud protseduur tuleb fikseerida dokumentatsioonis. Kõik nimetatud etapi toimingud peab läbi viima süsteemiadministraator, kusjuures teda peavad nõustama rakendusadministraatorid (nt et osata kindlaks määrata andmebaasi suurust).

3. Andmebaasi konfigureerimine

Kolmandas etapis tuleb ellu viia kasutaja- ja grupikontseptsioon ning olenevalt olukorrast kasutuselevõetav rollikontseptsioon. Selleks koostab süsteemiadministraator üksikud õiguseprofiilid ning seab sisse kõik grupid ja administratiivsed kasutajatunnused (rakendusadministraatoritele) Seejuures tuleb rakendada ja kontrollida meetmes M 2.132 Andmebaasi kasutajate ja kasutajagruppide konfigureerimise reeglid kindlaksmääratud eeskirju. Kui vastavad pääsuõigused sõltuvad

üksikutest andmebaasiobjektidest, on neid võimalik määratleda vaid juhul, kui eksisteerivad andmebaasiobjektid (vt etapp 4). Kui andmebaasitarkvara toetab andmete jaotamist mitmesse faili või mitmele kõvakettale, tuleb ette võtta täiendav parameetrite seadistamine, millega määratakse kindlaks nimetatud failide sisseseadmine selle juurde kuuluvate salvestuskohtade järgi. Kõik läbiviidud seadistused tuleb detailselt dokumenteerida (vt M 2.25 Süsteemi konfiguratsiooni dokumenteerimine). Kõik nimetatud etapi toimingud viib läbi süsteemiadministraator.

4. Andmebaasiobjektide loomine ja konfigureerimine

Vastavalt andmebaasi turvakontseptsioonile (vt M 2.126 Andmebaasi turvakontseptsioon) seatakse viimase etapi käigus sisse üksikute rakenduste andmebaasi objektid. Nimetatud toiming tuleks võimalusel skriptide kasutamisega automatiseerida ja logida. Pärast andmebaasi objektide sisseseadmist tuleb täiendada vajaminevaid rollide, gruppide ja kasutajate pääsuõigusi. Samuti saab nüüd olemasolevate õigusprofiilide abil luua konkreetsed kasutajad. Kõik nimetatud etapi toimingud viib läbi rakendusadministraator.

Täiendavad kontrollküsimused:

- Kas kasutajaid informeeritakse eelseisvatest installeerimistöödest?
- Kas enne andmebaasi loomist on teada kõik installeerimiseks vajalikud parameetrid ja nende väärtused?
- Kas on teada kõik pärast andmebaasi loomist läbiviidavad tööd?
- Kas on dokumenteeritud installeerimisprotsess, andmebaasi ja andmebaasi objektide loomine ja konfigureerimine?

M 2.126 Andmebaasi turvakontseptsioon

Algatamise eest vastutavad: IT-juht, IT-turbeosakond

Rakendamise eest vastutavad: IT-osakond

Andmete hoidmine andmebaasides pikema aja jooksul on enamasti asutuse või ettevõtte informatsioonihalduse keskne ja kriitiline aspekt. Andmebaasi tõrgeteta kasutamise organiseerimiseks tuleb õigeaegselt koostada andmebaasi turvakontseptsioon, mis annab ülevaate planeerimise, installeerimise, konfigureerimise, kasutamise, migratsiooni ja deinstalleerimise turvaaspektidest. Kui andmebaasid ei ole küllaldaselt kaitstud, võib salvestatud andmete konfidentsiaalsus, käideldavus või terviklus kaduma minna. Et seda ei juhtuks, on hädavajalik koostada hästi funktsioneeriv andmebaasi turvakontseptsioon.

Kontseptsioon peab sisaldama informatsiooni eeskätt selle kohta:

- kuidas toimub pääsuõiguste piiritlemine andmebaasi administratsiooni ja rakendusadministratsiooni vahel,
- kuidas toimub andmete salvestamine või olenevalt olukorrast andmebaasi peegeldamine,
- kuidas toimub andmete varundamine,
- milliseid mehhanisme rakendatakse andmebaasi toimingute monitooringuks ja kontrolliks ning
- kuidas peab toimuma andmebaasi mahu monitooring.

Andmebaasi turvalisus tagatakse tarkvara tasandil selle juurde kuuluva andmebaasihaldussüsteemi kaudu. **Selleks et andmebaasihaldussüsteem võiks pakkuda efektiivset kaitset, peavad olema täidetud alljärgnevad põhitingimused:**

- andmebaasihaldussüsteem peab põhinema laiaulatuslikul turvapoliitikal,
- andmebaasihaldussüsteem peab olema integreeritud organisatsiooni IT turvakontseptsiooni,
- andmebaasihaldussüsteem peab olema korrektselt installeeritud ning
- andmebaasihaldussüsteem peab olema korrektselt haldatud.

Otsene juurdepääs andmebaasile (nt SQL interpretaatori kaudu nagu SQL*Plus) võib olla vaid administraatoritest kasutajatel, et hoida ära andmete või andmebaasi objektidega manipuleerimine (nt tabelid ja indiitsid) (vt M 2.134 Andmebaasipäringute suunised). Andmebaasi objekte tohib teisendada eranditult vaid spetsiaalsete kasutajatunnuste abil kontrollituna. Vastavalt sellele peab andmebaasihalduril olema sobiv kontseptsioon juurdepääsu reguleerimiseks andmebaasile ning selles sisalduvale infole (vt M 2.128 Andmebaasisüsteemi pääsu reguleerimine ja M 2.129 Andmebaasiinfo pääsu reguleerimine). Kasutajatunnustel, mis saavad andmete teisendamist läbi viia vaid ühe rakenduse kaudu, ei tohi olla otsest juurdepääsu andmebaasile samal ajal kui andmebaasi objektide haldamiseks vajalikele tunnustele on lubatud kontrollitud otsene juurdepääs.

Lisaks eelpool kirjeldatule peab andmebaasi turvakontseptsioonis olema reguleeritud alljärgnevad tähtsad aspektid:

- Kindlaks tuleb määrata andmebaasi failide füüsiline salvestamine või peegeldamine, samuti nende jaotamine (nt andmebaasi tarkvara, andmebaas

ise või logifailid), et tõsta näiteks nende käideldavust ja vältida väljalangemisohtu. Käideldavuse tagamiseks peaksid peegeldatud kontrollfailid olema salvestatud erinevatele kõvaketastele. Ühe ketta väljalangemine ei tähenda siis koheselt kõikide kontrollandmete kadu. Kui ühe rakenduse andmebaasi objektid paigutatakse oma andmefailidesse, peaks andmefailide jaotamisel jälgima, et ühe kõvaketta väljalangemine ei puudutaks kõiki rakendusi.

Näide:

Üks andmebaas haldab kahe rakenduse andmeid, kummagi jaoks üks andmefail tabelite ja indeksite jaoks. Andmefailid võib jaotada suvaliselt neljale kõvakettale.

Andmefailide ebasobiv jaotamine näeb välja järgmine:

Kõvaketas 1: Andmefailide salvestamine mõlema rakenduse indeksite jaoks

Kõvaketas 2: Andmefailide salvestamine esimese rakenduse tabelite jaoks

Kõvaketas 3: Andmefailide salvestamine teise rakenduse tabelite jaoks

Kõvaketas 4: Esimese kõvaketta väljalangemine puudutaks sel juhul mõlemaid rakendusi ning neid ei oleks enam võimalik kasutada.

Andmefailide sobivam jaotamine kulgeks alljärgnevalt:

Kõvaketas 1: Andmefailide salvestamine esimese rakenduse indiitside jaoks

Kõvaketas 2: Andmefailide salvestamine esimese rakenduse tabelite jaoks

Kõvaketas 3: Andmefailide salvestamine teise rakenduse indiitside jaoks

Kõvaketas 4: Andmefailide salvestamine teise rakenduse tabelite jaoks. Ükskõik millise kõvaketta väljalangemine puudutaks vaid üht rakendust. Kui kõvaketas 1 ja 2 on lisaks peegeldatud kõvaketastel 3 ja 4 ning vastupidi, kõvaketas 3 ja 4 on peegeldatud kõvaketastel 1 ja 2, võiksid kuni kaks suvalist ketast rivist välja langeda, ilma et andmebaas ühe jaoks kahest rakendusest täielikult välja langeks.

- Vajalik oleks läbi viia regulaarne kontroll tegelikkuses olemasoleva andmemahu suuruse või suurenemise suhtes hilisema kasutamise käigus, et oleks võimalik dimensioneerida vajaliku suurusega salvestusruum ka tulevikuvajadusi silmas pidades.
- Rakendada tuleb andmevarunduseks sobivaid mehhanisme (vt M 6.49 Andmebaasi varundamine).
- Kindlaks on vaja määrata monitooringu-ja kontrollimehhanismid, st kas ja millises ulatuses peab toimuma andmebaasi toimingute logimine. Siin tekib muuhulgas küsimus, kas näiteks tuleks fikseerida vaid andmete teisendamise aeg või tuleb ka teisendamine ise logida (vt M 2.133 Andmebaasisüsteemi logifailide kontroll).

Andmebaasisüsteemi kontseptsiooni koostamiseks ja andmebaasisüsteemi kasutamiseks on tähtis sobiva personali olemasolu. Alahinnata ei tohi andmebaasisüsteemi käitamiseks kuluvat aega. Ainuüksi tekkivate logiandmete läbitöötamiseks kulub teadaolevalt palju aega. Andmebaasi administraator peab omama põhjalikke teadmisi rakendatud andmebaaside haldustarkvara kohta ning olema läbinud vastava koolituse.

Täiendavad kontrollküsimused:

- Kas turvasuunised andmebaasisüsteemi rakendamiseks on formuleeritud ja dokumenteeritud?

- Kas pääsuvõimalused on nii piiratud, et ainult administraatorid omavad interaktiivse päringukeele kaudu otsest juurdepääsu andmebaasidele?

M 2.127 Tuletamise vältimine andmebaasis

Algatamise eest vastutavad: IT-juht, IT-osakond

Rakendamise eest vastutavad: administraator

Andmebaasisüsteemis sisalduvate isikuandmete ja teiste konfidentsiaalsete andmete kaitseks on igale kasutajale põhimõtteliselt lubatud vaid juurdepääs andmetele, mis on tema tööks vajalikud. Ülejäänud andmebaasis sisalduvat informatsiooni tuleb kasutaja eest varjata. Selleks peab olema võimalik määratleda andmebaasiinfo pääsuõigused tabelitele ja nende väljadele. Seda on võimalik teostada vaadete ja pääsulubade abil (vt M 2.129 Andmebaasiinfo pääsu reguleerimine . Nendega on kasutajal võimalik kasutada ja töödelda ainult tema jaoks ettenähtud andmeid. Kui ta teeb andmebaasipäringuid muu informatsiooni kättesaamiseks, lükkab andmebaasihaldur nimetatud päringud tagasi. Statistiliste andmebaasidele, mis sisaldavad andmeid isikugruppide, rahvastikukihtide või muu taolise kohta, esitatakse seevastu teistsuguseid turvanõudeid. Statistilises andmebaasis alluvad üksikud isikuandmeid sisaldavad sissekanded andmekaitsele, statistiline informatsioon on aga kättesaadav kõigile kasutajatele. Siin on vajalik ära hoida see, et ühe grupi andmeid teades saaks teha järeldusi nimetatud grupi üksikute liikmete andmete kohta. Lisaks sellele peab olema võimalik takistada, et ei läheks kaduma andmebaasis salvestatud informatsiooni või andmete paigutusstruktuuris andmete anonüümsus vastavalt formuleeritud andmebaasipäringuid kasutades (nt kui andmebaasipäringu tulemus sisaldab vaid ühte andmekogumit). Kõne all olevat probleemi nimetatakse tuletamisprobleemiks ning kaitset taoliste võtete eest tuletamise vältimiseks. Ka siis, kui statistilises andmebaasis sisalduvad andmed on anonüümsed, on tuletamisvõtete abil võimalik taastada teatud andmekogumite seotus isikutega. Teatud päringute tagasilükkamisest (nt ühe või väheste tulemuste korteežiga) üldiselt ei piisa, kuna ka andmebaasihalduri vastusest keeldumine võib sisaldada informatsiooni.

Erinevate statistikate koostamise tõttu võib andmete anonüümsus samuti kaduma minna. Sellise kaudse ründe eesmärgiks on teha mitmete statistikate põhjal järeldusi üksikisiku isikuandmete kohta. Kaitsemeetmena tuleks sel juhul mitte lubada niinimetatud tundlike statistikate ühiskasutusse andmist, mida nimetatakse järelduste tegemise vältimiseks blokeerimise abil. Teiseks võimaluseks on taoliste statistikate moonutamine kontrollitud ümardamise kaudu (sarnased statistikad tuleb sarnaselt ümardada) või piiramine statistiliselt tähtsatele osahulkadele kohustusega, et ühesugused päringud viitavad alati ühesugustele osahulkadele. Kirjeldatud meetodit nimetatakse tuletamise vältimiseks moonutamise abil. Kui andmete konfidentsiaalsusele esitatakse täiendavaid nõudeid, on vajalik nende krüpteerimine (võrdle meetmega M 4.72z Andmebaasi krüpteerimine).

Täiendavad kontrollküsimused:

- Kas andmebaasisüsteemile esitatavad konfidentsiaalsusnõuded on koostatud ja dokumenteeritud?
- Kas konfidentsiaalsed andmed on küllaldaselt kaitstud volitamata juurdepääsu eest?

M 2.128 Andmebaasisüsteemi pääsu reguleerimine

Algatamise eest vastutavad: IT-juht, IT-osakond

Rakendamise eest vastutavad: administraator

Efektiivse pääsukontrolli tagamiseks peab andmebaasitarkvara olema varustatud sobiva mehhanismiga kasutajate identifitseerimiseks ja autentimiseks. Pääsuõiguste jaotamine peab toimuma kindlaks määratud reeglite järgi (vt M 2.132 Andmebaasi kasutajate ja kasutajagruppide konfigureerimise reeglid). Üldiselt peaks normaalsete kasutajate juurdepääsu tõkestamine tooteandmebaasile toimuma interaktiivse SQL interpretaatori kaudu. Taolistele andmebaasidele peaks olema võimalik vaid kaudne juurdepääs vastavate rakenduste kaudu. Ainsa erandi moodustavad siin andmebaasi paroolid haldustööde läbiviimiseks. Kaugpääsusid andmebaasides sisalduvatele andmetele juurdepääsuks tuleks anda eriti piiratult. Kui nimetatud pääsu liik ei ole just eriti vajalik, tuleks selle andmisest loobuda. Muudel juhtudel tuleks anda kaugpääsuõigus vaid kasutajatele, kes seda tõepoolest vajavad. Teistel kasutajatel ei tohi olla võimalust endale kaugpöörduse loomiseks. Mitte mingil juhul ei tohi kaugpöördus olla võimalik kehtiva kasutajatunnuse ning parooli sisestamiseta. Kõrgendatud turvanõuete korral peaks kontrollima, kas on vajalik eriti range autentimine, milleks ei piisa kasutajanime ja parooli sisestamisest. Siin tuleb kõne alla näiteks kiipkaartide või niinimetatud lubakaartide kasutamine.

Täiendavad kontrollküsimused:

- Kas on kasutajanimesid, millel on otsejuurdepääs andmebaasile? Kui jah, siis mis põhjusel on neil otsejuurdepääs?
- Kas võimalused kaugpöörduseks käesoleval ajal kasutuses olevatele andmebaasidele on kontrollitud ning vajadusel deaktiveeritud?

M 2.129 Andmebaasiinfo pääsu reguleerimine

Algatamise eest vastutavad: IT-juht, IT-osakond:

Rakendamise eest vastutavad: administraator

Andmebaasis olevate andmete konfidentsiaalsuse ja tervikluse efektiivse kaitse tagamiseks tuleb rakendada terve rida meetmeid. Lisaks andmebaasisüsteemi pääsu reguleerimisele, mida kirjeldatakse meetmes M 2.128 Andmebaasisüsteemi pääsu reguleerimine , on olulise tähtsusega ka alljärgnevalt kirjeldatud võimalused andmebaasiinfo pääsu reguleerimiseks:

Andmebaasiobjektide kaitse

Peaks toimuma loogiline andmebaasiobjektide, niisiis tabelite, indeksite, andmebaasiprotseduuride jne jaotamine rakenduste vahel, mis neid objekte kasutavad. Sellest tekkivad andmebaasiobjektide grupid jaotatakse rakenduste kaupa spetsiaalselt selleks sisseseatavate kasutajatunnuste alla. Sellega on võimalik seadistada andmebaasiobjektidele juurdepääsu selliselt, et ainult nende spetsiaalsete kasutajatunnuste kaudu saab toimuda objektide teisendamine. Kui mitmed rakendused kasutavad ühtesid ja samu andmebaasiobjekte, tuleks need omaette grupina isoleerida. Kui andmebaasis hallatakse näiteks kahe rakenduse A ja B andmeid, tuleb sisse seada kaks andmebaasi kasutajatunnust – AnwA ja AnwB. Kõik andmebaasiobjektid, mida on võimalik kindlalt jaotada rakenduse A juurde, seatakse sisse ja hallatakse andmebaasi kasutajatunnusega AnwA. Analoogselt toimuvad rakenduse B andmebaasiobjektide protseduurid. Mõlema rakenduse poolt kasutatava tsentraalse andmebaasiobjekti näiteks oleks tabel, mis sisaldab kõiki juhitavaid printereid. Nimetatud kategooria andmebaasiobjekte ei tohiks jaotada rakenduste (AnwA või AnwB) juurde, selle asemel tuleks taolised andmebaasiobjektid kokku võtta omaette kasutajatunnuse alla (nt printimine) ning nende haldamine peaks toimuma nimetatud tsentraalse kasutajatunnusega. Nimetatud spetsiaalsed kasutajatunnused ei ole seotud isikunimedega. Selle asemel saavad selleks spetsiaalselt volitatud isikud (nt andmebaasi administraator või juurdekuuluva rakenduse administraator) vajamineva kasutajatunnuse parooli, kui on vajalik andmebaasiobjektide teisendamine (vt M 4.68 Järjekindla andmebaasi halduse tagamine).

Andmekaitse

Vaadete ja protseduuride määratlemisega on võimalik luua andmete nägemiseks spetsiaalsed kasutaja vaated, mis tähendab, et andmebaasis olevad andmed muudetakse nähtavaks või jäetakse nähtamatuks teatud kindlate kriteeriumide põhjal. Vaate või protseduuri kaudu määratakse selgelt kindlaks, milliseid välju ühest või mitmest tabelist mingile kasutajale millises järjekorras näidatakse. Seejuures võidakse eritingimustel andmeid filtreerida ning spetsiifiliste kitsendustega mahu osas piirata. Andmebaasiinfo pääsuõiguste kitsendusega andmisega (alljärgnevalt kirjeldatud pääsulubadega) sellistele vaadetele ja protseduuridele on võimalik kaitsta konfidentsiaalseid andmeid volitamata juurdepääsu eest. Andmete ja funktsionaalsuse lahutamise, siin vaadete ja protseduuride lahutamise abil tegelikest andmetest ning salvestamise kaudu eraldiseisvasse andmebaasi on turvalisust veelgi võimalik suurendada. Kasutajal või rakendusel on juurdepääs vaid vaadetele ja protseduuridele väljasaalitud andmebaasis. Alles nimetatud vaadetel ja protseduuridel on juurdepääs andmebaasi salvestatud andmetele. Väljasaalitud andmebaasis võetakse kokku kasutajate ja rakenduste juurdepääsuõigused. Seejuures võib pääsuõigusi (grants) jagada ka tabelitele, vaadetele jne või isegi tabeli

üksikutele väljadele. Nimetatud õigused on alati seotud kindlate kasutajate, rollide või kasutajagruppidega. Siinjuures tuleb selgelt eelistada kasutajate pääsuõiguste lahutamist ühelt poolt (enamasti kasutajatunnuse ja parooli abil) ning kasutajagruppide ja rollide andmebaasiobjektide pääsuõiguste lahutamist teiselt poolt. Kasutajate ühendamine andmebaasiobjektide juurde toimub seejuures üksikute kasutajate jaotamise kaudu vajalike pääsuõigustega varustatud kasutajagruppidesse või rollidesse. Võimalik on eraldada pääsuõigusi andmete lugemiseks (read), muutmiseks (update), kustutamiseks (delete), lisamiseks (insert) või uuesti tekitamiseks (create), protseduuride juures lisandub täitmisõigus (execute). Pääsuõiguste andmine peaks olema andmebaasi kontseptsioonis täpselt kirjeldatud. Põhimõtteliselt tuleks anda vaid tõepoolest vajalikud pääsuõigused. Vastasel juhul on oht, et ülevaade kehtivatest pääsuõigustest läheb kaduma ning võivad tekkida täiendavad turvaaugud. Mitte mingil juhul ei peaks kasutama andmebaasihalduri poolt pakutavat võimalust pääsuõiguste andmiseks kõigile (GRANT . . . TO PUBLIC). Üldiselt on pääsuõiguste edasiandmise õigus teistele kasutajatele vaid andmebaasi omanikul. Mõned andmebaasid pakuvad siiski võimalust, et andmebaasi omanik võib pääsuõiguste edasiandmise õiguse anda ka teistele kasutajatele. Nimetatud võimalust tuleks kasutada vaid põhjendatud erandjuhtudel, kuna andmebaasiobjekti omanik kaotab sel moel kontrolli juurdepääsu üle andmetele või andmebaasiobjektidele.

Kitsendatud juurdepääs andmetele rakenduste kaudu

Rakendused peaksid toetama kitsendatud juurdepääsu andmetele, s.t sõltuvalt kasutajatunnusest ja grupikuuluvusest peaksid kasutamiseks kättesaadavaks tehtama vaid funktsioonid ja andmed, mida kasutaja vajab oma ülesannete täitmiseks. Üheks taolise rakenduse andmebaasi poolselt teostatud realiseerimise viisiks on niinimetatud salvestatud protseduuride (Stored Procedures) kasutamine. Salvestatud protseduurid on SQL käskude järjestus, mis salvestatakse andmebaasi eelnevalt optimeerituna. Salvestatud protseduuri käivitamisel on vaja sisestada vaid nimi ja vastavad parameetrid, et täita selle taga seisvaid käske. Ühelt poolt on selle eeliseks, et andmebaasi serverile ei pea üle kandma kõiki korraldusi, mis vähendab komplekssemate operatsioonide korral võrgu koormatust. Teiselt poolt saab andmebaasisüsteem salvestada korraldused optimeeritud, eelnevalt kompileeritud vormis, mille tulemusena täidetakse need käivitamisel kiiremini. Õiguste andmise kitsendustega tähendab pääsuõiguste andmist salvestatud protseduuridele, mitte tabelitele ja vaadetele. Kui antakse pääsuõigused ainult salvestatud protseduuridele, võivad kasutajad teostada vaid andmebaasi eest vastutavate isikute poolt kindlaksmääratud operatsioone.

Näited:

1. Andmebaasisüsteemis Microsoft Access on võimalik anda erinevaid pääsuõigusi, mis on seotud andmebaasi enda (avamine/käivitamine, välistamine (exclusive), haldamine) või tabelite ja päringutega (andmete lugemine, andmete uuendamine, andmete kustutamine, andmete lisamine). Nimetatud õigusi võib jaotada erinevatele kasutajatele või kasutajagruppidele. Standardi kohaselt on andmebaasisüsteemis Microsoft Access sisse seatud grupid “Administraatorid” ja “Kasutajad”, kusjuures grupp “Kasutajad” sisaldab õigusi andmete lugemiseks ja andmete uuendamiseks tabelites ja päringuteks ning õigust andmebaaside avamiseks/käivitamiseks. Pääsuõiguste de-

tailseks reguleerimiseks võib määratleda mõned grupid, kellele on võimalik anda erinevaid pääsuõigusi.

2. Oracle 'i andmebaasis saab käsklustega CREATE ROLE ja GRANT luua grupi "Jaotus 1" ning anda näiteks õiguse ühenduse loomiseks andmebaasiga (connect), seansi avamiseks (create session) ning valikuliste päringute teostamiseks kindlatele tabelitele (select). Olemasolevate andmebaasi kasutajate liitmisel gruppi "Jaotus 1" saavad nimetatud kasutajad kõik selle kasutajagrupi õigused. Selle näite põhjal omaks eranditult vaid grupi "Jaotus 1" koosseisu kuuluv kasutaja juurdepääsu nimetatud grupi jaoks ettenähtud tabelitele ning ainult lugemiseks (select), mitte aga teisendamiseks (insert, delete, update, jne).
3. Salvestatud protseduuril Oracle 'i all PL/SQL-käskudega on sisendparameeter, mis näitab artikli numbrit. Salvestatud protseduur otsib läbi kõik väljundparameetrite väljaarvestamiseks vajaminevad tabelid ning annab muuhulgas ka artikli hinna.

Kasutajad saavad pääsuõiguste andmise kaudu ainult õiguse kasutada salvestatud protseduure, kuid mitte vastavaid tabeleid. Sellega kulutatakse näiteks otsingutele vähem aega kui siis, kui on antud valikuõigus otse selle juurde kuuluvatele tabelitele.

Täiendavad kontrollküsimused:

- Kas andmebaasiobjektid on kaitstud volitamata juurdepääsu eest?
- Kas on antud juurdepääsuõigusi andmetele ja kas need on dokumenteeritud?

M 2.130 Andmebaasi tervikluse tagamine

Algatamise eest vastutavad: IT-juht, IT-osakond:

Rakendamise eest vastutavad: administraator, üksikute IT-rakenduste eest vastutavad isikud

Andmebaasi tervikluse kindlustamine ja monitooring peavad garanteerima andmebaasis olevate andmete korrektsuse, täpsemalt öeldes andmebaasi korrektse seisundi. Ebakorrektsete andmete või ebakorrektse seisundi vältimiseks andmebaasis tuleb pöörata tähelepanu alljärgnevatele tehnilistele võtetele:

- **Pääsukontroll** - Selle all mõeldakse konkreetse andmebaasi kaitset volitamata juurdepääsu eest pääsuõiguste jaotamisega, nagu on kirjeldatud meetmes M 2.129 Andmebaasiinfo pääsu reguleerimine . Sellega hoitakse ära andmete või andmebaasiobjektide (nagu nt tabelitele) muutmine manipulatiivsel eesmärgil. Andmebaasiinfo pääsu reguleerimise elluviimise eest vastutab andmebaasi administraator.
- **Sünkroonimise kontroll** - Sünkroonimise kontroll on vajalik vältimaks ebapüsivusi, mis võivad tekkida paralleelse juurdepääsu korral ühele ja samale andmekogumile. Selleks on erinevaid tehnilisi võtteid, nagu näiteks andmebaasiobjektide lukustamine (locking) või ajatemplite andmine (time stamps). Selle elluviimise eest vastutavad IT-rakenduste eest vastutavad isikud, kui on vaja käsutusse anda täiendav mehhanism, mis ületab andmebaasihalduri süsteemi poolt pakutavad võimalused. Üksikasjalistest seletustest loobutakse, kuna üldiselt teostab iga andmebaasisüsteem sünkroonimise kontrolli. Ilma nimetatud funktsioonita andmebaasisüsteemi ei soovitata mitte mingil juhul kasutada.
- **Tervikluse kontroll** - Selle all mõeldakse semantiliste vigade või semantiliselt absurdsete andmebaasi seisundite vältimist terviklusele esitatavate tingimuste täitmise ja monitooringu kaudu. Need võivad viidata üksikutele seostele või mitmeid seoseid omavahel ühendusse viia (viiteterviklus). Näideteks on ühe peavõtme parameetrid relatsiooni jaoks, üksikute atribuutide juurde kuuluvate väärtuspiirkondade defineerimine või spetsiaalsete tingimuste formuleerimine kindlate põhimõtete alusel. Seda on võimalik andmebaasihalduri kaudu automaatselt monitori abil kontrollida, mida on võimalik teostada trigerite ja salvestatud protseduuride kasutamisega. Selle abil on võimalik teostada põhimõtteliselt kõiki tehinguid, siiski tõukab andmebaasihaldur tagasi tehingud, mis võivad kahjustada andmebaasi konsistentsust. Vastutavad elluviimise eest on IT-rakenduste eest vastutavad isikud või süsteemiadministraator, kui tegemist on tervikluse tingimuste elluviimisega relatsiooni, peavõtmete või üldiste andmebaasiobjektide kujul.

IT-rakenduste kontseptsiooni koostamise käigus on vaja luua:

- andmete mudel, mis lisaks andmebaasiobjektidele kujutab ka nende omavahelisi seoseid ning
- erialane kontseptsioon, mis kirjeldab muuhulgas tingimusi, mille kohaselt tohib andmetega manipuleerida.

IT-rakenduse realiseerimise käigus tuleb pöörata tähelepanu alljärgnevatele aspektidele:

- Kindlaks tuleb määrata kontseptsiooni koostamise faasis määratletud andmemudeli konkreetne elluviimine. Selle hulka kuuluvad tabelite, indeksite, väärtuspiirkondade jne defineerimine ja koostamine.
- Trigerite ja salvestatud protseduuride määratlemine toimub erialase kontseptsiooni realiseerimise käigus. Trigereid ja salvestatud protseduure on võimalik kasutada nii rakenduse (programmides) kui ka andmebaasi piirides (tabelite juures). Trigerid, mida kasutatakse andmebaasi tasandil, toimivad sõltumatult olemasolevatest rakendustest ning seepärast peab nende haldamine toimuma tsentraalselt.

Näide:

Trigger “update” tabeli jaoks:

Alati, kui muudetakse tabeli ühte andmekogumit, tuleb läbi viia trigeri jaoks defineeritud korraldused. Üheks kõnealustest korraldustest võib olla salvestatud protseduuri (Stored Procedure) käivitamine. Rakenduste käigus on võimalik tervikluse tagamine sobivate korralduste commit või rollback abil vastavalt tehingute kinnitamiseks või tühistamiseks.

Täiendavad kontrollküsimused:

- Kas andmete tervikluse tagamiseks kasutatakse kõiki eespool nimetatud tehnilisi võtteid?
- Kas tingimused tervikluse tagamiseks on kooskõlastatud üksikute IT-rakenduste eest vastutavate isikutega?

M 2.131 Haldusülesannete lahusus andmebaasisüsteemides

Algatamise eest vastutavad: IT-juht, IT-osakond:

Rakendamise eest vastutavad: administraator, IT-osakond

Andmebaasisüsteemide korrastatud kasutamise võimaldamiseks tuleb määrata administraatorid. Nende kohustuseks on lisaks üldistele haldustöödele ka kasutajate haldamine, kaasa arvatud pääsuõiguste haldamine. Lisaks sellele on nad vastutavad hallatava andmebaasisüsteemi turvalisuse eest. M 2.26z Süsteemiülema ja ta asetäitja määramine ja M 3.10 Usaldusväärse administraatori ja tema asetäitja valimine nimetatud meetmetele tuleb spetsiaalselt andmebaasidega seoses tähelepanu pöörata alljärgnevatele asjaoludele. Põhimõtteliselt tuleb vahet teha kahe erineva administraatori rolli vahel:

- Andmebaasitarkvara haldav administratsioon
- Rakendusliku tähtsusega administratsioon.

Mõlemaid nimetatud ülesandeid peavad täitma erinevad isikud, et tagada ühe andmebaasi rakenduslik ja tehniline haldamine. Andmebaasihalduri põhimõtteline kasutamine, andmevarunduse või andmekogumite arhiveerimise läbiviimine on näiteks tehnilist laadi andmebaasihalduse osa. Rakendusspetsiifilise halduse käigus toimub seevastu üksikute rakenduste poolt andmebaasile esitatavate nõuete töötlemine. See võib näiteks sisaldada selle juurde kuuluvate andmebaasiobjektide haldamist, kasutajate toetamist probleemide või küsimuste korral või vastavate andmebaasi kasutajatunnuste haldamist. Viimane on võimalik siiski vaid juhul, kui andmebaasi kasutajatunnuste haldamist rakenduste kaupa vastava õiguste kontseptsiooni kaudu toetab vastav andmebaasi tarkvara ehk kui seda on võimalik lahutada tehnilise halduse õigustest. Tehniline administraator seab sisse rakendusspetsiifilise tähtsusega haldamise eest vastutavad administraatori kasutajatunnused koos nende juurde kuuluvate õigustega. Nende hulka kuulub eriti õigus luua andmebaase. Õiguste andmine üksikutele kasutajatele peaks seevastu toimuma iga rakendusspetsiifilise andmebaasi jaoks eraldi ning nimelt vastutava rakendusadministraatori poolt.

Täiendavad kontrollküsimused:

- Kas administraatorite rollid on lahutatud?
- Kes administraatoritest on määratud haldama andmebaasi tarkvara ja kes teostama rakendusspetsiifilist haldust?
- Kuidas on reguleeritud administraatorite vaheline koostöö? Kas tööülesanded ja vastutusvaldkonnad on kirjalikult fikseeritud?

M 2.132 Andmebaasi kasutajate ja kasutajagruppide konfigureerimise reeglid

Algatamise eest vastutavad: IT-juht, IT-osakond:

Rakendamise eest vastutavad: administraator

Kasutajate/kasutajagruppide konfigureerimine ühest andmebaasist loob eelduse sobivaks pääsuõiguste jaotamiseks (vt M 2.129 Andmebaasiinfo pääsu reguleerimine) ning selle süsteemse ja kontrolli all hoitava kasutamise tagamiseks. Põhimõtteliselt saab iga andmebaasi kasutaja andmebaasi kasutajatunnuse, mille kaudu andmebaas teda identifitseerib. Nende abil omavad andmebaasile juurdepääsu vaid volitatud isikud. Andmete muutmiseks tehtavad toimingud (värskendamine, lisamine, kustutamine jne), mille läbiviijateks ei ole andmebaasihaldur või administraatoriõigustega kasutajad, kujutavad endast suurt ohtu, mis võib viia andmebaasi hävimiseni. Andmete teisendamisega seotud õiguste andmisest süsteemitabelite kasutamisel tuleks seepärast põhimõtteliselt loobuda.

Piirata tuleb isegi lugemisõiguse andmist, kuna süsteemitabelite kaudu on võimalik välja selgitada kogu andmebaasis sisalduv informatsioon. Võttes eeskujuks M 2.30 Kasutajate ja kasutajarühmade määramise protseduurid tuleks koostada formular, et saada kõigepealt iga kasutaja või kasutajagrupi kohta teada andmed, mis on vajalikud kasutajate organiseeritud haldamiseks.

- Perekonnanimi, eesnimi,
- ettepanek kasutajatunnuseks (kui ei ole kokkulepetega ette antud),
- organisatsiooni üksus,
- kättesaadavus (nt meiliaadress, telefon, ruum),
- ülemus nõusolek,
- projekt (soovituslik),
- rakendused, mida on vaja kasutada ning mis andmebaasi poole pöörduvad (soovituslik),
- andmed andmebaasisüsteemis planeeritavate tegevuste kohta ning selleks vajalikud õigused, samuti tegevuse kestvus (soovituslik) ning
- piirangud aegadele, pääsuõigustele (teatud tabelite, vaadete jne suhtes), piiratud kasutajakeskkond (soovituslik).

Kindlaks tuleks määrata piiratud arv õigusprofiile. Uus kasutaja jaotatakse siis ühe või mitme profiili alla ning saab sellega täpselt oma tegevuseks vajalikud õigused. Seejuures tuleb kasutajate ja gruppide konfigureerimisel kasutada andmebaasispetsiifilisi võimalusi, mida tuleb arvesse võtta juba andmebaasitarkvara valimisel (vt M 2.124 Sobiva andmebaasitarkvara valimine). Mõttekas on kindlaks määrata nime kasutamise tava kasutaja- ja kasutajagruppide tunnuste loomiseks (nt kasutaja ID = organisatsiooniüksuse lühend pluss jooksev number). Seejuures võib kasutada kasutaja-, rolli- ja grupiprofiile. Kui vähegi võimalik, ei oleks vaja kasutada kasutajaspetsiifilisi profiile, kuna see toob suurearvulise kasutajaskonna korral endaga kaasa kõrged halduskulud. Grupiprofiilide määratlemisel tuleb valida piirangutega ja piiranguteta õigusprofiilide vahel. Kui grupiprofiile rakendatakse väga piiravalt, tuleb hallata suurt arvu gruppe, mis toob endaga kaasa suured halduskulud. Seevastu kui grupiprofiilide defineerimine toimub väga vabalt, võib tek-

kida erinevate gruppide vahel liiasus või põhjendamatult suurte õiguste jaotamine, mis jällegi võib viia andmete konfidentsiaalsuse või tervikluse hävimisele.

Igale kasutajale peab olema määratud oma andmebaasi kasutajatunnus, mitu kasutajat ei tohi sellesama tunnuse all töötada. Põhimõtteliselt peab tegema vahet andmebaasi kasutajatunnuse ja aluseks oleva operatsioonisüsteemi kasutajatunnuse vahel. Mõned tootjad pakuvad oma andmebaasitarkvaraga siiski operatsioonisüsteemi tunnuse ülevõtmise võimalust andmebaasisüsteemi. Sel juhul jääb kasutajatel, kui nad on end juba oma operatsioonisüsteemi kasutajatunnusega sisse loginud, andmebaasi juurdepääsu saamisel ära autentimine. Nii näiteks võib Oracle all kasutada OPS$-kasutajatunnuseid. Niisugune kasutajatunnus koosneb eesliitest “OPS$” ja kasutaja operatsioonisüsteemi tunnusest. Ainult juhul, kui üks kasutaja logib end andmebaasi oma operatsioonisüsteemi kasutajatunnusega, ei küsi andmebaasihaldur parooli. Kui kasutaja logib end sisse mõne teise kasutajatunnusega, küsitakse parooli. Nimetatud võimalus kätkeb endas siiski ohtu, et volitamata autentimise korral operatsioonisüsteemi tasandil (nt vastava paroolikaitse ületamine) ei ole juurdepääsu andmebaasile enam võimalik takistada. Seepärast tuleks enne OPS$-kasutajatunnuste kasutamist kontrollida, kas klientide operatsioonisüsteemi turvamehhanismid on vastava kasutusjuhuse jaoks piisavad. Kui kasutajatelt nõutakse lihtsustatud ühekordset sisselogimist (märksõna Single-Sign-On –SSO), tuleks alternatiivina kogu IT-töö tsentraalseks kasutajate haldamiseks kaaluda lisatoote kasutuselevõttu. Aga ka siin tuleb konkreetsed turvanõuded viia vastavusse vastava lisatootega.

Täiendavad kontrollküsimused:

- Kas juurdepääsuõigused andmetele jaotatakse kasutajagruppide, profiilide või rollide kaudu, selle asemel, et neid anda otse üksikkasutajatele?
- Millised organisatsioonilised eeskirjad on olemas andmebaasikasutajate või -kasutajagruppide konfigureerimiseks?
- Kas on kindlaks määratud nime kasutamise tava kasutajate ja kasutajagruppide kasutajatunnuste osas?
- Kas õigusprofiilid on sisse seatud?

M 2.133 Andmebaasisüsteemi logifailide kontroll

Algatamise eest vastutavad: IT-juht, IT-osakond

Rakendamise eest vastutavad: administraator, audiitor

Logimise, täpsemalt autentimise aktiveerimine andmebaasisüsteemis peab toimuma vajalikul määral. Kui logitakse liiga palju sündmusi, mõjutab see andmebaasi jõudlust negatiivselt ning logifailide hulk suureneb. Niisiis tuleb alati vaagida vajaduse vahel koguda võimalikult palju informatsiooni, et tagada andmebaasi turvalisus, ning nimetatud informatsiooni salvestamis- ja töötlemisvõimaluse vahel.

Seejuures pakuvad erilist huvi alljärgnevad sündmused:

- kasutajate seansside ajad ja kestus,
- andmebaasiühenduste arv
- nurjunud või tagasilükatud ühenduskatsed,
- tupikute esinemine andmebaasisüsteemis,
- iga kasutaja S/V statistika,
- pöördused süsteemitabelite poole (vt M 4.69 Andmebaasi regulaarne turvakontroll),
- uute andmebaasiobjektide genereerimine ning
- andmete muutmine (vajadusel kuupäev, kellaaeg ja kasutaja).

Turvalisuse seisukohalt tähtsate sündmuste logimine on turvameetmena efektiivne vaid juhul, kui logitud andmeid ka töödeldakse. Seepärast peab toimuma regulaarne logifailide töötlemine audiitori poolt. Kui organisatoorselt või tehniliselt ei ole võimalik usaldada logifailide töötlemist sõltumatule audiitorile, on administraatori tegevuse kontroll raskendatud. Lisaks sellele tuleb turvalisuse seisukohalt tähtsate sündmuste logimisel ning logifailide kontrollimisel (seire) tähelepanu pöörata alljärgnevale.

Nelja silma printsiip

Logifailide kontrollimiseks tuleb need põhimõtteliselt kopeerida teise keskkonda. Seejuures tuleks kasutada sobivaid instrumente. Vastutus logimise eest ja vastutus logimisele kuuluvate toimingute eest tuleb hoida lahus.

Logimist tuleb kaitsta alljärgneva eest:

- deaktiveerimine,
- logimisele kuuluvate sündmuste liikide muutmine,
- logifailide muutmine (sisu) ning
- andmete kadu logifailide andmekandjatelt, nt ülekirjutamise, vale täiskirjutamise, vale hoidmise tõttu.

Logiandmete töötlemine, kustutamine ja arhiveerimine

Logiandmeid on vaja andmete töötlemiseks kasutatavalt süsteemilt regulaarselt kustutada, et takistada logifailide ülemäärast kuhjumist. Neid tohib küll ainult siis kustutada, kui logifaile eelnevalt analüüsitakse ja kontrollitakse. Vajadusel tuleb

logifailid arhiveerida. Logifailide arhiveerimine või kustutamine võib toimuda käsitsi või automaatselt, kui on olemas selleks vajalikud vahendid. Kõrvalekallete korral tuleb teavitada infoturbe osakonda. Lisaks sellele tuleb juurdepääsu logifailidele rangelt piirata. Ühest küljest tuleb takistada seda, et ründajad saaksid oma toiminguid logifailide tagantjärele muutmisega varjata, teisest küljest saaks logifailide sihipärase analüüsimisega koostada kasutajate jõudlusprofiile. Seepärast ei tohi näiteks mingisuguseid muudatusi ning lugemispääs tuleb võimaldada vaid audiitoritele. Logimise ja logifailide töötlemise protseduuride kontseptsiooni väljatöötamises peavad õigeaegselt osalema andmekaitse eest vastutav isik ja töötajate või ettevõtte nõukogu. Logifailide töötlemise lihtsustamiseks võib andmebaasi administraator kasutada täiendavaid vahendeid, et viia läbi automatiseeritud monitooring. Taolised tooted võivad näiteks töödelda logifaile andmebaasisüsteemide poolt etteantud näidiste järgi ning vajadusel anda häiresignaali. Teistest meetmetest, millele sellega seoses tuleb tähelepanu pöörata, annab ülevaate M 2.64 Logifailide kontroll .

Täiendavad kontrollküsimused:

- Kes tegeleb logifailide töötlemisega? Kas kasutatakse nelja silma printsiipi?
- Kas administraatori toiminguid on võimalik küllaldaselt kontrollida?
- Kas silmatorkavate kõrvalekallete korral teavitatakse infoturbe osakonda?

M 2.134 Andmebaasipäringute suunised

Algatamise eest vastutavad: IT-juht, IT-osakond:

Rakendamise eest vastutavad: rakenduste arendaja

Relatsioonil põhinev andmebaasikeel SQL (Structured Query Language) on rahvusvaheliselt standardiseeritud keel relatsioonilistele andmebaasisüsteemidele (DBS), mis on laialdaselt levinud ning mis on võetud kasutusele enamikes andmebaasihaldussüsteemides (DBMS). Keele maht määratakse kindlaks tsükliliselt ületöötatud normides (ANSI SQL-92, ANSI SQL-99, ANSI SQL-2003). SQL abil on võimalik muuta andmeid (UPDATE, INSERT, DELETE), formuleerida andmebaasiobjekte (CREATE, ALTER, DROP) ning pärida informatsiooni (SELECT). Andmebaasipäringute efektiivseks, hooldatavaks ja mõistetavaks programmeerimiseks tuleb koostada suunised ning need programmeerimise käigus realiseerida.

Nimetatud suunistes tuleks kirjeldada alljärgnevaid asjaolusid:

- Andmebaasipäringud ei tohiks olla suunatud tabelitele otse, vaid võimaluse korral vaadete ja protseduuride kaudu. Ühest küljest on sellega võimalik paremini tagada andmete kaitset (vt M 2.129 Andmebaasiinfo pääsu reguleerimine). Teisest küljest on võimalik tagada, et kasutajate käsutusse antaks vajalik info vastavas vormingus ja hulgas. Lisaks sellele võib nimetatud vaated ja protseduurid välja saalida eraldi andmebaasi ning kasutajad ja rakendused võivad saada juurdepääsu ainult väljasaalitud andmebaasidele. Tabelites sisalduvad andmed on sel juhul peale protseduuride ja vaadete kaudu väljasaalitud andmebaaside juurdepääsetavad vaid teatud kindlale kasutajate ringile (administraatorid, jne).
- SQL-päringud tuleks formuleerida täpselt ja selgelt, võttes aluseks andmebaasimudeli. Seejuures tuleks täita selgelt ja arusaadavalt kõik väljad ning vältida “*”-operaatorit. Sellega on tagatud, et andmed antakse kasutaja käsutusse oodatud järjekorras ning et välja selekteeritakse vaid need andmed, mida on tõepoolest vaja.

Näide:

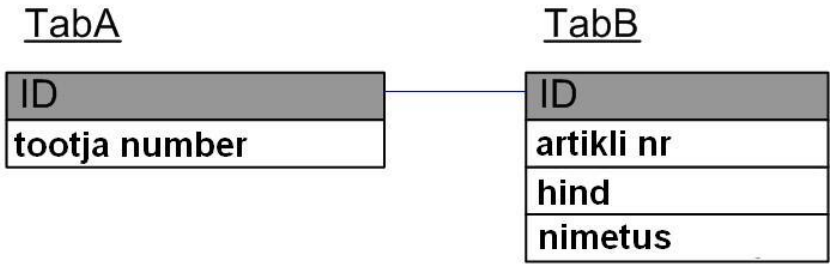
Andmebaasimudel sisaldab tabelit väljadega “Artikli number”, “Artikli nimetus”, “Kasutusotstarve” ja “Netohind”. Rakenduse laiendamise käigus lisatakse “Kasutusotstarbe” taha veel üks väli nimetusega “Tellimisnumber”. Mälu optimaalse ärakasutamise tõttu ei lisa andmebaasihaldur uut välja mitte küll sinna, kuid teisele kohale peale “Artiklinumbrit”. Kuna andmete päring toimub SELECT -*-käsu abil, annab andmebaas informatsiooni teises järjekorras tagasi, kui rakendus seda ootab. See kutsub rakenduse juures esile probleeme, mille tekkepõhjus ei ole esialgu äratuntav.

- Kitsendustega andmebaasipäringute korral (WHERE klausel) on teostamiskiiruse jaoks suure tähtsusega etteantud selekteerimistingimuste järjekord. WHERE klausel tuleks formuleerida selliselt, et enne antakse ette tingimus, mis selekteerib lühikese ajaga välja võimalikult väikese tulemuste hulga. Seejuures tuleks kõigepealt tegeleda indekseeritud väljade, alles seejärel indekseerimata väljadega, kusjuures numbrite kontroll toimub kiiremini kui

tekstide kontroll. Sama kehtib ka andmebaasipäringute kohta, mis formuleeritakse mitmeid tabeleid kasutades (niinimetatud join' id). Paljud andmebaasihaldurid optimeerivad andmebaasipäringuid juba iseseisvalt. Tihti pakutakse valikuks isegi mitmeid optimeerimisstrateegiaid, mida on võimalik välja valida erinevate parameetrite kaudu. Mõned andmebaasihaldurid pakuvad võimalust andmebaasipäringute uurimiseks (nt Oracle all käsu EXPLAIN või Ingres all käsu SETOEP abil). Lisaks sellele on võimalik niinimetatud HINTS kaudu andmebaasipäringute teostamist selgelt ja täpselt määratleda ning seega optimeerija põhimõtteliselt välja lülitada. Nimetatud võimaluse kasutamisel tuleks igatahes olla ettevaatlik.

- Milliseid optimeerijaid andmebaasihaldur kasutab ning millised eelised ja puudused neil on, on tavaliselt dokumenteeritud andmebaasihalduri juhendites. Alternatiivsete optimeerijate kasutamine andmebaasihalduri siseselt peaks olema kooskõlastatud administraatoriga.
- Join 'ide korral peaks lisaks sellele jälgima, et väljade liigitamine tabelite juurde toimuks selgelt.

Näide




```
select
  TabA.ID,
  TabB.nimetus ,
  TabB.
from
  TabA join TabB on
    TabA.ID = TabB.ID
```

Joonis: Väljade rühmitamine joinide korral

Väli "ID" on olemas mõlemas tabelis ning tuleb seetõttu andmebaasipäringu korral näidata selgelt koos selle juurde kuuluva tabeli nimetusega. Vastasel korral ei ole valiku ühetähenduslikkus enam tagatud ja andmebaasipäring katkestatakse vastava veateatega. Kõik teised väljad tuleb sel juhul ühetähenduslikult vastavate tabelite juurde jaotada. SQL ei nõua iga välja jaoks selle juurde kuuluva tabeli täpset äranäitamist. Vaatamata sellele peaks toimuma üksikute väljade ühetähenduslik jaotamine tabeli juurde, nagu eespool olevas näites tabeli TabB väljade "Hind" ja "Nimetus" puhul. TabA uurde välja "Nimetus" lisamine ei tekitaks ülemise näite puhul probleeme. See ei oleks aga nii, kui SQL käsk ei sisaldaks väljade selget jaotamist tabelite juurde. Enam ei ole ühemõtteliselt selge, kas väli "Nime-

tus” tuleb valida tabelist A või B, kuna pärast tabeli A muutmist on mõlemal tabelil sellenimeline väli. SQL käsu katkestaks veateade.

- Kõik andmebaasi transaktsioonid tuleks kinnitada selgelt ja arusaadaval käsuga COMMIT . Kui andmebaasihaldur toetab automaatset käsku COMMIT, ei tuleks seda aktiveerida, sest muidu võib andmebaasis teatud tingimustel esineda ebapüsivusi.

Näide:
Mitmed üksikud teisendamised kuuluvad loogiliselt kokku, need kinnitatakse aga iga üksiku muutuse läbiviimise järel automaatselt käsuga COMMIT : Kui toimub transaktsiooni kontrollimatu katkemine ning seetõttu operatsioonide tühistamine, on kõigepealt teostatud operatsioonid juba kinnitatud ning jäävad andmebaasi, samal ajal kui ülejäänud operatsioone ei suudetud veel läbigi viia.

- Tõkestuste või isegi tupikute vältimiseks on iga spetsiaalse sisuga andmebaasi jaoks vaja kindlaks määrata tõkestusstrateegia (nt kõikide tabelite hierarhiline või selgesti väljendatud sulgemine transaktsiooni alguses).
- Rakenduste arendajad peaksid pärast iga SQL käsku kontrollima vea staatust, nii et rakendus saab nii vara kui võimalik esinevatele vigadele reageerida.
- Õigustest süsteemispetsiifilistele käskudele, millega võib näiteks logimise välja lülitada või blokeerimisprotseduure muuta, tuleks kasutajad ilma jätta ning anda need ainult administraatoritele.
- Rakenduste arendamisel tuleks kõik andmebaasiühendused koondada ühte moodulisse või ühte kindlasse programmikoodi ossa, sest muidu peaks eespool nimetatud printsiipide ülekontrollimiseks kaasama rakendussüsteemi kogu programmkoodi. Sellega kergendatakse rakendussüsteemi järelvalvet ja hooldust, nt andmemudelite muutmisel.

Täiendavad kontrollküsimused:

- Kas on koostatud suunised andmebaasipäringute teostamiseks?
- Kas rakenduste arendajad on tuttavad andmebaasipäringute teostamiseks ettenähtud suunistega?
- Kuidas kontrollitakse nende suuniste täitmist?

M 2.135 Andmete turvaline teisaldus andmebaasi

Algatamise eest vastutavad: IT-juht, IT-osakond

Rakendamise eest vastutavad: administraator

Paljudes andmebaasisüsteemides on rakendamise seisukohalt vajadus teisaldada andmeid teistest süsteemidest. Seejuures on võimalik põhimõtteliselt eraldada alljärgnevaid kategooriaid:

Alg- või pärandandmete teisaldamine

Andmete teisaldamisel pärandsüsteemidest, kui näiteks on loodud uus andmebaasisüsteem, mida peab produktiivselt kasutama, tuleb kindlasti tagada:

- et andmed oleksid vormingus, mida on võimalik sihtandmebaasi üle võtta,
- et andmed oleks täielikud, s.t kõikide väljade jaoks, mis tuleb sihtandmebaasis täita, peaks andmed ülevõtmiseks olemas olema ning
- et oleks garanteeritud andmebaasi konsistentsus ja andmete terviklus.

Enne andmete teisaldamist tuleb koostada kontseptsioon, kuidas peab toimuma teisaldatavate andmete töötlemine ning kuidas tuleb teisaldamine konkreetselt läbi viia. Lisaks sellele tuleb läbi viia täieulatuslik pärandandmete varundamine. Kui andmete teisaldamine toimub mitme etapina, tuleb enne igat etappi läbi viia sõltumatu andmevarundus.

Regulaarne andmete teisaldamine

Kui sihtandmebaasis paiknevad andmete teisaldamisel juba andmed, mida ei tohi muuta, või teisaldatakse andmeid andmebaasi regulaarselt, siis:

- tuleb enne andmete teisaldamist läbi viia andmevarundus kogu andmebaasi ulatuses,
- peaks andmete teisaldamine toimuma võimalusel väljaspool regulaarset tööaega,
- tuleb tarvitusele võtta abinõud, et vältida samade andmete mitmekordset teisaldamist,
- tuleb enne andmete teisaldamist koostada kontseptsioon, kuidas peab toimuma teisaldatavate andmete töötlemine, täpsemalt öeldes, kuidas tuleb teisaldamine konkreetselt läbi viia. Erilist tähelepanu tuleb kontseptsioonis pöörata asjaolule, kuidas vältida konflikte sihtandmebaasis juba eksisteerivate andmete ja teisaldatavate andmete vahel, s.t mil määral säilib sihtandmebaasi terviklus ja konsistentsus.

Andmebaasi uuendamisest puudutatud kasutajaid tuleb eelseisvast andmete teisaldamisest õigeaegselt informeerida, eriti juhul, kui on vaja arvestada kitsendustega andmete käideldavuse või vastamisaegade osas. Enne andmete teisaldamist tuleb kindlaks teha, mida vigade esinemisel ette võtta. Selle hulka kuulub näiteks, kas vigase andmekogumi esinemisel võib jätkata järgmise kogumi teisaldamisega või tuleb kogu andmete teisaldamine katkestada. Lisaks sellele tuleb kindlaks määrata, kuidas peaks toimuma andmete teisaldamise taaskäivitamine pärast katkestust.

Täiendavad kontrollküsimused:

- Kas on koostatud andmete teisaldamise kontseptsioon?
- Kas andmete teisaldamisele eelneb kogu andmebaasi varundamine?
- Kas kasutajaid, keda andmete teisaldamine puudutab, informeeritakse sellest õigeaegselt ja igakülgselt?

M 2.137 Sobiva andmevarundussüsteemi hankimine

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: administraator

Suur osa andmete varundamisel või ennistamisel esinevatest vigadest on tingitud väärkasutusest. Seepärast ei tohiks andmevarundussüsteemi hankimisel pöörata tähelepanu ainuüksi selle jõudlusele, vaid ka selle kasutatavusele ja eelkõige selle tolerantsusele kasutajaväljade suhtes.

Varundustarkvara valimisel tuleks tähelepanu pöörata asjaolule, et see vastaks alljärgnevatele nõuetele:

- Andmevarundustarkvara peaks olema võimeline tuvastama varundusmehhanismis nii väära kui ka defektse varukandja.
- Sellel peaks olema täielik ühilduvus olemasoleva riistvaraga.
- Varundust peaks olema võimalik lasta läbi viia automaatselt ja etteantud aegadel või seadistatavate intervallidega, ilma et tuleks manuaalselt sekkuda (välja arvatud teatud juhtudel varunduseks vajalike andmekandjate valmispanek).
- Võimalik peaks olema valikuliselt ühe või mitme kasutaja automaatne varundustulemusest ja võimalikest veateadetest informeerimine meili või sarnaste mehhanismide kaudu. Andmevarunduse läbiviimine koos varundustulemuste ja võimalike veateadetega tuleks salvestada logifaili.
- Andmevarundustarkvara peaks toetama varukandja kaitset parooli või veelgi parem krüpteerimise kaudu. Lisaks sellele peaks see olema võimeline salvestama andmeid tihendatud kujul.
- Sobivate sissevõtu- ja väljavõtuloendite etteandmisega andmete ja kataloogide valikul peaks saama täpselt spetsifitseerida, millised andmed tuleb varundada ja millised mitte. Nimetatud loendeid peaks olema võimalik kokku võtta varundusprofiilideks, salvestada ning hilisemal andmete varundamisel taaskasutada.
- Varundatavaid andmeid peaks olema võimalik valida olenevalt nende loomise või viimase muutmise kuupäevast.
- Varundustarkvara peaks toetama loogiliste ja füüsiliste täiskoopiate ja astmeliste koopiate (muutuste varundamine) loomist.
- Varundatavaid andmeid peaks olema võimalik salvestada ka kõvaketastele ja võrgudraividele.
- Varundustarkvara peaks pärast andmete varundamist suutma läbi viia varundatud andmete automaatset võrdlust originaalandmetega ning pärast andmete taastamist vastavat võrdlust rekonstrueeritud andmete ja varukandjate sisu vahel.
- Failide taastamisel peaks olema võimalik valida, kas need taastatakse endisel kohal või mõnel teisel kettal või mõnes teises kataloogis. Samuti peaks olema võimalik juhtida tarkvara käitumist juhul, kui sihtkohas on juba sama nimega fail. Seejuures peaks saama valida, kas kõnealune fail kirjutatakse üle alati, mitte kunagi või ainult juhul, kui see on vanem kui rekonstrueeritav fail või et sel juhul esitatakse selge päring.

Kui rakendatava programmiga on võimalik andmevarundust parooliga kaitsta,

tuleks seda suvandit kasutada. Parool tuleb sel juhul deponeerida varundatult (vt M 2.22z Paroolide deponeerimine). Enamike operatsioonisüsteemide juurde kuuluvad programmid, mis on ette nähtud andmete varundamiseks. Mitte kõik nendest ei täida professionaalsele ja mugavale andmevarundusele esitatavaid nõudeid. Kui aga selliseid tooteid ei ole käsutuses, tuleks kasutada süsteemi juurde kuuluvaid programme.

M 2.138 Struktureeritud andmetalletus

Algatamise eest vastutavad: IT-juht, IT-osakond

Rakendamise eest vastutavad: administraator, kasutaja

Halvasti struktureeritud andmetalletus võib tekitada hulganisti probleeme. Seepärast tuleb kõigile IT kasutajatele selgitada, kuidas peaks hästi struktureeritud ja ülevaatlik andmetalletus välja nägema. Kõikidel serveritel peaks vastavad struktuurid olema administraatorite poolt ette antud. See on niikuinii eelduseks diferentseeritud pääsuõiguste andmise realiseerimisel.

Programmid ja rakendusfailid tuleb lahutada

Programmi- ja töötailid tuleks alati salvestada eraldi piirkondadesse. See annab parema ülevaate ja kergendab ka andmevarunduse läbiviimist ning tagab korrektse pääsuõiguste kaitse. Enamiku rakendusprogrammide juures muutuvad pärast installeerimist vaid vähesed konfiguratsioonifailid või ei muutu üldse. Võimaluste piires tuleks kõik regulaarselt muutuvad failid salvestada eraldi kaustadesse, niisiis tuleb regulaarsesse andmevarundusse kaasata ainult need. Programmide ja andmete korraliku lahutamise korral piisab, kui andmesalvestustest tehakse regulaarselt varukoopiad. Tähtis on töötailide hoolikas varundamine, neid saab sel juhul ka teistes süsteemides edasi töödelda. Võrgustatud süsteemide korral kerkib lisaks küsimus, millised programmid või failid tuleks paigutada lokaalsetele kõvaketastele või võrguserverile. Mõlemal on oma eelised ja puudused ning mõlema võimaluse puhul tuleb arvesse võtta nii organisatsioonilist struktuuri kui ka kasutatud riist- ja tarkvara. Nii näiteks tuleks faile, millele esitatakse kõrgeid nõudeid käideldavuse suhtes, hoida koos nende juurde kuuluvate rakendusprogrammidega pigem töökohaarvutitel kui võrguserveril. Sel juhul tuleb muidugi selle töökohaarvuti jaoks tekitada ka vastav valmisolek hädaolukorraks.

Ülesannete või projektide kaustad

Failide rühmitamise kergendamiseks tuleks sisse seada ülesannete või projektide kaustad. Isikuid puudutavatesse kaustadesse tuleks salvestada võimalikult vähe andmeid. Takistamaks olukorda, kus edasise töö aluseks olevatest failidest, nagu kirjade näidised, formularid, projektiplaanid ja muud sarnased materjalid, on olemas erinevad variandid, tuleks neid hallata tsentraalselt. Neid tuleks näiteks hoida ühel serveril selliselt kasutusvalmina, et kõigil oleks neile lugemispääs, kuid iga sellise faili puhul peaks olema vaid üks isik, kellel on õigus seda muuta.

Alljärgnev näide annab ülevaate sellest, kuidas on serveril kataloogide kasutusvalmina hoidmisega võimalik andmeid struktureerida:

- \
- \bin
- \bin\programm1
- \bin\programm2
- \bin\programm3
- \kasutaja
- \kasutaja\kasutaja1
- \kasutaja\kasutaja2
- \projektid

- \projektid\p1
- \projektid\p1\tekstid
- \projektid\p1\pildid
- \projektid\p2
- \projektid\p2\projektiplaan
- \projektid\p2\osaprojekt1
- \projektid\p2\osaprojekt2
- \projektid\p2\osaprojekt3
- \projektid\p2\tulemus
- \formularid

Kaustasid tuleb regulaarselt korrastada. Regulaarselt tuleks kontrollida, kas:

- andmed võib tootmissüsteemist eemaldada, kuna need võib arhiveerida või kustutada,
- ei tuleks projektigrupist lahkunud töötajad jätta ilma pääsuõigustest,
- kõikides IT-süsteemides on salvestatud formularide, näidiste ja muu taolise kehtivad versioonid.

Ülalnimetatu regulaarset kontrolli peaks teostama IT-süsteemide kasutajad või kasutajad, kelle ülesanne on vastavate kataloogide haldamine, ning serverite administraatorid. Nimetatud kontrolli tuleks läbi viia vähemalt kord kvartalis, vastasel korral on töötajad failide sisu ja päritolu taas unustanud.

Täiendavad kontrollküsimused:

- Kas andmete haldamiseks kasutatakse vaid ülesannete või projektide kataloge?
- Millal kontrolliti viimati, kas vanu faile on võimalik kustutada või arhiveerida?

M 2.139 Olemasoleva võrgukeskkonna läbivaatus

Algatamise eest vastutavad: IT-juht, IT-osakond:
Rakendamise eest vastutavad: administraator
Olemasoleva võrgu olukorra ülevaatus on aluseks olemasoleva võrgukeskkonna sihipäraseks turvaanalüüsiks. Samuti on see vajalik olemasoleva võrgu laiendamiseks. Võrkude planeerimiseks tuleb kontseptsiooni koostamiseks pöörata tähelepanu alljärgnevalt kirjeldatud punktidele.

Selleks on vajalik dokumenteeritud kontroll aspektide osas, mis osaliselt üksteisel põhinevad:

- võrgu topograafia,
- võrgutopoloogia,
- kasutatud võrguprotokollid,
- side üleminekukohad kohtvõrgus ja kohtvõrgust laivõrku
- võrgu jõudlus ja liiklusvoog.

Üksikute etappide planeerimisel tuleb põhiliselt fikseerida alljärgnev:
Olemasoleva võrgu topograafia läbivaatus
Olemasoleva võrgu topograafia läbivaatamiseks tuleb koostada võrgu füüsiline struktuur. Seejuures on mõttekas orienteeruda ruumilistele tingimustele, millele vastavalt toimub võrgu ülesehitamine.

Tuleb koostada plaan või olemasolev värskendada, mis sisaldab andmeid:

- Olemasoleva juhtmestiku asjakohased kaablikanalid (vt ka M 5.4 Kaabelduse dokumenteerimine ja märgistus ja M 2.396z IT-kaabelduse dokumenteerimise ja märgistuse nõuded ja M 1.69z Kaabeldus serveriruumides),
- IT-süsteemid, st klient- ja server-arvuti, aktiivsed võrgukomponendid (nagu marsruuter, kommutaatorid, WLAN Access Points), võrguprinterid jne.
- kõikide võrguosade, eelkõige kasutatud aktiivsete võrgukomponentide asukohtade,
- kasutatud kaablitüüpide (vt ka M 5.3 Sidetehniliselt sobivad kaablitüübid) ning
- kaablite kaitsele esitatud nõuete (M 1.22z Liinide ja jaotuskilpide füüsiline kaitse) kohta.

Kõnealuse plaani hooldamiseks on mõttekas kasutada abivahendina vastavat instrumenti (nt CAD programme, spetsiaalseid võrguplaanide instrumente, instrumente kaabli haldamiseks seoses süsteemihaldamise instrumentide või muu sarnasega).
Tagada tuleb nimetatud plaanide järjekindel uuendamine ümberehituste või laienduste käigus kui ka selge ja mõistetav dokumentatsioon (võrdle ka M 1.11 Trasside plaanid ja M 5.4 Kaabelduse dokumenteerimine ja märgistus).

Olemasoleva võrgutopoloogia läbivaatus

Olemasoleva võrgutopoloogia läbivaatuseks tuleb vaadelda võrgu loogilist struktuuri. Selleks on vajalik registreerida üksikute OSI kihtide segmenteerimine ja vastavalt vajadusele VLANi struktuur. Võrgutopoloogia kujutamise abil peab olema võimalik kindlaks määrata, milliste aktiivsete võrgukomponentide kaudu on võimalik rajada ühendus kahe suvalise lõppseadme vahel. Lisaks sellele tuleb dokumenteerida aktiivsete võrgukomponentide konfiguratsioonid, mida kasutatakse segmentide moodustamiseks. Need võivad loogilisel konfigureerimisel olla konfiguratsioonifailid, füüsilise segmenteerimise korral võrgukomponentide konkreetne konfiguratsioon.

Olemasolevate võrguprotokollide läbivaatus

Lähtuvalt valitud võrgu segmenteerimise viisist tuleb üksikutes segmentides kasutatavad võrguprotokollid ning selleks vajalikud konfiguratsioonid (nt MAC-aadressid, IP-aadressid ja alavõrgu mallid IP-protokollidele) kindlaks määrata ja dokumenteerida. Siinkohal tuleks ka dokumenteerida, millised teenused on lubatud (nt HTTP, SMTP, Telnet) ning milliseid teenuseid milliste kriteeriumide järgi filtreeritakse.

Side üleminekukohtade läbivaatus kohtvõrgus ja laivõrgus

Kirjeldada tuleb side üleminekukohti koht- ja laivõrgus, kui olemasolev dokumentatsioon seda veel ei sisalda. Iga kahe võrgu vahelise side üleminekukoha kohta tuleb kirjalikult fikseerida:

- milliseid edastusteid (nt raadiolinke LAN/LAN sidestuse jaoks) selleks kasutatakse,
- millised sidepartnerid ja –teenused millises suunas selleks on lubatud, ning
- kes on vastutav tehnilise realiseerimise eest?

Selle hulka kuulub ka kasutatud WAN-protokollide dokumentatsioon (nt ISDN, X.25). Tulemüüri kasutamisel (vt B 3.301 Turvalüüs (tulemüür)) tuleb lisaks dokumenteerida ka nende konfiguratsioon (nt filtreerimise reeglid).

Olemasoleva võrgu jõudluse ja liiklusvoo läbivaatus

Segmentide või osavõrkude vahel tuleb läbi viia võrgu jõudluse mõõtmine ja liiklusvoo analüüs. Iga kasutatud võrguprotokolli jaoks peavad toimuma vastavad mõõtmised. Võrgu olukorra iga muutuse korral tuleb korrata viimati läbiviidud läbivaatust. Läbivaatuse käigus koostatud dokumentatsiooni tuleb nii säilitada, et see on kaitstud volitamata juurdepääsu eest ning samas igal ajal kättesaadav infoturbe haldustöötajatele ja administraatoritele.

Kontrollküsimused:

- Kas toimub regulaarne jõudluse mõõtmise ja liiklusvoogude analüüsi läbiviimine ja hindamine?
- Kas toimub koostatud dokumentatsiooni jooksev uuendamine?
- Kas dokumentatsioon on arusaadav ja mõistetav ka kolmandatele isikutele?
- Kas võrgu segmenteerimise dokumentatsioon hõlmab ka volitatud teenuseid ja võrguprotokolle ning filtreerimise aluseks olevaid kriteeriume?
- Kas võrgukeskkonna dokumentatsioon hõlmab kõiki sideühenduste üleminekuid võrkude ja selleks kasutatud edastusteekondade vahel?

- Kas sideühenduste üleminekute dokumentatsiooni kaudu on suhtlusvoog ja andmevoog suhtluspartnerite vahel nähtav?
- Kas võrgukeskkonna dokumentatsioon on kaitstud volitamata juurdepääsu eest, kuid vastutavatele isikutele igal ajal kättesaadav?

M 2.140z Võrgu hetkeolukorra analüüsimine

Algatamise eest vastutavad: IT-juht, IT-osakond:

Rakendamise eest vastutavad: administraator

Nimetatud meede põhineb läbivaatuse tulemustele vastavalt meetmele M 2.139 Olemasoleva võrgukeskkonna läbivaatus ning nõuab eriteadmisi võrgutopoloogia, võrgu topograafia ja võrguspetsiifiliste kitsaskohtade valdkonnas. Lisaks sellele on vajalik kogemus kasutatud individuaalsete IT-rakenduste konfidentsiaalsuse, tervikluse või käideldavuse hindamisel. Kuna tegemist on komplekse valdkonnaga, mis lisaks põhjalikele teadmistele kõikides nimetatud valdkondades nõuab ka palju aega, võib olemasoleva võrgukeskkonna analüüsi läbiviimisel abi olla väljastpoolt tellitud nõustajast. Olemasoleva võrgukeskkonna analüüs koosneb põhiliselt struktuurianalüüsist, kaitsevajaduse kindlaksmääramisest ja kitsaskohtade analüüsist. Struktuurianalüüs koosneb meetme M 2.139 Olemasoleva võrgukeskkonna läbivaatus järgi koostatud dokumentatsiooni analüüsist. Struktuurianalüüsi peab läbi viima analüüsimeeskond, kes tunneb põhjalikult kõiki võimalikke võrguühendusi. Tulemusena peab analüüsimeeskond olema aru saanud võrgu funktsioneerimisviisist ning omama informatsiooni põhimõtteliste sidevõimaluste kohta. Tihti on juba struktuurialalüüsi käigus võimalik kindlaks määrata võrgu kontseptsionaalsed kitsaskohad. Edukalt läbiviidud struktuurianalüüs on kindel eeldus sellele järgneva detailse kaitsevajaduse või kitsaskohtade analüüsi teostamiseks.

Detailne kaitsevajaduse kindlaksmääramine

Struktuurianalüüsile järgneb kaitsevajaduse kindlaksmääramine, mis ei mahu IT etalonturbe protseduuride raamidesse. Siinjuures võetakse lisaks arvesse ka nõudeid konfidentsiaalsusele, käideldavusele ja terviklusele üksikutes võrguosades või segmentides. Selleks on vaja kindlaks määrata, milliseid nõudeid on vaja täita erinevate IT-protseduuride põhjal ning kuidas need mõjutavad antud võrgu segmenteerimist. Selle tulemusena peaks olema äratuntav, millistes võrgusegmentides on vajalikud eriturvanõuded.

Võrgu kitsaskohtade analüüs

Lähtuvalt hetkeseisuga olemasolevatest tulemustest viiakse läbi võrgu kitsaskohtade analüüs. Selle hulka kuulub eriti vastavate käideldavusele esitatavate nõuete juures mitteküllaldase varuga paigaldatud võrgukomponentide identifitseerimine (Single-Point-of-Failures). Lisaks sellele tuleb nimetada valdkonnad, milles ei ole võimalik täita käideldavusele, konfidentsiaalsusele või terviklusele esitatud nõudeid või mis vajavad erilist tähelepanu. Peale selle tuleb kindlaks määrata, kas valitud segmenteerimine sobib ribalaiust ja jõudlust silmas pidades (liiklusvoo analüüsi tulemuste abil meetmest M 2.139 Olemasoleva võrgukeskkonna läbivaatus).

Näitlik tõrkepunkt

Jõudluse ja liiklusvoo analüüs näitab üht ülekoormatud aktiivset võrgukomponenti. Kõnealusele sidekanalile esitati kaitsevajaduse kindlaksmääramisel kõrgeid nõudeid konfidentsiaalsuse ja sellega koos ka jõudluse osas. Nimetatud tõrkepunkt vajab võrgu segmenteerimise vastavusse viimist vajadustele või võrgukomponendi väljavahetamist võimsama mudeli vastu (vt M 5.13 Võrgu ühendusaparatuuri õige kasutamine , M 5.60 Sobiva magistraalvõrgutehnika valimine , M 5.61 Sobiv füüsiline segmenteerimine ja M 5.62z Sobiv loogiline segmenteerimine).

Täiendavad kontrollküsimused:

- Kas olemasolev võrgukeskkond on piisavalt dokumenteeritud?
- Kas võrgukeskkonna turvaanalüüsi läbiviimiseks on olemas küllaldane “know-how”?
- Kas võrgu ja andmete konfidentsiaalsusele, käideldavusele ja terviklusele esitatavad nõuded on defineeritud ja dokumenteeritud?

M 2.141 Võrgukontseptsiooni väljatöötamine

Vastutav algatuse eest: IT-juht, IT-osakond:

Vastutav elluviimise eest: administraator

Et nõuded käideldavuse (ka ribalaiuse ja jõudluse suhtes), konfidentsiaalsuse ja tervikluse suhtes saaks täidetud, tuleb võrgu ülesehitust, muutusi ja laiendusi hoolikalt planeerida. Selleks on vaja välja töötada võrgukontseptsioon. Võrgukontseptsiooni väljatöötamine jaguneb analüütiliseks ja kontseptuaalseks osaks.

Analüüs

Kõigepealt tuleb vahet teha, kas olemasolevat võrku tuleb laiendada või olenevalt olukorrast muuta või tuleb võrk täiesti uuesti üles ehitada. Esimesel juhul tuleb eelnevalt läbi töötada meetmed M 2.139 Olemasoleva võrgukeskkonna läbivaatus ja M 2.140z Võrgu hetkeolukorra analüüsimine . Teisel juhul jäävad nimetatud meetmed vaatluse alt välja. Selle asemel tuleb välja selgitada nõuded võrguühendusele ning viia läbi tulevase võrgu kaitsevajaduse kindlaksmääramine. Võrguühendusele esitatavate nõuete väljaselgitamiseks tuleb kindlaks määrata tulevikus oodatav andme- ja liiklusvoog loogiliste või organisatsiooniliste üksuste vahel, kuna oodatav koormus võib mõjutada tulevase võrgu segmenteerimist. Samuti tuleb kindlaks määrata vajalikud loogilised või füüsilised võrguühendused (teenuse-, kasutaja-, grupispetsiifilised) ning üleminekukohad LAN/LAN-sides või üle WANi. Nõuded võrgu kaitsevajadusele tuletatakse planeeritud või juba olemasolevatest IT-protseduuridest. Sellest tehakse järeldused füüsiliste ja loogiliste segmendistruktuuride kohta, nii et võrgu realiseerimisel oleks võimalik neid nõudeid (nt konfidentsiaalsuse suhtes) arvestada. Näiteks määrab IT-rakenduse kaitsevajadus kindlaks võrgu tulevase segmenteerimise. Lõpuks peab proovima tuletatud võrguühendusi harmoniseerida kaitsevajaduse nõuetega. Teatud juhtudel tuleb selleks piirata võrguühendusi, et täita kindlaksmääratud kaitsevajaduse nõudeid. Lõpuks tuleb kindlaks määrata käsutuses olevad ressursid. Selle hulka kuuluvad nii personaliressursid, mis on vajalikud kontseptsiooni koostamiseks ja rakendamiseks, täpsemalt öeldes võrgu käitamiseks, kui ka selleks vajalikud finantsressursid. Tulemused tuleb vastavalt dokumenteerida.

Kontseptsioon

Eelnevalt nimetatud seisukohtadest lähtuvalt tuleb planeerimise abil, millesse kaasatakse ka tulevased nõuded (nt ribalaiuse suhtes) ja samuti kohalikke tingimusi arvestades järgmiste etappide kaupa välja töötada ja kontseptsioonis fikseerida võrgustruktuur ja tähelepanu väärivad raamtingimused. Võrgukontseptsiooni väljatöötamine toimub analoogselt meetmega M 2.139 Olemasoleva võrgukeskkonna läbivaatus ning koosneb selle järgi põhimõtteliselt järgmistest etappidest, kusjuures need etapid ei pea alati rangelt üksteisele järgnema. Mõnedes osades mõjutavad etappide tulemused üksteist vastastikku, mistõttu on vajalik osatulemuste regulaarne kontroll ja konsolideerimine.

1. Võrgu topograafia ja topoloogia, füüsilise ja loogilise segmenteerimise kontseptsioon
2. Kasutatud võrguprotokollide kontseptsioon
3. Side üleminekukohtade kontseptsioon koht- ja laivõrgus

Üksikute etappidena tuleb läbi viia alljärgnevad tegevused:

1. etapp – Võrgu topograafia ja topoloogia kontseptsioon

Analüüsist lähtuvalt (vt eespoolt) ja konkreetsetest ehituslikest asjaoludest tuleb välja valida sobiv võrgu topograafia ja topoloogia (vt M 5.1 Tarbetute liinide kõrvaldamine või lühistamine ja maandamine , M 5.2 Võrgu sobiv topograafia , M 5.3 Sidetehniliselt sobivad kaablitüübid ja M 5.60 Sobiva magistraalvõrgutehnika valimine). Vaatluse alla tuleb võtta ka tulevased nõuded nagu skaleeritavus. Sellisel moel väljatöötatud kontseptsioon tuleb dokumenteerida (kaabelduse plaanid jne). Lähtuvalt kindlaksmääratud nõuetest ning nendele vastavalt oodatavale või kindlaksmääratud andmevoole tuleb võrgu topograafia ja topoloogia kontseptsiooni koostamisel läbi viia sobiv füüsiline ja loogiline segmenteerimine (vt M 5.13 Võrgu ühendusaparatuuri õige kasutamine , M 5.61 Sobiv füüsiline segmenteerimine ja M 5.62 Sobiv loogiline segmenteerimine).

2. etapp – Võrguprotokollide kontseptsioon

Nimetatud etapis peab toimuma kasutatavate võrguprotokollide valimine ja nende vastav kavandamine. Selle hulka kuulub näiteks IP-protokollile aadressiskeemi koostamine ja osavõrkude loomine. Võrguprotokollide valikul tuleb silmas pidada, et neid võib toetada võrgu topoloogia ja planeeritud või olemasolevad aktiivsed võrgu komponendid.

3. etapp – Side üleminekukohtade kontseptsioon koht- ja laivõrgus

Lähtuvalt kindlaksmääratud andmevoogude edastamisest side üleminekukohtade kaudu ning turvalisusele ja käideldavusele esitatavatest nõuetest on selles etapis võimalik kavandada side üleminekukohti.

Selle juurde kuulub sobivate ühenduselementide (vt M 5.13 Võrgu ühendusaparatuuri õige kasutamine), aga ka nende turvaline konfiguratsioon (vt B 3.301 Turvalüüs (tulemüür) ja M 4.82 Võrgu aktiivkomponentide turvaline konfigureerimine).

Järgnevad etapid

Lähtuvalt koostatud võrgukontseptsioonist on võimalik rakendada meetmeid võrguhalduse kontseptsiooni väljatöötamiseks (vt M 2.143 Võrguhalduse kontseptsiooni väljatöötamine , M 2.144 Sobiva võrguhaldusprotokolli valimine ja M 2.145 Nõuded võrguhaldusinstrumendile).

Peale selle tuleks kaaluda ka võrgukontseptsiooni plaani väljatöötamist.
Võrgukontseptsiooni plaani koostamisel tuleb eristada, kas tegemist on võrgu täieliku ülesehitamise, olemasoleva võrgukontseptsiooni muutmise ja/või täiendusega.

Täielikult uue võrgu planeerimisel tuleb arvestada eelnevalt välja töötatud võrgu kontseptsiooniga. Võrgu ülesehitamine toimub planeerimise käigus kindlaks määratud etappide alusel, alates vajalike sidekaablite paigaldamisest, tehnilise taristu ruumide sisseseadmisest, tehnilise taristu installeerimisest, vajalike ühenduselementide paigaldamisest (kommutaatorid, marsruuterid jne), võrguhaldusjaamade sisseseadmisest, vastavate võrguadapterite paigaldamisest lõppseadmetesse kuni lõppseadmete konfigureerimiseni välja.

Olemasoleva võrgu muutmise või laiendamise korral tuleb välja töötatavat võrgukontseptsiooni võrrelda hetkeolukorraga, lähtudes meetmest M 2.139 Olemasoleva võrgukeskkonna läbivaatus . Võttes aluseks soovitud erinevused ja toetudes eelnimetatud meetmetele, saab välja töötada võrgukontseptsiooni plaani nn võrgumigratsiooni tarbeks. Sealjuures tuleb arvestada, et mida rohkem erineb uus kontseptsioon võrgu hetkeolukorrast, seda suurem on ka teostusega seotud vaev.

Kontrollküsimused:

- Kas on olemas ajakohane võrgukontseptsioon?
- Kas võrgukontseptsioonis arvestatakse nõuetega, mis puudutavad kättesaadavust, usaldusväärsust ja terviklust võrgu täiendamisel, muutmisel või ülesehitamisel?
- Kas võrgu füüsilised ja loogilised segmendi struktuurid vastavad kaitsevajadusele?

M 2.142 Võrguplaani väljatöötamine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: administraator

Võrgu teostuse plaani koostamisel tuleb eristada, kas tegemist on võrgu täieliku ülesehitamisega, olemasoleva võrgu kontseptsiooni muutmisega ja/või täiendusega. Täielikult uue võrgu planeerimisel tuleb arvestada eelnevalt väljatöötatud võrgukontseptsiooniga (vt M 2.141 Võrgukontseptsiooni väljatöötamine). Võrgu ülesehitamine peab toimuma vastavalt planeerimise käigus kindlaksmääratud etappidele, alates vajalike sidekaablite paigaldamisest, tehnilise infrastruktuuri ruumide sisseseadmisest, tehnilise infrastruktuuri installeerimisest, vajalike ühenduselementide paigaldamisest (sillad, kommutaatorid, marsruuterid jne), võrguhaldusjaamade sisseseadmisest, vastavate võrguadapterite paigaldamisest lõppseadmetesse kuni lõppseadmete konfigureerimiseni välja. Olemasoleva võrgu muutmise või laiendamise korral tuleb omavahel võrrelda vastavalt meetmele M 2.141 Võrgukontseptsiooni väljatöötamine loodavat lõpplahendust ja võrgu hetkeolukorda, toetudes meetmele M 2.139 Olemasoleva võrgukeskkonna läbivaatus . Võttes aluseks soovitud erinevused ja toetudes eelnimetatud meetmetele, saab välja töötada võrgu teostuse plaani nn migratsiooni tarbeks. Sealjuures tuleb arvestada, et mida rohkem erineb uus kontseptsioon võrgu hetkeolukorrast, seda suurem on ka teostusega seotud vaev. Näide võrgu migratsiooni kohta, kus Shared Ethernet võrk asendatakse Switched Fast-Ethernet võrguga Võrgu migratsioon ühelt topoloogialt teisele toimub reeglina astmete kaupa. Järgnevalt on toodud üldistav näide, kuidas võiks toimuda migratsioon Shared Ethernet võrgult Fast-Ethernet võrgule koos Switching -tehnoloogiaga. Enne reaalse teostuse kallale asumist tuleb muidugi täpselt välja selgitada kõik raamtingimused, et nendega oleks võimalik migratsiooni kontseptsiooni loomisel arvestada.

- Migratsiooni samm nr 1 - Migratsiooni esimese sammuna võib olemasoleva Backbone -i asendada Fast-Ethernet-Backbone -iga või siis vajadusel ehitada üles täiesti uue magistraali. Ühendus alles jäänud Shared Ethernet -i segmentidega toimub läbi Backbone -i võrgukomponentide, mis peavad vastavalt toetama Standard-Ethernet -i funktsioone.
- Migratsiooni samm nr 2 - Struktureeritud juhtmestiku loomine, st toimub üleminek Standard-Ethernet -i juhtmestiku kontseptsioonilt uuele kontseptsioonile, kus iga töökohaarvuti ühendatakse tähekujulise struktuuri alusel jaotusruumiga ilma topoloogilisest siinistruktuurist loobumata.
- Migratsiooni samm nr 3 - Serverite ühendamine tsentraalselt ühe kommutaatori abil, millel on Fast-Ethernet i liidesed (nn serverifarmi installeerimine).
- Migratsiooni samm nr 4 - Suuremat ribalaiust vajavate kasutajate ühendamine Fast-Ethernet ga, vahetades selleks välja vastavad liidesed.
- Migratsiooni samm nr 5 - Alles jäänud Ethernet -i segmentide migratsioon täielikult kommuteeritud süsteemi loomiseks. Selleks võib näiteks Ethernet i kommutaatorid ühendada Backbone i Fast-Ethernet kommutaatorite külge.

M 2.143 Võrguhalduse kontseptsiooni väljatöötamine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator

Kohtvõrku ühendatud erinevaid IT-süsteeme nagu nt serverisüsteeme, lõppseadmeid, printereid, aktiivseid võrgukomponente jne peab saama võrgu tasandil sobivast kohast tsentraalselt administreerida ja jälgida. Võrgukomponentide administreerimisel tuleks hajutatud lahendustele eelistada tsentraliseeritud lahedusi, kuna viimaste puhul on administreerimisele kuluv vaev väiksem ning turvalisusele seatavaid nõudeid on võimalik tsentraalselt defineerida ja kontrollida. Tsentraliseeritud võrguhaldust kasutatakse eelkõige võrgu käideldavuse ja tervikluse tagamiseks, samuti võrgus edastatavate andmete tervikluse ja konfidentsiaalsuse tagamiseks. Nimetatud eesmärkide tagamine on küllaltki keerukas ning nende täitmise hõlbustamiseks tuleks kasutada mõnda võrguhaldusprogrammi. Enne vastava võrguhaldussüsteemi soetamist ja kasutuselevõttu tuleks esimese sammuna luua kontseptsioon, kus sõnastatakse kõik võrguhaldusega seotud turvanõuded ja pannakse kirja kõik ettepanekud võimalike meetmete kohta, mida tuleks rakendada võimalike vigade ja tõrgete puhul. Võrguhaldussüsteemi kontseptsiooni koostamisel tuleb erilist tähelepanu pöörata ja kokkuvõtlikult välja tuua järgmised võrguhalduskontseptsiooni koostisosad:

- võrgu analüüsimiseks tehtavad jõudluse (Performance) mõõtmised (vt M 2.140 Võrgu hetkeolukorra analüüsimine),
- haldusvõrgu valik (vt M 2.482 Exchange'i süsteemide regulaarsed turvakontrollid)
- reageerimine jälgitavate võrgukomponentide veateadetele,
- kaughooldus / Remote-Control , eriti just aktiivsete võrgukomponentide puhul,
- võrguprobleemide Trouble-Ticket'te genereerimine ja eskalatsioon (siinkohal võib toimuda süsteemihaldussüsteemide ja kasutajate Help-Desk - süsteemide ühendamine väliste, teateid edastavate süsteemidega nagu nt piipar, faks jne),
- logimine ja audit (Online ja/või Offline),
- võimalike tootjapoolsete süsteemide ühendamine, nt erinevate haldusprotokollidega süsteemide ühendamine (nt telekommunikatsiooni valdkond),
- kõigi kasutuses olevate IT-süsteemide konfiguratsioonide haldus (vt lisaks muule ka M 4.82 Võrgu aktiivkomponentide turvaline konfigureerimine),
- võrguhaldusfunktsioonide juurdepääsude jagamine (administreerimise või auditi tarbeks võib võrguhaldusfunktsioonide kasutamisel vaja minna kaugpöörduse võimalust. Siinkohal on hädavajalik pääsuõigused hoolikalt defineerida ja jagada.)

Konkreetsed nõuded, mida esitatakse võrguhaldust võimaldavale lahendusele, on kirjas meetmes M 2.145 Nõuded võrguhaldusinstrumendile . Need peavad võimaldama teostada võrguhalduskontseptsiooni.

Kontrollküsimus:

- Kas kõik võrguhaldust puudutavad turvanõuded on sõnastatud ja kirja pandud?
- Kas võrgukomponente administreeritakse tsentraalselt?

- Kas on ette nähtud reageerimine jälgitavate võrgukomponentide veateadetele?
- Kas on ette nähtud Trouble-Tickets'ite loomine ja eskalatsioon võrguprobleemide korral?
- Kas viiakse läbi võrguliikluse logimist ja auditeid?

M 2.144 Sobiva võrguhaldusprotokolli valimine

Algatamise eest vastutavad: IT juht, IT turvaosakond
Rakendamise eest vastutavad: administraator
SNMP peamised eelised ja puudused on järgmised:

- SNMP torkab silma oma lihtsusega ning seetõttu on lihtne ka selle juurutamine. Lihtsus vähendab vastuvõtlikkust vigadele ja suurendab protokolli stabiilsust.
- SNMP on väga laialt levinud ja seda võib pidada de-facto-standardiks. Seetõttu on peaaegu igal võrgu- ja süsteemitehnika tootel olemas SNMP tugi.
- Protokolli saab hõlpsasti muutuvate vajadustega kokku sobitada. Sellest tingituna, samuti eelpool nimetatud laia leviku tõttu, võib SNMP-d pidada ka väga heade tuleviku väljavaadetega protokolliks (kindel investeering).
- Tegemist on edastusvaldkonna jaoks loodud ühendusevaba ja lihtsa protokolliga. Seetõttu on SNMP-pakettide edastuse jõudlus võrgus suurem kui ühendustele orienteeritud CMIP (common management information protocol) puhul.
- SNMPv3 pakub piisavalt häid võimalusi autentimiseks ja krüpteerimiseks, nii et kõrvaldatud on versioonides SNMPv1 ja SNMPv2 olevad puudused.
- SNMPv1 või SNMPv2 kasutamine on seotud turvariskidega, mille tagajärjel võib ründajal olla olenevalt olukorrast võimalik koguda laialdasi andmeid nii süsteemi- kui ka võrgukeskkonna kohta. Juurdepääsul võrgukomponentidele puudub tõeline paroolikaitse, välja arvatud community-nimed, (mis võimaldavad SNMP-l rühmasid moodustada ning pakuvad SNMPv1 ja SNMPv2 puhul algelist paroolkaitset).
- Tänu protokolli lihtsusele ja funktsioonide vähesusele esineb SNMP kasutamisel puudusi väga suurte või tugevasti laienevate võrkude puhul.
- Versiooni nr 1 jõudlusest jääb mahukate MIB-päringute korral väheks, sest alati on tarvis ära näidata kogu MIB puu.

Agent või mõni teine haldur kasutavad InformRequest'i, et teavitada erakorralistest sündmustest. Vastupidiselt trapile peab haldur InformRequest'i vastuvõtu kinnitama.
Võrguhaldusprotokolli valiku lihtsustamiseks on järgnevalt välja toodud mõlema protokolli peamised eelised ja puudused.
SNMP
SNMP protokolli puhul on defineeritud kaks komponenti: haldaja ja agent. Kohtvõrgus installeeritakse iga SNMP poolt kontrollitava või konfigureeritava IT-süsteemi kohta kas üks või mitu haldajat ning üks agent. Agendid koguvad nende süsteemide abil informatsiooni ja salvestavad selle haldusinfobaasi MIB (Management Information Base). Agendid ja haldajad vahetavad omavahel teateid, kasutades selleks ühendusevaba protokolli, seega ei ole SNMP seotud mitte ühegi kindla edastusprotokolliga. Tänapäeval rakendatakse seda siiski enamasti UDP/IP abil. Samas on olemas ja võimalikud ka teised rakendusviisid (nt OSI, AppleTalk, SPX/IPX kaudu). SNMP protokollist eksisteerib erinevaid versioone. Hetkel kuuluvad enimlevinud SNMP versioonide hulka SNMPv1, SMPv2 ja SNMPv3. Nii algversioon SNMPv1 kui ka SNMPv2 (RFC 1901-1908) on kohati veel jätkuvalt kasutusel. Turvalisuse aspektist lähtudes tuleks SNMPv1 ja SMPv2 versioonide kasutamisest loobuda. Kahel esimesel SNMP-versioonil, SNMPv1 ja SMPv2, on ainult

lihtne autentimisfunktsioon, mis põhineb puhtalt teksti kujul edastatavatel Community nimedel (community strings). SNMPv3 puhul on tegu juba parendatud turvamehhanismidega ning seetõttu võib selle kasutamist soovitada. Juhul kui on tarvis rakendada mõnda SNMP versiooni, mis on vanem kui SNMPv3, tuleb seda põhjendada ja põhjused kirjalikult fikseerida, eelkõige seetõttu, et võimalikud riskid oleksid teada ja aktsepteeritud. SNMP puhul on standardina eelseadistatud Community nimed „public“ ja „private“, mille tüüpilisteks kasutusõigusteks on kas „read“ või „read and write“. Community nimed toimivad nagu paroolid.
SNMP puhul on tegu väga lihtsa protokolliga, mis tunneb ainult viit erinevat teadete tüüpi. Teadete abil vahetavad haldaja ja agendid omavahel nn haldusinformatsiooni, mis koosneb siinkohal peamiselt seisundit kajastavatest andmetest, mis on eelnevalt haldusagentidesse juba salvestatud, ja kirjeldavad endaga seotud objekti seisundit. Erinevate parameetrite seisunditeadete kirjeldused (nimi ja tüüp), mida üksikud agendid võivad sisaldada, on kirjas haldusandmebaasis (MIB). Vastav informatsioon on struktureeritud hierarhiliselt ning iga väärtusega on seotud kindel ID-number, mis määrab ära parameetrite seisunditeadete kindla järjekorra. Eraldi väljatooduna on teadete tüübid järgmised:

1. GetRequest: saadetakse haldaja poolt agentidele, et saada infot ühe või mitme seisundit kajastava parameetri kohta.
2. GetNextRequest: saadetakse haldajalt agentidele, et saada haldusandmebaasi (MIB) mõne parameetri väärtust või parameetrite järjekorras järgmiste parameetrite väärtusi.
3. SetRequest: saadetakse haldajalt agentidele, et määrata agendis ühe parameetri väärtust.
4. GetResponse: saadetakse agentidelt haldajale, et saata päringule vastuseks minevaid andmeid või et kinnitada teatud parameetri väärtuse muutumist.
5. Trap: kasutatakse agentide poolt, et haldajat teavitada erakorralistest sündmustest. Trap-teate edastamine toimub vastupidiselt GetResponse-teatele ilma eelneva haldajapoolse päringuta.
6. Agent või mõni teine haldur kasutavad InformRequest'i, et teavitada erakorralistest sündmustest. Vastupidiselt trapile peab haldur InformRequest'i vastuvõtu kinnitama.
7. Raport: saab esitada päringu reportableFlag'i kaudu ja teavitab varem saadetud päringu tulemusest.

Autentimine toimub SNMPv1 ja SNMPv2-ga üksnes krüpteerimata kooskonnastringi abil. Peaaegu kõikidel tootjatel on lugemispääsuga kooskonnastring seadistatud standardseadistusena väärtusele „avalik”, samal ajal kui lugemispääsuga kooskonnastring on seadistatud väärtusele „privaatne”. SNMP kooskonnastringe edastatakse võrgus loetava tekstina. SNMPv2 toetavate turvafunktsioonide puhul on siiski olemas erinevaid variante. Kui kasutatakse ebaturvalisi SNMP-versioone ja administraatorite jaoks ei ole paigaldatud eraldi administreerimisvõrku, võib ründe toimepanija saavutada hõlpsalt kontrolli võrgukomponentide üle, kui säilitatakse need vaikimisi seadistused. SNMPv1 ja SNMPv2 ei peaks seetõttu enam paigaldama, vaid nende asemel tuleks kasutada SNMPv3 (või kõrgemat versiooni). Alles alates sellest versioonist on olemas tugevamad autentimis- ja krüpteerimisvalikud.

Praktikas kasutatakse siiski sageli veel süsteeme, mis ei toeta versiooni 3 kasutamist ja seetõttu ollakse sunnitud kasutama protokolli vanemaid versioone. Sellisel juhul peab vanema versiooni kasutamine olema põhjendatud ja dokumenteeritud, eelkõige tuleks avalikustada riskid ja neid aktsepteerida. Neid ebaturvalisi protokolle tuleks parimal juhul kasutada üksnes eraldatud administraatorivõrgus (vt M 2.582 Võimalused haldusvõrgu loomiseks). Samas tohiks ka neil juhtudel vastavaid protokolle rakendada üksnes ajutise lahendusena ning pikas perspektiivis tuleks hakata kindlasti kasutama ainult selliseid seadmeid, mis toetavad ka SNMP-protokolle alates versioonist 3.
Seetõttu tuleb eelseadistusega määratud community-nimed ilmtingimata välja vahetada teiste, raskesti aimatavate nimede vastu, samuti tuleb neid ka regulaarselt vahetada (vt M 4.82 Võrgu aktiivkomponentide turvaline konfigureerimine). Individuaalsetel võrguelementidel peaksid olema erinevad community-nimed. Community-nimedega seotud pääsuõigused tuleb piirata absoluutselt hädavajaliku miinimumini. Peale selle tuleks juurdepääsu võrguelementidele SNMP kaudu piirata pääsuloendite abil üksnes võrguhaldusjaamadega (vt M 4.80 Kaugvõrguhalduse turvalised pääsumehhanismid). Kui SNMP vanemaid versioone enam ei vajata, tuleks need inaktiveerida.
Versioonis SNMPv3 asendati community-nimede kontseptsioon kasutajanimedega. Iga kasutaja on määratud ühte rühma, millel on üksikute kontrollitavate objektide jaoks täpselt reguleeritavad õigused. Rühma kuuluvuse järgi on võimalik ka reguleerida, milliseid automaatteateid (trappe) tohib kasutaja näha.
SNMPv3 pakub erinevaid protseduure, et tagada kasutajate autentimine: kasutajanime lihtne kontrollimine, autentimine MD5 või SHA abil. Edastatavad andmed võivad olla ka krüpteeritud. Alati tuleks kasutada kõige tugevamaid turbefunktsioone.
Turvalisuse aspektist lähtudes tuleks SNMPv1 ja SNMPv2 versioonide kasutamisest loobuda ja kasutada SNMPv3 . Suurem osa moodsaid IT-süsteeme ja aktiivseid võrgukomponente valdavad SNMPv3 samamoodi nagu võrguhalduse tarkvara. SNMPv3 konfigureerimisele tehtavad suuremad kulutused kompenseeritakse suurenenud turvalisusega.

Peamised eelised on järgmised:

- SNMP eeliseks on selle lihtsus ning seetõttu on ka selle juurutamine lihtne. Lihtsus vähendab vastuvõtlikkust vigadele ja suurendab protokolli stabiilsust.
- SNMP on väga laialt levinud ja seda võib pidada standardiks de facto . Seetõttu on peaaegu igal võrgu- ja süsteemitehnika tootel olemas SNMP tugi.
- Protokolli on võimalik muutuvate vajadustega väga kergelt kokku sobitada. Sellest tingituna, samuti eelpool nimetatud laia leviku tõttu, võib SNMPd pidada ka väga heade tulevikuväljavaadetega protokolliks (kindel investeering).
- Tegu on edastusvaldkonna jaoks loodud ühendusevaba ja lihtsa protokolliga. Seetõttu on SNMP-pakettide edastuse jõudlus võrgus suurem kui ühendustele orienteeritud CMIP puhul.

Peamised puudused on järgmised:

- SNMP kasutamine on seotud turvariskidega (SNMPv1 ja SNMPv2), mille tagajärjel võib ründajal olla sõltuvalt olukorrast võimalik koguda laialdasi andmeid nii süsteemi- kui ka võrgukeskkonna kohta. Võrgukomponentidele juurdepääsul puudub SNMP-l reaalne paroolkaitse, välja arvatud Community nimed, (mis võimaldavad SNMP-l moodustada rühmi ning pakuvad SNMPv1 ja SNMPv2 puhul algelist paroolkaitset).
- Tänu protokolli lihtsusele ja funktsioonide vähesele arvule esineb SNMP kasutamisel väga suurte või tugevasti laienevate võrkude puhul puudusi.
- Versiooni nr 1 jõudlusest jääb mahukate MIB-päringute korral väheks, kuna alati on tarvis ära näidata kogu MIB puu.

SNMP versiooni nr 1 suurimaks puuduseks on jälgitavate komponentide juurdepääsu autentimisfunktsiooni puudumine. Antud puudused on SNMP versioonis nr 2 osaliselt kõrvaldatud, lisaks on tõstetud ka MIB päringute jõudlust. SNMPv2 poolt toetatavate turvafunktsioonide puhul eksisteerib aga erinevaid variante. Võimalus sümmeetrilise kasutajapõhise autentimisfunktsiooni rakendamiseks tekib alles alates versioonidest SNMPv2* ja SNMPv2u, samal ajal kui versioon SNMPv2c on loodud jätkuvalt Community -te baasil. Community -t kasutatakse SNMP puhul ühelt poolt üksikute võrgukomponentide koondamiseks ning teiselt poolt paroolkaitsena võrgukomponentidele juurdepääsul. Alates versioonist SNMPv2* lisandub võimalus andmete krüpteerimiseks vastavalt Data Encryption Standard -ile, kasutades Cipher Block Chaining meetodit (DES-CBC). Kuna SNMPv2 eksisteerib erinevaid variante, on hetkel võrgukomponentide ja võrguhaldussüsteemide tootjate seas suur ebakindlus, mistõttu ei ole SNMPv2 alusel tehtud tooted veel väga laialt levinud ning nende koostalitlusvõime on samuti piiratud. Erinevad SNMPv2 variandid on koondatud SNMP järgmisse versiooni (SNMPv3).

Kontrollküsimused:

- Kas võrguhaldusega seotud turvanõuded on sõnastatud ja kirjalikult fikseeritud?
- Kas on kontrollitud võrgu aktiivkomponentide ja klientide ühilduvust vastavalt kas SNMP väljavalitud versiooni või CMIP suhtes?
- Kas algseadistusega Community -d on asendatud?
- Kas on loobutud vananenud võrguhaldusprotokollide SNMPv1 ja SNMPv2 kasutamisest?
- Kui vananenud võrguhaldusprotokollide kasutamine on tingimata vajalik, siis kas sellega kaasnevad riskid on dokumenteeritud?
- Kas community-nimed on muudetud, määratud individuaalselt võrguelementidele ja kas neid vahetatakse regulaarselt?
- Kas community-nimedega seotud pääsuõigused on piiratud absoluutselt hädavajaliku miinimumini?
- Kas juurdepääs võrguelementidele SNMP kaudu pääsuloendite abil on piiratud võrguhaldusjaamadega?

M 2.145 Nõuded võrguhaldusinstrumendile

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator

Võrgu efektiivse halduse tagamisel on palju abi võrguhaldusinstrumendist Võrguhalduse jaoks saadaolevate toodete valik on üsna lai, mistõttu tuleb enne konkreetse toote soetamist esmalt kontrollida selle sobivust, võttes aluseks eelkõige individuaalsed nõuded. Siinkohal on esmatähtis järgida vastavalt meetmele M 2.143 Võrguhalduse kontseptsiooni väljatöötamine kehtestatud turvanõuete täitmist ning arvestada ka järgnevate punktidega:

- Tootel peab olema väljavalitud võrguhaldusprotokolli tugi (vt M 2.144 Sobiva võrguhaldusprotokolli valimine).
- Toodet peab saama skaleerida, st toodet peab olema võimalik kohandada tulevastele nõuetele vastavaks.
- Tootel peab olema kõikide kohtvõrgus rakendatavate võrgukomponentide tugi.
- Tootel peab olema kõikide kohtvõrgus kasutatavate protokollide tugi.
- Toode peaks olema moodulite kaupa ülesehitatud, et ka tulevikus oleks võimalik uusi funktsioone ilma suurema vaevata olemasolevasse võrguhaldussüsteemi integreerida.
- Vajaliku info ülevaatlikuks ja arusaadavaks kuvamiseks peaks tootel olema graafiline kasutajaliides (Graphic User Interface, GUI).
- Kui lisaks muule kasutatakse ka süsteemihalduse tooteid, peaks olema võimalik neid „single point of administration“ kontseptsiooni alusel koos võrguhaldustoodetega ühe kasutajaliidese alla integreerida.
- Et võrguhaldussüsteem haldab võrgu konfiguratsiooni, peab see olema piisavalt kaitstud. Seetõttu peab juurdepääs olema piiratud ja see vajab samu miinimumnõudeid nagu administraatori pääsuõigused. Soovitatakse kahefaktorilist autentimist ja seda peaks toetama võrguhaldussüsteem.

Lisaks äsja loetletud üldistele nõuetele tuleb defineerida ka võrguhaldussüsteemile esitatavad funktsionaalsed nõuded. Järgnevad kriteeriumid püüavad luua ülevaadet hetkel saadaolevate toodete funktsioonidest, kuid tuleb arvestada, et mitte kõik funktsioonid ei ole kõikides toodetes esindatud. Enne kindla toote kasuks otsustamist tuleb seetõttu välja selgitada, millised funktsioonid on hädavajalikud ning milliseid funktsioone ei lähe tarvis:

- võrgu topoloogia kuvamine (nt koos võimalusega tagapõhjagraafika nagu ehitusjooniste jms kaasamiseks),
- topoloogia kuvamise erinevad valikuvõimalused,
- võrgu topograafiline kuvamine (nt koos võimalusega tagapõhjagraafika nagu ehitusjooniste jms kaasamiseks),
- võrgutopoloogia ja segmentimise automaatne tuvastamine ja kuvamine (Auto-Discovery),
- võrgu aktiivkomponentide konfiguratsioonide kuvamine pordi tasandil,
- jõudluse (performance) kuvamine pordi tasandil,
- võrgu aktiivkomponentide graafiline kuvamine,
- interaktiivne instrument haldusprotokolli tarbeks (nt MIB-brauser),

- lihtne navigeerimine võrguhaldusinstrumendi sees, nt zoom -funktsiooni või valitavate lõikude suurendamise abil,
- võimalus integreerida VLAN-haldajat koos VLAN-i graafilise kuvamisega,
- instrumendi kasutajaliidese intuitiivne kasutusvõimalus, eriti selle osa kus tegeletakse topoloogiliste, täpsemalt topograafiliste kuvapiltide monteerimisega (nt funktsioonid „Drag & Drop“),
- vigade ja rikketeadete kuvamine vabalt valitavate värvikoodide ja vabalt defineeritavate kriteeriumite alusel,
- jaotatud haldamise võimalus (Client/Server ja Manager-of-Manager) ning
- võimalus integreerida ja defineerida täiendavaid MIB-sid (Private-MIBs).

Kontrollküsimused:

- Kas kõik võrguhaldusinstrumendile seatud nõuded on sõnastatud ja dokumenteeritud?
- Kas vastava võrguhaldusinstrumendi abil on võimalik ellu viia võrguhalduskontseptsiooni?
- Kas on kindlaks määratud nõuded võrguhaldusinstrumendile?

M 2.146 Võrguhaldussüsteemi turvaline kasutamine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator

Võrguhaldusinstrumendi või ka keeruka võrguhaldussüsteemi, mis võib koosneda näiteks mitmest erinevast võrguhaldusinstrumendist, turvaliseks käitamiseks, tuleb kontrollida ja tagada, et kõikide komponentide konfiguratsioon oleks turvaline. Siia alla kuuluvad võrguhaldussüsteemi/ -süsteeme käitavad operatsioonisüsteemid, võrguhaldussüsteemi puhul enamikel juhtudel vajaminevad välised andmebaasid, rakendatav protokoll (vt M 2.144 Sobiva võrguhaldusprotokolli valimine) ning võrgu aktiivkomponendid. Enne võrguhaldussüsteemi kasutuselevõttu tuleb välja selgitada selle käitamisele esitatavad nõuded ja koostada vastav võrguhalduskontseptsioon (vt M 2.143 Võrguhalduse kontseptsiooni väljatöötamine). Eriti oluline on siinkohal arvestada järgnevate punktidega:

- Võrguhaldust puudutava informatsiooni volitamata lugemise ja muutmise takistamiseks peab vastav arvuti, mille peal võrguhalduse konsooli käitatakse, olema piisavalt kaitstud. Kaitsemeetmete alla kuuluvad näiteks arvuti ülesseadmine spetsiaalsetele turvanõuetele vastavasse ruumi, ekraanilukkude kasutamine, võrguhalduskonsooli paroolkaitse ning muud, sõltuvalt rakendatava operatsioonisüsteemi isesäradest tulenevad turvanõuded.
- Turvalise käitamise raames tuleks tähelepanu pöörata ka meetmele M 2.144 Sobiva võrguhaldusprotokolli valimine . Haldusandmebaaside (MIB) ja muu informatsiooni volitamata lugemise tõkestamisel on kõige olulisemaks meetmeks võrgu aktiivkomponentide õige konfigureerimine, mis lähtub kasutatavast protokollist (vt M 4.80 Kaug-võrguhalduse turvalised pääsumehhanismid ja M 4.82 Võrgu aktiivkomponentide turvaline konfigureerimine).
- Kui võrguhalduse funktsioone teostatakse detsentraliseeritud kujul, nt klient/server-mudeli või X-Window-tehnoloogia alusel, tuleb tagada ka nende turvaline käitus.
- Volitamata muudatuste varajaseks tuvastamiseks tuleb regulaarsete ajavahemike tagant läbi viia kasutatava tarkvara tervikluse kontrollid.
- Võrguhaldussüsteemi tuleb testida, et selgitada välja selle käitumine võimaliku krahhi puhul. Eriti oluline on siinkohal automaatse taaskäivituse võimalus, et ajavahemik, mille vältel on kohtvõrk seire alt väljas, oleks võimalikult lühike. Süsteemi krahh ei tohi põhjustada võrguhalduse andmebaasi kahjustumist ning taaskäivituse puhul peab see olema kättesaadav, kuna andmebaasis olevad konfiguratsiooniandmed on käitamisel määrava tähtsusega. Vastavaid andmeid tuleb seetõttu eriti hoolikalt kaitsta, et need oleksid ühelt poolt alati kättesaadavad ning aitaksid teiselt poolt vältida vananenud või vigaste konfiguratsiooniandmete kasutamist taaskäivitustel, mis võivad olla ründaja poolt tahtlikult saboteerimiseks esile kutsutud. Kasutatava andmebaasi kaitsmisel võib sõltuvalt olukorrast abi olla ka moodulist B 5.7 Andmebaasid .
- Varundatud andmebaaside uuesti sisselugemisel tuleb pöörata tähelepanu sellele, et võrguhaldussüsteemi turvaliseks käitamiseks vajaminevad failid

nagu näiteks reaalselt kasutatavate võrgukomponentide konfiguratsioonifailid, paroolifailid, samuti metakonfiguratsioonifailid oleksid alati olemas kõige värskemal kujul.

- Võrguhaldussüsteemi turvaliseks käitamiseks on olulised järgmised failid:
- Võrguhaldussüsteemi konfiguratsioonifailid, mis peavad asetsema sobilikul moel kaitstavates kaustades.
- Võrgukomponentide konfiguratsioonifailid (metakonfiguratsioonifailid), mis peavad samuti asetsema sobilikul moel kaitstavates kaustades.
- Võrguhaldussüsteemi paroolifailid. Siinkohal tuleb näiteks tähelepanu pöörata paroolide sobivusele ja võimalusele salvestada paroole krüpteeritud kujul (vt M 2.11 Paroolide kasutamise reeglid).
- Kui võrguhaldust puudutava informatsiooni konfidentsiaalsust ja terviklust puudutavaid nõudeid ei suudeta täita, tuleb võrgu kaudu võrgu aktiivkomponentide haldamist piirata ja tegeleda haldamisega kohapealsete liideste abil. Sellisel juhul tuleb tsentraliseeritud võrguhaldusest loobuda.

Täiendavad kontrollküsimused:

- Kas võrguhaldussüsteemi või võrguhalduse instrumendi paroolide kasutamise kohta on kehtestatud vastavad reeglid?
- Kas võrguhaldussüsteem toetab vajalikke turvameetmeid?

M 2.154 Viirusetõrje kontseptsiooni loomine

Algatamise eest vastutavad: IT-juht, IT turvaosakond

Rakendamise eest vastutavad: IT turvaosakond

Saavutamaks terve organisatsiooni ulatuses efektiivset arvutiviirustevastast kaitset, tuleb välja valida ja rakendada sobilikud kaitsemeetmed. Kõigi asjassepuutuvate IT-süsteemide kaasamine, nende varustamine sobilike kaitseabinõudega ja värskendamine, mille eesmärk on hädavajaliku kaitse tagamine, eeldab kontseptsioonilist lähenemist. Alljärgnevalt on välja toodud viirusetõrje kontseptsiooni näitlik sisukord.

Viirusetõrje kontseptsioon

Osa A. Teadlikkuse tõstmine

- 1 Institutsiooni sõltuvus IT kasutamisest
- 2 Ohupotentsiaali kirjeldamine
- 2.1 Viirused
- 2.2 Makroviirused
- 2.3 Trooja hobused
- 2.4 Pettemeilid
- 3 Kahjude stsenaariumid
- 4 Ohupotentsiaaliga IT-süsteemid

Osa B. Vajalikud kaitsemeetmed

- 5 Viirusetõrje strateegia
- 5.1 Võrguühenduseta IT-süsteemid
- 5.2 Võrguühendusega lõppseadmed
- 5.3 Server
- 6 Viirusetõrjetarkvara värskendamine
- 6.1 Võrguühenduseta IT-süsteemid
- 6.2 Võrguühendusega lõppseadmed
- 6.3 Server

Osa C. Reeglid

- 7 Viirusekaitsealane reeglistik
- 7.1 Aktsepteerimata tarkvara kasutuse keeld
- 7.2 IT-kasutajate koolitused
- 7.3 Buutimisjärjekorra muutmine
- 7.4 Avariidisketi loomine
- 7.5 Käitumisreeglid arvutiviiruse esinemisel
- 7.6 Meetmed mittelokaalselt toimiva viiruste kontrolliga IT-süsteemide puhuks
- 7.6.1 Viirusetõrjetarkvara regulaarne kasutamine
- 7.6.2 Andmekandjate ja andmeedastuse viirusekontroll

- 7.6.3 Laekuvate failide kontrollimine makroviiruste suhtes
- 8 Vastutusala reguleerimine
- 8.1 Arvutiviiruste kontaktisik
- 8.2 Administraatorite vastutusala
- 8.3 Iga üksiku IT-kasutaja vastutusala
- 8.4 IT turvahalduse vastutusala

Osa D. Abivahendid

- 10 Käitumisreeglid arvutiviiruse esinemisel
- 11 Arvutiviirusest teatamise protseduurid
- 12 Viirusetõrjetarkvara kasutamise käsiraamat

Alljärgnevalt esitletud meetmetega püütakse seletada, kuidas võiks teatud tähtsamaid kontseptsiooniosi välja töötada.

Kontrollküsimused:

- Kas turvaosakond on viirusetõrje kontseptsiooni ellu viinud?
- Kas viirusetõrje kontseptsioon on kõigile osapooltele teada?

M 2.155 Potentsiaalselt viiruste poolt ohustatud IT-süsteemide tuvastamine

Algatamise eest vastutavad: IT-juht, IT turvaosakond

Rakendamise eest vastutavad: IT-juht

Viirusetõrje kontseptsiooni loomisel tuleks esimese sammuna tuvastada kõik ametkonna/institutsiooni potentsiaalselt viiruste poolt ohustatud IT-süsteemid. Tuvastamiseks võiks kasutada kõikide kasutuses olevate või plaanitavate IT-süsteemide loetelu, mis peaks aitama välja filtreerida neid süsteeme, mida arvutiviirused võivad ohustada ja ka neid, mille kaudu võivad arvutiviirused hakata levima. Tüüpilised näited arvutiviiruste ohustatud IT-süsteemidest on kõik süsteemid, mis töötavad PC-baasil loodud operatsioonisüsteemidega, nagu DOS või Windows 3.x, 95/98, või IT-süsteemid, mille rakendusprogrammide hulka kuuluvad nt Microsoft Word või Excel, sest viimased võivad nakatuda makroviirustega. Serverid ei ole üldjuhul arvutiviiruste poolt otseselt ohustatud, kuid need võivad muutuda allikaks, mille kaudu hakkavad nakatunud programmid ja failid levima. Arvutiviiruste esinemist ei saa välistada ka teiste operatsioonisüsteemide või IT-rakendusprogrammide kasutamisel. See kehtib näiteks mõningatel üksikutel juhtudel Unix-süsteemide ja OS/2-süsteemide puhul, kuid oma vähese leviku tõttu on nende ohupotentsiaal siiski väike (vt G 5.23 Pahavara). Järgmise sammuna võib iga nakatunud IT-süsteemi kohta täiendavalt kokku võtta, millised on võimalikud kanalid, mille kaudu võib viirustesse nakatumine toimuda. Seda infot saab kasutada hiljem võimalike vastuabinõude valiku tegemisel.

Arvutiviirustesse nakatumise põhjused võivad olla näiteks järgmised:

- diskettide, CD-ROMide või muude vahetatavate andmekandjate kasutamine,
- uue tarkvara installeerimine,
- ligipääs andmetele, mis on salvestatud mitte lokaalsele kõvakettale, vaid võrgus olevale serverile või failivahetusvõrgus ühiskasutusse antud kausta,
- ligipääs väljastpoolt võrku saadud failidele (nt e-kirja manus, internetist laetavad failid),
- väljastpoolt tellitud hooldustööd.

Mõistlik oleks kas iga IDga varustatud IT-süsteemi või vähemalt näitena iga identifitseeritava IT-süsteemi tüübi kohta koostada kokkuvõtlik tabel võimalike liideste kohta, mille kaudu on võimalik süsteemi nakatumine viirustega.

Siia alla võivad kuuluda järgmised:

- kõik arvutite juures kohapeal olemasolevad, vahetatavate andmekandjate lugemiseks mõeldud seadmed (disketilugejad, CD-ROMi lugejad, striimerid, vahetatavad plaadid jms),
- kõik kohapeal arvutite külge ühendatavad mobiilsed, vahetatavate andmekandjate lugemiseks mõeldud lugemisseadmed (disketilugejad, CD-ROMi lugejad, striimerid, vahetatavad plaadid jms),
- ühenduse loomine teiste IT-süsteemidega oma turvaalas (kohtvõrguserverid, failivahetusvõrgu ühendused),

- liidesed, mille kaudu on võimalik andmete edastamine väljaspool asuvast IT-süsteemist kohapeal asuvasse IT-süsteemi (modem, internetiühendus).

Kõige olulisem on ülevaate koostamisel määrata kindlaks vastavate IT-süsteemide kontaktisikud, kelle poole saavad kasutajad oma probleemidega pöörduda ja kes peavad vastutama hädavajalike kaitsemeetmete elluviimise eest. Kuna ühe organisatsiooni IT-kooslus võib olla pidevas muutumises, tuleb võimalike muutuste korral vastavat informatsiooni selle aegumise vältimiseks vajaduse korral täiendada.

Näide informatsiooni kogumisest:

Olemasolevad ja planeeritavad IT-süsteemid / liidesed
Nimetus ja tüüp
lokaalse võrgu-ühendusega
lokaalsed lugemis-seadmed
välised lugemis-seadmed
sidekaardid
kontaktisik viiruseprobleemide korral
Server osak. X,
Novell 4
x
disketi-lugeja, CD-ROMi lugeja
striimer
modem
administraator Tamm
Kliendid osak. X
Windows 95
x
disketi-lugeja, CD-ROMi lugeja
PC-tugiisik Kask
Sülearvutid,
Windows NT
disketi-lugeja
sülearvutite haldaja Remmelgas
Serverid osakond nr XI,
Unix
x
disketi-lugeja, CD-ROMi lugeja
striimer
administraator Kikerpuu
Tööjaamad osakond nr XI
Unix
x
-
Büroo PC-d
Windows 95
x
proua Kadakas
. . .
. . .

. . .
. . .
. . .
Tabel. Olemasolevad ja plaanitavad liidesed
Täiendav kontrollküsimus:

- Kuidas tagatakse kasutatavate IT-süsteemide muutuste või uute IT-süsteemide kasutuselevõtu korral piisav arvestamine viirusetõrje kontseptsiooni vajalike meetmetega?

M 2.156 Sobiva viirusetõrjestrateegia valimine

Algatamise eest vastutavad: IT-juht, IT turvaosakond

Rakendamise eest vastutavad: IT-juht

Viirusekaitse elluviimiseks läheb tarvis nii personali- kui ka finantsressursse, mis peavad jääma sobivasse vahekorda tegeliku ohupotentsiaaliga. Kõigi identifitseeritavate, potentsiaalselt arvutiviiruste poolt ohustatud IT-süsteemide puhul tuleb uurida järgmisi mõjureid:

- Kui tihti leiab olemasolevate liideste kaudu aset andmevahetus, millega võiks kaasneda nakatumine või arvutiviiruste levik?
- Milliste tagajärgedega tuleb reaalse nakatumise puhul arvestada, kui viirusetõrjemeetmeid ei ole üldse võetud?
- Kui kindel on perioodilise täidesaatmiskohustusega IT turvameetmete rakendamine IT-kasutajate poolt?
- Kui suur on hinnanguline ajahulk, mida IT-kasutajad võiksid oma tööajast rakendada arvutiviiruste kaitsemehhanismide kasutamisele?

Eelnimetatud mõjurite analüüsist ja erialaväljaannetest saadud info põhjal arvutiviiruste esinemissageduse ja nende põhjustatud tagajärgede kohta tuleb koostöös IT turvaosakonnaga otsustada, kui suuri finantsressursse läheb tarvis vajalike kaitsemeetmete võtmiseks ning kui suurt personaliressurssi vastav ettevõtmine eeldab. Teades viirusetõrje rakendamiseks vajaminevat finantspoolt ja personaliressurssi ning omades ülevaadet identifitseeritavate, potentsiaalse ohu alla langevate IT-süsteemide kohta, saab välja valida strateegia, mis aitaks kõige paremini jõuda soovitud lõpptulemuseni. Järgnevalt esitletakse mõningaid võimalikke strateegiaid.

Viirusetõrjetarkvara igas lõppseadmes

Nakatunud programmide käivitamist või makroviirusesse nakatunud faili avamist on võimalik vältida seeläbi, et IT-süsteemis kasutatakse kogu aeg värsket residentset viirusetõrjetarkvara (st programmi, mis töötab kogu aeg taustal). Lõppseadme liideste kontrollimise võtab enda kanda lõppseadmele installeeritud residentne viirusetõrjetarkvara. Seeläbi välditakse viiruste kandumist IT-süsteemi. Ainult mitteresidentsete viirusetõrjeprogrammide (programmid, mida peavad käivitama kasutajad ise) kasutamine ei ole soovitatav, kuna nendega ei kaasne kulutustega seoses märkimisväärseid eeliseid, kuid seevastu IT-kasutajale tekitab vastav olukord aina enam probleeme, kuna programmi regulaarne kohustuslik käivitamine on jäetud kasutaja hooleks. Varustades kõik lõppseadmed residentse viirusetõrjetarkvaraga, tagatakse viiruste tuvastamine kohe nende tekkimisel ning nende leviku tõkestamine. Lisaks eelnevale peaks igal kliendil olema võimalik viirusetõrjetarkvara ka iseseisvalt käivitada, et kontrollida erinevaid objekte, näiteks e-kirja manuseid vajaduse korral enne avamist teadlikult.

Eelised:

- Sobiv ajakohane ja residentselt töötav viirusetõrjetarkvara pakub maksimaalset kaitset ning IT-kasutaja kohustused sellega seoses on minimaalsed.

Puudused:

- Iga konkreetse lõppseadmega on seotud vastav haldamiskulu ja programmi soetamiskulu.
- Vanematel IT-süsteemidel ei pruugi olla piisaval hulgal vajalikku põhimälu. Lisaks võib tekkida ka probleeme koostöös teiste programmidega.

Viirusetõrjetarkvara kõikides väliste liidestega varustatud lõppseadmetes

Võrku ühendatud IT-süsteemide puhul installeeritakse viirusetõrjetarkvara ainult nendele IT-süsteemidele, millel on lisaks oma võrguliidestele olemas veel ka täiendavad välised liidesed (disketilugeja, CD-ROM-i lugeja, modem). Võrguühendusega

IT-süsteeme, millel puuduvad otsesed välised liidesed, ei varustata viirusetõrjetarkvaraga.

Eelised:

- Soetamiskulud ja haldamisega seotud kulutused piirduvad väliseid liideseid omavate IT-süsteemidega.

Puudused:

- IT-süsteemide muudatusi, mis võivad endaga kaasa tuua uute väliste liidestе lisandumise, tuleb käsitleda piinliku täpsusega, kuna olenevalt olukorrast võib vastavaid IT-süsteeme olla tarvis täiendada ka sobiliku viirusetõrjetarkvaraga.
- Krüpteeritud failid või programmid, mis sisaldavad arvutiviirusi ning mille lahtikrüpteerimine toimub kaitseta lõppseadmes, toovad endaga kaasa nakatumise. Eelnev lause kehtib ka kokkupakitud failide kohta juhul, kui kasutatav viirusetõrjetarkvara osutub ebasobivaks.

Viirusetõrjetarkvara kõikidel serveritel

Sellisel juhul varustatakse residentselt töötava viirusetõrjetarkvaraga kõik IT-võrgus olevad serverid, kuid mitte võrku ühendatud lõppseadmed. Seeläbi tagatakse, et arvutiviirused ei saa ühelt lõppseadmelt teistele lõppseadmetele üle kanduda ning et võimalik viirusesse nakatumine jääb lokaalselt isoleerituks.

Eelised:

- Soetamiskulud ja haldamisega seotud kulud piirduvad serveritega.
- Serverite kaitsmine aitab vältida nakatumiste taasteket, nt arhiveeritud andmete lugemise korral.

Puudused:

- Väliste liidestega varustatud lõppseadmetes peab IT-kasutaja välistel andmekandjatel oleva info, aga ka edasisaadetavate andmekandjate ja failide kontrollimiseks käivitama serveril asuva viirusetõrjetarkvara käsitsi.
- Krüpteeritud failid ja programmid, mis sisaldavad arvutiviirusi ning mille lahtikrüpteerimine toimub kaitseta lõppseadmes, viivad sisenemiskontrolli puudumisel paratamatult nakatumiseni. Eelnev lause kehtib ka kokkupakitud failide kohta juhul, kui kasutatav viirusetõrjetarkvara osutub ebasobivaks.

- Väliste liidestega varustatud lõppseadme nakatumist viirustega ei ole võimalik välistada.
- Kui failivahetuseks kasutatakse täiendavalt ka võrdvõrgu funktsioone, on arvutiviirustel võimalik lõppseadmete vahel levida, ilma et kaitstud serverid seda kontrolliks.
- Negatiivne mõju jõudlusele, kuna kogu andmeedastuse sisu vajab läbikontrollimist.

Viirusetõrjetarkvara kõigil serveritel ja lõppseadmetel

Eelpool loetletud strateegiate kombinatsioon pakub maksimaalset kaitset, kuna arvutiviiruste tuvastamine toimub kohe nende ilmnemisel ja nende levik erinevate serverite kaudu on tõkestatud. Lisaks on võimalik kasutada erinevate tootjate viirusetõrjetarkvara, mis aitab veelgi tõsta arvutiviiruste tuvastamise tõenäosusprotsenti.

Eelised:

- Sobilik, ajakohane ja residentselt töötav viirusetõrjetarkvara pakub maksimaalset kaitset ning on IT-kasutaja jaoks seotud kõige väiksema töömahuga.
- Arvutiviiruste levik serverite kaudu on tõkestatud.

Puudused:

- Iga eraldi serveri ja lõppseadmega on seotud vastavad soetamiskulud, samuti vajavad kõik seadmed haldamist.

Viirusetõrjetarkvara kõigil kommunikatsiooniserveritel

Kommunikatsiooniserveritele võib viirusetõrjetarkvara installeerida ainsa või ka täiendava kaitsemeetmena. Kommunikatsiooniserverid on IT-süsteemid, mille kaudu toimub andmevahetus väljaspool asuvate IT-süsteemidega, nt tulemüüride või meiliserveritega. Selle lahenduse korral on lõppseadmed arvutiviiruste vastu kaitstud vaid juhul, kui lõppseadmetes puuduvad täiendavad liidesed, nagu CD-ROMi lugejad vms.

Eelised:

- Kõiki andmeid kontrollitakse kohtvõrku sisenemisel, mitte alles kohtvõrgus sees olles.
- Arvutiviiruste levik serverite kaudu on tõkestatud. Sellele vaatamata võib viiruste levik toimuda lõppseadmete vahendusel, kui faile transporditakse nende vahel otse (nt diskettidega).

Puudused:

- Nimetatud meetod on vastuvõtlik vigadele. Teatud osa e-kirjade manustest võib jääda tuvastamata. Vastavad programmid kontrollivad tihti e-kirjade manuste olemasolu ainult meili esimestest ridadest, st e-kirja päises. Võib esineda olukordi, kus viirusetõrjetarkvaral puudub e-kirja manust töödelnud kodeerimismeetodi (nt uuencode) tugi. Probleeme võib tekkida näiteks MIME

kasutamise puhul, kui meilikehasse soovitakse lihtsal moel kaasata ühte või mitut uuencode meetodi abil kodeeritud faili.
- Negatiivne mõju jõudlusele, kuna kogu andmeedastuse sisu vajab läbikontrollimist.
- Kõigil kommunikatsiooniserveritel peaks olema installeeritud vaid minimaalne operatsioonisüsteem, st ainult hädavajalikud teenused (vt M 4.95 Minimaalne operatsioonisüsteem).
- Teenusetõkestusrünnete vältimiseks peaks viirusetõrjetarkvara olema installeeritud ainult tulemüürile, äärmisel juhul proksile.

Andmepuhtus ja failide tsentraliseeritud kontrollimine

Selle lahenduse korral kontrollitakse kõiki sisenevaid ja väljuvaid faile ja andmekandjaid vastava viirusetõrjetarkvara abil ühest tsentraalsest kohast. Lisaks sellele kehtestatakse reeglid, mis keelavad IT-kasutajatel avada faile või programme, mille päritolus nad ei ole kindlad.

Eelised:

- Viirusetõrjeprogrammide litsentside ostmiseks tehtavad kulutused vähenevad, kuna litsentside arv kahaneb märgatavalt.

Puudused:

- Väliste andmekandjate sagedasel kasutamisel kulub arvutiviiruste tsentraliseeritud kontrollimiseks väga palju aega, mis omakorda venitab organisatsiooni tööprotsesse. Arvutiviirustesse nakatumist ei ole võimalik välistada, kuna mõne andmekandja kontrollimine võib kogemata ununeda.
- Kõiki arvuteid, millel ei ole viirusetõrjetarkvara, tuleb regulaarsete ajavahemike tagant kontrollida, et tuvastada nende võimalik nakatumine.

Sõltumata sellest, milline strateegia arvutiviirustevastaseks tõrjeks valitakse, tuleb alati arvestada võimaliku jääkohuga, et viirusetõrjetarkvara suudab tuvastada vaid neid viiruseid, mis olid vastava tarkvara väljatöötamise ajal teada. See tähendab, et viirusetõrjetarkvara ei pruugi uusi viiruseid ära tunda ning viiruste tekitatavat kahju ei õnnestu vältida. Õige ning kulutuste poolest mõistliku viirusetõrjestrateegia valik sõltub igast konkreetsest IT-kooslusest. Kuna enamike laialdasemalt levinud viirusetõrjetarkvarade litsentside ostul langeb hind koguse suurenedes üsnagi märgatavalt, tasuks kaaluda kõikide serverite ja lõppseadmete varustamist vajaliku viirusetõrjetarkvaraga.

Kontrollküsimused:

- Kas varasema kasutuse käigus on esinenud arvutiviiruseid? Millised olid arvutiviiruste tekitatud kahjud (rahaline kahju, tööseisak, . . .)?
- Kas viirusetõrjeks vajaminevate ressursside kasutamise kohta vastuvõetud otsuste eest vastutab juhatus?
- Kas IT-koosluse muutumise korral on tagatud, et toimub ka viirusetõrjet puudutava strateegia vastav ümbertöötamine?

- Kas viirusetõrjeks valitud strateegia kitsaskohti on IT turvaosakonnale piisavalt selgitatud?
- Kas ollakse valmis võimalikeks jääkohtudeks?

M 2.157 Sobiva viiruseskanneri valimine

Algatamise eest vastutavad: IT-juht, IT turvaosakond

Rakendamise eest vastutavad: IT-juht

Väljavalitav viirusetõrjetarkvara peaks üldjuhul täitma järgmisi kriteeriume:

- Programm peaks suutma tuvastada võimalikult palju erinevaid arvutiviiruseid ning peaks olema võimalikult ajakohane, eriti oluline on võime tuvastada kõiki väga laialt levinud arvutiviiruseid.
- Programmi tootja peab tagama viirusetõrjetarkvara pideva värskendamise seoses uute viirustega.
- Programm peaks suutma tuvastada arvutiviiruseid ka kokkupakitud kujul, samuti peaks see toetama enamlevinud pakkimisfunktsioone, nagu nt PKZIP.
- Programm peab näitama tuvastatud arvutiviiruseid koos täieliku informatsiooniga nende raja (path) kohta.
- Programm peab suutma enne viiruseotsingu funktsiooni käivitamist tuvastada, kas ta ise on viirustest vaba.
- Võimaluse korral peaks residentselt töötaval programmil olema võimalus permanentse viirusetõrje funktsiooni rakendamiseks.
- Mõistlik oleks funktsioon, mis lubab tuvastatud arvutiviiruseid kõrvaldada ilma, et seeläbi tekiks programmides või failides täiendavaid kahjustusi.
- Programm peaks suutma kuvada hoiatavat teadet, kui on tuvastanud, et värskendus on jäänud tegemata (süsteemi kuupäeva ja programmi värskendamise vahele on jäänud rohkem kui 6 kuud).
- Programm peaks sisaldama nimekirja arvutiviirustest ja nende kirjeldustest, mida see on võimeline tuvastama. Lisaks sellele peaks programm kuvama probleemide kiirlahenduste ja arvutiviiruste kõrvaldamise meetmekirjeldusi.

Programmil peaks olema logifunktsioon, mis salvestab järgnevat infot:

1. programmi versioon,
2. teostatud kontrolli kuupäev ja kellaaeg,
3. info kõikide kasutatud parameetrite kohta,
4. kontrolli tulemus ja selle ulatus,
5. kontrolli alt välja jäänud failide ja objektide arv ning ID.

M 2.158 Viirusnakkustest teatamine

Algatamise eest vastutavad: IT-juht, IT turvaosakond

Rakendamise eest vastutavad: IT-juht

Arvutiviiruste esinemisel tuleb eelisjärjekorras takistada nende levikut teistele IT-süsteemidele. Selleks tuleb institutsiooni sees kindlaks määrata kontaktisik, kellele tuleb arvutiviiruste tuvastamisel olukorrast viivitamata teada anda. Kindlaksmääratud kontaktisik saab meetmes M 2.155 Potentsiaalselt viiruste poolt ohustatud IT-süsteemide tuvastamine kirjeldatud dokumentide kohaselt kiirelt otsustada, milliseid kasutajaid tuleb vajaduse korral arvutiviirusest teavitada. Organisatsioonisisese teavitamisprotseduuri raames tuleb kindlaks määrata ka protseduurid, mille alusel toimub teavitamine väljaspool organisatsiooni. Lisaks oma töötajatele tuleb olukorrast teavitada ka organisatsioonivälised osapooli, kes on viirustesse nakatumisest potentsiaalselt ohustatud. Siia alla kuuluvad eriti need osapooled, kes võivad viirust levitada või vastu võtta enesele teadmata.

Kindlaksmääratud kontaktisikute kaudu tuleb korraldada ka nende abinõude rakendamine, mis peavad tagama tuvastatud arvutiviiruste kõrvaldamise. Vastavate isikute ülesandeks jääb muu hulgas ka kõikide nakatumise kaasa toonud arvutiviiruste, nende tagajärgede ja kõrvaldamise dokumenteerimine. Kirjapandud informatsioon on aluseks viirusetõrje kontseptsiooni värskendamisele, samuti kahjude ning kahjude likvideerimiseks vaja läinud tegevuste dokumenteerimisele.

Arvutiviirustest teavitamise protseduuri kehtestamiseks tuleb kõiki töötajaid teavitada sobival moel vastavatest kontaktisikutest. Töötajate informeerimiseks võib koostada näiteks infolehe (vt M 6.23 Käitumisreeglid arvutiviiruste esinemisel).

Õigete kontaktisikute teavitamine turvaintsidentide kahtluse korral on eriti oluline pettemeilide (vt G 5.80 Pettemeilid) puhul, et asjaga saaksid tegeleda viiruste eripäraga tuttavad inimesed ning et töötajad ei hakkaks neid levitama. Vastav kontaktisik peab ennast regulaarselt uute viirustega kursis hoidma, et vajaduse korral kas olemasolevat viirusetõrjetarkvara värskendada või teavitada turvaintsidendi korral asjassepuutuvaid osapooli.

Kontrollküsimused:

- Kas on tagatud, et kõigile IT-kasutajatele on teada nende kontaktisikud, kelle poole tuleb pöörduda arvutiviiruste esinemise korral?
- Kas on tagatud, et arvutiviiruste kontaktisik saab võimalikult kiiresti teavitada kõiki potentsiaalselt arvutiviiruse ohustatud osapooli?

M 2.159 Viiruseskanneri värskendamine

Algatamise eest vastutavad: IT-juht, IT turvaosakond

Rakendamise eest vastutavad: IT-juht

Viiruseskanneri usaldusväärsuse kindlustamiseks tuleb IT-süsteemidele paigaldatud viirusetõrjetarkvara regulaarselt värskendada, et programmid suudaksid tuvastada ka uusi, aina juurde tekkivaid arvutiviirusi. Värskendamise toimimiseks tuleb kindlaks määrata isikud, kes vastutavad täiendite hankimise ja levitamise eest. Viiruseskanneri värskendamisele lühikeste ajavahemike tagant (mitte harvemini kui iga kuue kuu tagant) tuleks mõelda juba sobiva viiruseskanneri soetamisel (vt M 2.157 Sobiva viiruseskanneri valimine). Kuna viiruseskannerite programme uuendatakse erinevatel aegadel, olenevalt olukorrast, nt uute viiruste avastamise tagajärjel, peaks arvutiviiruste tõkestamise eest vastutav töötaja regulaarselt (vähemalt kord nädalas) uurima, kas programmi tootja on väljastanud uut informatsiooni.

Viirusetõrjetarkvara täiendite levitamisel peab olema tagatud, et vastavad täiendid paigaldataks IT-süsteemidele ka reaalselt, võimalikult kiiresti pärast täiendite saabumist. Kui paigaldamine ei toimu automaatselt (võrguühendusega IT-süsteemid), tuleks täiendid teha vastavatele IT-kasutajatele võimalikult kiiresti kättesaadavaks.

Kuna viirusetõrjetarkvara täiendatakse pidevalt, jääb selle testimisele kulutatav aeg reeglina lühikeseks, mistõttu on need küllaltki vastuvõtlikud erinevatele vigadele. Seepärast tuleks enne viiruseskannerite kasutamise kinnitamist ja installeerimist neid praktikas testida (vt lisaks M 2.83 Tüüptarkvara testimine). Täiendite installeerimise käigus on tähtis jälgida, et täiendite algseadistuse parameetrid ei muudaks viiruseskanneri olemasolevat konfiguratsiooni. Näiteks võib juhtuda, et täiendite installeerimise käigus lülitatakse eelnevalt residentselt töötanud viirusetõrjeprogramm ümber hoopis vallasrežiimile. Lisaks tuleb hoolitseda ka selle eest, et mitte ühegi kindla töötajaga seotud ning ilma võrguühenduseta arvutid, nagu nt sülearvutid, varustataks vajalike täienditega.

Kontrollküsimused:

- Kas täiendite jagamiseks mõeldud duplikaatide puhul on võimalik tõestada, et need loodi viirustest puutumata IT-süsteemi abil?
- Kui kaua võtab aega täiendite paigaldamine kõikidele IT-süsteemidele?
- Kas täiendite paigaldamist kontrollitakse pisteliselt?

M 2.160 Viirusetõrje eeskirjad

Algatamise eest vastutavad: IT-juht, IT turvaosakond

Rakendamise eest vastutavad: IT-juht

Efektiivse viirusetõrje saavutamiseks tuleb lisaks viirusetõrjetarkvarale võtta ka mõningaid lisameetmeid. Vastavate meetmete alla kuuluvad muu hulgas järgmised:

Viiruseskannerite kasutamine

Viirusetõrje strateegia ja seda toetava tarkvaraprogrammi valiku kohta tuleb langetada otsus ning see dokumenteerida (vt M 2.156 Sobiva viirusetõrjestrateegia valimine ja M 2.157 Sobiva viiruseskanneri valimine). Lisaks tuleb nimetada isikud, kes peavad kindlaksmääratud ajavahemike tagant viirusetõrjetarkvara värskendama (vt M 2.159 Viiruseskanneri värskendamine).

IT-kasutajate koolitused

IT-kasutajatele tuleb tutvustada ohte, mida võivad põhjustada arvutiviirused, makroviirused, Trooja hobused ja pettemeilid (vt G 5.21 Trooja hobused, G 5.23 Pahavara, G 5.43 Makroviirused ja G 5.80 Pettemeilid), samuti tuleb töötajaid koolitada, kuidas kasutada hädavajalikke IT turvameetmeid, kuidas käituda arvutiviiruste esinemise korral ning kuidas viirusetõrjetarkvara õigesti kasutada (vt M 3.4 Väljaõpe enne programmi tegelikku kasutamist , M 3.5 Turvameetmete koolitus ja M 6.23 Käitumisreeglid arvutiviiruste esinemisel).

Aktsepteerimata tarkvara kasutuse keeld

Aktsepteerimata, eriti viirustega seoses kontrollimata tarkvara installeerimine ja kasutamine tuleb keelata (vt M 2.9 Aktsepteerimata riist- ja tarkvara kasutuse keeld). Lisaks tuleb vajaduse korral reguleerida ka see, milliste ajavahemike tagant vastava keelu täitmist regulaarselt kontrollitakse (vt M 2.10 Riistvara ja tarkvara inventuur).

IT-süsteemi turvameetmed

Operatsioonisüsteemi käivitamise buutimisjärjekorda tuleb muuta selliselt, et andmeid loetaks esimesena kõvakettalt (või võrgust) ning alles seejärel mõnelt väliselt andmekandjalt (disketilt, CD-ROMilt) (vrd M 4.84 BIOSi turvamehhanismide kasutamine). Lisaks tuleb iga arvuti tüübi kohta koostada avariidiskett, mis peab aitama arvutiviirustesse nakatumise korral süsteemi edukalt puhastada (vt M 6.24 Rikkejärgse buutimismeedia olemasolu). Neil juhtudel, kus arvutiviirused on suutnud tekitada suuremat kahju, tuleb abi otsida andmevarundusest. Selleks otstarbeks tuleb andmeid regulaarselt varundada (vt M 6.32 Regulaarne andmevarundus). Varundatud andmete sisselugemisel tuleb jälgida, et andmete taastamise käigus ei avataks mõnda viirustest nakatunud faili.

Meetmed mitteresidentselt toimiva viirusetõrjega IT-süsteemide puhuks

Üldjuhul tuleks eelistada kõikide IT-süsteemide varustamist residentselt töötava viirusetõrjetarkvaraga. Arvutiviiruse kiireks tuvastamiseks ja leviku tõkestamiseks nendes IT-süsteemides, kus ei ole installeeritud residentselt töötavat viirusetõrjetarkvara, tuleb kindlaks määrata regulaarselt läbiviidav viiruseskanneri kasutamine (vt M 4.3 Viirusetõrjeprogrammide kasutamine) ning andmekandjate ja andmeedastuse kontrollimine (vt M 4.33 Viirustõrjeprogrammi kasutamine andmekandjate vahetamisel ja andmete edastamisel).

Viirusnakkustest teatamine

Tuleb määrata kindlaks isikud, kellele peab arvutiviiruste esinemise korral sellest viivitamata teatama. Samuti tuleb kindlaks määrata teavitamise vormiline külg (ankeet) ning informatsiooni edastamise viis (telefonitsi, isiklikult, kirjalikult, e-kirjaga) (vt M 2.158 Viirusnakkustest teatamine).

Vastutusala reguleerimine

Arvutiviirustevastase kaitse valdkonnas vajavad reguleerimist järgmised ülesanded, volitused ja kohustused:

- arvutiviirustest teavitamise kontaktisikud,
- võrguserverite administraator,
- lõppseadmete IT-kasutajad ning
- IT turvaosakond.

Viirusetõrje kontseptsiooni täiendamine

IT-süsteemide muudatuste, uute IT-süsteemide installeerimise ning võrgu muudatuste korral tuleb viirusetõrje kontseptsiooni täiendada ja viia see olukorraga vastavusse (vt M 2.34 IT-süsteemi muutuste dokumenteerimine). Seotud osapooli tuleb muudatustest teavitada. Tagamaks viirusetõrje kontseptsiooni läbivat rakendamist, tuleb reeglistikust kinnipidamist pisteliselt kontrollida.

Kontrollküsimused:

- Millal toimus viimane kontroll? Kas kontrolli tulemus fikseeriti kirjalikult?
- Kuidas toimub seotud osapoolte teavitamine olulistest reeglitest?

M 2.161 Krüptokontseptsiooni väljatöötamine

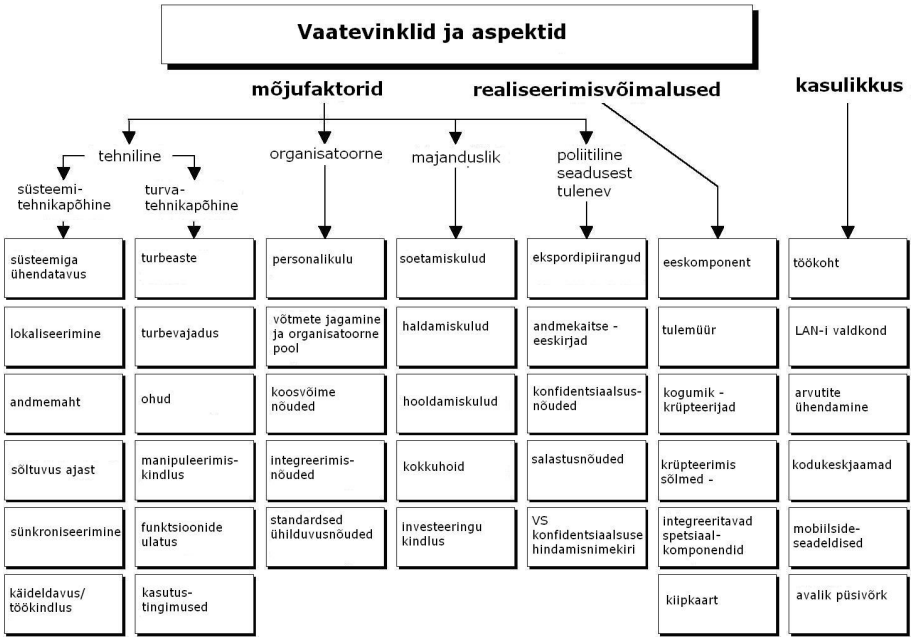
Algatamise eest vastutavad: IT turvaosakond

Rakendamise eest vastutavad: IT turvaosakond

Nii ettevõtted kui ka ametiasutused sõltuvad tänapäeval üha rohkem oma infotehnoloogilisest taristust. Sel põhjusel on terviksüsteemis tarvis rakendada turvafunktsioone, mis on palju keerukamad kui tavalised krüpteerimisvõimalused.

Krüptograafiliste probleemiasetuste rohkus ja võimalike mõjufaktorite paljusus on loonud ka mitmekesiseid lahendusi, mille abil saab vastavat turvet realiseerida. Siinkohal ei ole võimalik lähtuda printsiibist, et on olemas üks lahendus, mis suudab kõrvaldada kõik arvutivõrgus ja/või sidesüsteemides esilekerkivad turbeprobleemid. Piisava turbeastme saavutamiseks tuleb enamasti tegeleda omavahel kokkusobivate komponentide valimise ja nendevahelise koostöö loomisega. Seetõttu on tarvis välja töötada krüptokontseptsioon ning muuta see ametiasutuse või ettevõtte IT turbekontseptsiooni kindlaks koostisosaks.

Sobivate krüptograafiliste komponentide valik peaks toetuma vastavale krüptokontseptsioonile. Krüptokontseptsiooni üks kriitilisemaid elemente on võtmehaldus. Kontseptsioone ja lahendusi on võimalik edukalt välja töötada ja sihipäraselt ellu rakendada vaid juhul, kui eelnevalt on täpselt teada, milliseid spetsiaalseid turbefunktsioone, st teenuseid vaja läheb. Lisaks tuleb läbi töötada terve rida süsteemipõhiseid aspekte ja küsimusi, mis ei ole turbefunktsioonidega otseselt seotud. Siia alla kuuluvad näiteks jõudlusele, süsteemide ühendamisele või koostalitlusvõimele ning ühilduvusele seatud tüüpnõuded.



Joonis: vaatevinklid ja aspektid

Võrguühendusega IT taristutes ei piisa enam üheainsa domeeni turvalisuse tagamisest. Tarvis on tagada kõikide protsessis osalevate lõppseadmete ja ülekandesüsteemide turvalisus üksteise suhtes. Eri komponentide turvalisuse tagamine

üksteise suhtes muutub eriti keeruliseks neil juhtudel, kus ei ole tegu mitte ainult ühe võrguühendusega üksusega (nt kohtvõrgu keskkonnaga), vaid erinevate vastutus- ja rakendusaladega IT-installatsioonide kooslusega. IT turvet võimaldava süsteemi kasutamine, samuti selle funktsioonide valik ning tehnoloogiline lahendus sõltuvad paljudest mõjufaktoritest, nagu nt lokaliseerimisest, turbeastmest, rakenduse kasutussagedusest ja -ulatusest, mis seavad IT turvaosakonnale ette olulised raamtingimused vajalike otsuste tegemisel. Lisaks on ka IT turvet pakkuva süsteemi koostamise ja rakendamise tehnilised võimalused väga laialdased, nt töökohaarvuti rakendustesse integreeritud turbefunktsioonid, tulemüür või võrgukomponentide spetsiaalsed osad, nagu kommutaatorid või marsruuterid. Krüptotootele tehtavate kulutuste põhjendatust on võimalik tagada vaid seeläbi, kui toodet kasutatakse võimalikult läbivalt. Siinkohal mängivad tähtsat rolli näiteks standardne süsteemiühendusvõimalus, ühesugused kasutamistingimused jne. Viimane punkt puudutab turvateenuste koostöötamisvõimet erinevates protokollikihtides. Ülemiste protokollikihtide (OSI etalonmudeli järgi) pakutavad turvateenused kaitsevad reeglina piisavalt vaid siis, kui ka alumised kihid suudavad pakkuda vastavat kaitset (vt M 4.90w Krüptoprotseduuride kasutamine ISO/OSI etalonmudeli eri kihtides).

Oluline on ka organisatsioonisisese krüptokontseptsiooni määratlemine.

Turvaosakonna vaatevinklist vajavad selgitamist järgmised asjaolud:

- Milline on kaitsevajadus, st millist turbeastet on tarvis saavutada?
- Kui suur on eelarve ja kui palju on kasutada personaliressurssi, et soovitud turbemehhanisme ellu rakendada ning mis veelgi olulisem, et tagada turvamehhanismide pidev toimimine?
- Milline on soovitav süsteemiga ühendamise viis, st millised on turvalisust tagavate komponentide enamlevinud kasutustingimused?
- Millised on soovitud funktsioonid ja selleks vajaminev jõudlus?
- Kes selle kõige eest vastutab?

Krüptokontseptsioonis tuleb lisaks muule kirjeldada ka krüptotoodete tehnilisi, täpsemalt organisatoorseid kasutusvaldkondi, näiteks:

- Millised töötajad saavad pääsuõigused?
- Millistele teenustele võimaldatakse kaugpöördust?
- Kuidas reguleeritakse paroolide ja võtmete haldus seoses nende kehtivuse, märkide kasutamise, pikkuse ja väljastamisega?
- Kas, millal ja kuidas peavad andmed olema krüpteeritud või signatuuridega varustatud?
- Kes tohib kellega suhelda krüptokaitseta ja krüptokaitsega?
- Kes on volitatud jagama teatud õigusi jne?

Olenevalt süsteemi etteantud tehnilistest raamtingimustest, mis on järgmised:

- käideldavate andmete hulk ja ajaline sõltuvus,
- kättesaadavusele esitatavad nõuded ja vastuvõtlikkus ohtudele,

- kaitstavate rakenduste liik ja esinemissagedus,

saab analüüsida sobilikke realiseerimisvõimalusi ning arvestada kontseptsiooni tehnilise lahenduse väljatöötamisel juba konkreetsete rakendusvaldkondadega, nagu nt PC-töökoht, kohtvõrk või kodukeskjaam. Vaid eelnimetatud tervikliku lähenemisviisi abil on võimalik tagada, et krüptograafiliste toodete valikukriteeriumite ja kasutustingimuste loetlemisel saadud ülevaatliku pildiga kaasneb loodetud lõpptulemus nii IT turbe kui ka majanduslikkuse seisukohast.

Siinkohal soovime rõhutada asjaolu, et eespool näidatud jaotus ei ole mitte mingil juhul kohustuslik või määrava tähtsusega, pigem on tegu vaid abistava võttega. Oluline on vaid, et lähteolukord oleks võimalikult täpselt välja selgitatud, ja et küsimused peegeldaksid läbivalt seda, kuidas lõpptulemust ette kujutatakse.

Loomulikult esineb praktikas olukordi, kus teatud küsimuste asetused ja vastused on üksteisega vastastikuses seoses või sõltuvuses, kuid üldjuhul on neist olukordadest siiski kasu, kuna need aitavad ülevaadet täiendada.

Krüptograafiliste protseduuride rakendamist puudutavad erinevad mõjurid tuleb defineerida ja arusaadavalt dokumenteerida (vt M 2.163 Krüptoprotseduure ja -tooteid mõjutavate tegurite määramine). Seejärel tuleb välja töötada ja dokumenteerida nende sobivad kasutusmeetodid. Lõpetuseks peab ametiasutuse või ettevõtte juhtkond vastu võtma otsuse nende rakendamise kohta. Lõpptulemused tuleks kaasata krüptokontseptsiooni selliselt, et neid oleks võimalik värskendada ja täiendada. Järgnev krüptokontseptsiooni sisukord on toodud näitena kontseptsiooni ühe võimaliku ülesehituse kohta:

Krüptokontseptsiooni sisukord

1. Definitsioonid

- Krüptograafiline protseduur

2. Vastuvõtlikkus ohtudele ja motivatsioon

- Institutsiooni sõltuvus andmete kättesaadavusest
- Tüüpiliste ohtude loetelu
- Institutsiooni puudutavate kahjude põhjused
- Seni esinenud kahjud

3. Organisatsioonisisese turvapoliitika määratlemine

- Vastutusalade defineerimine
- Eesmärgipüstitus: turbeaste

4. Mõjurid

- Kaitsmist vajavate andmete identifitseerimine
- Andmete konfidentsiaalsusnõuded
- Andmete tervikluse nõuded
- Andmete kättesaadavuse nõuded
- Nõuded jõudlusele
- Võtmete jagamine

- Andmemahud
- Andmete liigid – lokaalsed/jagatud (kohtvõrk/laivõrk)
- Rakenduste liigid, kus hakatakse kasutama krüptograafilisi protseduure
- Krüptograafilise protseduuri kasutamissagedus
- Krüptograafiliste algoritmide, st protseduuri vastupanuvõimele esitatavad nõuded (manipuleerimiskindlus)
- Turvatud andmete taastatavus
- Vajalik personaliressurss
- Vajaminevad funktsioonid
- Kulutused koos täiendavate kuludega (hooldus, haldamine, täiendid, . . .)
- IT kasutajate teadmised / andmetöötlusega seotud kvalifikatsioonid

5. Kasutusala defineerimine

- Krüptograafilise protseduuri liik
- Krüptograafiliste toodete kasutustingimused
- Kasutuse sagedus ja aeg
- Vastutavate töötajate nimetamine
- Organisatoorsete reeglite määratlemine
- Personali puudutavate meetmete rakendamine (koolitamine, asendamise korraldamine, kohustused, rollijaotus)
- Kasutustingimuste/konfiguratsiooni dokumenteerimine
- Koostalitlusvõime, standardne ühilduvus, investeeringukindlus

6. Võtmehaldus

Mõningaid selle kontseptsiooni punkte kirjeldatakse lähemalt meetmetes M 2.162 Krüptoprotseduuride ja -toodete vajaduse määramine , M 2.163 Krüptoprotseduure ja -tooteid mõjutavate tegurite määramine ja M 2.166 Krüptomoodulite kasutamist reguleerivad sätted . Krüptokontseptsiooni koostamine ei ole mitte ühekordne ettevõtmine, vaid pigem dünaamiline protsess. Seetõttu tuleb krüptokontseptsioon viia regulaarselt vastavusse hetkeolukorraga.

Kontrollküsimused:

- Kas olemasolev kontseptsioon kajastab hetkeolukorda?
- Kas kontseptsioon loetleb üles kõik selle valdkonna alla kuuluvad IT-süsteemid?
- Kuidas toimub töötajate teavitamine seoses neid puudutava kontseptsiooni osaga?
- Kas kontseptsiooni järgimist kontrollitakse?
- Kuidas arvestatakse mõjurite võimalikku muutumist?

M 2.162 Krüptoprotseduuride ja -toodete vajaduse määramine

Algatamise eest vastutavad: IT turvaosakond

Rakendamise eest vastutavad: administraator, üksikute IT-rakenduste eest vastutavad töötajad

Selgitamaks, millised on krüptoprotseduuride ja krüptotoodete kasutamisega seotud raamtingimused ja reaalsed nõuded, mis peaksid tagama usaldusväärsuse ja kasutajasõbralikkuse konfidentsiaalse info levitamisel ja edastamisel, tuleb kaitsmist vajav informatsioon kõigepealt identifitseerida ja liigitada.

Kaitsmist vajavate andmete identifitseerimine

Kõigepealt tuleb määratleda, milliste ülesannete täitmiseks hakatakse krüptoprotseduure kasutama ja millist liiki andmeid soovitakse seeläbi kaitsta.

Krüptoprotseduuride kasutamise vajadus võib tekkida erinevatel põhjustel (vt M 3.23w Sissejuhatus krüptograafia põhimõistetesse):

- andmete konfidentsiaalsuse ja tervikluse tagamine,
- autentimine,
- saatmise ja vastuvõtu kinnitus.

Olenevalt kasutusvaldkonnast võib olla mõistlik kasutada erinevaid krüptoprotseduure, nagu näiteks krüpteerimine või räsimine (hash). **Krüptoprotseduuride tüüpilised kasutusvaldkonnad on järgmised:**

1. lokaalne krüpteerimine,
2. side turvamine kasutus- ja edastustasandil,
3. autentimine,
4. salgamatus,
5. terviklus.

Alljärgnevalt on toodud mõningad näited krüptoprotseduuride erinevate tüüpiliste kasutusvaldkondade kohta:

- PC kõvakettale on salvestatud andmed, mida soovitakse krüpteerimise abil kaitsta volitamata juurdepääsu eest.
- Andmeid soovitakse edastada telefoni, faksi või andmevõrkude abil, näiteks e-kirja vahendusel või vahetatavate andmekandjatega.
- Kaitsmist vajavat informatsiooni kontrollib rohkem osapooli kui ainult organisatsiooni allüksuse vastutavad töötajad (kohtvõrk kulgeb läbi hoone erinevate osade, mis on teiste firmade käsutuses; isikuandmetega serverit teenindab töötaja, kes ei kuulu ise personali hulka).
- Kaugpöördused, mis vajavad kontrollimiseks tugevat autentimist.
- E-postiteenuse kasutamine, kui on tarvis ümberlükkamatult tõestada, kes olid meilide saatjad ja kas e-kirjade sisu on edastatud muutumatul kujul.

Sobilike krüptoprotseduuride ja krüptotoodete väljaselgitamiseks ja kaitset vajavatest andmetest ülevaate saamiseks tuleb esmalt välja selgitada IT hetkestruktuur.

Struktuuri kohta oleks vaja välja selgitada järgmised punktid:

- milliseid IT-süsteeme kasutatakse andmete töötlemiseks ja salvestamiseks (PC-d, sülearvutid, serverid) ning milliseid andmete edastamiseks (sillad, marsruuterid, turvalüüsid, tulemüürid);
- millised on võimalikud sidekanalid. Selleks tuleb välja selgitada võrgu loogiline ja füüsiline struktuur (vt M 2.139 Olemasoleva võrgukeskkonna läbivaatus).

Andmete kaitsevajadus (konfidentsiaalsus, terviklus, autentsus, salgamatus)

Välja tuleks selgitada kõik rakendused ja andmed, mille puhul on olemas erivajadused konfidentsiaalsuse, tervikluse, autentsuse ja salgamatuse vallas. Samas tuleb silmas pidada, et krüptograafilisi tooteid ei lähe tarvis mitte ainult spetsiaalsete, kõrgendatud kaitsevajadusega IT-süsteemide, rakenduste või andmete puhul, vaid ka keskmise kaitsevajaduse korral.

Näiteid spetsiaalse konfidentsiaalsusvajadusega andmete kohta:

- isikutega seotud andmed,
- paroolid ja krüptograafilised võtmed,
- konfidentsiaalne info, mille avalikuks tulek võib endaga kaasa tuua regressinõude,
- andmed, mille abil võib konkureeriv ettevõte saada finantsilist tulu,
- andmed, mille konfidentsiaalsuse kadu seaks ohtu tööülesannete täitmise (nt uurimuse tulemused, ohustatud taimeliikide asukoharegister),
- andmed, mille avalikustamine võib kaasa tuua kellegi maine kahjustamise.

Teadmiseks: andmekogu kaitsevajadused suurenevad koos andmehulga kasvamisega, mistõttu võib krüpteerimine osutuda vajalikuks ka neil juhtudel, kus andmekogu üksikutele andmehulkadele ei kehti kõrgendatud konfidentsiaalsusenõue.

Näiteid spetsiaalse terviklusevajadusega andmete kohta:

- finantsvaldkonna andmed, millega manipuleerimine võib kaasa tuua finantskahjusid,
- informatsioon, mille võltsimise avalikuks tulek võib endaga kaasa tuua regressinõude,
- andmed, mille võltsimine võib viia ettevõtlust puudutavate valede otsuste langetamiseni,
- andmed, mille võltsimine võib endaga kaasa tuua toote kvaliteedi languse,

Üks näide kõrgendatud autentimisvajadusega rakendusest on kaugpöördusfunktsiooni kasutamine. Kõrgendatud salgamatuse nõudega andmete kohta võib näitena tuua tellimused või reserveeringud, mille korral peab tellija olema identifitseeritav. Kaitsevajaduse kindlaksmääramise lõpptulemusena peaks olema määratletud, millised rakendused või andmed vajavad krüptograafilist kaitset. Nimetatud määratlust võib hiljem veel täiendada ning see tuleks regulaarselt üle vaadata. Tulemusena peaks valmima ülevaade kõikidest salvestuskohtadest ja andmeedastuskanalitest, mida oleks tarvis krüptograafiliselt kaitsta. Seeläbi saadakse

põhimõtteliselt kogu IT-koosluse kaart, millele on märgitud krüptoprotseduuridega kaetud alad.

Vajaduste ja nõuete väljaselgitamine

Vajaduste väljaselgitamisel võib abivahendina kasutada alajaotustega küsimuste kataloogi, nagu seda on kujutatud järgneval joonisel. Tehnilised, organisatoorsed ja majanduslikud aspektid saab seejuures veel omakorda nelja alamkategooriasse jaotada.

Tehnilised aspektid	Organisatsioonilised aspektid	Majanduslikud aspektid
kasutajateenused ja rakendused	kasutusvaldkond	ratsionaliseerimisaspektid / kulude kokkuhoid
kasutusprofiil	migratsiooni kontseptsioon	tükiarvud
võrgu infrastruktuur	ettekujutus ajakulust	soetamiskulud
IT-lõppseade	kasutamise raamtingimused	halduse ja hooldusega seotud kulud

Joonis: näide teemade võimalikust jaotumisest küsimuste kataloogi koostamisel

Tehnilisi aspekte uurides on näiteks kasutajateenuste ja rakenduste valdkonnas tähtis välja selgitada, kas vaadeldakse peamiselt reaalajas kajastuvaid või mittereaalajas kajastuvaid andmeid. Kasutusprofiili kategoorias tuleb uurida, millised rakendused ja andmed vajaksid krüptoprotseduuride kasutamist, nt kas välise andmeside valdkond või lühiajaline või pikaajaline konfidentsiaalsete andmete töötlemine. Eelnevale lisaks tuleb välja selgitada ka võrgu infrastruktuur ja lõppseadet puudutav info, nagu nt ühenduse konfiguratsioon. Organisatoorsete aspektide alla kuuluvad kasutusala, st osalejate või võrgu valdkond; informatsioon selle kohta, kas olemas on migratsiooni kontseptsioon ja ettekujutus, kui suur on lõppkasutajale vajalik ajaline ressurss ning millised on kasutamise raamtingimused.

Tähtsamad majanduslikud aspektid on järgmised:

- ratsionaliseerimine, nt toote kasutamine, mis töötab käsitsi juhtimise asemel hoopis läbipaistval krüpteerimisprotseduuril,
- tükiarvude ja soetamiskulude hindamine ning
- eeldatavate haldamis- ja hoolduskulude tuvastamine.

Toetudes eespool kirjeldatud küsimustikule, on võimalik koostada küllaltki praktikalähedane kasutuse ja nõuete kontseptsioon, mille saab võtta aluseks edasiste konkreetsete realiseerimisotsuste langetamisel ning sobilike krüptokomponentide/-toodete valikul (vt M 2.165 Sobiva krüptotoote valimine). Siin esitletud lähenemismeetod peaks aitama IT turbe eest vastutavatel töötajatel tuvastada, hinnata ja koordineerida turvatehnika kasutust ning ulatust erinevates süsteemi osades, võrguüleminekutes ja lõppseadmetes. Seejärel tuleks planeerimisfaasis välja selgitada, milline on hädavajalik kaitse (kaitsevajadus), et vastata küsimusele, kas IT turbega tegelemine on otstarbekas või mitte. Eelnevalt visandatud hindamismeetod pakub võimalust pragmaatiliseks lähenemiseks, mis võimaldab arvestada turvaaspektidega avatud, laialijaotatud IT struktuurides, nagu see on paljudel juhtudel. Eespool toodud näidete alusel hinnatud IT turbesse

tehtavad investeeringud peavad end oma kasutusalas ka majanduslikult õigustama. Ellu viidud turvastrateegiate funktsioonid ja kasutamine peavad vastama lõppkasutajate ootustele seoses süsteemi paindlikkuse, läbipaistvuse ja jõudlusega. Plaanitavad ja integreeritud turbealased teenused ei tohi lõppkasutajate tööd ülemääraselt piirata.

M 2.163 Krüptoprotseduure ja -tooteid mõjutavate tegurite määramine

Algatamise eest vastutavad: IT turvaosakond

Rakendamise eest vastutavad: administraator, üksikute IT-rakenduste eest vastutavad töötajad

Enne konkreetsete krüptoprotseduuride või -toodete kasuks otsustamist tuleb välja selgitada terve rida erinevaid mõjureid. Mitmekesiste tegurite väljaselgitamiseks võib küsitleda üksikute IT-süsteemide ja IT-rakenduste eest vastutavaid töötajaid. Küsitluse tulemused tuleb kõigile arusaadaval kujul kirja panna.

Kõikide meetmes M 2.162 Krüptoprotseduuride ja -toodete vajaduse määramine kirjeldatud salvestuskohtade ja edastusteekondade kohta tuleb välja selgitada järgmised mõjurid:

Turbeaspektid

- Milline on kaitsevajadus, st milline turbeaste tuleb saavutada?
- Millised krüptograafilised funktsioonid on vajalikud soovitud turbeastme saavutamiseks (krüpteerimine, tervikluse kaitse, autentsus ja/või salgamatus)?
- Võimalikud ründajad: milliste potentsiaalsete ründajatega tuleb arvestada (ründajate ajalised ja finantsressursid, tehnilised oskused)?

Vastuste saamiseks äsjaloetletud küsimustele tuleb läbi töötada meede M 2.162 Krüptoprotseduuride ja -toodete vajaduse määramine .

Tehnilised aspektid

Laiaulatuslike IT-struktuuride kasutamine, milles on palju hargnemisi ning suurel hulgal üksikkomponente ja spetsiaalseid seadmeid (võrgusõlmi, servereid, andmebaase jne) muudab vajalikuks ka laiaulatusliku, mitmete funktsiooniüksustega (turvahalduse, turvaserverite ja kasutajapoolsete turvakomponentidega) varustatud turvasüsteemi kasutamise. Reeglina tuleb selleks koostada süsteemi ülevaade, mis peab kajastama lisaks reaalselt kasutatavatele funktsioonidele veel ka ehitust ja organisatoorset poolt puudutavaid aspekte. Selgelt eristades on tarvis välja tuua ka turvakomponentide tehniline asetus ja nende integreerituse aste mitteturvakomponentidesse, kuna see mõjutab otseselt turvafunktsioonide rakendamist, operatsioonisüsteemide pakutavat hädavajalikku tuge, tööde keerukust ja kulusid ning loomulikult ka eesmärgiks seatud turbeastet.

Turvalisuse hindamisel on määrava tähtsusega asjaolud, millistes geograafilistes asukohtades ja millises protokollikihis on vastavad turvateenused realiseeritud ning millisel moel on need kaasatud kaitstavate IT-süsteemide tööprotsessidesse.

Toetudes eelnevale, tuleb leida vastused järgnevatele küsimustele:

- Ümbritseva keskkonna pakutav kaitse: millist kaitset pakub ümbritsev keskkond (taristu (juurdepääs), organisatoorne pool, personal, tehniline pool (operatsioonisüsteemi pakutav kaitse))?
- IT-süsteemikeskkond: millised on kasutatavad tehnoloogiad, operatsioonisüsteemid jne?
- Andmemahud: kui suurt andmemahtu on tarvis turvata?

- Sagedus: kui sageli esineb vajadus krüpteerimise järele?
- Jõudlus: kui kiiresti peavad krüptograafilised funktsioonid töötama (offline-, online-rate)?

Personali ja organisatoorse töö aspektid

- Kasutajasõbralikkus: kas turbelahenduste kasutamiseks on töötajatel tarvis krüptograafilisi algteadmisi? Kas krüptotoote kasutamine segab tööülesannete täitmist?
- Vastuvõtlikkus: kui palju võib töötajaid täiendavate ülesannetega koormata (tööaeg, hooldusele kuluv aeg)?
- Usaldusväärsus: kui usaldusväärselt suudavad töötajad krüptotehnoloogiaga ümber käia?
- Koolitusvajadus: millises mahus on töötajaid tarvis koolitada?
- Personalivajadus: kas on tarvis täiendavat personali, nt installeerimiseks, kasutamiseks, võtmete haldamiseks?
- Kättesaadavus: kas teatud krüptotoote kasutamine võib vähendada kättesaadavust?

Majanduslikud aspektid

- Finantsilised raamtingimused: kui suured võivad olla krüptograafilisele kaitsele tehtavad kulutused?

Kui palju kulub raha

- ühekordseteks investeeringuteks,
- jooksvatele kuludele, kaasa arvatud personalikuludele,
- litsentsidele?
- Investeeringukindlus: kas plaanitavad krüptograafilised protseduurid ja tooted on varustatud kaasaegsete standardite toega? Kas on tagatud nende koostalitlusvõime teiste toodetega?

Võtmetaaste (key recovery)

Juhul kui krüpteerimiseks kasutatavad võtmed lähevad kaduma, pole üldjuhul ka nendega kaitstud andmed enam kättesaadavad. Seetõttu pakuvad paljud krüptotooted funktsioone, mis võimaldavad andmeid taastada. Enne vastavate andmetaastusfunktsioonide kasutamist tuleks tutvuda võimalike kaasnevate riskidega. Kui funktsioonidega on võimalik taastada konfidentsiaalseid võtmeid, tuleb tagada, et seda saaksid teha ainult vastava volitusega isikud. Kui funktsioonid võimaldavad ligipääsu kasutaja andmetele ilma originaal-krüptovõtme omaniku teadmiseta, pole originaali omanikul tema nime alt tehtud pahatahtliku manipuleerimise korral hiljem enam mingisugust võimalust oma süütust tõestada. Võtmetaastefunktsioonide kasutamine toob endaga tihti kaasa ka usaldusväärsuse languse ja eelarvamuste tekke, seda nii ettevõtte või ametiasutuse sees kui ka sidepartnerite vahel. Andmeedastuse puhul tuleks seetõttu üldjuhtudel võtmetaastefunktsioonidest loobuda. Selleks puudub ka otsene vajadus, kuna võtmete või andmete kaotsimineku puhul võib lihtsalt nende saatmist korrata. Andmete lokaalse salvestamise korral

tuleks selle kasutamine hoolikalt läbi vaagida (vt M 6.56 Andmevarundus krüptoprotseduuride kasutamisel). IT etalonturbe abivahendite alt võib leida ka artikli võtmetaastefunktsiooni võimaluste ja ohtude kohta.

Krüptograafiliste protseduuride kasutusiga

Krüptograafiliste protseduuride ja toodete puhul tuleb regulaarselt kontrollida nende ajakohasust. Kasutatavad algoritmid võivad tehniliste edasiarenduste, nagu nt kiiremate ja odavamate IT-süsteemide või uute matemaatiliste teadmiste tõttu nõrgaks muutuda. Krüptotoodetes võib esineda vigu, mis on tekkinud nende juurutamise käigus. Seetõttu tuleks juba krüptoprotseduuride hulgast valikut tehes kindlaks määrata toote kasutamise ajaline piirang. Sel hetkel tuleks ka põhjalikult läbi mõelda, kas rakendatavad krüptomoodulid suudavad pakkuda just sellist kaitset, mida soovitakse saavutada.

Seadustest tulenevad raamtingimused

Krüptograafiliste toodete kasutamisel tuleb järgida erinevaid seadustest tulenevaid ettekirjutusi. Teatud riikides tuleb krüptoprotseduuride kasutamiseks taotleda nt vastav luba.

Seetõttu tuleb eelnevalt välja selgitada (vt M 2.165 Sobiva krüptotoote valimine) järgmised punktid:

- Kas krüptotoote plaanitavasse kasutuspiirkonda jäävates riikides tuleb täita sellekohaseid seadustest tulenevaid lisakohustusi?
- Kas väljavalitud toodetele võib olla kehtestatud ekspordipiirang?

Tuleb arvestada, et lisaks krüptograafilistele algoritmidele või protseduuridele seatud maksimumnõuetele eksisteerivad ka miinimumnõuded. Näiteks peab isikuandmete edastamisel olema tagatud, et andmete krüpteerimisel kasutatakse krüpteerimisprotseduuri, mille krüptovõti on piisava pikkusega.

Näiteid tehniliste lahenduste kohta:

Järgnevalt on toodud mõningaid näiteid krüptograafiliste protseduuride erinevatest rakendusvaldkondadest. Näidetest selgub, et paljud tooted suudavad täita korraga mitme eri kasutusvaldkonna nõudeid.

Näide nr 1: Kõvaketta krüpteerimine

Eraldiseisva PC kõvakettale on salvestatud tundlikku informatsiooni, mida on tarvis kaitsta nõnda, et

- PC-d saaksid käivitada ainult selleks volitatud isikud,
- salvestatud andmetele oleks juurdepääs ainult volitatud kasutajatel,
- salvestatud andmed oleksid ka siis, kui PC on välja lülitatud – muu hulgas ka varguse puhul – piisavalt kaitstud, et volitamata isikutel ei oleks võimalik nendele andmetele ligi pääseda.

Siinkohal peaks olema esmatähtis konfidentsiaalsuse kaitse. PC-d tuleb kaitsta järgmiste ohtude eest:

- volitamata juurdepääs kõvakettale salvestatud andmetele,

- kõvakettale salvestatud andmetega manipuleerimine,
- krüptosüsteemi manipuleerimine.

PC või kõvaketta varguse või kadumise korral on ründajal andmetele ligipääsemiseks väga palju aega. Kaitsemeetmed peavad ka niisuguste, pikaajalist lähenemist võimaldavate rünnete puhul tagama, et salvestatud andmete konfidentsiaalsus säiliks. Seetõttu tuleks kaitsemeetmena rakendada toodet, mis võimaldab kasutada buutimiskaitset ja kõvaketta krüpteerimist. Kaitse realiseerimiseks on saadaval erinevaid lahendusi. Kaitse teostamisel võib rakendada erinevaid lahendusi, nagu nt krüpteerimistarkvara (variant A), riistvaralisi krüpteerimiskomponente (variant B) või tarkvara ja riistvara komponentide kombineerimist (variant C).

Variandi C tüüpiline lahendus on juurdepääsu kontrolli tagamine, kasutades krüpteerimistarkvara koos kiipkaardi lugejaga.

Variandi valik sõltub erinevatest kriteeriumitest:

- **Turvalisus** (krüpteerimise algoritm ja krüptovõtme pikkus, krüpteerimise toimimismeetod, juurdepääsu kaitse, võtmete genereerimine/jagamine/salvestamine/sisestamine, integreerimine operatsioonisüsteemiga jne) – operatsioonisüsteemide platvormid, mille peal krüpteerimisfunktsiooni soovitakse kasutada, seavad tarkvaralistele lahendustele (variandile A või C) tahes-tahtmata omad piirid. Kui operatsioonisüsteemilt ei saa turvalisust, st valdkondade Task ja Save selget lahutamist eeldada (siiani ei ole seda veel ühegi operatsioonisüsteemi puhul kindlalt tõestatud!), tuleb krüpteerimisel ja dekrüpteerimisel kasutatavat võtit hoida vähemalt lühikest aega kaitsmata kujul PC mälus. Võtme konfidentsiaalsus ei ole seeläbi enam tagatud. Riistvaralised krüpteerimiskomponendid (variant B) võivad (kuid ei pruugi!) pakkuda rohkem kaitset. Võtme saab salvestada riistvaralistesse komponentidesse ja seda hoitakse seal lugemise eest kaitstuna. Riistvarakomponendist võti enam ei lahku ning seeläbi on need väljanuhkimise eest kaitstud. Võtit saavad aktiveerida vaid volitatud isikud, kellel on vajalikud vahendid ja teadmised (nt kiipkaart ja parool). Tähtsad on ka muud aspektid, nagu nt krüpteerimisel kasutatavad algoritmid (enamasti plokk-krüpteerimisalgoritm), nende töörežiimid (nt CBC) ning see, mil moel on need PC-süsteemi integreeritud. Ideaaljuhul peaks krüpteerimise riistvara olema integreeritud selliselt, et krüpteerimine toimub kohustuslikus korras terve kõvaketta ulatuses ning et ründajatel ei oleks võimalik seda märkamatult välja lülitada või sellest mööda minna. Kui krüpteerimisse haaratakse vastupidiselt eelnevale näitele ainult üksikud failid, mitte terve kõvaketas, tekib oht, et krüpteeritud failide sisu salvestatakse kõvakettale vähemalt osaliselt ka loetaval kujul (nt erinevate operatsioonisüsteemide lehtjaotuse või varundusfailidesse).
- **Jõudlus** (kasutatavate programmide töökiirus) – tarkvaraline krüpteerimislahendus kasutab PC süsteemiressurssi, st koormab CPU-d ja vajab töömälu. PC jõudlus langeb hiljemalt siis, kui korraga tuleb krüpteerida terve kõvaketas. Oma protsessoriga varustatud riistvarakomponendid võivad krüpteerimist teostada ilma PC CPU-d koormamata, st ilma et sellega kaasneks jõudluse märkimisväärset langust. Oluline tegur on siinjuures kasutatava krüpteerimisriistvara läbilaskevõimsus.

- **Organisatoorse töö maht** / personalikulu (haldamine, võtmehaldus, koolitus jne) – organisatoorse töö maht ehk personalikulu sõltub suurel määral turvapoliitika ellu rakendamisest ning sellest, millise mugavusastmega krüpteerimiskomponente kasutatakse. Üldkehtivaid poolt- või vastuargumente pole kolme eespool loetletud variandi kohta võimalik eraldi välja tuua.
- **Majanduslikkus** (soetamiskulud, koolituskulud, haldamiskulud) – suuri üldistusi pole majanduslikkuse kohta võimalik välja tuua. Kui võtta vaatluse alla ainult soetamiskulud, näeme, et tarkvaralised lahendused on tihti soodsama hinnaga kui riistavaralised lahendused. Võttes seevastu arvesse kõik kahjud, mida ebapiisav kaitse võib endaga pikemas perspektiivis kaasa tuua, võib selguda, et investeering turvalisemasse ja võibolla ka kallimasse lahendusse tasub ennast siiski ära. Majanduslikkusele võib halvasti mõjuda ka PC-süsteemi jõudluse langus.
- **Jääkohud** (operatsioonisüsteem, kõvaketta krüptovõtme kompromiteerimine jne). Sobilike krüpteerimiskomponentide valimisel on küllaltki oluline, et selle käigus arvestataks ka võimalike jääkohtudega. Muu hulgas võivad esile kerkida järgmised küsimused – milliseid jääkohtusid võib endale lubada ning milliseid jääkohtusid saab, st on võimalik teiste meetmete (nt materiaalsete või organisatoorsete meetmete) abil minimeerida? Erinevate meetmete kombineerimine võib siinkohal pakkuda mitmeid vettpidavaid lahendusi.

Näide nr 2: e-kirja krüpteerimine

Elektronposti saatmine ja vastuvõtt läbi arvutivõrkude on muutumas aina olulisemaks. Kui e-kirjad sisaldavad muu hulgas ka tundlikku informatsiooni (nt firmasaladusi) ja nende vahetamine toimub läbi ebaturvaliste võrkude, tuleb kasutada täiendavaid turvamehhanisme, et tagada e-kirjade konfidentsiaalsus või autentsus. Neil eesmärkidel võib rakendada e-kirjade krüpteerimisprogramme.

Kõige laiemalt on siinkohal levinud kaks programmipaketti, täpsemalt standardit, mis pärinevad USA-st.

- PGP (Pretty Good Privacy) ning
- S/MIME (Secure Multipurpose Internet Mail Extensions).

PGP puhul on tegemist programmipaketiga, mille laialdast levikut põhjendab asjaolu, et algselt oli see internetis saadaval vabavarana. S/MIME standardit kasutavad muu hulgas firmade Microsoft, Netscape ja RSA Data Security Inc Secure-E-Mail rakendused.

Millised on niisugusele e-kirja krüpteerimisprogrammile esitatavad nõuded?

Vastus sellele küsimusele sõltub teatud määral loomulikult ka ümbritsevatest turvameetmetest. Kõige kõrgemad on vastavad nõuded vaieldamatult neil juhtudel, kus e-kirju soovitakse saata ja vastu võtta läbi suurte, avatud, ebaturvaliste võrkude, nagu nt internet. Sellistel juhtudel on võimalik, et omavahel soovivad konfidentsiaalselt ja kõrge autentimiskindlusega suhelda ka need isikud, kes ei ole omavahel isiklikult tuttavad. Millised krüptograafilised teenused on selle tagamiseks vajalikud?

Konfidentsiaalsus

Kuna e-kirjad tuleb krüpteerida, tuleb rakendada (ühte või mitut) krüpteerimisalgoritmi. Suurema jõudluse tõttu sobivad siinkohal kasutamiseks sümmeetrilised protseduurid.

Võtmehaldus

- Genereerimine: sümmeetrilise krüpteerimisprotseduuri võtmed tuleb genereerida sobiva (juhu-) protsessi abil, mis muudab võtmete ära arvamise, st järgnevate võtmete ennustamise praktiliselt võimatuks ka neil juhtudel, kus mõningad eelnevad võtmed on eelnevalt teada.
- Võtmete kokkuleppimine/vahetus: kuna internetis ei tule tsentraliseeritud, sümmeetrilisel protseduuril töötav võtmetega varustamine juba lõputu hulga kommunikatsioonipartnerite tõttu kõne alla, tuleb võtmete kokkuleppimiseks, st vahetuseks kasutada asümmeetrilist protseduuri.

Autentsus

Kuna asümmeetriline protseduur võib võtmehaldusest tulenevalt juba niigi kasutusel olla (ning võibolla tuleb tagada ka salgamatus), rakendatakse autentsusnõuete täitmiseks digitaalset allkirja. Digiallkirjade võtmeid tuleb kasutada eranditult vaid digitaalsete allkirjade andmiseks. Sealjuures tuleb – nagu avaliku võtme protseduuri rakendamise puhul alati – lahendada avalike võtmete autentsuse küsimus.

Salgamatus

Salgamatuse tagamine eeldab avaliku võtme taristu olemasolu (PKI, osalejate registreerimine ja avalike võtmete sertifitseerimine usaldusväärse kolmanda osapoole poolt koos kasutusreeglitega). Seni puudub siiski veel globaalne PKI, mistõttu on väga raske saada eelnevalt mitteteadaolevate osalejate puhul ümberlükkamatut tõendit nende päritolu kohta. Kohtvõrgus tuleks sel eesmärgil luua sobilik PKI.

Standardne ühilduvus

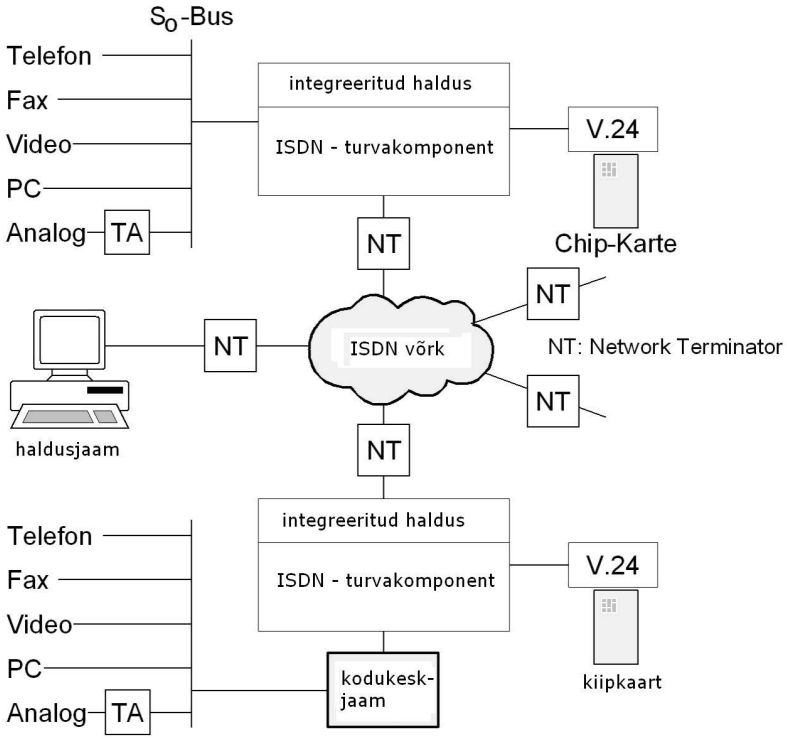
Koostalitlusvõime ja investeeringukindluse nõuetest lähtuvalt oleks mõttekas kasutada võimalikult laialt levinud ja aktsepteeritud internetistandardeid. Nii S/MIME kui ka PGP on staadiumis, kus need hakkavad muutuma standardiks.

Näide nr 3: turvaline kõne- ja andmeedastus ISDN-võrguühenduste kaudu

Järgnevas näites vaadeldakse kommunikatsiooni, mis toimib ISDN-i kaudu. Kaitset vajavad siinkohal rakendused, nagu telefoniside ja videokonverentsid ning arvutuskeskustevaheline andmeside. Eesmärk on saavutada edastatavate konfidentsiaalsete andmete ja ümberlükkamatute isikuandmete tõhus kaitse. Lähtutakse olukorrast, et kõik edastatavad andmed on olemas digitaalsel kujul (PCM-Code), ning et firmasisestes võrkudes ja kodukeskjaamades tavapäraselt kasutatavat kõnekompressiooni saab krüpteeritud rakenduste tarbeks välja lülitada, et tarbekanaleid (B-kanaleid) oleks võimalik krüpteerida. Selleks on tarvis rakendada ISDN-turvakomponente, mis võimaldavad muuta S0-ühenduse kahe 64 kbit/s-kanaliga turvaliseks. Siinjuures pole üldse oluline, kas S0-siiniga on ühendatud üksikud ISDN-lõppseadmed (telefon, faks, ISDN pistikkaardiga PC jne) või on sellega ühendatud väike kodukeskjaam. Kõikide ühenduste puhul peab saama valida

krüpteeritud ja krüpteerimata töörežiimi vahel, sama kehtib ka ühenduste loomise kohta.

Alljärgneval joonisel on kujutatud vastav süsteemi konfiguratsioon.



Valik on langenud ISDN-krüpteerimisseadmele, mida on võimalik kaitsta volitamata kasutamise eest kiipkaardi abil. Alternatiivina on võimalik kasutada ka V.24-liidest, mille puhul saab turvakomponente konfigureerida PC abil. Kasutaja või lõpprakendus saavad krüpteerimist juhtida otse kiipkaardi või spetsiaalsete parameetrite eelvalikuga. Samuti on võimalik ISDN-turvakomponente konfigureerida selliselt, et teatud ühenduste (numbrite) krüpteeritud või krüpteerimata töörežiim määratakse kindlaks juba eelseadistusega. Võtmehalduse, st võtmesertifikaatide genereerimise ja jagamise tarbeks ühendatakse ISDN-võrgu ühte kesksesse kohta vastav haldusjaam. Sellega tagatakse, et kõiki üksikud võrku ühendatud ISDN-turvakomponente on võimalik registreerida ja varustada värske võtmeinfoga.

Informatsiooni ja kaitset vajavate andmete turvaliseks transportimiseks läbi ISDN-võrgu on olemas palju erinevaid ja keerukaid lahendusi. Siinjuures on tarvis, et iga oluline ohuallikas likvideeritaks konkreetse turbemeetme rakendamisega.

Konfidentsiaalsuse tagamiseks tuleb edastava andmevoo puhul kasutada võrgukrüpteeringut, mis annab kõige paremaid tulemusi lülikihis. Selleks krüpteeritakse andmed automaatselt enne nende edastamist krüptograafilise riistvara

poolt ja dekrüpteeritakse adressaadi juures. Kasutatav krüpteering jääb seejuures läbipaistvaks nii lõppkasutajale kui ka rakendusprogrammidele. Kasutatav krüptomoodul võimaldab töötlust mitte ainult reaalajas, vaid pakub vastupidiselt failide krüpteerimisele (tarkvaralahendusele) ka palju suuremat kaitset võimalike rünnete vastu. Kindlustamaks salgamatuse nõuete või tõestamiskohustusega andmete edastamist, on võimalik varustada saadetis ka saatja digitaalse allkirjaga. Seeläbi on adressaadil võimalik määrata vastuvõetud teadete päritolu ja autentsust, mis võimaldab eksimatult tuvastada võimalikke avalikus võrgus asetleidnud manipulatsioone.

Digitaalse allkirja võtmete turvaliseks genereerimiseks ja salvestamiseks kasutatakse jällegi kiipkaardi võimalusi, mis on turvakontseptsiooni üks olulisemaid koostisosi. Arvutite omavaheliseks ühendamiseks on ülimalt oluline, et kasutusele oleks võetud sobilikud meetmed soovimatute valeühenduste ärahoidmiseks, kuna vastupidiselt telefonikõnedele ei ole arvutite puhul tihti võimalik neid enne edastust või edastuse ajal ära tunda. Probleemi lahendamiseks võib kasutada ISDN-turvakomponentidesse sisseehitatud tulemüüri funktsioone. Signaliseerimiskanali (D-kanali) kontrollimise abil on turvakomponente võimalik seadistada selliselt, et luuakse eranditult vaid rangelt eelseadistatud krüpteeritud ühendusi.

Hilisemaks ühenduse saamiseks kodukeskjaamaga on ette nähtud teatud telefoninumbrid ja funktsioonid. Nii turvalise võtmehalduse kui ka kiire kasutajaandmete krüpteerimise tagamiseks reaalajas tuleks rakendada hübriidprotseduure. Jätkates informatsiooni krüpteerimist sümmeetrilise protseduuri abil kasutatakse nn seansivõtme vastastikuse vahetuse jaoks asümmeetrilist protseduuri. Praktikas toimuvad nimetatud protsessid täiesti automaatselt. Ilma kasutusmugavust seeläbi märkimisväärselt pärssimata võib iga uue ISDN-ühenduse puhul omavahel kokku leppida uued seansivõtmed.

ISDN-turvakomponentide valikul ja kasutamisel peaks lõpposaleja turvalisuse tehnilistest aspektidest lähtudes arvestama järgmiste kasutuskriteeriumite ja kohustustega:

- (Hinnang: + = oluline kuni +++ = väga oluline):
- Individuaalsed osalejate võtmed ja autentimisinfo tuleb salvestada turvalisele andmekandjale (näiteks kiipkaardile) ning kindlustada usaldusväärse allkirjaga (+++).
- Kommunikatsiooniühenduse (kõne, andmete, pildimaterjali jne) krüpteerimiseks tuleb edastuse puhul kasutada salajast võtit, niinimetatud seansivõtit, mis lepitakse iga kord uuesti kokku (++).
- Kasutatavad turvateenused toimivad automaatselt ning lõppsüsteemi ja lõpposalejate jaoks peavad need jääma täiesti läbipaistvaks (+).
- Väljavalitud ühenduste jaoks on turvakomponent seadistatud nõnda, et see töötab alati krüpteerimisrežiimil (+++).

- Turvakomponentide kasutamisel tuleks olemasolev taristu säilitada täies mahus (+).
- Turvakomponentide turvalisuse seadeid peaks saamata hallata kogu võrgu ulatuses ning võimaluse korral ühest tsentraalsest kohast (+).
- Soovitatav oleks töö jälgimise funktsioon, mis töötab sidusrežiimil, ning kõikide turvakomponentide registreerimisvõimalus dialoogis haldusjaamaga (+).

Valik tuleks langetada selliste ISDN-turvakomponentide kasuks, mis ei nõua muudatuste tegemist kaitset vajavates lõppseadmetes, millel oleks normeeritud liidesed ja mida oleks kerge ühendada olemasoleva kommunikatsioonikeskkonnaga.

M 2.164 Sobiva krüptoprotseduuri valimine

Algatamise eest vastutavad: IT turvaosakond
Rakendamise eest vastutavad: IT turvaosakond
Krüptoprotseduuri valik jaguneb kahe järgmise ülesande vahel:

- krüptograafilise algoritmi väljavalimine ning
- tehniliste lahenduste väljavalimine.

Enne kui kasutaja seob ennast ühe või teise protseduuriga, peaks tal olema täpne ettekujutus sellest, millised on tema nõuded töödeldavate andmete konfidentsiaalsusele ja autentsusele igas informatsiooni töötleva süsteemi „punktis".

Krüptograafiliste algoritmide valimine
Krüptograafiliste algoritmide valimisel tuleb esmalt selgeks teha, milliseid krüptograafilisi protseduure soovitakse kasutada, ehk siis kas sümmeetrilisi, asümmeetrilisi või hübriidprotseduure ning seejärel tuleb langetada valik sobiva, st vastava mehhanismitugevusega algoritmi kasuks.

Krüpteerimisprotseduur

- Sümmeetriline krüpteerimine: sümmeetriliste protseduuride eelised ja puudused on kokku kogutud meetmesse M 3.23w Sissejuhatus krüptograafia põhimõistetesse . Sobivate algoritmidena tulevad kõne alla nt 3DES, IDEA, AES, RC 5, kusjuures võtme pikkus peab olema vähemalt 100 bitti.
- Asümmeetriline krüpteerimine: asümmeetriliste protseduuride eelised ja puudused on samuti kokku kogutud meetmesse M 3.23w Sissejuhatus krüptograafia põhimõistetesse . Sobilike algoritmidena tulevad kõne alla nt RSA või elliptilistel kõveratel põhinevad krüpteerimisprotseduurid (võtme pikkuse kohta lugege tekstist allpool).

Autentimisprotseduurid

- Teadete autentimine – teadete autentimiseks võib kasutada erinevaid autentimisprotseduure, nagu nt sõnumiautentimiskood (MAC) või digitaalset allkirja. MAC protseduuri kasutamine annab eelise juhul, kui on tarvis tagada äärmiselt suuri läbilaskevõimsusi (või kui kasutada on ainult väga väike arvutusressurss) ning kui võtme ilmsikstuleku oht on mõlemas otsas väga väike. Digitaalse allkirja kasutamine annab eelise juhul, kui (allkirja) võtme ilmsikstuleku oht on ühes otsas märgatavalt suurem kui teises otsas ning see on vajalik, kui soovitakse kasutada ümberlükkamatuse nõudega teenuseid. Olgu siinkohal veelkord rõhutatud, et ümberlükkamatuse funktsiooniga teenuste kasutamiseks peab olemas olema usaldusväärsete kolmandate osapoolte pakutav taristu. Kõige tuntum MAC-algoritm on teadete krüpteerimine DESi abil või plokkšifreerimisprotseduuriga kas CBC või CFB režiimis. MAC-koodi moodustab sealjuures teatele viimasena lisatav krüpteeritud plokk. Täpsemalt on nimetatud variante kirjeldatud standardites ISO 8731-1 ja ISO 9797. Plokkšifreerimisel põhinevate MAC-konstruktsioonide loomise ettepanekuid on laekunud ka alles hiljuti, millest laialdaselt aktsepteeritud MAC-protseduurina on suutnud ennast kehtestada Ameerika NIST

standardiseeritud protseduur C-MAC (varasem nimetus OMAC1). Selle kõrval on ka MAC-konstruktsioone, mis põhinevad räsifunktsioonidel, mille näitena võib esile tuua laialdaselt aktsepteeritud ja kasutust leidva HMAC kommentaarinõudest RFC 2104. Digiallkirjade jaoks sobilikud algoritmid on näiteks RSA, DSA (digitaalsignatuuri algoritm) või elliptilistel kõveratel põhinevad DSA variandid, näiteks ISO/IEC 15946-2, IEEE-standard P1363, lõik 5.3.3 (Nyberg-Rueppel Version), IEEE-standard P1363, lõik 5.3.4 (DSA Version).

- Kasutajate või komponentide autentimine – lihtne protseduur parooli küsimise autentimiseks. Kui paroolid edastatakse sealjuures krüpteerimata kujul üle võrgu, tehakse nende volitamata lugemine suhteliselt lihtsaks. Seetõttu tuleks siinkohal kasutada keerukamaid protseduure. Sobilikud protseduurid on näiteks ühekordsed paroolid (vt M 5.34 Ühekordsed paroolid), mille genereerimiseks võib kasutada nii tarkvaralisi kui ka riistvaralisi lahendusi. Siinkohal tuleks eelistada riistvaral põhinevaid autentimisprotseduure, sest nendega seotud organisatoorse töö hulk on väiksem ning saavutatav turbeaste on tarkvaralahendustega võrreldes suurem. Lisaks autentimine PAP või CHAP abil, mida rakendatakse kakspunktprotokolli puhul. Võimalik on ka autentimine CLIP/COLP abil, mida rakendatakse ISDN-i baasil toimiva kommunikatsiooni puhul.
- Üks levinud autentimisprotseduure on ka Kerberos-protokolli kasutamine, mille on välja töötanud MIT (Massachusetts Institute of Technology). Kerberose peamine rakendusala on võrgus olevate kasutaja/kliendi ja serveri vastastikune autentimine. Kerberose tsentraalseks turvalahenduseks on autentimispileti server (ticket-granting server), mis jagab pileteid, mille abil saavad kliendid ja serverid üksteist autentida. Nimetatud piletite abil on kasutajatel võimalik pärast ühekordset autentimist taotleda endale erinevate teenuste kasutamiseks vastavat seansivõtit.

Siin nimetatud digitaalallkirjadest tuleb eristada EL-i direktiivides või riiklikes õigusaktides määratletud elektroonilisi allkirju. Millisel määral saab siin nimetatud digitaalallkirju nende õigusaktide raames pidada elektroonilisteks allkirjadeks, tuleb eraldi kontrollida, ja see ei ole selle meetme objekt.

- Autentimine PAP või veel parem CHAP abil, mida rakendatakse kakspunktprotokolli puhul (vt ka M 5.50 Autentimine protokollidega PAP/CHAP).
- Autentimine CLIP/COLP abil, mida rakendatakse ISDN-i baasil toimiva kommunikatsiooni puhul (vt ka M 5.48 Autentimine funktsiooni CLIP/COLP kaudu).

Räsiprotseduur (hash)

Räsifunktsioonide krüptoanalüüsis on viimasel ajal tehtud suuri edusamme. Uute tulemuste valguses tuleb tõdeda, et SHA-1 kasutamist ei saa enam soovitada kõikide kasutusvaldkondade jaoks, kuid HMAC kasutamine on seevastu jätkuvalt turvaline. Sobivad algoritmid on veel RIPEMD-160 (juhul kui põrkekindlusele esitatavad nõuded on madalad, st umbes 80 bitti) ning eelkõige SHA-2 uuemad versioonid (SHA-224, SHA-256, SHA-384, SHA-512), mis on välja töötatud suuremat põrkekindlust vajavate rakenduste jaoks.

Räsialgoritm MD5 on vananenud ja ilmutab väga suuri puudusi, mida on võimalik juba praktiliste näidete abil esitleda. MD5 ei peaks seetõttu enam kasutama. Samuti ei soovitata enam RIPEMD-160.

Valikukriteeriumid

- **Mehhanismide tugevus** / **võtmepikkus** – krüptograafilise protseduuri üks olulisemaid valikukriteeriumeid on selle mehhanismide tugevus. Sümmeetriliste protseduuride puhul on väga oluline, et võtmed oleksid piisava pikkusega. Mida pikem on krüptograafilise protseduuri käigus kasutatava võtme pikkus, seda kauem võtab aega selle väljaselgitamine nt jõuründe korral. Teiselt poolt jällegi muutuvad protseduurid pikkade võtmete kasutamisel aeglasemaks, mistõttu tuleb alati kaaluda, milline on sobilik võtme pikkus, arvestades otstarbekuse ja vajaliku jõudluse aspektidega. Hetkel kehtib heade protseduuride (3DES, IDEA, RC5, AES) ja keskmise turbeastme kohta rusikareegel, et kasutatavate võtmete pikkus peaks olema vähemalt 100 bitti. Suuremate, struktureeritud andmehulkade krüpteerimisel plokkšifritega tuleks ECB-režiimist loobuda. Selle asemel tuleks kasutada kas CBC-režiimi või CFB-režiimi. Seetõttu peaks olema juurutatud vähemalt üks nimetud režiimidest. Asümmeetriliste protseduuride puhul peaks mehhanismide tugevus olema valitud selliselt, et põhjapanevate matemaatiliste probleemide lahendamine ei nõuaks üleliia suurt ehk siis praktiliselt võimatut arvutusvõimsust (valitav mehhanismitugevus sõltub seega ka algoritmide ja arvutustehnika hetkeseisust). Praegu võib lähtuda sellest, et umbes 2100 operatsiooniga ollakse veel „turvalisel poolel". Arvestatavad eksperdid on ennustanud, et 1024-bitiste RSA-moodulite murdmiseks läheb tarvis operatsioonide mahtu, mille suurusjärk on umbes 270 ning ka kõige paremate geneeriliste algoritmide 160-bitise korraldusega diskreetse logaritmiprobleemi murdmise töömaht jääb suurusjärku 280. Kuna operatsioonide maht 280 hakkab arvutustehnika arenguga liginema juba valdkonnale, mis on tehniliselt mõeldav, tuleks hetkel kasutatavad algoritmid, mille turbeaste on 80 bitti uuemate arenduste puhul kõrvale jätta ja pikemas perspektiivis välja vahetada. Plokkšifrite kasutamise korral peaks mitte ideaalselt juhuslikult jaotatud andmeid krüpteerima asjakohases autenditud krüpteerimisrežiimis, nagu GCM-režiim, või kombineerides plokkšifri režiimi, nagu CBC, CFB, või Counter-režiimi turvalise MAC-protseduuriga, nagu CMAC või HMAC, encrypt-then-MAC-režiimis (täiendavat teavet leidub selle kohta TR-02102-1 2. peatükis).

Hetkel võib lähtuda teadmisest, et kasutades

- RSA puhul mooduleid pikkusega 1536 bitti või
- sobival elliptilisel kõveral töötava ElGamal-protseduuri alamgruppide jaotusi suurusjärgus 200 bitti,ollakse hetkel veel „turvalisel poolel".

Pikema kasutuseaga turberakenduste jaoks tuleks kasutada 2048-bitiseid RSA-mooduleid või alamgruppide korraldust vähemalt 224-bitise võtmepikkusega.

Näiteid sobilike elliptiliste kõverate kohta leiate veebiaadressil www.eccbrainpool.org. Hoiduda tuleks „tundmatute" algoritmide kasutamisest, st kasutada tuleks algoritme, mis on avaldatud, paljude vastava eriala spetsialistide poolt intensiivselt läbi uuritud ja mille kohta puuduvad tuvastatud

turvaaugud. Tihti pakuvad tootjad müügiks turvatooteid, mis on varustatud uute algoritmidega, mis on „veelgi kindlamad ja töötavad palju kiiremini” kui kõik ülejäänud algoritmid. Kuid tundmatute, sellistest allikatest, mille krüptograafiaalane kompetents ei ole piisavalt tõestatud, pärinevate algoritmide kasutamise eest võib küll ainult hoiatada.

Sümmeetrilised või hübriidprotseduurid?

Puhtakujulisi avaliku võtmega süsteeme ei rakendata tavaliselt krüpteerimise eesmärgil, sest need vajavad suurt jõudlust. Kõik hetkel levinud avaliku võtmega krüptograafia juurutused kasutavad hübriidprotseduure (vt M 3.23w Sissejuhatus krüptograafia põhimõistetesse). Rakendustes, mille puhul on tegu kas suurte või avalike kasutajarühmadega, on enamasti soovitatav kasutada hübriidprotseduure (võtmehaldusest tulenevate eeliste tõttu). Väikeste, suletud kasutajarühmade puhul (eriti muidugi ka üksikkasutaja puhul) võib piirduda sümmeetriliste protseduuridega. Hübriidprotseduure kasutades on mõttekas viia sümmeetrilise ja asümmeetrilise protseduuri tugevused omavahel kooskõlla. Kuna asümmeetrilise protseduuri käigus toimub enne võtmete vahetamist reeglina paljude võtmete ülekrüpteerimine sümmeetrilise protseduuri tarbeks, tuleks asümmeetriline algoritm valida pigem veidi tugevam.

Tehniliste nõuete teostatavus

Šifreerimisalgoritmid peavad olema valitud sellised, et nende juurutamisel vajaminevaid tehnilisi nõudeid, eriti mis puudutab jõudlust, oleks võimalik ka reaalselt rakendada. Siia alla kuuluvad näiteks nõuded vigade leviku piiramiseks (nt kui edastus toimub tugeva müraga kanalites), aga ka sünkroonimine overhead'ile ja ajalisele nihkele (näiteks juhul, kui soovitakse suurte andmehulkade krüpteerimist reaalajas).

Näide: kõne krüpteerimine ISDN-i puhul

Kommunikatsioonivõrgu planeerimisel tuleb arvestada terve rea erinevate parameetritega, mis mõjutavad oodatavat kõnekvaliteeti ja mis võivad esineda müra, klõpsatuste, läbikostvuse või vilistamise näol. Niisuguste mõjurite hulka kuuluvad näiteks ka rakendatavad krüpteerimisprotseduurid. Korraliku kõnekvaliteedi tagamiseks tuleb arvestada ja hinnata kõiki piki ülekandeteed kulgevaid seadeldisi.

Üksikkomponentide eraldi vaatlemine ei ole oluliste üksikefektide koosmõju tõttu küll eriti õigustatud, kuid sellele vaatamata on siiski tähtis teada ka iga üksikkomponendi (nt krüpteerimiskomponendi) võimalikke mõjusid. Eelnevast võib tuletada raamtingimusi nii teostuse kui ka valiku tarbeks.

Krüpteerimiskomponendi käitumist iseloomustatakse sealjuures järgmiste tegurite abil:

- andmebloki krüpteerimiseks kuluv aeg (üldjuhul tekitab see viivitusi),
- sünkroonimise otstarbel andmevoogu täiendavalt sisseviidud juhtimisinfo (võib olenevalt olukorrast kaasa tuua kõikumisi),
- krüptokomponendi maksimaalselt töödeldav andmehulk (võib viia samuti kõikumiste tekkeni, kui on vajalikud vahesalvestamised),
- krüpteerimisest tulenev vastuvõtlikkus vigade levikuks (toob üldjuhul endaga kaasa vigade kasvu).

Äsja loetletud tegurite negatiivne mõju tuleb kõige selgemini esile kõne krüpteerimisel (reaalajas toimiv teenus), suurendades läbivatele protsessidele kuluvat aega, kutsudes esile kõikumisi protsesside kestvuses ning suurendades vigade tekke võimalust, st tegu on kvaliteedi langusega mida on võimalik mõõta ja siduda krüptokomponentidega.

Muud mõjurid

Teatud osa krüptograafilisi algoritme, (nt IDEA) on majanduslikul otstarbel kasutamiseks patenteeritud (sama kehtib ka ametiasutustele), mistõttu tuleb arvestada, et olenevalt olukorrast tuleb võibolla maksta ka litsentsitasusid.

M 2.165 Sobiva krüptotoote valimine

Algatamise eest vastutavad: IT turvaosakond

Rakendamise eest vastutavad: IT turvaosakond

Krüptograafiliste rakenduste valik on väga lai, pakkudes lahendusi alates lihtsatest andmete krüpteerimiseks mõeldud programmidest ühe kasutajaga PC jaoks, kohtvõrgu turvalisuse tagamiseks loodud krüptofunktsioonidega tulemüüriarvutitest kuni videokonverentside „reaalajas“ toimivate riistvaraliste krüpteerimislahendusteni välja. Nii laia valiku puhul saab mõistagi anda vaid üldistavaid soovitusi, mida tuleks krüptograafiliste toodete puhul arvesse võtta. Enne valiku tegemist tuleks kasutajal kindlaks määrata kõik tootele seatavad nõuded. Toode, mille kasuks otsustatakse, peaks katma võimalikult paljusid kasutaja esitatud nõudeid.

Funktsionaalsus

Väljavalitud tootel peavad olema kasutaja jaoks tähtsad funktsioonid, millest eriti olulised on järgmised kriteeriumid:

- põhiliste krüptograafiliste teenuste kasutamisvõimalus,
- võimalike kasutuskeskkonnast tulenevate lisanõuete täitmine (nt Single-User-/Multi-User-PC, LAN-keskkond, WAN-ühendamisvõimalus),
- piisava jõudlusega vajalikud tehnilised näitajad (nt läbilaskevõime),
- nõutud turvafunktsioonide olemasolu, mille puhul on eriti oluline, et kasutatavad krüptograafilised mehhanismid oleksid piisava tugevusega.

Koostalitlusvõime

Reeglina lisatakse väljavalitud toode juba olemasolevasse IT-keskkonda. Seetõttu on vaja, et toode oleks suure ühildumisvõimega. Valitud toote koostalitlusvõime tagamiseks olemasolevate IT-süsteemide ja süsteemikomponentidega on tarvis kinni pidada majasisestest standarditest. Rahvusvaheliste standardite rakendamine peaks krüptograafiliste tehnikate kasutamise puhul olema iseenesestmõistetav, kuna see kergendab muu hulgas ka krüptograafiliste komponentide turvalisuse hindamist.

Majanduslikkus

Väljavalitud toode peaks end võimalikult hästi ära tasuma. Arvesse tuleb võtta nii soetamiskulusid, tükiarve, hooldusele ja tehnilisele toele kuluvaid summasid kui ka võimalikku kulude kokkuhoidu, mida võivad endaga kaasa tuua ratsionaliseerimisefektid.

Sertifitseeritud tooted

Viimastel aastatel on suutnud kanda kinnitada rahvusvaheliselt tunnustatud IT turvatoodete hindamise metodoloogia: Euroopa ITSEC (Information Technology Security Evaluation Criteria), täpsemalt nende edasiarendus CC (The Common Criteria for Information Technology Security Evaluation). ITSEC, st CC pakub raamistikku, mille abil on võimalik hinnata IT-toote turbefunktsioone, leides neile tunnustatud kriteeriumide alusel täpse koha kindla määratlusega turvaklasside hierarhias. Paljude riikide infoturbeametid on nende kriteeriumite alusel koostanud omad riiklikud sertifitseerimisskeemid. Sertifikaadiga varustatud toote kasutamine annab kindluse, et vastava toote turbefunktsioone on kontrollinud sõltumatud

osapooled, ning et toote omadused ei ole nõrgemad, kui sertifikaadi väljastamisel kehtiv standard seda lubab (vt M 2.66z Sertifikaatidega arvestamine IT soetamisel).

Imporditud tooted

Paljudes riikides, eriti USAs kehtivad tugevatele krüptograafilistele toodetele hetkel (veel) ranged ekspordipiirangud. Piirangute tagajärjel muudetakse algselt väga tugevaid krüpteerimistooteid kunstlikult (võtme mitmekesisuse kahandamise teel) nõrgemaks. Niisuguste kunstlikult nõrgestatud krüpteerimisprotseduuride mehhanismide tugevus ei suuda enam tagada tavapärasele kaitsevajadusele esitatavaid nõudeid. Paljudes riikides ei ole kehtestatud krüptograafiliste toodete kasutamisele riigisiseseid piiranguid. Imporditud toodete puhul tuleks alati kontrollida, kas need on võimelised töötama täisvõimsusel või mitte.

Piirideülene kasutamine

Paljud ettevõtted ja ka asutused seisavad üha sagedamini silmitsi probleemiga, et ka rahvusvahelist kommunikatsiooni, nt välismaal paiknevate tütarettevõtetega, oleks tarvis krüpteeringuga kaitsta.

Probleemi lahendamiseks tuleks esmalt välja selgitada:

- kas kõnealustes riikides on kehtestatud piiranguid krüptograafiliste toodete kasutamisele ning
- kas väljavalitud toodetele võivad olla kehtestatud ekspordi- või impordipiirangud.

Väärkasutuse- ja tõrkekindlus

Krüptograafiliste toodete kasutamine on seotud ohuga, et kasutajad võivad hakata ennast tundma – tihtilugu siiski põhjendamatult – turvaliselt: „Kõik on ju krüpteeritud!” Seetõttu tuleb erilist tähelepanu pöörata meetmetele, mis aitaksid ära hoida ohtusid, mis tulenevad kasutajavigadest või tehnilistest riketest, sest nende tagajärjed ei piirdu mitte ainult lihtsa defektiga, vaid need võivad tekitada ka turvaaugu. Tuleb tõdeda, et varundatud süsteemide loomise ja täiendavate seirevõimaluste sisseseadmine on väga laiaulatuslik ettevõtmine ning täiendavate seadmetega seotud kulud on küllaltki suured, mistõttu tuleb vastavaid meetmeid vaadata iga juhtumi puhul eraldi ning lähtuda konkreetsetest nõuetest.

Juurutamine tarkvarasse, püsivarasse, riistvarasse

Krüptograafilisi algoritme on võimalik juurutada nii tarkvarasse, püsivarasse kui ka riistvarasse. Tarkvaralahendusi juhitakse reeglina vastava IT-süsteemi operatsioonisüsteemi abil. Püsivara alla liigitatakse programmid ja andmed, mis on salvestatud püsivalt riistavarasse selliselt, et salvestuste sisu ei ole võimalik dünaamiliselt muuta ega ka töötamise ajal modifitseerida. Riistavaraliste lahenduste puhul on krüptoprotseduur realiseeritud otse riistvaras, nt eraldiseisva turvamooduli või pistikkaardi näol.

Piisav dokumentatsioon

Väljavalitud toote dokumentatsioon peab kajastama seal kasutatavaid krüptograafilisi algoritme ja protokolle, et oleks võimalik õigel ajal reageerida nende vananemisele ja ebaturvaliseks muutumisele.

Üldistavaid soovitusi selle kohta, millist eespool loetletud variantidest eelistada, on väga raske välja tuua, kuna otsustamine sõltub erinevatest teguritest:

- krüptograafilise protseduuriga kaitstavate andmete kaitsevajadus ehk eesmärgiks seatav turbeaste,
- andmete soovitud läbilaskevõime,
- majanduslikud kaalutlused ja sundolukorrad,
- kasutuskeskkond ja ümbritsevad turbemeetmed,
- töödeldavatele andmetele kehtiv võimalik riigisisene liigitus.

Tarkvaralahenduste eelis seisneb on nende kergemas kohaldatavuses ja soodsamas hinnas. Riistavaralahendused on üldjuhul võimalike manipulatsioonide suhtes palju kindlamad (pakuvad seega ka suuremat kaitset) ning võimaldavad andmete suuremat läbilaskevõimet kui tarkvaralahendused, kuid on seevastu ka kallid. Püsivaralahendusi võib vaadelda kompromissina kahe eelneva lahenduse vahel.

Iga väljavalitud lahenduse eelised ja puudused on alati seotud vaid konkreetsete kohapealsete oludega (eelkõige puudutab see võtmehaldust). Kui andmed on juba kord krüpteeritud ja mööda kommunikatsiooniteekonda kuhugi teel, pole sellel, mil moel krüpteerimine aset leidis, põhimõtteliselt enam suurt tähtsust.

Üks näide (suhteliselt) soodsatest, kaasaskantavatest ja kasutajasõbralikest krüptomoodulitest on kiipkaardid, mida kasutatakse lokaalsel krüpteerimisel turvalise salvestusvahendina krüptograafiliste võtmete talletamiseks või autentimise valdkonnas paroolide genereerimiseks ja krüpteerimiseks.

Kõikide krüptograafilisele tootele seatud tingimuste kokkukogumisel saab koostada nõuete kataloogi, mida saab vajaduse korral kasutada ka hanke väljakuulutamisel.

Kontrollküsimused:

- Kas rakendatavad krüpteerimistooted täidavad kõiki neile esitatud nõudeid?

M 2.166 Krüptomoodulite kasutamist reguleerivad sätted

Algatamise eest vastutavad: IT turvaosakond

Rakendamise eest vastutavad: IT turvaosakond

Ka krüptomoodulite kasutamise käigus tuleb arvestada terve rea turbealaste nõuetega. Vastavad nõuded peavad olema adekvaatselt seotud tehnilise ja organisatoorse kasutuskeskkonnaga. Selle tagamiseks tuleb kehtestada teatud organisatsioonilised reeglid:

- Tuleb kindlaks määrata isikud, kes vastutavad krüptokontseptsiooni loomise, krüptotoodete väljavalimise ning nende toodete turvalise kasutamise eest.
- Kindlaks tuleb määrata personali puudutavad vajalikud meetmed ja need ka ellu rakendada (koolitus, kasutajatugi, töötajate asendamise kord, kohustused, tööjaotus).
- Töötajate koolitamine ei tohiks piirduda ainult sellega, kuidas käia ümber nende käsutusse antavate krüptomoodulitega. Töötajatele tuleb selgitada ka krüptomoodulite kasutamisega seotud eeliseid ja kasutamise hädavajalikkust, samuti peaksid nad saama ülevaate krüptograafilistest põhimõistetest (vt lisaks M 3.23w Sissejuhatus krüptograafia põhimõistetesse).
- Juhuks, kui krüptomoodulite kasutamise käigus tekib probleeme või koguni turvaintsidendi kahtlusi, peab olema selgelt määratletud edasine tegevuskava. Kõik töötajad peavad olema teadlikud vastavatest käitumisreeglitest ja teavitamisprotseduuridest.
- Krüptokontseptsiooni raames tuleb kindlaks määrata, kes, millal ja milliseid krüptotooteid kasutama peab ja seda teha tohib ning millised on sealjuures kehtivad peamised tingimused (nt võtmete deponeerimine).
- Et krüptomoodulid töötaksid korrektselt, tuleb neid regulaarselt kontrollida. Samuti tuleb regulaarselt kontrollida, kas kasutatavad krüptograafilised protseduurid vastavad kaasaja nõuetele või mitte (vt lisaks M 2.35 Teabe hankimine turvaaukude kohta).
- Tõrgeteta töö tagamiseks tuleb krüptomooduleid varuda kättesaadavusele esitatavate nõuete kohaselt, et vajaduse korral oleks neid võimalik kiirelt välja vahetada. Eriti oluline on see juhul, kui ligipääs krüpteeritud andmetele sõltub ühestainsast krüptomoodulist, nagu nt andmete arhiveerimisel või ISDNi krüpteerimisel.

Kohustuslik on tagada krüptomoodulite turvaline töö, mille alla kuuluvad järgmised punktid:

- Krüptomoodulite optimaalse konfiguratsiooni kindlaksmääramine enne nende kasutuselevõttu, nt seoses võtme pikkuse, töörežiimide või krüptograafiliste algoritmidega.
- Kindlaksmääratud konfiguratsiooni dokumenteerimine, et süsteemi võimaliku tõrke või taasinstalleerimise korral oleksid need kiirelt taastatavad.
- Krüptomoodulite konfigureerimine administraatorite poolt selliselt, et maksimaalne turvalisus oleks tagatud ilma kasutaja sekkumiseta.
- Käsiraamatute kättesaadavuse tagamine keerukamate krüptomoodulite korral.

- Krüptomoodulite turvaline installeerimine ja sellele järgnev testimine (nt kontroll, kas krüpteering toimib korrektselt ning kas kasutajad suudavad krüptomooduliga ümber käia).
- Kasutuskeskkonnale esitatavate nõuete määratlemine, mille teostuse puhul võib olenevalt olukorrast vaja minna ka täiendavate, IT-keskkonda puudutavate meetmete rakendamist. IT-süsteemidele, millel hakatakse kasutama krüptograafilisi protseduure, kehtivad omad kindlad turvanõuded, mida kajastatakse vastavates süsteemipõhistes moodulites, nt klientidele (ka süle-arvuti klientidele) ja serveritele esitatavad nõuded leiate moodulite kihist nr 3.
- Krüptomoodulite hooldusintervalli kindlaksmääramine.

Erinevaid vajalikke reegleid tuleb kehtestada ka võtmehalduse valdkonnas (vt M 2.46 Krüpteerimise õige korraldus):

- reeglid võtmete genereerimise ja valiku kohta,
- reeglid krüptograafiliste võtmete turvalise salvestamise kohta,
- võtmevahetuse strateegia ja intervalli määratlemine.

Kontrollküsimused:

- Kas krüptograafiliste protseduuride kasutamisele on kehtestud kindlad reeglid?
- Kas krüptokontseptsioon vastab hetkeolukorrale?
- Kelle poole võivad töötajad pöörduda krüptomoodulite kasutamist puudutavate küsimustega?

M 2.167 Andmete kustutamiseks või hävitamiseks sobivate lahenduste valik

Algatamise eest vastutavad: infoturbespetsialist, IT-juht, organisatsiooni juht

Rakendamise eest vastutavad: infoturbespetsialist, IT-juht, organisatsiooni juht

Kaitstavate andmete konfidentsiaalsuse tagamiseks tuleb need pärast kasutamist kustutada või hävitada nõnda, et andmete rekonstrueerimine oleks suure tõenäosusega välistatud. Andmete turvaline kustutamine ja hävitamine eeldab ühelt poolt sobivaid protseduure ja teisalt ka seadmeid, rakendusi või teenuseid.

Andmekandjatesse talletatud andmete kustutamiseks ja hävitamiseks on erinevaid meetodeid. Asjakohase lühiülevaate leiate meetmest M 2.433w Ülevaade meetoditest andmete kustutamiseks ja hävitamiseks . Alljärgnevalt antakse mõned olulisemad soovitused, mida järgida tänapäeva levinud andmekandjate kustutamisel ja hävitamisel.

Soovitusi andmete kustutamiseks

Operatsioonisüsteemide lihtsad kustutamisfunktsioonid ja andmekandjate formaatimine ei ole andmete kustutamiseks piisavalt turvalised. Seetõttu tuleks andmete turvaliseks kustutamiseks kasutada kas füüsikalisi lahendusi, nt mehaanilise, termiline või magnetiline töötlus, või kirjutada andmekandja sihipäraselt vähemalt üks või ka mitu korda üle. Ülekirjutamiseks on soovitatav kasutada juhuslikke andmejadasid. Andmekandjate puhul, mida hakatakse edasi kasutama täpselt sama turbeastmega valdkonnas, võivad andmete kustutamiseks võetavad meetmed olla leebemad kui nende andmekandjate puhul, mis endisest kasutuskeskkonnast lahkuvad ja nt edasi müüakse.

Järgneb enamlevinud andmekandjate kustutamismeetodite ülevaade.

- Paberdokumendid: usaldusväärne meetod puudub.
- Mikrofilm ja mikrofišš: usaldusväärne meetod puudub.
- Magnetiliste andmekandjatega kõvakettad, magnetlintkassetid, disketid: andmekandja kogu salvestiruumi täielik ülekirjutamine juhuandmetega ja tulemuse kontrollimine.
- Pooljuhtsalvestitega kõvakettad (SSD/hübriid): tavapärasest suuremate kaitsevajaduste jaoks seni usaldusväärne meetod puudub. Andmekandja on soovitatav krüpteerida täies mahus alates esmasest kasutamisest. Enne utiliseerimist tuleks see juhuandmetega üle kirjutada.
- Optilised andmekandjad (CD, DVD): tavapäraste kaitsevajaduste korral võib ülekirjutatavad andmekandjad, nagu CD-RW-d ja DVD-RW-d, kustutamise eesmärgil juhuandmetega üle kirjutada.
- Pooljuht-muutmälude (SRAM, DRAM) kustutamiseks tuleb elektritoide välja lülitada. Kui on olemas, tuleb enne väljalülitamist eemaldada varutoite aku. Väga suurte turbenõuete korral tuleb mälu eelnevalt ka juhuandmetega üle kirjutada.
- Pooljuht-püsimälud (EPROM, EEPROM, välk-EPROM) USB mälupulk, välkkaart, välkketas, PCMCIA-kaart. Väga suurte turbenõuete korral tuleb kogu mälu sobiva tarkvaraga kolm korda üle kirjutada.
- Kiipkaardid: usaldusväärne meetod puudub.
- Mitme funktsiooniga seadmed (koopiamasinad jne), millel on kõvakettad: tavapäraste turbenõuete korral tuleks andmed pärast väljaprintimist kustu-

tusfunktsiooniga vahemälust ära kustutada, suurte turbenõuete korral tuleb kõvaketas iga kord pärast andmete väljaprintimist juhuandmetega üle kirjutada.

Seadmete äraandmise ja väljavahetamise korral järgige meedet M 2.400 Printerite, koopiamasinate ja multifunktsionaalsete seadmete turvaline kasutuselt kõrvaldamine .

Järgmiste kustutamismeetodite kasutamisest tuleks loobuda, sest need ei ole piisavalt usaldusväärsed, st nende kasutamise järel on andmeid võimalik rekonstrueerida:

- kustutamiskäsud,
- üksikute failide ülekirjutamine,
- high-level formatting,
- low-level formatting.

Soovitusi andmete hävitamiseks

Standardi DIN 66399:2012 „Andmekandjate hävitamine" esimeses osas jaotatakse turbevajadused turvaklassidesse. Turvaklasside liigituse alusel kehtestatakse andmekandjatele erinevad turbeastmed. Tavapärastele turbenõuetele vastab turvaklass 2. Erinevate turvaklasside hävitamismeetodid ja purustamisel tekkivate osakeste suurus on reguleeritud standardi DIN 66399 teises osas.

Andmekandjate hävitamise võib jätta ka usaldusväärsete teenusepakkujate hooleks (vt M 2.436z Andmekandjate hävitamine välise teenusetarnija poolt).

- Paberdokumendid: hävitamiseks tuleks kasutada paberipurustajaid. Tavapäraste turbevajaduste korral tuleks lähtuda standardi DIN 66399 turbeastmest P-3, seevastu suuremate turbenõuete korral turbeastmetest P-4, P-5 või P-6 (vt ka M 2.435z Sobiva dokumendipurusti valik).
- Mikrofilm ja mikrofišš: turbeastme F-4 nõuete täitmiseks soovitatakse standardis DIN 66399 kasutada mehaanilist purustamist, kuid seni leidub nendele nõuetele vastavaid seadmeid väga vähe. Seetõttu tuleks andmekandjad pigem põletada. Põlemistemperatuur peab ületama 300 C ja põlemisprotsess peab kestma vähemalt 60 minutit.
- Kõvakettad: saab hävitada mehaaniliselt purustitega. Suurte turbenõuete korral ei tohi purustist väljuvate osakeste suurus ületada 300 ruutmillimeetrit (turbeaste H-5, DIN 66399). Tavapäraste turbenõuete korral võib osakeste suurus olla koguni 2000 ruutmillimeetrit (turbeaste H-4, DIN 66399). Väikesemõõtmeliste ajamimehhanismide korral peaks purustist väljuvate osakeste suurus olema vajaduse korral väiksem. Kõvakettaid saab hävitada ka termiliselt. Selleks tuleb kõvaketta ajamisüsteemi kuumutada vähemalt 15 minutit temperatuuril, mis ületab 1000 C.
- Magnetlindid, magnetlintkassetid: tuleks purustada seadmetes, mis vastavad standardi DIN 66399 turbeastmele T-3. Suuremate turbenõuete korral ei tohiks purustist väljuvate osakeste suurus ületada 30 ruutmillimeetrit (turbeaste T-5).

- Disketid, optilised andmekandjad (CD-d, DVD-d): neid andmekandjaid võib hävitada mehaaniliselt purustitega. Optiliste andmekandjate puhul ei tohi standardi DIN 66399 järgi purustist väljuvate osakeste suurus ületada 160 ruutmillimeetrit (turbeaste O-3). Suuremate turbenõuete korral (turbeaste O-4) peab osakeste suurus jääma alla 30 ruutmillimeetri. Optilisi andmekandjaid võib hävitada ka termiliselt. Selleks tuleb neid kas vähemalt 60 minutit kuumutada temperatuuril, mis ületab 300 C või põletada.
- Pooljuhtmälud (SRAM, DRAM, EPROM, EEPROM, USB mälupulgad, välkmälud, SSD-kõvakettad, PCMCIA-kaardid): neid andmekandjaid võib hävitada mehaaniliselt, kasutades sobivaid purusteid. Sobivad seadmed peavad vastama standardi DIN 66399 turbeastmele E-4. Neid võib ka põletada. Põletamisel tuleb andmekandjaid töödelda vähemalt 15 minutit temperatuuril, mis ületab 800 C.
- Kiipkaardid: võib hävitamise eesmärgil nii põletada kui ka purustada. Tavapäraste turbenõuete korral piisab, kui purustid vastavad standardis DIN 66399 kirjeldatud turbeastmele E-4.

Institutsiooni jaoks sobivate kustutamis- ja hävitamismeetodite valik sõltub andmesalvestuse liigist, andmekandjatest ja salvestatud andmetele kehtivatest turbenõuetest. Samuti tuleb arvestada andkandjate võimaliku edasise kasutusotstarbega. Seetõttu tuleb sobivate kustutamis- ja hävitamismeetodite väljavalimiseks teha vajaduste analüüs.

Analüüsimisel tuleks muu hulgas vastata järgmistele küsimustele:

- Mis tüüpi faile (millistes operatsioonisüsteemides ja millistes rakendustes), mis tüüpi andmekandjaid (nt optilisi või magnetilisi) ja kui suuri andmemahte (megabait, gigabait, terabait) on vaja turvaliselt kustutada?
- Kui suur on andmekandjatele salvestatud andmete turbeaste?
- Kui suur on andmekandja mälumaht? Kas analüüsitava hävitamismeetodi tulemus vastab turbeastme nõuetele?
- Kas andmekandjaid kasutati/kasutatakse edasi suure turbeastmega valdkonnas?
- Kas institutsioonil on juba soetatud andmete kustutamiseks ja hävitamiseks vajalikud vahendid? Kas need vahendid täidavad institutsiooni erinevat liiki andmekandjatele esitatud turbenõudeid?
- Millised kustutamis- ja hävitamismeetodid sobivad kõige paremini kasutatavate erinevat tüüpi andmekandjate turbevajaduste rahuldamiseks? Kui suured on koolituskulud, et tagada nende meetodite turvaline rakendamine?
- Kui suured on erinevat tüüpi andmekandjate oletatavad kogused, mida on tarvis kas kustutada või hävitada?

Andmete kustutamine ja andmekandjate hävitamine peaks toimuma võimalikult töökoha lähedal ja võimalikult kiiresti, et vältida andmekandjate vaheladustamist. Nõnda väheneb ka töötajate hulk, kes peavad andkandjatega kokku puutuma, ning seeläbi suureneb ka turve.

Olenevalt andmete turbevajadustest ja andmekandjate tüübist tuleb andmete turvaliseks kustutamiseks ja hävitamiseks kasutada erinevaid tööriistu või sead-

meid. Osade selliste tööriistade ja seadmete soetamine võib olla väga kallis, samuti võib tekkida probleeme nende korrektse kasutamisega. Seetõttu võib osutuda mõttekaks vajalike protsesside soetamine teenusena. Selleks tuleb kõik utiliseerimisele minevad andmekandjad asutuses esmalt kokku koguda. Kogumiseks tuleks sobivatesse kohtadesse üles seada muukimiskindlad anumad ja neid regulaarselt tühjendada.

Purustites tekib tavapärase kasutuse käigus loomulik kulumine. Seevastu seadmete väärkasutus ja nende rakendamine mitte ette nähtud andmekandjate hävitamiseks võib purusteid ka kahjustada. Seetõttu tuleb regulaarselt kontrollida, kas purustist väljuvate osakeste suurus vastab jätkuvalt nõuetele, nt vaadata aeg-ajalt oma silmaga, kas suurus vastab seadme kasutusjuhendis loetletud andmetele.

Otsus, milliste kustutamis- ja hävitamismeetodite kasuks erinevat tüüpi andmekandjate ja erinevate turbeastmete puhul otsustati, tuleb dokumenteerida. Samuti tuleb kirjalikult fikseerida nende nõuetekohane kasutamine. Töötajaid tuleb koolitada, kuidas väljavalitud kustutamis- ja hävitamismeetodeid õigesti kasutada ja seda eriti siis, kui kustutamis- ja hävitamiskohustus lasub töötajatel.

Kontrollküsimused:

- Kas erinevatele andmeliikidele on nende turbeastme alusel kehtestatud sobivad kustutamis- ja hävitamisprotseduurid?
- Kas töötajatele on korraldatud andmete kustutamis- ja hävitamisprotseduuride koolitus, mis õpetab eelkõige olemasolevaid tööriistu ja seadmeid õigesti kasutama?
- Kas erinevat liiki andmekandjatele salvestatud andmete turvaliseks kustutamiseks ja hävitamiseks on olemas asjakohased seadmed ja tööriistad?
- Kas hävitamisprotseduuri tulemuslikkust kontrollitakse regulaarselt?
- Kas andmekandjate hävitamiseks valitud meetod vastab tänapäeva tehnika tasemele (nt sobib andmekandja suurusega)?

M 2.168 IT-süsteemi analüüs enne süsteemihaldussüsteemi evitust

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: administraator

Enne süsteemihaldussüsteemi juurutamist peab vastavaid IT-süsteeme, mida hakatakse tulevikus sellega haldama, uurima ja analüüsima. Analüüsi tulemusel peab valmima süsteemi dokumentatsioon, mille saab võtta aluseks järgneva etapi planeeringute tegemiseks ja otsuste langetamiseks ehk süsteemihalduse strateegia väljatöötamiseks (vt M 2.169 Süsteemihalduse strateegia väljatöötamine). Väärate otsuste vältimiseks on vajalik, et hallatavaid süsteeme kirjeldav oluline informatsioon oleks võimalikult täpsel kujul olemas juba planeerimise faasis. Lisaks on võimalik kohapealsetest oludest tuletada konkreetseid nõudeid, mida soetatav süsteemihaldussüsteem peab suutma täita (K.O.-kriteeriumid). Kasutusele tuleb võtta järgnevad meetmed (koos nende kirjeldatud alammeetmetega), mis on ideaalvariandis süsteemi planeerimise ja jooksva töö käigus vastavalt IT-etalonturbe nõuetele juba rakendatud või hakatakse rakendama:

- Olemasoleva võrgukeskkonna läbivaatus (vt M 2.139 Olemasoleva võrgukeskkonna läbivaatus)
- Süsteemi konfiguratsiooni dokumenteerimine (vt M 2.25 Süsteemi konfiguratsiooni dokumenteerimine)

Kõik IT-süsteemid tuleb kaasata ja kirja panna. Eriti oluline on, et näiteks heterogeensete süsteemide puhul loetletaks kõik olemasolevad operatsioonisüsteemid, et hiljem oleks võimalik nende baasil sõnastada süsteemihaldussüsteemile vajalikke nõudeid.

- Riistvara ja tarkvara tuvastamine ja kontrollimine (vt M 2.10 Riistvara ja tarkvara inventuur) - Kui süsteemihalduse raames soovitakse hallata ka tarkvara (rakendustarkvarahaldus), tuleks siinkohal teha inventuur ja tulemus dokumenteerida. Alternatiivse lahendusena võib haldussüsteemile seada nõude, et see peaks suutma tarkvara automaatselt tuvastada (Autodiscovery , Software Discovery funktsioonid). Kumba varianti konkreetsel juhul eelistada, see sõltub tarkvarahaldusele seatud ülesannetest. Kui haldussüsteemi soetamise eesmärgiks on näiteks soov hallata automaatselt (laadida täiendeid, paigaldada uut tarkvara) juba olemasolevat tarkvarakogu, mille koostisosad ei ole täpselt teada, peab haldussüsteem suutma peale installeerimist tarkvara kooslust automaatselt tuvastada. Kui rakendusprogrammide halduse raames tahetakse täiendavalt hallata ka kasutajatasandil üksikuid tarkvarapakette, tuleb välja selgitada, kas vastav tarkvara toetab sellist funktsiooni (nt sobiva protokolli abil), mistõttu on jällegi vajalik kogu tarkvara eelnevalt inventuuri käigus üles märkida. Sellest tulenevalt koostatakse tulevasele haldussüsteemile erinevad nõuded (nt rakenduste haldusprotokolli olemasolu). Kui näiteks veebiserverit soovitakse hallata HTTP-l baseeruva haldusliidese abil, peavad haldussüsteemil olema HTTP-d toetavad hal-

dusfunktsioonid või liides vastavate laienduste jaoks, mis lubab integreerida ka oma tarkvaraarendusi. Lisaks hetkeolukorra dokumenteerimisele tuleks pöörata tähelepanu pöörata tulevase IT-süsteemi kujundamisele, sest haldussüsteem tuleb valida selline, mis suudaks kaasas käia ka IT-süsteemi planeeritavate muutustega (nt skaleeritavus).

M 2.169 Süsteemihalduse strateegia väljatöötamine

Algatamise eest vastutavad: IT-juht, IT turvaosakond

Rakendamise eest vastutavad: administraator, IT-juht

Administraatorid peavad võrgus olevaid komponente regulaarselt haldama. Vastavad tööd võivad olla väga erinevad, alates näiteks uute kasutajate loomisest kuni täiendava tarkvara installeerimiseni välja, mille jagatud ülesehitus võib nõuda osalise tarkvara installeerimist kõigile arvutitele eraldi (töövoosüsteemid, dokumendihaldussüsteemid jms). Suurte organisatsioonide puhul on ainuüksi uue kasutaja loomine küllaltki suur administratiivne ettevõtmine, sest võimaldamaks ligipääsu kasutaja jaoks volitatud arvutitele tuleb näiteks üksikrežiimis töötavad arvutid kõik üksipulgi vastavalt ümber konfigureerida. Moodsad võrgu toega operatsioonisüsteemid (nt Unix, Novell) on selleks otstarbeks varustatud mehhanismidega, mis aitavad administratiivset töökoormust langetada (nt tsentraliseeritud kasutajahalduse abil). Kui aga terve kohtvõrgu kõiki riistvaralisi ja tarkvaralisi komponente soovitakse hallata kõikidel tasanditel (tehniliselt ja organisatoorselt) ühtmoodi, tuleb ühelt poolt rakendada sobilikke tehnilisi abivahendeid ehk haldussüsteeme, kuid teiselt poolt arvestada ka asjaoluga, et vastavate süsteemide edukas toimimine sõltub suuresti loodavast haldusstrateegiast. Haldusstrateegias sõnastatud nõuded ja reeglid panevad aluse süsteemihaldusele, mida hakatakse teostama vastava haldustarkvara abil. Haldusstrateegia peab olema koostatud selliselt, et see arvestaks konkreetse ettevõtte või ametiasutuse spetsiaalsete vajadustega. Strateegia väljatöötamiseks tuleb läbida järgnevad sammud:

Haldussüsteemi hallatavate objektide kindlaksmääramine

Enne objektide tuvastamiseks vajalikku inventuuri (vt M 2.168 IT-süsteemi analüüs enne süsteemihaldussüsteemi evitust) peab olema kindlaks määratud, milliseid IT-süsteemi valdkondi tulevane haldussüsteem haldama hakkab:

- Millised arvutid, täpsemalt riistvara peaks kuuluma tulevase haldussüsteemi haldusalasse?
- Milline tarkvara peaks olema kaasatud haldussüsteemi töösse?
- Millised kasutajad ja kasutajarühmad peaksid olema haldussüsteemi töösse kaasatud?

Haldussüsteemis kasutatavate turvaeeskirjade kindlaksmääramine

Lisaks turvaeeskirjade kehtestamisele tuleb arvestada ka juba olemasolevate eeskirjade ja meetoditega. Asutuse või ettevõtte turvaeeskirjad on halduskontseptsiooni üks osa ja lisaks sellele peab halduskontseptsioon sisaldama ka näiteks andmekaitse eeskirju ning uue tarkvara juurutamise nõudeid, sest neid kõiki tuleb ka haldussüsteemi kasutamisel järgida. Ka haldussüsteemi kasutamise kohta tuleb vastu võtta reeglid või siis olemasolevad reeglid üle vaadata ja vajaduse korral muutunud olukorraga vastavusse viia ning seejärel kindlasti ka ellu rakendada.

Eriti kehtib see järgnevate valdkondade kohta:

- haldusfunktsioonide juurdepääsuõigused,
- haldussüsteemi dokumentatsioon,

- hädaolukorraks valmisoleku plaanide koostamine või kohandamine haldussüsteemi või selle üksikute komponentide avarii puhuks.

Algfaasis tuleks kindlaks määrata ka see, kuidas reageeritakse süsteemihalduse turvapoliitika reeglite rikkumistele. Sarnaselt IT teiste valdkondadega tuleb ka süsteemihalduse jaoks luua oma turvapoliitika või siis rakendada ametiasutuse või ettevõtte olemasolevat turvapoliitikat. Kuna haldussüsteem töötab tähtsamate võrgu- ja süsteemikomponentidega koostöös, hallates ja kontrollides nende funktsioone, on turvapoliitika rikkumisi selles valdkonnas väga raske tuvastada. Eriti oluline on defineerida asjakohased eeskirjad ja protseduurid, mida tuleb rakendada turvaeeskirjade rikkumise korral. Siia alla kuuluvad nii tehnilised (nt uute paroolide jagamine töötajatele pärast halduskonsooli turvarikke tuvastamist) kui ka organisatoorset laadi ümberkorraldused. Auditeerimise, andmekaitse ja IT-turbega tegelevad üksused tuleks protsessi kaasata juba planeerimisfaasis. Pärast haldussüsteemi evitamist peab vastavatel osakondadel olema juba selge, milliseid ülesandeid tuleb neil haldussüsteemi puhul täitma hakata. Näide: andmekaitse eest vastutav töötaja saab juba planeerimisfaasis järgida andmekaitsenõudeid, nt milliseid kasutajaandmeid süsteemihalduses kasutama hakatakse või kasutada tohib. Pärast süsteemi evitamist peab ta olema võimeline kontrollima andmekaitse eeskirjadest kinnipidamist. Sarnased nõuded kehtivad ka auditite ja IT-turbe eest vastutavatele töötajatele.

Haldussüsteemi tootevalikule kehtivate raamtingimuste kehtestamine

Süsteemihaldussüsteemi evitamine nõuab ulatuslikku ja hoolikat planeerimist. Paljud süsteemihaldussüsteemi strateegia osad sõltuvad muu hulgas ka sellest, kas neid on võimalik realiseerida ühe konkreetse toote abil või mitte. Kõik see toob endaga kaasa vajaduse haldusstrateegia koostamiseks ja toote (eel-) valikukriteeriumite kehtestamiseks.

Süsteemihaldusstrateegia koostamisel tuleks arvestada järgmiste punktidega:

- Kas on tarvis mitut haldusdomeeni? Kui vastus on jah, siis kuidas tuleks need moodustada? Haldusdomeenid võimaldavad jaotada hallatava süsteemi komponente erinevatesse rühmadesse. Rühmi omakorda on võimalik hallata jällegi teineteisest lahus. Väiksemate ja keskmise suurusega süsteemide puhul ei ole rühmadesse jaotamine ilmtingimata vajalik, kuid see võib aidata süsteemihaldust paremini struktureerida. Suuremate hallatavate süsteemide puhul on haldusdomeenide rühmadesse jagamine üldjuhul kohustuslik.

Haldusregioonide planeerimine sõltub siinjuures paljudest tegureist:

- Võrgu topoloogia – süsteemi jagamine haldusdomeenideks konkreetse võrgutopoloogia alusel on hea lahendus keskmise suurusega süsteemidele (eriti neil juhtudel, kui töötajate vastutus ei ole jaotatud eri astmete vahel).
- Organisatsioonilised vastutusalad ettevõtte või ametiasutuse sees – haldussüsteemi on võimalik üles ehitada organisatsiooni struktuuri alusel, luues näiteks domeenid nimedega „Arvepidamine”, „Programmeerimine” või

„Tootmine” ja „Tarkvaraarendus”. Ka turvatehnilised põhjused, mis jooksevad otsapidi kokku halduspoliitikasse, võivad olla aluseks erinevate haldusregioonide loomisel. Näitena võib siinkohal tuua olukorrad, kus teatud organisatsiooniüksuste haldusfunktsioone soovitatakse delegeerida nõnda, et lokaalne administraator saaks juurdepääsuõigused ainult nendele komponentidele, mis jäävad otseselt tema vastutusalasse.

- Olemasolev taristu – siia alla kuulub nt erinevate filiaalide geograafiline jaotus või töörühmade ruumiline jaotus hoone eri korruste vahel.
- Turvalisuse tegurid
- Mitut haldusregiooni võib vaja minna juhtudel, kus halduseks väljavalitud toode toetab küll iga regiooni puhul erinevaid krüpteerimismehhanisme, kuid milledest iga regiooni puhul saab kasutada vaid ühte. Kui üksikute halduskomponentide vahel soovitakse tõepoolest kasutada erinevaid mehhanisme, tuleb haldus mitmete regioonide vahel ära jagada. Näide: hallatav süsteem koosneb konfidentsiaalsete andmetega andmebaasiserveritest ja sinna juurde kuuluvatest klientidest, kes ise andmeid ei salvesta. Halduskonsool peaks serveritega suhtlema ainult tugeva krüpteeringu toel, sest haldussüsteem haldab ka vastavaid andmebaase. Klientidega suhtlemine seevastu peaks jõudluse nõuetest lähtuvalt toimuma ainult nõrga krüpteeringu toel. Niisuguse näite puhul tuleb üldjuhul moodustada kaks haldusregiooni: üks regioon serverite tarbeks ja teine regioon klientide haldamiseks.
- Mitme haldusregiooni loomine tõstab töökindlust, sest nt ühe haldusregiooni äralangemisel on võimalik teisi haldusregioone sellest sõltumata edasi hallata.
- Oma mõju on ka haldusregiooni kuuluvate hallatavate arvutite tükiarvul. Enamikul toodetel on kaasas ka soovitused, kui paljusid arvuteid suudab ühe regiooni haldusserver korraga hallata. Näiteks 200 arvutit ühe serveri kohta ei ole siinkohal üldse haruldane.
- Millised seadmed peaksid täitma haldusserverite funktsioone? Klientide arvu kasv toob endaga kaasa haldusserveri jõudluse languse. Seda asjaolu tuleb planeerimisel arvestada.
- Milline peab olema haldusserverite füüsiline järjekord ja millisesse kohta need üles seatakse? Serveri füüsilisel asukohal on näiteks oma mõju sellele, kuidas on serveri hallatavaid arvuteid võimalik võrgu kaudu serveriga ühendada. Mõningate platvormide puhul eksisteerivad näiteks miinimumnõuded serveri ja kliendi vahelise andmeside ribalaiusele (nt TME 10 klientide ühendamisel on ühenduse kiiruse miinimumnõue 14,4 kbit/s). Sellel on otsene mõju haldussüsteemi konfiguratsioonile ja see muudab vajalikuks nt uute arvutite soetamise või võrguühenduse väljaehitamise.
- Kas läheb tarvis nn lüüse (gateways) ja proksisid, mis peaksid võimaldama halduse hierarhilist ülesehitust ja/või looma võimalusi kolmandate isikute toodete ühendamiseks?
- Mõningad süsteemid teevad vahet niinimetatud hallatud sõlmede (managed nodes) ja lõppseadmete (endpoints) vahel. Mõlemal juhul on tegu töökohaarvutitega, kuid nende erinevus seisneb selles, mil moel need haldussüsteemiga koos töötavad. Näiteks lõppseadmed ei koosta vastupidiselt hallatud sõlmedele enda jaoks mitte ühtki haldusinformatsioone sisaldavat lokaalset andmebaasi, samuti ei ole lõppseadmeid võimalik kasutada haldusinformatsiooni edastamiseks teistele arvutitele. Siinkohal tuleb otsustada, millised

arvutid tuleks haldussüsteemi kaasata hallatava sõlme ja millised vaid lõppseadme töörežiimis. Üldjuhul tuleks suurem osa töökohaarvutitest ühendada lõppseadme režiimis.

Sellisel meetodil koostatud haldusstrateegia loob mitmeid nõudeid, mida soetatav haldustoode peaks suutma täita. Konkreetse toote väljavalimisel on abiks see, kui seada nõuded tähtsuse järjekorda. Haldusstrateegia tuleb uuesti läbi vaadata, et välja selgitada, kas olemasolevad funktsioonid suudavad tagada, et strateegiat oleks võimalik täies mahus realiseerida. Seetõttu võib olla hädavajalik strateegiat mõne valdkonna puhul ümber sõnastada. Näide: tootevalikust selgub, et süsteem, mis pakub tugevat krüpteeringut, ei toeta kahjuks haldusülesannete delegeerimist „alam-administraatoritele". Sellest lähtuvalt tuleb haldusstrateegiat kohandada (eelduseks on muidugi seatavate nõuete tähtsuse korrektne hindamine).

M 2.170 Nõuded süsteemihaldussüsteemile

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator

Süsteemihaldussüsteem on loodud kohtvõrgu (või virtuaalse kohtvõrgu) administraatori töö hõlbustamiseks. Selleks, et süsteemihaldussüsteem suudaks administraatorit piisavalt abistada, peab see vastama teatud nõuetele. Vastavale süsteemile esitatavad nõuded sõltuvad suurel määral plaanitavast kasutusvaldkonnast (vt M 2.169 Süsteemihalduse strateegia väljatöötamine) süsteemihaldussüsteemi jaoks välja valitud arhitektuurist (vt M 2.171 Sobiva süsteemihaldustoote valimine). Süsteemihaldussüsteemil peaksid olema järgmised funktsioonid:

- Kasutajahaldus - Siia alla kuulub kasutajakontode ja kasutajarühmade kontode lisamine, muutmine ja kustutamine.
- Kasutusreeglite haldus - Hallata peab olema võimalik nii kohtvõrku sisenevaid kui sellest väljuvaid, samuti Internetist kohtvõrku ja kohtvõrgust Internetti suunduvaid juurdepääsuõigusi.
- Tarkvarahaldus - Süsteemihaldussüsteemi abil peab olema võimalik lisada ja kustutada tarkvarakomponente ja laadida neile täiendeid. Sõltuvalt olukorrast võib olla vajalik, eriti juurutamisfaasis, automaatse installeeritud tarkvara tuvastusfunktsiooni olemasolu. Tarkvaralitsentside haldusfunktsioon on küll soovitatav, kuid tänapäevased süsteemid seda eriti ei toeta (vt lisaks lõiku rakendustarkvarahaldusest allpool). Erand: litsentsid on olemas nt faili kujul, st litsentsifaile on võimalik haldussüsteemi failijagamismehhanismide abil hallata.
- Süsteemi konfiguratsiooniandmete tuvastamine, muutmine ja haldamine.
- Rakendusandmete haldamine - Andmebaasifaile või rakenduste konfiguratsioonifaile peab olema võimalik hallata, st süsteem peab võimaldama andmebaaside uusi versioone või uusi konfiguratsioonifaile laiali jagada.
- Süsteemikomponentide jälgimine - See võib olla mõttekas ka väliste komponentide puhul, mis enda administreerimise alla ei kuulu nagu nt Internet Service Provider -i (ISP) marsruuterid, mille abil Internetiühendus toimib.
- Rakendustarkvarahaldus - Tarkvara peaks olema võimalik hallata rakenduste tasandil, nt WWW-serveri (realm) andmetele ligipääsu võimaldavate HTTP-pääsuõiguste haldamine. Reeglina sellist liiki halduse tugi toodetel puudub, sest selle eelduseks on rakenduste endi koostöövõime.

Ideaalis peaks niisugune süsteem lubama administreerivate ülesannete delegeerimist, nt et süsteemi administraator saaks anda töörühmade süsteemi administraatorile õiguse töörühma kuuluvatele arvutitele tarkvara installeerimiseks. Nimetatud mehhanism on eriti vajalik keskmiste ja suurte võrkude puhul. Võrgu ja süsteemi administreerimine toimub reeglina ettevõtte või ametiasutuse ühest ja samast haldusüksusest. Kuna mõningates valdkondades ei pruugi võrgu ja süsteemi administreerimise ülesannete erinevus päris selgelt esile tulla, on soovitatav jälgida, kui suures mahus oleks võimalik olemasolevat võrguhaldussüsteemi soetatavasse süsteemihaldussüsteemi integreerida. Lisaks äsjaloetletud eelkõige funktsionaalset laadi nõuetele tuleb süsteemihaldustarkvara valimisel arvestada ka oluliste tehniliste nõuetega (vt M 2.171 Sobiva süsteemihaldustoote valimine). Eriti olulised on siinkohal järgmised tehnilised nõuded:

- Haldussüsteem peab toetama kõiki halduses kasutatavaid ja hallatavate arvutite operatsioonisüsteeme (haldussüsteemil peavad olema operatsioonisüsteemide spetsiifikat arvestavad komponendid ja graafiline kasutajaliides).
- Kui lokaalne andmebaasisüsteem on juba olemas, peaks haldussüsteemis olema võimalus oma haldusalast informatsiooni olemasolevasse andmebaasisüsteemi ka salvestada.
- Haldussüsteem peaks olema laiendatav. See puudutab ühelt poolt haldussüsteemi komponente (nt moodulitele ülesehitatud kontseptsioon koos võimalusega mooduleid igal ajal juurde osta ja integreerida), kuid samas ka haldussüsteemi funktsioone (nt API-programmeerimisliides, mille abil oleks võimalik oma komponente järgi ühendada).

Käesoleva meetme raames esitletud nõuete kategoriseerimiseks võib üldjuhul kasutada meetmes M 2.171 Sobiva süsteemihaldustoote valimine kirjeldatud kriteeriumeid. Spetsiifiliste kategooriate nõuded saab tuletada, kui määrata kindlaks konkreetsed nõuded teatud „väärtusskaala“ piires.

Kontrollküsimused:

- Kas on kindlaks määratud nõuded kasutatavale süsteemihaldussüsteemile?
- Keskmised ja suured võrgud: kas süsteemihaldussüsteem võimaldab administratiivsete ülesannete delegeerimist?

M 2.171 Sobiva süsteemihaldustoote valimine

Algatamise eest vastutavad: IT-juht,
Rakendamise eest vastutavad: administraator
Peale süsteemi hetkeolukorra kindlaksmääramist (vt M 2.168 IT-süsteemi analüüs enne süsteemihaldussüsteemi evitust) ja haldusstrateegia väljatöötamist (vt M 2.169 Süsteemihalduse strateegia väljatöötamine) tuleb langetada valik sobiliku süsteemihaldussüsteemi kasuks. Sõltuvalt hallatava süsteemi suurusest võib antud ettevõtmine nõuda erinevaid lahendusi:

- Väiksemate süsteemide puhul võivad süsteemihaldust teha süsteemi administraatorid „käsitsi“.
- Väiksemate ja keskmise suurusega süsteemide süsteemihaldust on võimalik lahendada ka üksikute instrumentide (tools) kokkupanekuga.
- Suurte süsteemide haldamiseks tuleks kasutada süsteemihaldussüsteeme.

Moodsad võrgutoega operatsioonisüsteemid on reeglina juba varustatud funktsioonidega, mis lubavad kasutajaid ja kasutajarühmasid tsentraalselt hallata. Unixi puhul saab kasutada nt NIS või NIS+ protokolle, Windowsi keskkonnas saab kasutajaid hallata tsentraalselt Domain Controlleri abil. Sarnaseid võimalusi pakub ka Novell oma Intranetware ga. Reeglina eksisteerivad lisaks ka veel võimalused hallata kogu võrgu kasutusreegleid. Väikeste ja keskmise suurusega võrkude puhul on kõige suurematekskitsaskohtadeks tarkvarahaldus, arvutite konfiguratsioonide haldus ja süsteemikomponentide jälgimine. Probleemide kõrvaldamiseks võib kasutada täiendavad tarkvaralahendusi, mis suudavad ülesandeid ühe kaupa üle võtta. Võrguhaldusinstrumendi kasutamist võiks kaaluda eelkõige neis valdkondades, mis on võrguhaldusega juba kaetud (konfiguratsioonihaldus, jälgimine). Windows-keskkonna jaoks võib siinkohal nimetada erinevaid lahendusi nagu nt „Novell Zero Administration Kit“, mis suudab administraatorit aidata uute arvutite installeerimisel, „Microsoft Management Console“, mille abil saab luua tsentraliseeritud ülevaaate kõigist haldusinstrumentidest ning „Microsoft Systems Management Server (SMS)“.

Toode nimega SMS pakub administraatorile näiteks järgmisi võimalusi:

- riist- ja tarkvarakomponentide inventariseerimine
- andmete ja rakenduste installeerimine ja jagamine võrguarvutite vahel
- võrgurakenduste kasutamise kontrollimine
- võrgutugi arvutite administreerimiseks
- võrguliikluse jälgimine

Siinkohal tuleb arvestada, et SMS ei ole loodud heterogeense võrgukeskkonna tarbeks. Lisaks toimib kaughooldus samuti vaid poolautomaatselt ning nõuab administraatori kohalolu, mistõttu sobib see kasutamiseks ainult väikeste ja ruumiliselt üksteise ligidal asuvate võrkude puhul. Unixi keskkonnas saab näiteks tarkvara jagamise ja halduse jaoks kasutada programmi „rdist“, mis võimaldab installeerida tarkvara eemalasuvatele arvutitele. Sealjuures on võimalik tsentraalsest mälupuulist (pool) valida arvutite jaoks välja just selline tarkvara, mida töötajatel läheb konkreetselt oma tööülesannete täitmiseks tarvis. Täiendavad, ka tasuta kättesaadavad lisaprogrammid (tihti ülikoolide juures välja töötatud) võimaldavad

võrku jälgida näiteks SNMP protokolli abil. Eelneva näite põhjal koostatud lahendused on soodsa hinnaga alternatiiviks väikeste ja keskmise suurusega võrkudele.

Eelnimetud alternatiivsete lahenduste kasutamine nõuab siiski reeglina ka küllaltki kogenud administraatorit, kes peab sõltuvalt olukorrast suutma iseseisva programmeerimise teel süsteeme kohandada või lisafunktsioone integreerida. Suuremate ja suurte võrkude jaoks ei ole niisugused lahendused sobivad, sest funktsioonid on erinevate, omavahel integreerimata instrumentide vahel hajutatud. Suurte ettevõtete ja ametiasutuste võrkude haldamiseks tulevad kõne alla süsteemihaldussüsteemid. Enne niisuguse süsteemi evitamist tuleb endale teadvustada, et vastav ettevõtmine toob üldjuhul endaga kaasa laiaulatusliku sekkumise olemasoleva süsteemi töösse ning vajab seetõttu hoolikat planeerimist. Suurte võrkude puhul ei ole harvad juhtumid, kus süsteemi evitamisele kulub rohkem kui 12 kuud ja kuuekohaline summa eurodes. Seetõttu on õige haldussüsteemi valimine väga oluline.

Soetatava süsteemi valimisel tuleks arvestada järgmiste valikukriteeriumitega:

- Millised on toote poolt pakutavad funktsioonid?
- Kulutused:
- tarkvara soetamisega seotud kulud
- täiendava riistvara soetamise kulud (mõningate süsteemide puhul on tarvis soetada üks või mitu tsentraalset haldusserverit)
- installeerimise ja kasutamisega seotud kulu (sõltuvalt olukorrast tuleb plagata täiendavat tööjõudu väljastpoolt)
- töötajate koolitamiskulud
- muud kulud (nt olemasoleva platvormi migratsiooni kulud, lokaalse tarkvara kohandamine/uusarendused, ehituslikud meetmed nagu nt turvalise serveriruumi ehitamine)
- Investeeringukindlus
- Millisel määral on süsteemihalduse toode skaleeritav (nt kui paljudele arvutitele on võimalik seda laiendada)?
- Kas platvorm suudab ettevõtte kasvuga kaasas käia (nt võimalike loodavate haldusdomeenide arv, ülesannete delegeerimise võimalus)?
- Millised on platvormini viivad migratsiooniteed?
- Kuidas on olemasoleva platvormi migratsiooniteed häälestatud mõne teise platvormi suhtes?
- Teiste toodete integreerimisvõimalused?
- Milliseid serveri ja kliendi süsteemiplatvorme toetatakse?
- Kas olemasolevat võrguhaldussüsteemi on võimalik integreerida?
- Kas olemasolevat andmevarundussüsteemi on võimalik integreerida?
- Millised kolmandate tootjate poolt loodud rakendusi on antud toote kohta saadaval?
- Usaldusväärsus ja töökindlus
- Kas on olemas infot või koguni garantiisid maksimaalse seisakuaja kohta?
- Kas tsentraalsete komponentide puhul on võimalik kasutada hotswap funktsiooni?

- Kas süsteemil on olemas oma backup ja recovery mehhanismid? Haldussüsteemi sees peavad olema mehhanismid korrapäraseks taaskäivitamiseks, mis hakkavad tööle haldussüsteemi äralangemise korral. Mehhanismid peavad sõltuvalt vajadustest sisaldama ka võimalust varundatud andmete laadimiseks ja automaatseks järjepidevuse kontrolliks, mis peaks omakorda ideaalvariandis suutma lahendada ka tuvastatud ebakõlad.
- Kas tootele väljastatakse regulaarselt täiendeid? Kas nende lisamine on lihtne?
- Turvalisus: haldusfunktsioonide juurdepääsude piiramine
- Kas kasutaja-ID-tasandi juurdepääsu on võimalik piirata (millised kasutajad tohivad mida teha)?
- Kas komponentide tasandi juurdepääsu on võimalik piirata (millised arvutid tohivad mida teha)?
- Kas täidesaatvate käskude juurdepääsusid on võimalik kasutaja- või süsteemipõhiselt piirata?
- Kas haldusülesandeid on võimalik jaotada? Kas näiteks komponentide haldamist on võimalik piirata teatud valdkondade (nt ainult teatud osakonna arvutite) kaupa?
- Turvalisus: arvutite haldamine võrgu kaudu
- Kuidas kaitstakse kaugpöördusi?
- Kas kaugpöörduste puhul on võimalik kasutada krüpteeringut?
- Kas on tagatud, et enne kaugpöörduse teel läbiviidavat haldust toimub (tugev) autentimine?
- Kas õigust kaugpöörduse teel haldust teostada on võimalik siduda teatud kindlate isikute või töörollidega?
- Kas kasutajat informeeritakse kaugpöörduste kohta automaatselt?
- Turvalisus: andmete turvalisus, andmekaitse
- Kas kogutud andmed pannakse turvaliselt hoiule (juurdepääsu piirangud, krüpteerimine)?
- Kas halduskomponentide vahel aset leidev andmeside toimib turvaliselt (autentimine, krüpteerimine, tervikluse tagamine)?
- Kas kogutud andmete liiki on võimalik reguleerida (anonüümseks muutmine, tekke tuletamine, tõestatavus)?
- Kas viirusetõrjeprogrammide integreerimine on võimalik?
- Millised on pakutavad logimisvõimalused?
- Kas lokaalset tarkvara sisestamist on võimalik jälgida või takistada?
- Kasutajasõbralikkus
- Kas toode on varustatud graafilise kasutajaliidesega (nt X-Window, Motif, Windows-kasutajaliides, Web-Browser)?
- Kui lihtne on sellega navigeerida?
- Kas tootel on kohaliku keele või erinevate keelte tugi (globaalse kasutuse jaoks)?
- Kas programmide käivitamine on lihtne (ka eemalolevates arvutites)?
- Kui lihtne on kasutajal oma kasutajaliidest ümber kujundada?
- Kas toode informeerib kasutajat erandite ja hoiatuste kohta?
- Kas monitoring funktsiooni on võimalik ka detailselt seadistada?
- Kas võrgukomponentide keerukus on piisavalt „peidetud“ (selleks, et kasu-

taja ei peaks olema ilmtingimata iga hallatava komponendi ekspert)?
- Kas kõik funktsioonid on ligipääsetavad ühe ja sama kasutajaliidese kaudu?
- Kas tootel on olemas online abi ja kasutusjuhendid?
- Ergonoomilisus keerukate süsteemide haldamisel
- Kas tootel on erinevate võrguprotokollide, võrgukomponentide ja operatsioonisüsteemide tugi?
- Kuidas käitub platvorm geograafiliselt jagatud süsteemidega ja kuidas toimub nende kuvamine?
- Kui lihtne on uute komponentide süsteemi integreerimine või nende süsteemist eemaldamine (autodiscovery , käsitsi)?
- Vastavus standarditele (sõltuvalt keskkonnast võib olla vajalik, et toode vastaks vähemalt ühele standardile)
- Platvormid
- Arvutitootjate sihtasutuse (Open Software Foundation – OSF) poolt loodud Distributed Management Environment (DME)
- Desktop Management Task Force (DMTF) spetsifikatsioon
- Network Management Forum -i (NMFi) OMNIpoint spetsifikatsioon
- Andmebaas
- Milliseid DBMS-e (Data Base Management System -e) toetatakse?
- Kas neil juhtudel, kui haldustarkvara sisaldab oma andmebaasi, toetatakse päringukeelena ka SQLi?
- Object Management Group-i (OMG) CORBA (Common Object Request Broker Architecture)
- Application Program Interface (API), nendeks juhtudeks, kui haldussüsteemi on tarvis ise laiendada (nt API-d SNMP, XMP ja DMI jaoks).

Siin loetletud aspekte tuleks võtta kui haldussüsteemide hindamise pidepunkte. Haldussüsteemile esitatavate nõuete sõnastamisel tuleb arvestada kohalike olude ja süsteemi hetkeolukorraga (vt M 2.168 IT-süsteemi analüüs enne süsteemihaldussüsteemi evitust), samuti haldusstrateegiaga (vt M 2.170 Nõuded süsteemihaldussüsteemile), sõnastades nende abil „K.O.-kriteeriumid“ mis on abiks otsuste langetamisel. Ülalnimetatud kriteeriumid tuleks seada tähtsuse järjekorda, mis peegeldaks kohalikest oludest tulenevaid eelistusi. Haldussüsteemile seatavaid nõudeid ja väljavalitud haldussüsteemi kasutusvõimalusi ei ole reeglina võimalik viia teineteisega täielikult kooskõlla. Seetõttu tuleb eelnevalt koostatud haldusstrateegia pärast konkreetse toote väljavalimist vastavalt toote funktsioonidele ümber töötada.

Kontrollküsimused:

- Kas sobiva süsteemihaldussüsteemi valik toimub varem kindlaks määratud nõuete alusel?

M 2.172 Veebilehe kasutamise kontseptsiooni väljatöötamine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT-turvaosakond

Rakendamise eest vastutavad: administraator, IT-juht

Enne veebilehe sisseseadmist tuleb luua vastav kontseptsioon, mis võtab kokku, millist informatsiooni ja teenuseid hakatakse pakkuma. Kontseptsioon peaks koosnema vähemalt ühest üldosast ja ühest organisatoorset külge puudutavast osast.

Eesmärkide ja sisu kindlaksmääramine

Kontseptsiooni üldosas tuleks kirjeldada:

- millised on organisatsiooni eesmärgid seoses veebilehe loomisega,
- millised on veebilehe sihtgrupid ning
- millist informatsiooni või teenuseid tahetakse veebilehe vahendusel pakkuma hakata.

Välimus ja sisu toimetamine

- Kontseptsiooni organisatoorset külge käsitlevas osas tuleks anda ligilähedane ülevaade sellest, kes vastutab organisatsiooni sees
- Info kättesaadavuse ja uuendamise eest ning
- Veebilehe optilise välimuse kujundamise ja hooldamise eest (webdesign).

Tehniline osa

- WWW-kontseptsiooni organisatoorses osas tuleks kindlaks määrata isikud, kes hakkavad vastutama veebiserveri tööshoidmise tehniliste aspektide eest. Veebilehe kontseptsiooni tuleks regulaarselt kontrollida, et see ei oleks aegunud. Organisatsiooni enda strateegia ja eesmärkide muutumisel tuleb kontrollida, millised on nende mõjud WWW-kontseptsioonile.

Kontseptsiooni väljatöötamise käigus tuleb arvestada järgmiste aspektidega:

- Kasutusotstarve mõjutab turvalisuse nõudeid - Veebilehe võib sisse seada ka ainult lihtsa sisenemisinformatsiooniteenusena, mis on intraneti keskseks osaks, või siis avaliku ligipääsuga Internetis, pakkudes sel juhul juba erinevaid teenuseid. Sõltuvalt planeeritavast kasutusalast on erinevad ka veebiserveri teenustega seotud turvanõuded. Väikestes organisatsioonides, kus veebiserverit kasutatakse intraneti serverina ilma turvalisuse seisukohast kriitiliste rakendusteta, on vastavad turvanõuded hoopis teistsugused kui veebiserveri puhul, mida on tarvis ühendada Internetti ja mis võib sisaldada isegi andmeid, millele ei peaks igaüks juurde pääsema.
- Tulemüür - Juhul kui WWW-teenuseid soovitakse pakkuda nii intraneti kui ka Interneti keskkonnas, on soovitatav kasutada kahte teineteisest lahutatud süsteemi: üks veebiserver intraneti jaoks ja üks veebiserver Interneti jaoks. Kui Interneti veebiserverit on tarvis ühendada lisaks ka mõne sisevõrguga, tuleb sisevõrku üleminekut tulemüüriga kaitsta, vt B 3.301 Turvalüüs (tulemüür) . Kui on ette nähtud, et veebiserveri teatud sisu saadakse mõnest andmebaasist, tuleb veebiserveri tulemüüri kontseptsiooni koostamisel silmas pidada ka veebiserveri ja andmebaasi vahelist ühendust. Infoserverite

paigutuse alased nõuanded on kokku kogutud meetmesse M 2.77 Serverite integreerimine tulemüüri . Veebilehe kontseptsiooni väljatöötamisel tuleks vähemalt üldistavalt paika panna see, kuidas toimub Internetti ühendamine ning millist liiki internetiühendusi on selleks tarvis. Internetti ühendamine võib aset leida alles siis, kui eelnevalt on kontrollitud, kas väljavalitud WWW-kontseptsioon ja töötajate poolt täidetavad ning organisatsioonilised raamtingimused on piisavad, et tulla toimekõikvõimalike ohtudega.

- Väljasttellimise kaalumine - Veebiserverit, mis esitleb organisatsiooni Internetis, ei pea ilmtingimata antud sama organisatsioon ise käitama. Kui organisatsiooni enda käituskulud või halduskulud osutuvad selleks liiga kõrgeks või kui jääkohtusid on liiga raske hinnata, võib kaaluda veebiserveri käitamiseks kas vastavate internetiteenuse pakkujate (Internet Service Providers) või muude teenusepakkujate teenuste kasutamist (vt B 1.11 Väljasttellimine (Outsourcing))

Täiendavad kontrollküsimused:

- Kas veebilehe kohta on olemas vastav kontseptsioon?
- Kas vastavat kontseptsiooni kontrollitakse ja täiendatakse vajadusel pidevalt?

M 2.173 Veebiserveri turbestrateegia väljatöötamine

Algatamise eest vastutavad: asutuse/ettevõtte juhtkond, IT-turvaosakond

Rakendamise eest vastutavad: administraator, IT-juht

Veebiserverid on ründajatele küllaltki atraktiivsed sihtmärgid, sest edukaks osutunud ründega kaasneb tihti väga suur avalik tähelepanu. Seetõttu tuleb veebiserveri turbesse suhtuda väga tõsiselt. Enne veebiserveri sisseseadmist tuleks koostada veebiserveri turbestrateegia, milles kirjeldatakse kasutatavaid turvameetmeid ja nende ulatust. Veebiserveri turbestrateegias kindlaks määratud nõuete põhjal on võimalik regulaarselt kontrollida, kas kasutatavad meetmed on piisavad.

Veebiserveri käitamisega seotud turbestrateegia peaks andma vastused alljärgnevatele küsimustele:

- Kes vastutavad veebiserveri turvalise käitamise eest (administraatorid) ja kelle ülesanne on hallata sisu (toimetajad)?
- Kuidas on korraldatud vastutavate töötajate koolitamine, eriti seoses võimalike ohtude ja kohustuslike turvameetmetega?
- Kes saavad veebiserveri pääsuõigused ja millised on nende volitused?
- Kes tohib millist informatsiooni kättesaadavaks teha?
- Kes vastutab info värskuse ja korrektsuse eest? Kui teatud valdkonnas on info kättesaadavaks tegemise õigusega isikuid või organisatsiooni allüksuseid rohkem kui üks, peab olema ametisse nimetatud ka peavastutaja, kes otsustab võimalike konfliktide üle.
- Millised teised süsteemid ja võrguühendused on vajalikud veebiserveri turvalise töö tagamiseks? Kas süsteemide rikete ja avariide korral on vajadusel võimalik neid ajutiselt ümber lülitada?
- Millist infot ei tohi veebiserveris kättesaadavaks teha (nt põhjusel, et see on konfidentsiaalne, avaldamiseks ebasobilik või et see ei sobi firma/asutuse poliitikaga kokku)?
- Kas andmete edastamisel veebiserverilt kliendile tuleb kaitsta nende terviklust ja konfidentsiaalsust? Kas on vajalik kasutada veebiserveri autentimist kliendi suhtes või kliendi autentimist veebiserveri suhtes?
- Millised võiksid olla veebiserveri juurdepääsule kehtivad piirangud (vt M 2.175 Veebiserveri ülesseadmine)?

Organisatsiooniliste reeglite või tehniliste lahendustega tuleb tagada alljärgnevad turbeaspektid:

- Veebiserverile tohib paigutada ainult selliseid faile, mida on lubatud avalikustada. Tuleb määrata kindlaks, millist liiki infot tohib avalikustada ning kes seda teeb.
- Enne failide paigutamist veebiserverile tuleb neid kontrollida kahjurvara ja keelatud jääkinfo suhtes. Lisaks tuleb kontrollida (vähemalt pisteliselt), kas failide sisu avalikustamine on lubatud.
- Veebilehel on tungivalt soovitatav aktiivsisust loobuda.

Kõik veebiserveri kasutamise reeglid tuleb esitada kirjalikult ning need peaksid olema töötajatele alati kättesaadavad. Toimetajad peavad enne veebiserveri ka-

sutamist läbima koolituse, et vältida väärkasutust ja tagada organisatsioonisisese poliitika järgimine. Eelkõige tuleb töötajaid teavitada võimalikest ohtudest ja nõutavatest turvameetmetest.

Tegutsemine turvaintsidentide korral

Eriti neil juhtudel, kus veebiserver majutab ka avalikku veebilehte, peab turbestrateegia sisaldama muu hulgas tegutsemisjuhiseid selle kohta, kuidas toimida veebiserveriga seonduvate võimalike turvaintsidentide korral (vt B 1.8 Turvaintsidentide käsitlus).

- **Infoleke** - Kindlaks tuleb määrata, kuidas toimida, kui tuvastatakse, et veebiserveril on avalikustatud lubamatut infot. Mõningatel juhtudel ei pruugi nende dokumentide kustutamisest ainuüksi piisata, sest paljud külastajad võivad olla seda infot juba lugenud. Selline juhtum tuleb vähemalt dokumenteerida. Olenevalt informatsiooni sisust tuleb vajaduse korral informeerida olukorrast pressiteenistust, infosüsteemide haldajat, ettevõtte või asutuse juhtkonda või väliseid osakondi.
- **Häkkerite rünnak** - Tuleb kirjeldada, kuidas toimida siis, kui tekib kahtlus, et häkkerid võivad rünnata veebiserverit. Ennekõike tuleb lahendada küsimus, millal tuleks server avariikorras võrgust lahti ühendada ning kes peab selleks otsuse langetama.
- **Näotustamine** - Tuleks määrata kindlaks, kuidas reageerida veebiserveri näotustamise ehk defacement 'i korral ehk juhul, kui pärast veebiserveri edukat rünnet on ründajad muutnud veebiserveril olevaid andmeid või koduleh-te. Üldjuhul tuleb niisuguses olukorras teavitada juhtunust ka ametiasutuse või ettevõtte juhtkonda või info avalikustamise eest vastutavat organisatsiooni allüksust.

Nende punktidega tuleks arvestada isegi siis, kui veebilehe kaitsevajadust on hinnatud väikeseks. Häkkerite rünnak või näotustamine ehk defacement ei sõltu konkreetsest kaitsevajadusest ning selle ohvriks võivad langeda kõik avalikud veebilehed. Üks turbestrateegia osa peab olema ka regulaarne info hankimine võimalike ohtude kohta, et ennetada nende võimalikke tagajärgi. Peale meetmes M 2.35 Teabe hankimine turvaaukude kohta nimetatud andmeallikate on heaks kohaks veebikasutuse turbeinfo hankimisel veel ka „World Wide Web Security FAQ". Selle dokumendi leiate ka aadressilt http://www.w3.org/Security/Faq/.

Kontrollküsimused:

- Kas on olemas värske veebiturbestrateegia, milles on toodud ka vastavate turbemeetmete maht?
- Kas on olemas eeskirjad, mis reguleerivad veebiserveri spetsiifikaga seotud turvaintsidentide käsitlemist?
- Kas turvaaukude ennetamiseks hangitakse regulaarselt infot?

M 2.174 Veebiserveri turvaline kasutamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

Veebiserverid on ründajatele atraktiivsed sihtmärgid ja nende turvaline käitamine eeldab väga hoolikat konfigureerimist. Operatsioonisüsteem ja tarkvara peavad olema konfigureeritud selliselt, et arvuti oleks võimalikult hästi rünnakute eest kaitstud. Niikaua kuni arvuti ei ole piisavalt turvaliselt konfigureeritud, ei tohi arvutit võrku ühendada. Veebiserveri rakenduse konfigureerimisel tuleks olenemata kasutatavast rakendusest arvestada teatud üldiste aspektidega. Kuidas neid üksikutel juhtudel konfigureerida, sõltub konkreetsest veebiserveri rakendusest. Enamasti on võimalik valikutest kindlaks määrata, kas HTTP-päringu korral, kui sellega soovitakse pääseda mõnda kataloogi (st korrektset failinime sisestamata), kuvatakse päringu puhul vastava kataloogi sisu või selle asemel hoopis mõned muud kindlad failid (nt index.html). Konfigureerimiseks tuleb toimida järgmiselt:

- Kui indeksifail on olemas, saadetakse see päringule vastuseks.
- Kui indeksifaili ei ole, saadetakse vastuseks asjakohane veateade.

Programmide ja skriptide käivitamine

Kui on võimalik kehtestada, et programme ja CGI-skripte tohib käivitada ainult teatud kataloogide piires, tuleks need võimalused seadistada kõikidel juhtudel võimalikult suurte piirangutega. Mitte mingil juhul ei tohiks lubada programmide käivitamist terve WWW-valdkonna raames. Programmide ja skriptide jaoks on soovitatav luua eraldi kataloog ning lubada käivitamist ainult selles konkreetses kataloogis.

Sümbolilised lingid ja kiirvalikud

Tihti on võimalik määrata, kas faile või katalooge kuvatakse WWW-failipuus koos sümboliliste linkide (Unix) või kiirvalikutega (Windows) või jäetakse need kuvamata. Sellise info kuvamist tuleks võimaluse korral vältida, sest niimoodi võivad muutuda liiga kergelt kättesaadavaks ka need failid, mida ei soovita avalikustada. Näiteks on turvalise käitamise tagamiseks soovitatav regulaarselt läbi töötada järgmine kontrollnimekiri.

Kontrollnimekiri

1. Kas installitud on ainult vajalikud komponendid?

2. Kas veebiserverirakenduse konfiguratsioonis on kehtestatud võimalikult suured piirangud? Näiteks peaks CGI-programmide kasutus olema kas täielikult tõkestatud või piirduma kindla kataloogiga. Veebiserveri tööprotsessiks vajalik juurdepääs failidele peaks olema võimaldatud ainult ühe kindla kataloogipuu osa kohta. Serveri haldamiseks ja kasutamiseks tuleks kasutada eraldi, privilegeerimata kasutajatunnuseid.

3. Kas kõik liigsed CGI-programmid, asp-leheküljed, muud demo -rakendused ja veebilehed on kustutatud?

4. Kas juurdepääs on võimaldatud ainult vajalikele portidele (vt ka M 4.97 Ainult üks teenus serveri kohta)? Tavaliselt kasutatakse veebiserveri HTTP-teenust läbi pordi nr 80. Kui serverit hallatakse või veebiserveri faile hooldatakse läbi võrgu, võib tarvis minna ka lisateenuseid. Niisugusel juhul tuleks juurdepääsu vastavate

teenuste kasutamisele võimalikult suurel määral piirata (vt M 4.98 Side piiramine miinimumini paketifiltritega).

5. Kas on tagatud andmete sobilik regulaarne varundamine (vt B 1.4 Andmevarunduspoliitika)?

6. Juhul kui kasutatakse CGI-programme, kas need on programmeeritud piisavalt turvaliselt? Sisestatavaid väärtusi ei tohi olla võimalik kontrollimata üle võtta. Tuleb tagada, et Buffer-Overflows ja Race-Conditions oleksid välistatud. Kõikides Perl-skriptides peab olema aktiveeritud Taint-Check.

7. Kas regulaarseks tervikluse kontrolliks on olemas toimiv meetod (nt Tripwire, vt M 4.93 Regulaarne tervikluse kontroll)?

8. Kas konfiguratsiooni kontrollitakse regulaarselt? Kas konfiguratsiooni muudatused dokumenteeritakse?

Näide: Lihtsa veebiserveri ülesehitus

Lihtsa veebiserveri all mõeldakse serverit, mille lehekülgede sisu muutub harva, mille puhul ei kasutata CGI-programme ning millel pole ka spetsiaalset juurdepääsukaitset. Veebidokumendid laaditakse veebiserverile mõnelt andmekandjalt. Sellise serveri puhul saab kõik süsteemifailid ja HTML-leheküljed varustada ülekirjutuskaitsega. Niisuguse ülesehituse puhul on ründajal võimalik muuta küll ajutisi faile ja logi sissekandeid, kuid süsteemi ennast enam mitte. Selline juurdepääsukaitse tuleks lahendada füüsilise andmekandjaga, millel on ülekirjutuskaitse, nt CD-ROM-iga või ülekirjutuskaitsega vahetatava kettaga. Siiski tuleks regulaarselt korraldada vähemalt tervikluse kontrolle (vt M 4.93 Regulaarne tervikluse kontroll). Http-deemoni ebavajalikud funktsioonid, näiteks CGI-skriptide käivitamine, tuleb välja lülitada. Alati tuleb eemaldada kaasa pandud CGI-programmid. Lihtsa veebiserveri ühe levinud variandi puhul on võimalik veebiserveri dokumente vastavate õigustega muuta interaktiivseks. Sellistel juhtudel on eriti oluline, et oleks tagatud volitamata muudatuste kaitse ja regulaarne, lühikeste intervallide tagant korraldatav tervikluse kontroll.

Täiendavad kontrollküsimused:

- Kas veebiserver on tööle seatud selliselt, et see oleks võimalikult hästi rünnete eest kaitstud?
- Kas veebiserveri turvalist käitamist kontrollitakse regulaarselt?
- Kui indeksifail puudub, kas kataloogi kohta laekuvatele HTTP-päringutele kuvatakse vastuseks veateade, ja kui indeksifail on olemas, siis indeksifail?
- Kui programmide või CGI-skriptide jaoks on võimalik määrata kohad, kus need käivitatakse, siis kas programme ja CGI-skripte saab käivitada ainult nende jaoks määratud kataloogides?
- kas linkide (Unix) või otseteede (Windows) kuvamine WWW-failipuus on võimalik?

M 2.175 Veebiserveri ülesseadmine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtorgan

Rakendamise eest vastutavad: administraator, IT-juht

Veebiserveri kasutuselevõtt

Veebiserveri ülesehitamiseks on tarvis soetada lisaks sobivale riistavarale ka asjakohane tarkvara. Antud valdkonna tootevalik on väga lai. Toodete valimisel on lisaks stabiilsusele üheks väga oluliseks faktoriks ka turvalisus (vt B 1.10 Tüüptarkvara).

Organisatsiooni struktuuri kohandamine

Eelnevalt tuleks läbi mõelda, millist informatsiooni soovitakse teha Interneti või intraneti keskkonnas kättesaadavaks. Samuti tuleks selgitada, kus ja kuidas vastavad dokumendid luuakse, kes loob millised dokumendid, milliseid dokumente hakatakse kasutama ning kellele on neid dokumente tarvis. Eelnimetatud info põhjal tuleks luua ühtsed reeglid dokumentide, failinimede ja kataloginimede läbivalt ühtlase välimuse kujundamiseks ning määrata võimalusel ka standardsed arendustööriistad. Sõltuvalt vajadustest tuleks võibolla moodustada töörühm, kes hakkab tegelema veebi toimetamisega (vt M 2.272 Veebitoimetajate meeskonna loomine .

Vastutavate töötajate nimetamine

Veebiserveri kasutamise puhul, ükskõik, kas tegu on organisatsioonisisese või väljapoole avatud lahendusega, ei tohiks igal kasutajal olla õigust faile oma suva järgi seadistada. Seetõttu tuleks nimetada informatsiooni kättesaadavuse eest vastutav töötaja, kes vaatab uued failid enne avaldamist üle ning kontrollib muuhulgas ka nende vastavust reeglitele. Sõltuvalt organisatsiooni suurusest võib ametisse nimetada ka osalise vastutusega töötajad, kelle ülesanded on seotud kas konkreetse allüksuse või veebiserveri kindlaksmääratud valdkondadega. Sõltuvalt sellest, kuidas organisatsiooni struktuuri veebiserveril kajastatakse, tuleb kindlaks määrata ka veebiserveri pääsuõiguste jagamine ja kataloogistruktuur. Esmatähtis on see, et igal osalise vastutusega töötajal oleks juurdepääs ainult tema poolt hallatavatele alamkataloogidele.

Reeglite järgimise automaatne kontroll

Vastav kontrollimine, kas serveril olevad failid ja kataloogid on kooskõlas asjakohaste reeglitega, peaks toimuma automaatselt, nt sobivate skriptide ja makrode toel. Sobilikul moel ettevalmistatud programm tuleks teha kõigile kättesaadavaks ning see tuleks käivitada peale igat muutust. Protsessi käigus tuleks eriti hoolikalt kontrollida, kas kõikide

- kataloogide,
- failide ja
- CGI-skriptide (juhul kui kasutatakse)

pääsuõigused on korrektselt seadistatud. Tehtud muudatused peaksid kajastuma kohe logis, mis on vastava protsessiga otseselt seotud.

Õiguste ja töörollide kontseptsioon

Veebiserveri sisseseadmisel ja käitamisel on üheks levinumaks probleemiks küsimus, kuidas tuleks lahendada paljude erinevate töötajate omavaheline koostöövõime juhtudel, kui töötajate kompetentsid on erinevad. Erinevaid tööülesandeid nagu näiteks:

- uute materjalide koostamine,
- veebiserveri haldamine,
- veebilehe graafiline disain,
- üksikute tabelite koostamine,
- veebiserveri lisafunktsiooni programmeerimine (nt ühendamine andmebaasiga) ja
- lisafunktsioonide programmeerimine, mida kasutavad WWW-kliendid (Javascript jne),

täidavad reeglina ka erinevad töötajad. Tehnilistel põhjustel ei ole pääsuõiguseid võimalik teineteisest lõplikult eraldada, st see ei õnnestu mitte kunagi täielikult. Seetõttu ei saa arendatava süsteemi puhul reeglina pääsuõiguste piirangute sisseseadmisel aluseks võtta eelnevalt loetletud tööülesandeid. Niisugustel juhtudel tuleb näiteks pöörata tähelepanu sellele, et arendatavas süsteemis ei hoitaks konfidentsiaalset infot. Produktiivse veebiserveri pääsuõigustele on võimalik seada ka sellises keskkonnas piiranguid. Lisaks vastutusaladele tuleb planeerimise käigus arvestada ka vajalike tegevuste ülekandevõimalustega. Lisaks eelpool mainitud pääsuõiguste kontrollivajadusele puudutab see veel ka avalikuks tehtavate materjalide sisu kontrollimist.

Veebiserveri pääsuõiguste piiramine

Enne veebiserveri kasutuselevõttu ja täiendamist tuleb kindlaks määrata, kellel on õigus veebiserveril olevale infole ligi pääseda. Tuleb kindlaks määrata, kas infole pääsevad ligi ainult organisatsiooni enda töötajad, vajadusel ka mõningad kaugtöötajad või hoopis kõik organisatsioonivälised kasutajad või ainult mõned väljavalitud isikud. Vastavad piirangud võivad sõltuvalt informatsiooni sisust erineda. Kui veebiserverile juurdepääsu omavate inimeste ring peaks olema piiratud, tuleb selleks rakendada vastavaid meetmeid nagu nt M 4.94 Veebiserveri failide turve . Lisaks on tarvis eelnevalt kindlaks määrata, kas veebiserveril olevatele andmetele on võimalik ainult ligi pääseda või saavad kasutajad ka ise lisada sinna uut informatsiooni. Ka siin tuleb kindlaks määrata inimesed, kellele antakse vastavad volitused.

Ülevaatlik struktuur

Kuna HTML-faile ei ole tarvis hierarhiliselt struktureerida, ei ole kataloogi struktuur veebiserveri funktsioneerimise seisukohast üldse oluline. Hooldamise lihtsustamiseks tuleks siiski püüelda ülevaatliku struktuuri loomise suunas.

Ülevaatlikud andmeteede nimed

Kataloogi struktuur on soovitatav valida selline, et URL, mille kaudu teatud failini jõutakse, annaks juba ka ise mõningast informatsiooni selle faili kohta. Sõltuvalt olukorrast võivad andmeteede nimed seeläbi venida küll suhteliselt pikaks, kuid andmeasukohtade meeldejätmine ja uuesti ülesleidmine muutub külastajatele seeläbi palju lihtsamaks. Kuna paljud Interneti otsingumootorid näitavad päringu tulemusena ära terve WWW-andmetee, parandab sellisel moel loodud kataloogistruktuur ka informatsiooni ülesleidmist. Kuna ka teistes veebiserverites võidakse luua linke teie serveril asuvatele dokumentidele, tuleks vältida dokumentide ja kataloogide nimede muutmist. Seetõttu tuleb kataloogi struktuuri planeerimisel arvestada ka võimalike laiendamisvajadustega.

Dokumentide kättesaadavaks tegemine

Internetti ülespandud avalik veebileht on organisatsiooni visiitkaardiks. Seetõttu tuleb Internetis avalikustatavad materjalid piisavalt hoolikalt ette valmistada. Enne veebiserveri ühendamist Internetti on soovitatav veebilehte katsetada intraneti keskkonnas. Alustada tuleks siinkohal väheste ja lihtsamate rakendustega. Tavaliselt luuakse veebilehel kasutatavad materjalid HTML-failidena, mida kuvatakse otse veebilehitsejas. Lisaks HMTL-failidele on võimalik infot allalaadimise teel kättesaadavaks teha ka ükskõik millistes muudes formaatides. Sellistel juhtudel peab kasutaja IT-süsteemis olema sobiv rakendus, mis suudab avada vastavaid failiformaate, ning kui kasutaja soovib faile edasi töödelda, tuleb need reeglina salvestada kasutaja IT-süsteemi. Kui kättesaadavaks tehtud dokumentide puhul ei ole ette nähtud, et kasutajad võiksid neid iseseisvalt muuta (nt blankette täita), tuleks dokumendid teha kättesaadavaks niisugustes failiformaatides, kus muudatuste tegemine on raskendatud. Tootjapoolseid dokumendiformaate tuleks võimaluse korral vältida.

Kvaliteedi tagamine

Kõik Internetis avaldatavad HTML-dokumendid ja WWW-failid peaksid enne avaldamist läbima täpselt samasuguse kvaliteedikontrolli ja saama avaldamiseks kinnituse nagu ükskõik millised muud avaldamisele minevad materjalid. HTML-dokumendid luuakse üldjuhul spetsiaalsete HTML-editoridega. Muudes failiformaatides loodud dokumente saab HTML-konverterite abil muuta HTML-dokumentideks. Kui avaldamist vajavate dokumentide arv on suur ning avaldatud dokumentide sisu võib tihti muutuda, on mõttekas ühendada veebiserver vastava dokumendiandmebaasiga. Niisugune lahendus pakub kasutajatele kiireid võimalusi dokumentide otsimiseks, vaatamiseks ja haldamiseks. Samuti võib olla tööks kasulik, kui andmebaasiühenduse kaudu luuakse juurdepääs juba olemasolevatele firmaandmetele. Sellisel juhul tuleks siiski andmebaasiserver ja dokumendi andmebaas kaasata WWW-turvapoliitikasse. Enne uute failide lisamist veebiserverile tuleb kontrollida, kas need sisaldavad mingisugust jääkinformatsiooni (vt M 4.64 Ülekantavate andmete kontrollimine enne edastamist/peidetud info kõrvaldamine).

Konfiguratsiooni haldus

Kogemustele toetudes võib öelda, et WWW-leheküljed muutuvad küllaltki tihti, seetõttu on vajalik, et oleks loodud hästi toimiv konfiguratsioonide haldus. Kontrollida tuleb linkide ja viidete aktuaalsust, samuti tuleb enne avaldamist läbi teha viiruste kontroll, kasutades selleks kõige värskemate täienditega viirusetõrjetarkvara.

Kontroll ja kinnitamise protseduur

Väga oluline on, et kõik avaldatavad materjalid läbiksid eelnevalt kindlaksmääratud ja arusaadava kontrolliprotsessi. Kontroll peaks hõlmama nii sisu kvaliteedi kontrollimist kui ka formaalset kinnitamisprotseduuri. Kontrollida tuleb muuhulgas ka seda, kas materjalid on üleüldse avaldamiseks sobivad, et välistada nt konfidentsiaalsete materjalide, andmekaitsest tulenevate piirangutega või autoriõigustega kaitstud materjalide avaldamist. Suuremahuliste veebilehtede puhul oleks mõttekas kasutada Web-Content-Management -süsteeme. Vastavad süsteemid muudavad paljud veebilehe hooldamisega seotud tööprotsessid lihtsamaks. Informatsioon, mille avaldamine on saanud heakskiidu elektroonilise meedia vahendusel, peaks olema varustatud digitaalse allkirjaga, andes niiviisi kõigile lugejatele võimaluse kontrollida kättesaadava informatsiooni autentsust. Materjalid, mis ei peegelda organisatsiooni seisukohti, tuleb vastavalt tähistada.

Õiguslike raamtingimuste järgimine

Veebiserveri käitamisel tuleb arvestada erinevate seadustest tulenevate raamtingimustega. Näiteks ärilistel eesmärkidel loodud veebilehe puhul nõutakse, et veebileht peab olema varustatud kontaktandmetega, kus on välja toodud vastutava isiku nimi ja kontaktaadress. Sõltuvalt veebilehe sisust ja tegevusvaldkonnast võivad kehtida veel ka täiendavad kohustuslikud nõuded. Enne veebilehe avalikuks muutmist peab olema selgeks tehtud, millist informatsiooni seal avaldatakse ning kus ja millisel kujul seda avaldada tuleb.

Täiendavad kontrollküsimused:

- Kas veebiserveril avaldatavate dokumentide jaoks on kehtestatud ühtsed reeglid nende sisu ja kuju kohta? Kas on olemas reeglid ühtse välimuse kohta?
- Kuidas tagatakse dokumentide piisav kvaliteet enne nende avaldamist?
- Kas õiguste ja töörollide jaotumise kohta on olemas vastav kontseptsioon?
- Kas dokumendid läbivad enne veebiserveril avaldamist loa saamise protseduuri?
- Kas linkide toimimist kontrollitakse regulaarselt?
- Kas kõik kohustuslikud andmed nagu nt kontaktandmed on olemas?

M 2.176z Sobiva internetiteenuse pakkuja valimine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: IT-juht

Internetiteenuse pakkujad (Internet Service Providerid, lühidalt ISP-d) pakuvad erinevaid teenuseid, infot ja tehnilisi lahendusi, mis toetavad interneti kasutamist ja veebilehtede tööshoidmist. Institutsioonid peaksid teenusepakkuja valimisel olema hoolikad. Teenusepakkuja, kelle vahendusel on kasutajad internetti ühendatud, koondab enda kätte mitte ainult andmed sisenevate ja väljuvate meilide kohta, vaid ka info kõikide veebilehtede kohta, mida kasutajad on külastanud. Lisaks liiguvad kõik andmed, mida kasutaja arvuti ja internetis asuv server omavahel vahetavad, läbi teenusepakkuja IT-süsteemi. Internetiteenuse pakkuja valimisel tuleks välja selgitada:

- kas kõnealune teenusepakkuja suudab tehniliste probleemide korral tagada ööpäevaringse kompetentse abiteenuse;
- kuidas on teenusepakkuja valmistunud ühe või mitme IT-süsteemi avariiks (avariiplaan, andmevarunduse kontseptsioon);
- kui suurt käideldavust suudab teenusepakkuja tagada (maksimaalne seisakuaeg);
- kas teenusepakkuja kontrollib regulaarselt kliendini viivaid ühendusi, et need oleksid stabiilsed, ja võtab vastumeetmeid, kui ühendused ei ole stabiilsed;
- millised interneti kasutamist kajastavad andmed salvestatakse teenusepakkuja süsteemi ja kuidas teenusepakkuja neid andmeid lubamatu ligipääsu eest kaitseb;
- milliseid abinõusid kasutab teenusepakkuja oma ja kliendi IT- süsteemide turbeks.

Teenusepakkujal tuleks lasta kirjalikult kinnitada, et ta käitab oma IT-süsteeme turvaliselt (vt M 2.174 Veebiserveri turvaline kasutamine) kirjeldatud nõuetele. Teenusepakkuja peaks täitma kõiki võrguühenduses olevatele süsteemidele ja andmeedastusseadmetele kehtivaid olulisi nõudeid. Iga teenusepakkuja puhul peaks olema iseenesestmõistetav, et tal on olemas nii IT-turbe kontseptsioon kui ka turbe-eeskirjad. Teenusepakkuja peaks võimaldama turbe-eeskirjadega tutvumist. Teenusepakkuja töötajad peaksid olema teadlikud IT-turbega seotud aspektidest, turbe-eeskirjade järgimine peaks neile olema kohustuslik ning nad peaksid regulaarselt läbima koolitusi (mitte ainult turvalisuse vallas). Teenusepakkuja juures salvestatakse kasutaja andmed, mida on tarvis arve koostamiseks (nimi, aadress, kasutajatunnus, pangaandmed), samuti ühenduse andmed ning olenevalt teenusepakkujast ka lühema või pikema perioodi jooksul edastatud andmete sisu. Teenuse tellijad peaksid teenusepakkuja käest järele uurima, milliseid kasutaja kohta salvestatud andmeid kui pika aja jooksul säilitatakse. Teenusepakkujaga tuleb lepinguliselt kinnitada kõik koostöötingimused ja kokku leppida sobivad teenusetaseme lepingud (Service Level Agreements, SLA-d), nt kontaktisikud, reaktsiooniajad, IT-ühendused, teenuse kontroll, turvanõuete täitmine, konfidentsiaalse info käsitlemine (vt M 2.253 Välise teenusepakkujaga sõlmitava lepingu koostamine).

Täiendav kontrollküsimus:

- Kas institutsiooni ja teenusepakkuja vahelise koostöö raamtingimused on reguleeritud lepinguga?

M 2.177 Kolimise turve

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: organisatsiooni juht, tehnikajuht, IT-juht, IT turvaosakond

Kolimise käigus tuleb lisaks mööblile transportida ka erinevaid andmekandjaid (nt paberit, diskette, magnetlinte, CD-ROM-e) ja IT-süsteeme. Transpordi käigus lahkuvad IT-süsteemid, info ja muu materjal bürooruumide turvalisest keskkonnast ning nende transportimisega tegeleb personal, kellel puudub tavaolukorras juurdepääs vastavatele vahenditele. Kolimise käigus, eriti kui kolitakse organisatsiooni suuri üksusi, tekib alati teatud määral segadust, mida ei saa kunagi lõplikult vältida ning igat kolimiskasti ei ole võimalik pidevalt isiklikult jälgida. Sellele vaatamata tuleks hoolitseda, et kolimise käigus ei tekiks olukordi, kus volitamata isikud võiksid tundlikule infole ligi pääseda, samuti tuleb vältida info kaotsiminekut või kahjustamist. Kolimisest tuleks IT turvaosakonnale ja andmekaitse eest vastutavale töötajale võimalikult varakult teada anda, et vastavad üksused saaksid kolimise jaoks omad raamtingimused määrata:

- Kolimise planeerimise käigus tuleks juba algfaasis detailselt paika panna, kes, millal ja milliste kolimisele kuuluvate vahenditega kuhu ümber kolib (kolimise kontseptsiooni loomine). Kolimiskontseptsiooni loomine peaks olema iseenesest mõistetav, sest see aitab pärast kolimist tööfunktsioonidega sujuvalt jätkata.
- Olenevalt andmete kaitsevajadusest tuleb kindlaks määrata raamtingimused, millega peab transportimise käigus arvestama. Näiteks tundlike andmete transportimiseks tuleks kasutada lukustatavaid transportimiskaste (vt M 2.44 Andmekandjate pakkimine edasiandmiseks) või tuleb andmed enne tarnsportimist krüpteerida.
- Enne igat IT-süsteemi transportimist tuleks luua nendes olevate andmete varukoopiad. Siinkohal tuleb lisaks meetmes M 6.35 Andmevarunduseks vajalike protseduuride määratlemine kirjeldatud nõuannetele jälgida hoolikalt ka seda, et varundatud andmeid ei tohi mitte mingil juhul transportida koos IT-süsteemidega, millest need andmed varundati. Selle nõudega välistatakse olukorrad, kus kõik salvestised saavad kas korraga kahjustada või lähevad üheskoos kaduma.
- Kolimisega seotud töötajate jaoks tuleb välja töötada kontrollnimekiri (kolimise kontrollnimekiri), kus on täpselt kirjas, millised turvameetmed on töötajatele kohustuslikud.

Kolimise käigus ei ole kriitiline faktor sugugi mitte ainult transportimine, vaid ka transportimisele vahetult eelnev või järgnev ajavahemik, sest kogemused näitavad, et just neil hetkedel võivad paljud asjad kaotsi minna ja standardsed turvamehhanismid, nagu nt sissepääsu kontroll, ei toimi veel piisavalt.

Kolimise käigus peaksid olema täidetud vähemalt teatud minimaalsed organisatsioonilised nõuded:

- Kõikide transporditavate materjalide kohta tuleb koostada transpordipaberid, millest on võimalik välja lugeda,

1. kas transportimisel tuleb arvestada mõne kindla transpordiliigiga (nt purunemisohtlik, spetsiaalsed arvutitransportimise nõuded jne),
2. kuhu tuleb saadetis kohale toimetada (täpsed andmed hoone, korruse ja ruumi kirjelduse kohta),
3. kes on volitatud isikud saadetist vastu võtma,
4. kes saadetisele järele tuli või kes selle kohale toimetas (koos nime, kuupäeva ja kellaajaga).

- Transporditav kaup peab olema tähistatud selliselt, et seda on võimalik üheselt identifitseerida ja jälgida seeläbi ka transpordi teekonda. Transporditava kauba tähistus ei tohiks sisaldada liigset infot kaubas leiduva võimaliku tundliku info kohta. Märgistamine tuleks valida selline, et seda ei oleks võimalik liiga kergesti võltsida. Kolimise eeltöödega seotud töötajad võivad selle tarbeks luua spetsiaalsed kolimisetiketid. Etikettide kasutamisel tuleks arvestada ka sellega, et etikette peaks saama kolimise järel ilma kaupa määrimata eemaldada, st ilma et need kolitavat kaupa liigselt määriks või kahjustaks.
- Inimeste tulek ja minek ei tohiks kolimise käigus olla suvaline ja kontrollimatu. Kolimisteenuse kasutamise puhul peaksid kolimisfirmad organisatsioonile eelnevalt teada andma oma töötajate isikud. Töötajate ootamatu vahetumise korral (puhkus, haigestumine jne) tuleks kolimisfirmal teada anda ka asendustöötajate isikud. Kolimisega seotud isikute nimekirja alusel saavad uksehoidjad või muud organisatsioonisisesed töötajad teha pistelisi või ka lauskontrolle. Kolimisega seotud väljastpoolt tulev tööjõud peaks olema varustatud nähtavate lubadega (vajaduse korral koos nimedega), et sissepääsuõigusega inimesed oleksid teistest selgesti eristatavad.
- Transporditav kaup, eriti andmekandjad, tuleb pärast transportimist turvaliselt hoiule panna. Ruumid, kus kolimisega seotud tegevused on lõppenud ja ühtki töötajat kohal ei viibi, nt ruumid, mis on kas veel tühjaks kandmata või kuhu on just äsja kogu kaup kohale toimetatud, tuleks lukku panna.

Pärast kolimise lõppu tuleks võimalikult kiiresti taastada korrapärane töö. Esimese sammuna tuleb bürooruumides taastada taristuline ja organisatoorne turvalisus:

- sissepääsu kontroll tuleks taastada täies mahus,
- koridoridest tuleks eemaldada kogu tuleohtlik materjal, st kolimiskastid tuleks paigutada koridoridest uutesse tööruumidesse,
- kolitav kaup tuleb üle kontrollida, kas loetelu on täielik, kas kõik töötab nii nagu peab ja kas manipuleerimine on välistatud,
- juhul kui kolitav kaup tuleb iga vastava töötaja poolt kohe pärast kohaletoimetamist üle kontrollida, tuleks ette valmistada ka blankett ehk kadunud asjade nimekiri. Vastava blanketi võib töötajatele juba eelnevalt laiali jagada, et kolimisele minev kaup üles märkida. Niimoodi saab ka asendustöötaja, kelle kolleeg viibib puhkuse, haiguse või kiireloomuliste tööülesannete tõttu parasjagu eemal, kolimise käigus kaduma läinud asjad kiiresti kindlaks teha ja sellest teada anda. Töötaja, keda kolimise käigus asendati, peaks saama vastavast kolimisdokumendist koopia, et võimalike vastuolude ilmnemisel oleks tõend, mille alusel saab ebakõladest teada anda.

Erilise hoolega tuleks kolimise käigus jälgida serverite ja võrguühenduselementide käekäiku, sest ka üheainsa võrgukomponendi avarii võib põhjustada olukorra,

kus terve võrgu funktsioon on halvatud. Seetõttu peaks IT-administratsioon võtma enne kolimist tarvitusele erinevad abinõud, mis tagaksid, et tööprotsessid kulgeksid tõrgeteta:

- Võimalikult vara enne kolimist tuleb välja töötada plaan, kuidas viiakse läbi vajalikud muudatused seoses kasutajate ühendamisega. Siinkohal tuleb eriti täpselt analüüsida, kas töötajate arvutite probleemivaba ühendamise jaoks on tarvis soetada uusi vahendeid või mitte. Ka turbe seisukohast on tähtis teada, milliseid muudatusi toob kolimine endaga kaasa IT-süsteemide omavahelises andmesides. Olenevalt töövaldkondade kaitsevajadusest võivad tekkida näiteks nõuded, et teatud võrguühendused tuleb varustada krüpteeringuga või siis tuleb keelata juurdepääs teatud andmebaasidele.
- Enne kui töötaja ümber kolib, peab olema tagatud, et ta on oma uues bürooruumis kohtvõrgu abil kättesaadav, ning et tema jaoks vajalikud rakendused ja teenused on töövalmis. Selle tagamine nõuab lisaks lõppseadmetes tehtavatele muudatustele (marsruutimine, tarkvara konfigureerimine jne) ka kiireid muudatusi serveri poolel koht- või laivõrgu marsruuterites. Vajalike tööde hulka võib kuuluda uute aadresside või marsruuterite sisseseadmine ja vanade kustutamine. Vajaduse korral tuleb eelnevalt soetada uusi võrgukomponente ja need vastavalt seadistada.
- Kolimise käigus tuleb tihti ette, et kolivatele töötajatele tuleb uue serveri alla luua uued kasutajakontod. Siinkohal tuleb jälgida, et kasutaja uued pääsuõigused oleksid seadistatud ka rakenduste ja protokollide kohta. Ka kasutajakeskkonna turvaseadistused peavad töötajate turvaprofiilides säilima. Kasutajate vanad sisestused ja lõppseadmete pääsu sisestused tuleb vanas süsteemis kas vastavalt kohandada või ära kustutada. Juurdepääs kasutaja enda andmetele peaks siiski teatud üleminekuaja jooksul säilima, kuid samas tuleb selgelt teada anda, et juurdepääs on ajutine ning üleminekuaja möödudes need andmed kustutatakse. Pärast üleminekuaja möödumist peab administraator vastavad andmed kustutama.

Arvutuskeskuse komponentide, nt andmeserverite või kommunikatsiooniserverite puhul tuleb kolimise käigus järgida spetsiaalseid meetmeid. Alljärgnevalt kirjeldatakse meetmeid, mis peaksid tagama vastavate komponentide võimalikult lühikese seisakuaja:

- Kui võimalik, tuleks uus server installeerida juba enne kolimist ja selle tööd tuleks uutes ruumides katsetada. Kui see ei ole võimalik, tuleks vanale serverile teha võimalikult hea eelseadistus ning server tuleks uuesti üles seada sellisel ajal, kus võib eeldada, et serverit kasutatakse vähe ning üleminekust tuleb piisavalt ette teavitada. Vana konfiguratsioon tuleks seejuures alati eelnevalt varundada.
- Enne kolimist tuleks server täielikult varundada. Kui ettevõttel või ametiasutusel puudub veel buutimisvõimeline salvestusvahend, siis tuleb see nüüd luua. Tundlikud serveriosad, nagu nt kõvakettad, tuleb originaali avarii puhuks salvestada kettatõmmisefailina ning kolimise käigus tuleks neid transportida serverist eraldi. Tuleb jälgida, et varundatud andmed ja kettatõmmisefailid oleksid kolimise käigus samamoodi turvatud nagu server (nt krüpteering, lukustatav kast, jälgimine).

- Enne kolimist tuleb veenduda, et uute ruumide taristulised võimalused tagavad serveri tõrgeteta töö ja on läbinudvastava testimise. Lisaks võrkude olemasolule (voolutoide, koht- ja laivõrk) on kolimise käigus oluline jälgida ka komponentide õiget järjekorda. Kolimist ei ole näiteks eriti mõttekas alustada veebiserverist, kui tulemüür koos andmeside marsruuteritega paigaldatakse alles tunduvalt hiljem.
- Enne kolimist tuleks kontrollida, kas kolitava kauba hulgas on selliseid IT-komponente, mis nõuavad, et kolimisel oleks tagatud spetsiaalne keskkond. Näiteks on olemas suurte (ja kallite!) IT-süsteemide kontrollereid, mis eeldavad lisaks konditsioneeriga varustatud ruumidesse ülesseadmisele ka töötava konditsioneeriga varustatud keskkonnas transportimist.

Lisaks eelnevale peab olema kindlaks tehtud, kas töötajad on kohe peale ruumidesse sissekolimist oma uutel telefoninumbritel kättesaadavad. Ühe asukoha piires kolides tuleks püüda vanu telefoninumbreid säilitada vähemalt teatud üleminekuaja jooksul. Kolimise käigus peaks olema tagatud, et töötajad on telefoni teel kättesaadavad nii vanas kui ka uues asukohas, et võimalike probleemide korral oleks võimalik alati vastutavate töötajate käest nõu küsida.

Kontrollküsimused:

- Kas planeeritava kolimise korral töötatakse vastavad turvaeeskirjad välja õigel ajal?
- Kas kõiki töötajaid on informeeritud, milliseid IT turvanõudeid tuleb enne kolimist, kolimise käigus ja pärast kolimist järgida?
- Kas kolimise käigus transporditavad varad on kantud nimekirjadesse?

M 2.182 IT-turvameetmete regulaarne läbivaatus

Algatamise eest vastutavad: IT-turvaosakond

Rakendamise eest vastutavad: IT-juht, IT-turvaosakond

Etteteatamata kontrollid

IT-etalonturbe kataloogides tutvustatakse paljusid erinevaid reegleid ja turvameetmeid ning antakse nõu turvaliste konfiguratsioonide loomise kohta, mis on vajalikud soovitud turbeastme saavutamiseks. Vastavate reeglite teadaandmisest üksi ei piisa, st reeglite järgimist tuleb regulaarselt ka kontrollida. Regulaarselt ei tähenda siinkohal sugugi seda, et kontrollid toimuvad etteaimatavatel kuupäevadel, sest etteteatatud kontrollimiste tulemused annavad meile tervikust vaid hägusa pildi. Kontrollimise eesmärgiks peaks olema esmajoones võimalike puuduste likvideerimine. Selleks, et töötajad aktsepteeriksid vastavaid kontrolle, on tähtis, et kontrolli eesmärk oleks kontrollitavatele selge, mistõttu ei tohi jääda muljet nagu oleks tegu suvalise näpuvibutusega. Seetõttu oleks mõttekas kontrolli käigus teha töötajatega võimalikest probleemilahendustest juttu, et vastavaid abinõusid ette valmistada.

Reeglid peavad olema tööprotsessidega kooskõlas

Reeglite eiramine töötajate poolt või nendest kõrvalehiilimine on tihti märk sellest, et nende täitmine kas ei ole tööprotsessiga kooskõlas või ei ole töötaja võimeline neid täitma. Näiteks nõue, et konfidentsiaalseid dokumente ei tohi jätta järelvalveta printeri juurde laokile võib olla täiesti mõttetu, kui printimiseks on võimalik kasutada ainult ühte kaugelasuvat võrguprinterit.

Turbealaste puudujääkide põhjuste kõrvaldamine

Puudujääkide tuvastamisel kontrolli käigus ei ole määravaks mitte ainult tulemuste kõrvaldamine. Palju olulisem on siinkohal probleemide põhjuste väljaselgitamine ja võimalike lahenduste väljapakkumine. Lahendusteks võivad olla näiteks olemasolevate reeglite muutmine või täiendavate tehniliste võimaluste kasutuselevõtt.

Süüdistamise vältimine

Kontrollid peaksid aitama kõrvaldada võimalikke veaallikaid. Kontrollide aktsepteerimiseks on ülimalt oluline, et selle käigus ei toimuks töötajate avalikku häbistamist või süüdlaseks tembeldamist. Kui töötajad peavad silmitsi seisma äsjakirjeldatud ebameeldivustega, tekib oht, et töötajad ei soovi neile teadaolevatest kitsaskohtadest või turvaaukudest enam rääkida, vaid proovivad probleeme pigem varjata.

Täiendavad kontrollküsimused:

- Kas kõiki reegleid ja IT-turbemeetmeid kontrollitakse, et neid oleks võimalik ka reaalselt täita?
- Kui tihti kontrollitakse olemasolevate reeglite ja IT-turbemeetmete järgimist?

M 2.188 Mobiiltelefonide kasutamise eeskirjad ja turvasuunised

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: IT-juht, IT-turvaosakond

Mobiiltelefonide väärkasutuse ärahoidmiseks on olemas palju erinevaid võimalusi. Selleks, et vastavaid võimalusi ka aktiivselt rakendataks, tuleks koostada asjakohased turvasuunised, kus oleks välja toodud kõik kohustuslikud turvamehhanismid. Kasutajatele tuleks koostada ka lühike ja ülevaatlik infoleht mobiiltelefonide turvalise kasutamise kohta.

Tekkivad andmeliigid

Kohe pärast seda, kui mobiiltelefon sisse lülitatakse, registreerib ta ennast lähima tugijaama vahendusel võrgu operaatori juures. Võrgu operaator logib ja salvestab kasutajat identifitseerivad andmed, mobiiltelefoni seerianumbri ning tugijaama andmed, mille kaudu kasutaja end parasjagu registreeris. Nimetatud protsess toimub ka juhul, kui ühtki kõnet ei tehta. Lisaks salvestatakse ka info iga ühenduse loomise katse kohta, sõltumata sellest, kas ühendus loodi või mitte. Telekommunikatsiooni käigus tekkivad andmed võib üldistades jagada kolme gruppi:

- Püsiandmed on niisugused andmed, mis salvestatakse teenuse või võrgu puhul püsivalt ning mida hoitakse alati kasutusvalmis. Siia alla kuuluvad näiteks telefoninumber ning täiendavalt võib olla lisatud ka teenusekasutaja nimi ja kontaktaadress, info kasutatava lõppseadme kohta, võib-olla ka ühenduse jaoks kasutatavad jõudlusnäitajad ning volitused, samuti info võimalikku kasutajarühma kuulumise kohta.
- Sisulised andmed ehk „kasutajaandmed“ ehk edastatud informatsioon ja sõnumid.
- Ühendusandmed annavad informatsiooni sideprotsesside lähimatest asetleidnud sündmustest. Siia alla kuulub info sidepartnerite kohta (nt helistava ja sihtkoha ühenduse telefoninumber), andmed ühenduse kellaaja ja kestvuse, kasutatud süsteemiteenuste, kasutatud ühenduste, liinide ja muude tehniliste seadmete kohta, teenuste kohta ning mobiiliteenuste puhul ka mobiilsete seadmete asukohatunnused.

Järgnevalt on välja toodud mõned soovitused, kuidas vastavaid andmeid väärkasutamise eest kaitsta.

Kaitse kaartide väärkasutamise vastu

Mobiiltelefoni ja SIM-kaarti tuleb hoida turvalises kohas. Töölähetuste ajal ei tohi neid jätta järelvalveta. Eriti oluline on, et neid unustataks kuhugi sõidukitesse. Mobiiltelefone ja sellega seotud pakutavaid teenuseid on võimalik kaitsta erinevates kohtades kas PIN-koodide või paroolide abil kaitsta. Siia alla kuuluvad:

- SIM-kaardi juurdepääsu kaitse,
- lõppseadme ehk mobiiltelefoni juurdepääsu kaitse,
- mobiiltelefoni erinevate funktsioonide juurdepääsu kaitse, nt telefoniraamatu kaitse,
- elektronpostkasti juurdepääsu kaitse, st automaatvastaja või muude võrguoperaatori teenuste kaitse,
- võrguoperaatori andmete juurdepääsukaitse (infoliinile helistades ja arve kohta infot soovides tuleb öelda lepingusse kantud salasõna).

Loetletud turvamehhanisme tuleks mitte ainult teada, vaid ka kasutada (vt M 4.114 Mobiiltelefonide turvamehhanismide rakendamine). Kõige olulisem on siinjuures vaieldamatult SIM-kaardi kaitse, sest selle väärkasutus võib endaga kaasa tuua suuri finantskahjusid. Personaalset identifitseerimisnumbrit (PIN-koodi) ei tohi mitte mingil juhul hoida ühes ja samas kohas koos mobiiltelefoni juurde kuuluva SIM-kaardiga. SIM-kaardi kaotsimineku korral tuleks kaardi väärkasutuse ja võimalike finantskahjude ennetamiseks esitada kohe võrguoperaatorile taotlus kaardi sulgemise kohta (vt M 2.189 Mobiiltelefoni blokeerimine kaotamise korral).
SIM-kaardi võimaliku väärkasutuse õigeaegseks tuvastamiseks tuleb kontrollida arvete kõnede eristust, kas seal esineb teenuseid või telefoninumbreid, mille kasutamist ei ole võimalik seletada. Nutitelefonide puhul on ka seadme enda kaitsmine kas PIN-koodi või parooliga väga oluline, sest nutitelefonide rakendused võivad muu hulgas sisaldada ka konfidentsiaalseid andmeid nagu identsustõendid ja paroolid. Seetõttu tuleb kõikides nutiseadmetes lülitada sellised turvafunktsioonid kindlasti sisse ja keelata nende desaktiveerimine. Lisameetmena peaks seade end automaatselt lukustama (nt kui kümne minuti vältel seadet ei kasutata).

Kõnede eristus

Võrguoperaator salvestab kõnega seotud andmed, mille alusel väljastatakse kliendile arve. Mobiiltelefoni kasutuse kontrollimiseks peaks klient võrguoperaatorilt tellima kõnede eristuse. Kõnede eristusest saab välja lugeda nt järgnevaid andmeid:

- arve kuupäev,
- valitud numbrid (täielik loetelu või siis viimased numbrid hägustatud),
- ühenduse algus, lõpp või kestvus,
- kõne hind.

Kõik mobiiltelefoni kasutajad peavad olema informeeritud, et tellitud on ka kõnede eristus ning sellest, millist liiki andmeid kõnede eristus sisaldab. Kui ametiasutus või ettevõte tellib kuluarvestuse kontrollimise eesmärgil kõnede eristuse ja tegeleb nende läbivaatamisega, tuleb protsessi kaasata ka töövõtjate esindajad ning andmekaitse eest vastutav töötaja ning protsessist tuleb teavitada ka kasutajaid. Kõnede eristused tuleb kohe peale laekumist läbi kontrollida, et selgitada, kas arvetes esineb ebakõlasid või mitte. Selliselt toimides on võimalik välja selgitada ka kulude kokkuhoiuvõimalused.

Telefoninumbrite avalikustamine

Telefoninumbrite puhul on võimalik valida, kas üldse ja milliseid andmeid lubatakse kanda avalikku telefoniraamatusse või tehakse kättesaadavaks telefoni infoliini kasutamiseks. Avalik telefoninumber muudab sidepartneritele helistamise lihtsamaks. Samas ei ole see iga kasutusvaldkonna puhul eriti mõistlik, nt kui tegu on ühiskasutuses olevate mobiiltelefoni numbritega, või kui helistajate arvu tahetakse hoida võimalikult väiksena. Kui mobiiltelefoni numbrinäidu teenus on sisse lülitatud, on helistajatel (sõltuvalt varustusest) võimalik näha, millise numbri pealt neile helistatakse. Antud teenust saab üldjuhul lasta võrguoperaatoril nii sisse kui ka välja lülitada kui ka ise seadetest valides.

Numbrinäidu keeld

GSM võrgus osalevatel sidepartneritel on võimalik näidata teineteisele oma telefoninumbreid. Kui seda ei soovita, tuleks järgida meedet M 5.79 Kaitse mobiiltelefoni numbri tuvastamise vastu .

Kaitse telefonikõnede pealtkuulamise vastu

Ainuke tõhus kaitse telefonikõnede turvamiseks on koostalitlusvõimeline võrkudeülene end-to-end krüpteering. Kuna vastavat krüpteeringut pole veel loodud, tuleb tõdeda, et iga, ükskõik kas püsivõrgu või mobiilivõrgu ühendus on potentsiaalselt pealtkuulatav. Paljudes riikides krüpteeritakse mobiiltelefoni ja tugijaama vaheline side automaatselt. Ohtude vähendamiseks on soovitatav kasutusele võtta järgmised kaitseabinõud:

- Helistada ei tohiks valimatult ükskõik kus kohas ja suvalisel kellaajal. Helistamiseks tuleks valida koht, kus teid ei segata (seeläbi häirite vähem ka teisi).
- Üldjuhul tuleks lähtuda põhimõttest, et konfidentsiaalne info ei ole telefonivestluse teema.
- Mõningad mobiiltelefonid suudavad kasutajat informeerida, kas mobiiltelefoni ja tugijaama vaheline side parasjagu krüpteeritakse või mitte. Kui seda infot on kohustuslik jälgida, tuleb kasutajat sellest ka teavitada. Aeg-ajalt peaks kasutaja sellise kohustuse puhul telefoniekraanile pilku heites veenduma, kas ühendus krüpteeritakse või mitte. Näiteks teatud riikides ei krüpteerita mobiiltelefoni ja tugijaama vahelist sidet.
- Lisaks on olemas ka väheseid ja suhteliselt kalleid mobiiltelefone, mille sidet on võimalik krüpteerida ka end-to-end meetodil. Selle lahenduse puhul peab mõlemal sidepartneril olema vastav seade. Antud variant võib olla mõttekas juhul, kui mobiiltelefoni teel on tihti vaja edastada väga tundlikku informatsiooni.
- Kui andmeid edastatakse nt sülearvutist GSM-i vahendusel, tuleks edastatavad andmed eelnevalt sülearvutis krüpteerida. Selleks on saadaval erinevaid lihtsasti kasutatavaid programme.
- Kui mobiiltelefonid või SIM-kaardid vahetavad omanikke, on sihipärane telefonivestluste pealtkuulamine vägagi raskendatud. Seetõttu võib vahetamine olla mõttekas, kui edastatakse kõrge konfidentsiaalsusega infot või andmeid.
- Tuleks kontrollida, kas kõik sideteenused kajastuvad arvel konkreetselt seoses teenuse kasutajaga. Kui teatud ühenduste puhul ei ole tasu arvestatud, võib see olla viide võimalikule pealtkuulamisele.

Töötajate turbeteadlikkuse suurendamine

Kuna sidevaldkonna pealtkuulamisohuga käiakse tihti liigagi kergelt ümber, peaksid ametiasutused ja ettevõtted kontrollima, kas senised töötajate teavitamised sidevaldkonnaga seotud ohtudest on olnud piisavad. Sõltuvalt vajadusest tuleb töötajatele võib-olla koguni regulaarselt pealtkuulamisohtu meelde tuletada ja neid selle suhtes tähelepanelikumaks muuta.

Ettevaatus info edasiandmisel

Töötajatele tuleb selgitada, et konfidentsiaalset infot ei tohi niisama telefoni teel lihtsalt edasi anda. Enne detailse info edasiandmist on eriti oluline, et oleks välja selgitatud isik, kellega täpselt telefoni teel parasjagu suheldakse (vt G 3.45 Sidepartnerite puudulik autentimine). Mobiiltelefonide kasutamise puhul tuleks jälgida ka seda, et konfidentsiaalset juttu ei aetaks kuskil avalikus kohas. Ikka ja jälle

liiguvad ringi dramaatilised, kuid valed hoiatusteated (vt G 5.80 Pettemeilid). Selleks, et tööaega ei raisataks liigselt niisuguste teadete tõepõhja kontrollimiseks, tuleks kõiki töötajaid võimalikult kiiresti teavitada, kui on jälle liikvele läinud mõni uus pettemeil. Vastavasisuliste hoiatuste edastamiseks saab kasutada erinevaid informeerimisteenuseid.

Mobiiltelefonide kasutusreeglid

Ametiasutuse või ettevõtte töö raames mobiiltelefonide kasutamiseks tuleks kehtestada teatud reeglid. Reeglid puudutavad nii isiklike kui ka töötelefonide kasutamist.

Isiklike mobiiltelefonide kasutamine

Kui töötajad ei ole tööandja poolt vastavate töövahenditega varustatud, võib juhtuda, et isiklikke telefone hakatakse kasutama ka tööülesannete täitmiseks. Sellistel juhtudel tuleks eelnevalt kindlaks määrata järgmised punktid:

- Kes maksab tööga seotud kõnede eest ning kuidas toimub nende arveldamine?
- Moodsatel telefonidel on olemas kalendermärkimikud, aadressiraamatud, e-maili tugi jpm. Vastavate funktsioonide mõistlik kasutamine eeldab üldjuhul PC-ga sünkroniseerimist. Seetõttu peab olema selge, kas töökohal lubatakse vajaliku riist- ja tarkvara installeerimist või mitte.

Nende funktsioonide mõistlikuks kasutamiseks tuleb mobiiltelefone enamasti sünkroonida kas mõne arvuti või internetiteenusega. Seetõttu peab kasutajatele olema teada, kas tööandja lubab sünkroonimiseks vajalikku riist- ja tarkvara installeerida ning kas internetiteenustega on lubatud tööandja andmeid töödelda ja salvestada.

Töökoha mobiiltelefonide kasutamine

Ka töötelefonide kasutamise puhul tuleb erinevad punktid eelnevalt paika panna:

- Töötajaid tuleb teavitada sellest, kas erakõnede tegemine on töökoha mobiiltelefonilt lubatud ning kui on, siis kui suures mahus on see lubatud.
- Mobiiltelefonide puhul tuleks kaaluda, kas nende kasutamine peaks olema piiratud teatud kindlate suhtluspartneritega, nt kulude kokkuhoiu eesmärgil või selleks, et vältida informatsiooni liiga suurt levikut (vt M 2.42 Võimalike suhtluspartnerite määramine). Selleks võib kehtestada organisatsioonilised piirangud, kuid võib kasutada ka tehnilisi lahendusi, nagu on kirjeldatud allpool märksõnade „Kõnede piirangud“ ja „Suletud kasutajarühmad“ juures.
- Töötajaid tuleks informeerida ka töökoha mobiiltelefonide arvete suurusest, et need ei paisuks üleliia suureks. Töötajaid tuleb teavitada kõnetariifidest ja Roaming -teenuste hindadest, et neil oleks näiteks välismaal viibides võimalik valida kõige soodsam operaator.
- Kasutajaid tuleb koolitada, kuidas mobiiltelefonidega võimalikult hoolikalt ümber käia, et nad teaksid, kuidas telefoni kadumist ja varastamist ennetada ning tagaksid oma käitumisega seadmete pika kasutusea (nt aku eest

hoolitsemine, seadme hoidmine väljaspool büroo- või eluruume, liiga kõrgete või liiga madalate temperatuuride taluvus).
- Reguleeritud peaks olema ka mobiiltelefonide haldamine, hooldamine ja edasiandmine. Selleks on soovitatav luua mobiiltelefonide ühikasustus (pool) (vt M 2.190 Mobiilikogu sisseseadmine).
- Iga kord, kui telefoni kasutaja vahetub, tuleb PIN-koodid turvaliselt edasi anda (vt M 2.22 Paroolide deponeerimine).

Üldreeglid

Sõltumata sellest, kas töö juures kasutatakse isiklikult soetatud või tööandja ostetud mobiiltelefone, peab tööandja võtma töötaja käest kirjaliku kinnituse järgmiste kohustuste kohta:

- Töö otstarbel kasutatava sõiduki juht ei tohi mobiiltelefoni kasutada sõidu ajal, sest õnnetuse korral ähvardab töötajat vastasel korral kaasvastustuse oht.
- Töösaladusi ei tohi edasi anda telefoni teel. Siinkohal peetakse rohkem silmas mitte kõnede pealtkuulamise ohtu (võrgu kaudu), vaid lähikeskkonnas olevaid inimesi, kes võivad telefonivestlust kuulda.
- Enne siseinfo telefoni teel edasiandmist ei tohi töötaja teha ennatlikke oletusi, st töötaja peab olema veendunud oma suhtluspartneri identiteedis.

Mobiiltelefoni ei tohiks järelvalveta kuhugi laokile jätta. Kui mobiiltelefoni on tarvis jätta kuhugi sõidukisse, tuleks seda teha nii, et telefon ei jääks sõidukisse nähtavale kohale. Mobiiltelefon peaks olema pilkude eest varjatud või kuhugi laekasse suletud. Mobiiltelefon on vara, mis võib ligi meelitada potentsiaalseid taskuvargaid. Kui mobiiltelefoni kasutatakse võõrastes bürooruumides, tuleb järgida vastava organisatsiooni kohapealseid turvareegleid. Võõrastes ruumides nagu nt hotellitubades ei tohiks mobiiltelefoni niisama laokile jätta. Hiljemalt nüüd tuleks aktiveerida kõik parooli kaitsemehhanismid. Seadme lukustamine kappi aitab ennetada juhuvargusi.

Institutsioon peaks muu hulgas reguleerima ka mobiiltelefoni kaotamisega seotud toimingud (M 2.189 Mobiiltelefoni blokeerimine kaotamise korral) ja töötajaid nendest ka teavitama. Juhul kui moodsate mobiiltelefonide jaoks soetatakse tarkvara, mis võimaldab seadmeid positsioneerida, seadmes olevaid andmeid kustutada ja seadet blokeerida, tuleb töötajaid koolitada, et nad oskaksid neid programme õigesti kasutada. Samuti tuleb reguleerida, kuidas toimida ajutiselt kaduma läinud ja seejärel uuesti üles leitud seadmetega, et välistada seadmete kallal toime pandud manipulatsioonid. Selliste seadmete mälu on soovitatav täielikult kustutada ning paigaldada kõik vajaminevad andmed ja programmid uuesti.

Kuluinformatsioon

GSM-kõned muutuvad küll aasta-aastalt soodsamaks, kuid sellele vaatamata on ka mõningaid valikuvõimalusi, mis võivad pikas perspektiivis põhjustada ka suuri kulutusi. Kuna tariifid muutuvad suhteliselt sageli, peaksid kasutajad regulaarselt välja uurima, kui palju maksavad erinevad paketid, kõneajad ja muud võimalused. Mõnikord võib osutuda tasuliseks ka mobiilikõne vastuvõtmine, näiteks kui kõne vastuvõtja viibib parasjagu välismaal või kui kõne on edasi suunatud püsivõrku. Kuna helistaja ei tea, kus riigis parasjagu tema suhtluspartner võib viibida, siis ei kanna edasisuunamise kulusid mitte helistaja, vaid kõne vastuvõtja.

Kättesaadavuse reeglid

Mobiiltelefoni kasutaja ei pruugi alati olla mobiili teel kättesaadav, samuti ei pruugi kasutaja seda ise kogu aeg tahta. Mobiiltelefonide kasutamine valimatult igas olukorras võib jätta selle kasutajast halva mulje. Kui vähegi võimalik, tuleks mobiiltelefonid nõupidamiste ja loengute ajaks välja lülitada. Vähemalt telefoni helin peaks olema välja lülitatud või siis valitud selline, et see oleks vaikne ja ei häiriks teisi. Situatsioonides, kus telefoniga niikuinii vabalt rääkida ei saa (nõupidamistel, restoranis jne), tuleks mobiiltelefoni kasutamist vältida juba algusest peale. Teiselt poolt on jällegi tarvis tagada, et inimesed oleksid kättesaadavad. Selleks on olemas erinevaid võimalusi nagu näiteks:

- kindlate helistamise kellaaegade määramine,
- automaatvastaja funktsiooni kasutamine või
- kõnede ümbersuunamine büroosse.

Mobiiltelefonide kasutamiskeeld

Tuleks läbi mõelda, kas mobiiltelefonide kasutamist või koguni kaasavõtmist oleks tarvis ametiasutuse raames või teatud kindlates ruumides piirata. Sellised kitsendused võib kehtestada näiteks nõupidamisruumidele (vt M 5.80 Kaitse mobiiltelefonidega pealtkuulamise eest). Kui teatud institutsiooni IT-turvapoliitika näiteks ei luba mobiiltelefone endaga kaasa võtta, tuleb sissepääsude juures sellest ka selgelt märku anda. Vastavate piirangute täitmist tuleb ka regulaarselt kontrollida.

Mobiiltelefone ei tohi asetada serverite peale!

Mobiiltelefonide kasutamine võib sõltuvalt olukorrast rikkuda ka teiste tehniliste seadmete tööfunktsioone. Seetõttu tuleb näiteks lennukites või intensiivraviosakondades mobiiltelefonid välja lülitada. Mobiiltelefonid võivad segada ka paljude muude tundlike IT-süsteemide tööd. Mobiiltelefonide segavat mõju on täheldatud näiteks serveriruumides ja arvutuskeskustes. Mida väiksem on telefoni leviulatus ja mida kaugemal see tundlikest seadmetest asub, seda väiksem on ka segava mõju tekke tõenäosus.

Kaitse mobiiltelefonide abil andmete edasiandmise vastu

IT-süsteemides, mis töötlevad tundlikke andmeid või on ühendatud arvutivõrku, peaks mobiilside kaartide kasutamine olema keelatud (vt M 5.81 Turvaline andmeedastus mobiiltelefoni kaudu). Absoluutselt vettpidavat kaitset mobiiltelefonide abil andmete volitamata edasiandmise vastu, eriti kui tegu on siseringi kasutajaga, ei ole olemas. Sellele vaatamata tuleks keelata mobiiltelefonide kaasavõtmine teatud ruumidesse ja regulaarselt kontrollida antud keelu järgimist.

Telefoniraamat

Mobiiltelefoni telefoniraamatusse on võimalik salvestada telefoninumbreid koos sinna juurdekuuluvate nimede ja muu infoga. Telefoniraamatut on võimalik salvestada nii seadmesse, st mobiiltelefoni kui ka selle SIM-kaardile. Telefoni ja SIM-kaardi telefoniraamatud ei pea teineteisega kattuma. Seetõttu võib vastavate PIN-koodide abil valikuliselt kaitsta juurdepääsu kas seadme mällu salvestatud telefoniraamatule ja/või SIM-kaardi telefoniraamatule. See, kas telefoninumbrite salvestamisel tuleks eelistada seadmemälu või SIM-kaarti, sõltub erinevatest faktoritest

nagu nt asjaolust, kui lihtne on vastavaid andmeid teiste andmekandjate peale varundada (vt M 6.72 Ettevaatusabinõud mobiiltelefoni tõrgete puhuks). Üldjuhul võiks eelistada andmete salvestamist SIM-kaardile, sest:

- SIM-kaardi vahetamisel on andmed kättesaadavad ka teiste seadmetes ning
- võimalikku tundlikku informatsiooni on nõnda lihtsam seadmest eemaldada (oluline nt parandustööde või kasutaja vahetumise puhul).

Võimalusel tuleks piirduda ainult üht liiki salvestusvariandiga. Valitud telefoniraamatusse tuleks salvestada kõik tähtsamad andmed, et need oleks vajadusel alati olemas. Salvestatud telefoninumbreid tuleks aeg-ajalt kontrollida, kas need andmed on õiged ning kas need on ka vajalikud. Kõik telefoninumbrid tuleks salvestada sellisel kujul, mis võimaldaks neid kasutada rahvusvahelisel, st koos riigi ja piirkonna eelkoodidega olenemata asukohast. Kuna rahvusvaheliselt on kokku lepitud ainult riikide koodid, mitte sinna ette valitavad 0d, tuleks iga telefoninumber salvestada kujul "+", millele järgneb riigi kood (nt Eesti puhul +372), piirkonna kood ilma 0-ta ja seejärel telefoninumber. Kui mobiiltelefoni kasutavad erinevad töötajad, tuleks siinkohal salvestada ainult ühiselt kasutatavad telefoninumbrid. Lisaks peaks olema võimalik telefoniraamatut kaitsta olemasolevate tõkestusfunktsioonidega muudatuste tegemise eest.

Automaatvastaja funktsioonide kasutamine

Võrguoperaator võimaldab mobiiltelefoni puhul kasutada ka kõnepostiteenust. Sissetulevad kõned salvestatakse operaatori juures nn kõnepostis ning kasutajal on võimalik neid vabalt valitud ajal kuulata. See võib olla sõltuvalt olukorrast väga kasulik, kuid reeglina kaasnevad sellega ka suured kulud. Juurdepääs kõnepostile peaks olema PIN-koodiga kaitstud. Isegi siis, kui kõneposti ei kasutata, tuleks selle algne PIN-kood kiiresti ära muuta, et takistada kõneposti volitamata kasutamist. Sissetulnud kõnesid tuleb regulaarselt kuulata. Kõiki kasutajaid tuleb teavitada, kuidas vastav funktsioon töötab.

Kõnede suunamine

Kõnede suunamise funktsiooniga on võimalik sissetulevaid kõnesid kas kõneposti või teistele telefoninumbritele ümber suunata. Selleks on olemas erinevaid variante:

- Edasi on võimalik suunata kõiki sissetulevaid kõnesid.
- Kõnesid on võimalik edasi suunata, kui number on parasjagu hõivatud.
- Kõnesid on võimalik edasi suunata, kui number ei ole kättesaadav, nt leviaugu tõttu või kui mobiiltelefon on välja lülitatud.
- Edasi on võimalik suunata ka liigiti, nt kõnesid, andmeedastust või fakse.

Siinjuures tuleks siiski arvestada ka sellega, et mobiilikõnede suunamine püsivõrku võib põhjustada suuri kulutusi, sest kõne vastuvõtja kannab ka suunamisega seotud kulud.

Kõnede piiramine

Kõnede piirangutega on võimalik takistada nii sissetulevaid kõnesid kui ka teatud telefoninumbritele helistamist. Vastavaid funktsioone pakuvad mobiilsidevõrgu operaatorid ning neid on võimalik mobiiltelefoni abil muuta. Üldjuhul on muutmiseks tarvis sisestada vastav parool. Kõnede piirang võib olla mõttekas juhtudel, kui mobiiltelefoni on tarvis edasi anda kolmandatele isikutele. Kõnede piirangute seadistamiseks on olemas erinevaid võimalusi:

- Kõikide väljuvate kõnede piiramine - Selle seadistusega on võimalik ainult kõnesid vastu võtta ning ainukese erandina on võimalik helistada hädaabinumbritele.
- Kõikide väljuvate rahvusvaheliste kõnede piiramine - Antud piirangu kehtestamisel on võimalik helistada ainult selle riigi riigisisestel telefoninumbritel, kus seade parasjagu asub. Välismaalt tulevaid kõnesid saab vastu võtta ilma piiranguteta.
- Kõikide väljuvate rahvusvaheliste kõnede piiramine, välja arvatud kodumaale - Selle seadistusega on võimalik võtta kõnesid välismaalt (võrguoperaatori) kodumaale. Kõned teistesse riikidesse on tõkestatud.
- Kõikide sisenevate kõnede piiramine - Välja helistada on võimalik kõikidele numbritele. Segamine sissetulevate telefonikõnede näol on välistaud.
- Kõikide sisenevate kõnede piiramine välismaal viibides - Kodumaa piires on võimalik jätkuvalt harjumuspäraselt helistada. Välismaal viibides ei ole võimalik ühtki kõnet vastu võtta. Antud funktsioon võib olla mõttekas siis, kui välismaal vastuvõetavatele kõnedele on kehtestud osaliselt väga kõrged tariifid.

Kas kõnede piiranguid tuleks kasutada ning milliseid funktsioone valida, see sõltub suuresti mobiiltelefoni kasutusvaldkonnast.

Suletud kasutajarühmad

- Teenusega „Suletud kasutajarühm“ (closed group) saab sidepidamise võimalusi piirata vastava kasutajarühma lõikes (vt M 5.47 Kinnise kasutajagrupi konfigureerimine).
- Kasutajarühma liikmed tuleb mobiilsidevõrgu operaatori juures registreerida. Valikut „Suletud kasutajarühm“ saab sisse lülitada mobiiltelefonist. Suletud kasutajarühmade loomine võib olla vajalik nt siis, kui tahetakse mobiilside abil piirata andmete edastamist.

Kontrollküsimused:

- Kas mobiiltelefonide kasutamisekohta on olemas aktuaalne turvaeeskiri?
- Kuidas kontrollitakse mobiiltelefonide kasutamise turvaeeskirjade järgimist?
- Kas iga mobiiltelefoni kasutaja on saanud vastavast mobiilieeskirjast koopia või infolehe selle kohta, millised on tähtsamad turvamehhanismid?
- Kas IT-turvameetmete koolituse raames käsitletakse ka mobiiltelefonide kasutamise turvaeeskirja?
- Kas mobiiltelefonide kasutajaid on teavitatud reeglitest, mida nad peavad kohustuslikus korras järgima?
- Kas mobiiltelefonide kasutajaid on teavitatud sellest, millised on seadmete sobivad hoiutingimused?

M 2.189 Mobiiltelefoni blokeerimine kaotamise korral

Algatamise eest vastutavad: IT-juht, IT-turvaosakond, kasutajad

Rakendamise eest vastutavad: kasutajad

SIM-kaardi või telefoni kadumise korral tuleb võimalikust väärkasutusest tingitud lisakulud kanda SIM-kaardi omanikul. Seetõttu tuleks kadumise korral esitada võrguoperaatorile kohe vastav SIM-kaardi blokeerimise taotlus, et ennetada võimalikku väärkasutust ja sellega seotud lisakulusid.

Lisaks sellele peaks telefonis olema sisse lülitatud SIM-kaardi PIN-koodi küsimise funktsioon (vt M 4.114 Mobiiltelefonide turvamehhanismide rakendamine). Varguse või kadumise korral takistab see SIM-kaardi kasutamist ja seal oleva info kättesaamist. PIN-koodi küsitakse siiski ainult telefoni sisselülitamisel. Kui mobiiltelefon on varastamise ajal sisse lülitatud, saab seda kasutada vähemalt nii kaua, kuni aku tühjaks saab!

Mobiiltelefoni kadumise või varguse korral saab võrguoperaator lisaks muule piirata mobiiltelefoni kasutamist ka seeläbi, et kannab selle „musta“ nimekirja. Selleks on võrguoperaatoril vaja teada seadme koodi (IMEI - International Mobile Equipment Identifier). IMEI-kood on sageli kantud seadme tagaküljele ning see tuleks üles kirjutada ja hoida seadmest lahus. Mobiiltelefoni ostu puhul tuleks samuti jälgida, et ostjale antaks muuhulgas kirjalikult edasi ka seadme IMEI-kood. Koodi on võimalik vaadata ka mobiiltelefonist, kuid vastavad protseduurid ei toimi kõikide telefonide puhul ühtmoodi. Seadme number on tihti ära näidatud seadme tüübisildil, mis asub aku all, või siis saab seda näha mobiiltelefoni ekraanil, sisestades nupukombinatsiooni *#06#.

Nutitelefonide jaoks on saadaval vargustevastane tarkvara, mis võimaldab mobiiltelefoni selle GPS-vastuvõtja abil mobiilivõrgus positsioneerida, kustutada mobiiltelefoni salvestatud andmeid ja seadme täielikult lukustada. Mõned tarkvaralahendused suudavad IT-osakonnale edastada isegi automaatteateid seadme asukoha ja lukustumise kohta, nt olukorras, kus seadme SIM-kaart asendatakse mõne teisega. Paljud sellised programmid võimaldavad telefonidesse saata ka sõnumeid või aktiveerivad ekraanikuva, millega palutakse seadme leidjal helistada vastavale IT-osakonna numbrile või toimetada seade teatud aadressile. Ühelt poolt võib sellise tarkvara soetamine ennast kiiresti ära tasuda, sest kaduma läinud nutitelefonid leitakse kiiremini üles ja andmed on varaste eest paremini kaitstud. Teisalt tuleb arvestada, et nende funktsioonide kasutamiseks peab GPS olema pidevalt sisse lülitatud ja seadmes peab olema loodud mobiilsideühendus. Selline olukord võib kulutada liigselt akut ning samuti on oht, et kolmandad isikud võivad seadme positsioneerimist kuritarvitada (vt M 5.78 Kaitse mobiiltelefonide järgi asukoha määramise eest ja M 4.115 Mobiiltelefonide toite tagamine).

SIM-kaardi võimaliku väärkasutuse õigeaegseks tuvastamiseks tuleb kontrollida arvete kõnede eristust, kas seal esineb teenuseid või telefoninumbreid, mille kasutamist ei ole võimalik seletada. SIM-kaart tuleb lasta kadumise korral kohe blokee-

rida Kõik andmed, mida läheb tarvis SIM-kaardi kasutamise blokeerimiseks, tuleb hoida alati käepärast, kuid mitte koos telefoniga samas kohas. Vajalikud andmed on:

- telefoninumber ning telefoninumbriga seotud SIM-kaardi number,
- mobiiltelefoni seerianumber (GSM-USSD-Code *#06#),
- võrguoperaatori telefoninumber, kuhu kadumisest teatada, ning
- võrguoperaatori teenusekasutamise parool ja kliendinumber, ehk siis andmed, mille alusel toimub operaatori juures kasutaja autentimine.

Kontrollküsimused

- Kas mobiiltelefonide kaotamise korral on tagatud nende kiire blokeerimine?
- Kas kõik mobiiltelefoni blokeerimise jaoks vajalikud andmed on telefoni kaotuse korral kiiresti leitavad?

M 2.190z Mobiilikogu sisseseadmine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator

Mobiilikogu sisseseadmine

Juhul kui ametiasutuses või ettevõttes on kasutusel suurem hulk mobiiltelefone, mille kasutajad võivad tihti muutuda, oleks mõttekas need telefonid, mida parasjagu ei kasutata, kokku koguda ühte kindlasse mobiilikogusse (pool). Mobiilikogus tuleks tagada kõikide telefonide töövalmidus ehk akude laadimine, et seadmed oleks vajadusel koheselt kasutatavad. Siinkohal tuleb meeles pidada, et akud tühjenevad aja jooksul ka siis, kui mobiiltelefonid on välja lülitatud. Kui mobiiltelefone kasutatakse intensiivselt pikema aja jooksul, tuleks varuda ka lisaakusid. Teadmiseks: telefonide akulaadijad peavad olema üheselt ja arusaadavalt märgistatud, et oleks aru saada, milline laadija millisele telefonile sobib. Vaatamata sellele, et akulaadijad näevad üksteisele suhteliselt sarnased välja, ei saa kõiki laadijaid kasutada suvaliselt läbisegi. Lisaks tuleb kirjalikult fikseerida ka mobiiltelefoni väljastamine ja tagastamine, et oleks kindlalt teada, kes millist telefoni parasjagu kasutab. Väljastamisvihikusse tuleb üles märkida mobiiltelefoni saanud töötaja nimi, töökoha allüksuse nimi, kuupäev ja kellaaeg.

Telefonide väljastamisel ja tagastamisel tuleb lisaks eelnevale arvestada ka järgnevate punktidega:

Üleandmine:

- Kasutaja peab saama kõik mobiiltelefoni kasutamiseks vajalikud PIN-koodid ja paroolid. Kui väljastatud koode ja paroole on iseseisvalt muudetud, tuleb muudetud andmed tagastamisel kirjalikult fikseerida.
- Kasutajale tuleb anda mobiiltelefoni telefoninumber.
- Kasutajale tuleb anda infoleht mobiiltelefoni turvalise kasutamise kohta. Lisaks peaks kasutaja saama ka mobiiltelefoni kasutusjuhendi. Lisaks telefoni tavafunktsioonide kasutamisele peaks kasutaja suutma eelkõige lugeda ja mõista ka võimalikke hoiatusteateid (nt ekraanile ilmuvaid piktogramme).
- Mobiiltelefoni aku peab olema väljastamise hetkel laetud ning kasutajale tuleb kaasa anda ka akulaadija. Kui mobiiltelefon I tuleb hoida kasutusvalmis pikema aja jooksul, tuleks kasutajale väljastada ka laetud lisaaku.

Tagasivõtmine ja edasiandmine:

- Töötaja edastab info viimati tema poolt kasutatud PIN-koodide ja paroolide kohta. Seejärel tuleb kontrollida, kas vastav info on õige. Vastavad andmed tuleb üles kirjutada ja (turvalisse kohta) hoiule panna.
- Tuleb kindlaks teha, kas seade, seadme lisad ja dokumentatsioon on terviklikud. Seade tuleb üle kontrollida, et välistada seadme defektid.
- Kasutaja peab veenduma, et enne seadme tagastamist saavad kõik talle vajalikud andmed tema jaoks ligipääsetavale andmekandjale ümber kopeeritud (nt tema PC-le). Sellele lisaks peab kasutaja ise hoolt kandma, et kõik tema poolt lisatud andmed (nt telefoninumbrid) saaksid seadmest kustutatud.

- Viimati kasutatud telefoninumbrid salvestatakse telefonis olevasse kõneregistrisse.

Kui telefonil on olemas numbrinäidu funktsioon ja see on sisse lülitatud, salvestatakse telefonis ka info viimaste sissetulnud kõnede kohta. Vastavad andmed tuleb enne mobiiltelefoni kasutaja vahetumist kustutada. Telefoniraamatusse on võimalik numbreid salvestada nii telefoni kui ka SIM-kaardi mällu. Isiklikud telefoninumbrid tuleks enne telefoni edasiandmist kustutada. Kõik tööeesmärkidel kasutatavad telefoninumbrid peaksid olema kasutajatele alati kättesaadavad.

- Mobiiltelefonid, täpsemalt SIM-kaardid võivad sisaldada ka muud informatsiooni nagu nt lühisõnumeid, fakse või e-maile. Ka need tuleks enne telefoni edasiandmist kustutada.
- Seadmes tuleb täies ulatuses taastada tehaseseaded ning kõik seadmesse, seadme mälukaardile ja SIM-kaardile salvestatud andmed tuleb kustutada. See on oluline, sest ainult nii saab tõrjuda kahjurvara levikut ja tõkestada andmete soovimatut lekkimist. Pärast kustutamist saab seadmesse taas paigaldada kõik vajalikud programmid ja salvestada vajaminevad andmed.

Kontrollküsimused:

- Kas mobiiltelefonide kasutajaid teavitatakse seadme väljastamise käigus reeglitest ja turvameetmetest, mida nad peavad kohustuslikus korras järgima?
- Kas mobiiltelefonide kasutajaid teavitatakse väljastamise käigus sellest, millised on seadmete sobivad hoiutingimused?
- Kas mobiiltelefonide väljastamine ja tagastamine fikseeritakse kirjalikult?
- Kas pärast mobiiltelefonide tagastamist taastatakse nendes tehaseseaded?

M 2.192 Infoturbepoliitika koostamine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond

Rakendamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT turvaspetsialist

Kehtestatud turvaeesmärkide järgimiseks ja soovitud turbeastme saavutamiseks tuleks kõikide töötajate jaoks kokku koguda kõik tähtsamad turvastrateegia juhised ning koondada need ühtseks infoturbepoliitikaks. Turbepoliitika koostamisega annab ametiasutuse või ettevõtte juhtkond selgelt märku, et võtab oma vastutust seoses infoturbe tagamisega tõsiselt.

Infoturbepoliitika koostamisel tuleb pöörata tähelepanu järgnevatele punktidele:

- ametiasutuse või ettevõtte juhtkonna vastutus – ettevõtte või ametiasutuse juhtkond peab infoturbepoliitikat toetama täie tõsidusega ja tegema kõik endast oleneva, et saavutada turbepoliitikas püstitatud eesmärgid. Seetõttu peab infoturbepoliitika olema vastavalt kas ametiasutuse või ettevõtte juhtkonna poolt allkirjastatud ja nende nimel ka avaldatud. Isegi siis, kui turbeprotsesside raames delegeeritakse erinevaid ülesandeid edasi kas kindlatele isikutele või organisatsiooni allüksustele, jääb infoturbealane koguvastutus siiski ametiasutuse või ettevõtte juhatuse kanda;
- kehtivusala määratlemine – infoturbepoliitikas peab olema kirjeldatud, millistele valdkondadele see kehtib. Kehtivusala võib olla institutsioon tervikuna või ka ainult selle üksikud osad. Siinkohal on oluline, et vastutusalas oleksid täielikult määratletud erialased ülesanded ja vajalikud tööprotsessid;
- turbe-eesmärkide määratlemine – turbeprotsesside juurutamiseks tuleb ametiasutuse või ettevõtte juhtkonnal määratleda, kooskõlastada ja dokumenteerida infoturbega seotud eesmärgid. Eesmärke on võimalik tuletada tööprotsessidest ja -ülesannetest, seadusega etteantud raamtingimustest ning ametiasutuse või ettevõtte üldistest eesmärkidest. Infoturbepoliitika koostamise aluseks tuleb võtta infoturbele seatud eesmärgid;
- infoturbepoliitika sisu – infoturvet puudutav poliitika peaks olema sõnastatud lühidalt ja lihtsalt, kuna praktika on näidanud, et pikemad kui kahekümnelehekülgelised dokumendid ei ole osutunud otstarbekaks. Infoturbepoliitika sisus peaksid kajastamist leidma kõik järgnevad punktid:
- infoturbe osatähtsuse kirjeldus ning olulisema info, tööprotsesside ja IT tähtsus institutsiooni jaoks. Siinkohal tuleks kirjeldada turbealaseid eesmärke ja vastavate eesmärkide seotust ettevõtte või ametiasutuse tööalaste eesmärkidega;
- turbestrateegia kõige olulisemate elementide loetelu. Juhtkond peab andma kõigile töötajatele märku, et juhtkond on turbepoliitika kandja ja jälgib selle rakendamist. Samuti peavad olema sõnastatud üldised suunised, mille abil saab mõõta protsesside tulemuslikkust;
- turbeprotsesside juurutamiseks vajaliku organisatsioonilise struktuuri kirjeldus (vt M 2.193 Infoturbeks sobiva organisatsioonilise struktuuri rajamine).

Infoturbepoliitika avalikustamine

Töötajad järgivad kehtestatud turvameetmeid ja organisatoorseid töökorraldusi enamasti vaid siis, kui nad on nende vajalikkusest aru saanud. Seetõttu tuleb infoturbepoliitika avalikustada, et vastutava juhtkonna strateegia oleks ka dokumenteeritud. See peaks toimuma nii, et ilmneks selgelt infoturbe osatähtsus. Kõik töötajad peavad tingimata teadma infoturbepoliitika sisu ja mõistma selle tähtsust. Uutele töötajatele tuleks infoturbepoliitikat tutvustada juba enne seda, kui töötajad saavad juurdepääsu tööprotsesside jaoks olulisele infole. Turvapoliitika olulisuse rõhutamiseks tuleks lasta kõigil töötajatel allkirjaga kinnitada, et nad on sellest teadlikud. Infoturbepoliitika tuleks enamikul juhtudel sõnastada võimalikult üldiselt, et seda lugedes tunneksid ennast ühtmoodi kohustatuna terve institutsiooni erinevate osakondade kõik töötajad. Samas on võimalik infoturbepoliitikat muidugi ka täiendada, lisades sinna infot institutsiooni spetsiaalsete rakenduste või valdkondade kohta, mida edastatakse ainult teatud piiratud isikutegrupile ning mis võib olla koguni konfidentsiaalne. Vastav informatsioon on soovitav paigutada infoturbepoliitika lisadesse, mis võimaldab muu hulgas ka paindlikku ja kiiret reageerimist võimalikele muudatustele, ilma et oleks tarvis ümber töötada kogu turbepoliitika põhiteksti. Vajaduse korral võib vastavad lisad liigitada täiendavalt konfidentsiaalse info alla ning kehtestada neile spetsiaalsed hoiutingimused.

Infoturbepoliitika värskendamine

Infoturbepoliitikat tuleks regulaarsete ajavahemike tagant kontrollida, et teha kindlaks, kas see on veel piisavalt ajakohane, ning seda vajaduse korral kohandada. Raamtingimustes, ärilistes või tööülesannetega seotud eesmärkides ning turbestrateegias toimunud muudatusi tuleb dokumentatsioonis pidevalt kajastada. Kuna nii IT kui ka turbevaldkonnas toimuvad sageli väga kiired arengud, on soovitatav töötada infoturbepoliitika läbi iga kahe aasta tagant.

Kontrollküsimused:

- Kas juhatus on kehtestanud infoturbepoliitika?
- Kas turbepoliitikale on määratletud kindel kehtivusala?
- Kas turbepoliitika kirjeldab infoturbe osatähtsust, turbealaseid eesmärke, turbestrateegia olulisimaid elemente ja infoturbeks vajalikku organisatsioonilist struktuuri?
- Kas kõiki töötajaid on infoturbepoliitika olemasolust teavitatud?
- Kas infoturbepoliitika on ajakohane?

M 2.193 Infoturbeks sobiva organisatsioonilise struktuuri rajamine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtorgan

Rakendamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT turvaosakond

IT turvaosakonna planeerimine ja juurutamine

IT turbega seotud protsesside edukaks planeerimiseks, rakendamiseks ja töös-hoidmiseks on tarvis, et organisatsioonis oleks loodud vastava ülesandega allüksus. IT turbega seotud ülesannete täitmiseks on tarvis kindlaks määrata töötajate erinevad töökohustused. Lisaks tuleb ametisse nimetada töötajad, kellel on olemas asjakohane kvalifikatsioon ning anda nende käsutusse piisavalt ressursse, mis võimaldaksid täita tööülesandeid. IT turbealaste protsesside planeerimisega algust tehes võib selguda, et IT turbe valdkonnas puudub ülevaatlik ja kõikehõlmav struktuur. Sellele vaatamata on enamikes ametiasutustes ja ettevõtetes siiski tööl inimesed, kes vastutavad erinevate IT turbega seotud valdkondade eest. Tarvis on luua kõikehõlmav IT turbe organisatoorne pool. Ka neil juhtudel, kui IT turbe organisatsiooniline struktuur on juba loodud, tuleks regulaarselt analüüsida, kas vastav struktuur on jätkuvalt sobilik või tuleb seda kohandada näiteks uute raamtingimustega.

IT turvalisuse eest vastutavate töötajate funktsioon

IT turbe organisatsiooniüksuse liik ja ulatus sõltub vastava institutsiooni enda suurusest, iseloomust ja struktuurist. Kõikidel juhtudel tuleb siiski luua ka IT turbe eest vastutava töötaja amet, kes peab vastutama kõigi IT turbega seotud asjaolude eest.

IT turbe eest vastutava töötaja ülesannete hulka kuuluvad muu hulgas järgmised punktid:

- IT turbega seotud protsesside juhtimine ja koordineerimine,
- IT-süsteemi turvasuuniste väljatöötamine, rakendamine ja koordineerimine,
- IT turvakontseptsiooni, hädaolukorraks valmisoleku kontseptsiooni ja muude osakontseptsioonide koostamise koordineerimine,
- IT turvameetmete evitusplaani loomine, meetmete võtmine ja kasutuse kontrollimine,
- aruandluse koostamine juhtkonnale ja IT turvaosakonna meeskonnale,
- turbealaste projektide koordineerimine ja infovahetuse tagamine IT alamvaldkondade, IT projektijuhtide ja IT-süsteemi turvalisuse eest vastutavate töötajate vahel,
- turvalisust puudutavate sündmuste uurimine ning
- IT turbega seotud teavitustöö ja koolituste algatamine ja juhtimine.

IT turbe eest vastutav töötaja tuleb kaasata kõikidesse IT-ga seotud projektidesse, et oleks tagatud piisav tähelepanu ka turvalisusega seotud aspektidele. Siia alla kuuluvad ka IT-süsteemide soetamise ja IT-toega tööprotsesside väljatöötamisega seotud projektid. Kindlustamaks otsest sidet ametiasutuse või ettevõtte juhtkonnaga on soovitatav siduda vastav ametikoht sõltumatu ekspertgrupiga.

Väikestes organisatsioonides võib IT-turvalisuse eest vastutava töötaja funktsiooni üle võtta ka mõni selleks kvalifitseeruv isik, kes täidab lisaks ka veel teisi

tööülesandeid. Väga oluline on selle töö juures asjaolu, et IT turvalisuse ees vastutavale töötajale peab jääma oma tööülesannete täitmiseks piisavalt aega. Eriti oluline on piisava ajalise ressursi planeerimine siis, kui IT turbealaseid protsesse hakatakse juurutama esmakordselt. IT turbega seotud organisatoorse poole planeerimisel on oluline ka see, et lisaks vastutavale töötajale nimetataks ametisse ka IT turvalisuse eest vastutava töötaja kvalifitseeritud asendaja.

IT-turvalisuse eest vastutavate töötajate selekteerimine

IT-turvalisuse eest vastutaval töötajal peavad olema ette näidata piisavad teadmised infotehnoloogia ja IT turbe vallas.

Lisaks sellele peaksid töötajal olema järgmised isikuomadused ja kvalifikatsioon:

- võime identifitseerida ennast institutsiooni eesmärkide läbi,
- arusaam IT turbe rakendamise vajalikkusest,
- võime töötada iseseisvalt ja meeskonnas,
- oskus ennast kehtestada,
- projektitöö kogemus.

IT turvalisuse eest vastutav töötaja ei suuda piisavat IT turvet kõikides institutsiooni valdkondades üksi tagada. Seetõttu on väga oluline, et vastav isik suudaks hästi suhelda ja infot esitleda. IT turbega seotud kesksetesse küsimustesse tuleb alati kaasata ka juhtkond, samuti on tarvis nõuda, et juhtkond võtaks vastu vajalikud otsused. Koostöö IT kasutajatega nõuab suurt suhtlusoskust, sest töötajate hädavajalik kaasamine (nende jaoks tihti tüütuna tunduvasse) IT turbe rakendamisse vajab pikka veenmistööd. Vähemalt sama tundlik teemavaldkond nagu meetmete rakendamine on ka töötajate küsitlemine seoses turvalisust puudutavate võimalike riskide, asetleidnud sündmuste ja kitsaskohtadega. Kasutuskõlblike tulemuste saavutamiseks neis valdkondades peavad töötajad olema eelnevalt veendunud, et ausad vastused ei too endaga kaasa täiendavaid probleeme.

IT turvaosakonna meeskonna loomine

Suuremate organisatsioonide puhul on mõttekas sisse seada oma IT turvaosakonna meeskond, kes tegeleb IT turvalisuse eest vastutava töötaja abistamisega kõikides IT turbe üldistes küsimustes, samuti plaanide koostamisel ning nõuete ja suuniste väljatöötamisel. IT turvaosakonna meeskonna suurus ja sinna kuuluvate töötajate valik peaks sõltuma IT turbega seotud protsesside ulatusest ja nende teostuseks vajalikest ressursside ja ekspertteadmiste mahtudest.

IT turvaosakonna meeskonna töötajate valimine

Selleks, et IT turvaosakonnas oleks olemas läbilõige organisatsiooni erinevatest allüksustest, peaks IT turvaosakonnas olema esindatud järgmised töötajad:

- IT turvalisuse eest vastutav töötaja,
- IT eest vastutav töötaja,
- IT kasutajate esindaja,
- andmekaitse eest vastutav töötaja,
- IT auditi eest vastutav töötaja,
- organisatsiooni juriidilise osakonna esindaja,

- töötajate esinduse esindaja.

Vastutava juhi ametisse nimetamine

Juhtkonnas peaks vastutus IT turbe eest olema seotud kindla tegevjuhiga, kellele IT turvalisuse eest vastutav töötaja esitab oma aruanded. Väikestes organisatsioonides võib selle ülesande enda kanda võtta ka juhatuse esimees.

IT turbe organisatoorse poole kontrollimine

Kord loodud IT turbe organisatoorne külg ei ole sugugi staatiline. Tööprotsessid ja nendega seotud raamtingimused muutuvad pidevalt, mistõttu tuleb ka IT turbe organisatoorset poolt pidevalt täiendada. Läbivaatamise käigus tuleb näiteks selgitada, kas IT turbega seotud tööülesannete ulatus ja vastutused on sõnastatud piisavalt selgelt, samuti seda, kas ettenähtud ülesandeid on võimalik ka päriselt täita.

Ennekõike tuleks läbi töötada järgmised punktid:

- töötajate vastutuse jälgimine jooksva töö käigus – regulaarselt tuleks kontrollida, kas vastutusala ja tööjaotus on töötajate puhul täpselt kindlaks määratud ning kas sellest peetakse ka kinni;
- reeglitest kinnipidamise kontrollimine – regulaarselt tuleb kontrollida, kas IT turvaosakonna kehtestatud juhiseid ja protsesse rakendatakse nii, nagu on ette nähtud. Lisaks tuleb siinkohal kontrollida, kas IT turbe jaoks ülesehitatud organisatoorne külg suudab täita kõiki IT turbega seotud vajalikke nõudeid.
- protsesside ja organisatoorsete reeglite tõhususe hindamine – regulaarselt tuleb kontrollida, kas IT turvaosakonna kehtestatud erinevad protsessid ja organisatsioonilised kohustused on praktikas kasutatavad ja efektiivsed. Juhul kui IT turbega seotud protsessid või reeglid osutuvad liiga keerulisteks või kui need nõuavad liiga palju aega, jäetakse need tihti kas täitmata või püütakse nendest mööda hiilida, mis viib turvaintsidentide tekkimiseni.
- juhtkonna antavad hinnangud – eespool loetletud kontrollide tulemustest tuleb regulaarselt teavitada ka juhtkonda. Aruanded ei ole mitte ainult hädavajalikud, et lahendada ruttu kiiret reageerimist nõudvaid probleeme, vaid sisaldavad ka olulist informatsiooni, mida juhtkond vajab IT turbega seotud protsesside juhtimiseks.

IT turvaosakonna töö kohandamine ja tõhustamine

IT turvaosakonna tööd tuleb pidevalt optimeerida, et muuta see võimalikult tõhusaks. Kui selgub, et IT turvaosakonna tööprotsessides või nende väljastatud reeglites on puudusi, tuleb need kõrvaldada.

Dokumenteerimine

IT turvaosakonna ülesanded, vastutusala ja kompetents peavad olema arusaadavalt kirja pandud. Siia alla kuuluvad ka üldised töökirjeldused ja organisatoorse töö reeglid.

Kontrollküsimused:

- Kas IT turvalisuse eest vastutav töötaja on juba ametisse nimetatud?
- Kas IT turvalisuse eest vastutav töötaja vajab oma tööülesannete täitmises IT turvaosakonna tuge?
- Kas IT turbeprotsessidega seotud ülesanded ja kompetentsid on selgelt defineeritud?
- Kas IT turvaosakonna töö efektiivsust kontrollitakse regulaarselt? Kuidas?

M 2.195 Infoturbe kontseptsiooni loomine

Turvameetme kasutuselevõtmise eest vastutavad: ametiasutuse/ettevõtte juhatus, IT turvaosakond

Turvameetme rakendamise eest vastutab: IT turvaosakond

Eesmärgi seadmine

Infoturbe kontseptsioon aitab ellu viia infoturbe strateegiat ja selles kirjeldatakse planeeritud meetodit, et saavutada eesmärke, mida institutsioon on endale püstitanud. Infoturbe kontseptsioon on ettevõtte või ametiasutuse infoturbe protsessis keskne dokument. Iga konkreetne meede peab viimaks ikkagi sellel põhinema. Seepärast tuleb infoturbe kontseptsiooni hoolikalt planeerida, rakendada ja regulaarselt uuendada.

Kehtivusvaldkond

Institutsiooni kõik valdkonnad ei pea kuuluma üheainsa infoturbe kontseptsiooni alla. Kui IT etalonturbe elluviimine ühe suure sammuna näib liiga ebamäärase ülesandena, siis võib olla mõistlikum viia vajalik turvatase esmalt sisse ainult väljavalitud valdkondades. Sellest lähtudes peaks infoturbe protsess laienema kogu organisatsioonile. Eelkõige suurtes ametiasutustes ja ettevõtetes võib olla mitu infoturbe kontseptsiooni, mis hõlmavad organisatsiooni erinevaid valdkondi. Peab olema tagatud, et institutsiooni kõik valdkonnad kuuluksid sobivate infoturbe kontseptsioonide alla. Ka komplekssеid äriprotsesse või rakendusi võib käsitleda spetsiaalselt neile mõeldud infoturbe kontseptsioonides. See on otstarbekas eelkõige uute ülesannete või rakenduste kasutuselevõtu korral.

IT-kooslus

Kindlaksmääratud kehtivusvaldkonda nimetatakse edaspidi IT-koosluseks ja see on täpsemalt öeldes valdkond, milles tuleb infoturbe kontseptsiooni rakendada. IT-kooslus võib seega tugineda erialastele ülesannetele, äriprotsessidele või organisatsiooni üksustele. See hõlmab peaaegu kõiki taristulisi, organisatsioonilisi, personaalseid ja tehnilisi komponente, mida kasutatakse ülesannete täitmiseks infotöötluse selles rakendusvaldkonnas. IT-kooslus peab olema kindlaks määratud nii, et vaadeldavaid äriprotsesse ja teavet oleks võimalik liigitada täies mahus sellesse valdkonda kuuluvaks. Arvestada tuleb kõikide infoturbe seisukohalt oluliste protsesside juhitavate komponentidega. Puutepunktid teiste valdkondadega tuleb selgesti kindlaks määrata, nii et kogu ettevõtte IT-kooslus oleks minimaalse otstarbeka suurusega.

Riskide hindamine

Infoturbespetsialistid peavad välja valima riskide hindamise meetodi, mis võimaldab analüüsida ja hinnata turvaintsidentidest tingitud potentsiaalseid kahjusid. Valida võib ka mitu üksteisest tulenevat riskihindamismeetodit. IT etalonturbe nõuetele vastava meetodi abil viiakse varjatud kujul läbi riskide hindamine normaalse turbevajadusega valdkondades. Kui vaadeldav IT-kooslus sisaldab kõrge turbevajadusega komponente, peab lisaks IT etalonturbe analüüsile läbi viima ka täiendava infoturbeanalüüsi.

IT-koosluse ülevaade

Iga riskihinnangu aluseks on kaitstavate infomaterjalide ja äriprotsesside kirjeldamine. Et saada ülevaadet äriprotsesside jaoks olulistest IT struktuuridest, tuleb mõista IT-koosluse struktuuri. Lisaks tehnilistele komponentidele, IT-rakendustele ja töödeldavale informatsioonile tuleb mõista ka ruumilist taristut ja võrguks ühendamist. Seejuures tuleb salvestada ka erinevate komponentide omavahelised juhitavused.

Turbevajaduse kindlakstegemine

Turbevajaduse kindlakstegemine koosneb järgmistest sammudest:

- ebapiisavast infoturbest institutsiooni jaoks tulenevate ohtude ja riskide analüüs;
- konfidentsiaalsuse, tervikluse või käideldavuse eiramise tagajärjel tekkida võivate kahjude tuvastamine;
- infoturbe kompetentsi kuuluvate juhtumite ja muude infoturbe riskide potentsiaalsete tagajärgede analüüs ja hinnang seoses äritegevuse või ülesannete täitmisega.

Nende vaatluste abil on võimalik hinnata ettevõtte või ametiasutuse riski või kindlaks määrata informatsiooni, IT-rakenduste ja IT-süsteemide turbevajadust.

Planeeritud ja tegelike kulude võrdlus

Üldiste infoturbe eesmärkide, tuvastatud turbevajaduse ja riskide hindamise põhjal töötatakse välja konkreetsed IT turvameetmed, mis vastavad käsitletavale IT-kooslusele. Selleks tuleb välja valida infosüsteemide etalonturbe kataloogide konkreetsed moodulid, kus käsitletakse IT-koosluse turvanõudeid, mille tulemusel saadakse IT turvameetmete spetsiifiline pakett, mis sisaldab planeeritud väärtusi. Tuvastamaks, milliseid turvameetmeid on juba võetud ja kus esineb veel lünki, viiakse läbi põhjalik turvakontroll.

Infoturbe täiendav analüüs

Normaalse, mõnel juhul ka kõrgema turbevajaduse korral piisab IT etalonturbele vastavate meetmete võtmisest. Valdkondade puhul, mis on seotud kõrge turbevajadusega, tuleb täiendava turvaanalüüsi põhjal otsustada, kas edasine riskianalüüs on vajalik. Kindlaksmääratud valdkondades tuleks läbi viia infosüsteemide etalonturbe nõuetele vastav riskianalüüs.

Meetmete konsolideerimine

Enne infoturbe kontseptsiooni koostamise lõpetamist tuleb täiendava riskianalüüsi käigus identifitseeritud meetmed konsolideerida infosüsteemide etalonturbe meetmetega. Seejuures tuleb infoturbe kõigi hiljuti kindlaksmääratud meetmete puhul kontrollida, kas need asendavad või täiendavad olemasolevaid meetmeid või vähendavad nende efektiivsust.

Meetmete elluviimise planeerimine

Infoturbe kontseptsiooni koostamisel tuleks üksikuid turvameetmeid valides planeerida kohe ka nende elluviimine. Selleks tuleb fikseerida, millise perioodi jooksul tuleb üksikuid meetmeid rakendada, milliste meetmete üheskoos rakendamine oleks mõistlik ja milliseid meetmeid ei jõutaks võib-olla ajaliselt rakendada.

Meetmete rakendamise planeerimine tuleks fikseerida infoturbe kontseptsioonis või lisana esitatud realiseerimisplaanis. See peaks sisaldama eelkõige meetmete rakendamise järjekorda ja vastutavaid isikuid või osakondi.

- Realiseerimisplaan – prioriteetide kindlaksmääramine (rakendamise järjekord)

Kõikide IT-turvameetmete prioriteetsus tuleks määrata nende tähtsuse ja efektiivsuse järgi. Põhimõtteliselt tuleks esmajärjekorras rakendada eriti tõsiste ohtude vastu suunatud meetmed. See on eriti oluline siis, kui nende ohtude eest ollakse siiani vaid vähesel määral kaitstud. Kui nt rahalistel põhjustel ei ole kõiki meetmed kohe võimalikud, tuleks kontrollida, milliste meetmete mõjupiirkond on kõige laiem ja mis kaitseksid seega eriti paljude ohtude vastu.

Neid meetmeid tuleks rakendada kõigepealt.

- Meetmete järjekorra koostamisel tuleks arvestada ka võimalike meetmetevaheliste seostega.
- Vastutavad isikud: iga meetme puhul tuleb kindlaks määrata, kes vastutab meetme kasutuselevõtmise, rakendamise ja kontrollimise (nt auditi) või lõpliku kontrollimise eest.

Turvameetmeid valides tuleb alati tähelepanu pöörata ka nende sobivusele ja majanduslikkusele. Peab olema võimalik tõendada, miks väljavalitud meetmed sobivad infoturbe eesmärkide saavutamiseks ja nõuete täitmiseks. Seetõttu peaks dokumentatsioon sisaldama konkreetset informatsiooni vastutavate isikute ja ametkondlike alluvuste ning planeeritud tegevuste kontrolliks, auditiks ja järelevalveks. Tuleb fikseerida avalike tegevuste läbiviimise järjekord. Lisaks sellele tuleb dokumenteerida planeeritud või rakendatud ressursid, mis on ette nähtud üksikute IT-turvameetmete jaoks.

Infoturbe käigushoidmine ja täiustamine

Et infoturve on pidev protsess, ei piisa kõikide turvameetmete ühekordsest rakendamisest. Infoturbeprotsessi peab pidevalt täiustama, reageerima uutele tehnilistele arengutele ja eelkõige peab silmas pidama protsessi haavatavust ja selles avastatud turvaauke. Seepärast tuleb infoturbe protsessi regulaarselt kontrollida ja värskendada ning tehtud muudatused dokumenteerida. Tähtsad meetodid on seejuures regulaarselt koostatavate aruannete (vt M 2.200 Infoturbearuanded juhtkonnale ja hinnangud infoturbele) sisseviimine ja teavitamisprotsessid. Infoturbeprotsessi sertifitseerimine dokumenteerib kindlast meetodist kinnipidamist ja sertifitseerimist kui sõltumatut review-meetodit on võimalik infoturbe protsessiga ühendada.

Infoturbe kontseptsiooni struktureerimine

Sageli võetakse infoturbe kontseptsioon praktikas kasutusele selleks, et kontrollida konkreetsete turvameetmete toimimist või nende ajakohasust. Seetõttu peab kontseptsioon olema struktureeritud nii, et

- spetsiifilisi piirkondi oleks võimalik kiiresti leida ja
- seda oleks võimalik minimaalsete kuludega värskendada (selleks kasutatakse ühte tööriista).

Lisaks sellele peaks üksikute turvameetmete kirjeldus olema piisavalt konkreetne, et töötaja asendamise vajaduse korral saaks keegi teine infoturbe spetsiifilised ülesanded üle võtta. Infoturbe kontseptsioon võib sisaldada informatsiooni, mida ei tohiks suvaliselt edasi anda. Selline informatsioon võib olla näiteks teave veel kõrvaldamata haavatavuste kohta või informatsioon meetmete kohta, mis võimaldavad turvameetmetest mööda minna või neist jagu saada. Sellise informatsiooni konfidentsiaalsus tuleb tagada nii, et eranditult asjaosalistele antakse juurdepääs üksnes nende jaoks olulistele kontseptsiooni osadele. Infoturbe kontseptsiooni vastav liigendus võib seda põhimõtet toetada. Oluline on luua institutsioonis ühtne arusaam infoturbest. Selle juurde kuulub ka ühtsete ja selgete mõistete kasutamine. Seepärast tuleks aegsasti koostada olulisemaid infoturbealaseid mõisteid seletav sõnastik, mida tuleks kasutada kõigi infoturbe seisukohalt oluliste dokumentide koostamisel. Sõnastiku võib avaldada infoturbe kontseptsioonis või eraldi väljaandena.

Kontrollküsimused:

- Kas infoturbe kontseptsioon on olemas?
- Millal infoturbe kontseptsiooni viimati uuendati?
- Kus infoturbe kontseptsioon asub?
- Kes tohib seda kasutada?
- Kas iga töötajat on vähemalt temale otseselt vajalikest infoturbe kontseptsiooni osadest informeeritud?

M 2.197 Töötajate kaasamine turbeprotsessi

Turvameetme kasutuselevõtmise eest vastutab: IT turvaosakond

Turvameetme rakendamise eest vastutavad: ülemused, IT turvaosakond

Infoturve puudutab eranditult kõiki töötajaid. Iga töötaja peab vastutustundlikult ja kvaliteediteadlikult tegutsedes vältima kahjude teket ja edu saavutamisele kaasa aitama. Töötajate infoturbe protsessi kaasamise juurde kuuluvad alljärgnevad valdkonnad.

Motivatsioon ja töötingimused

Ametiasutuse või ettevõtte juhatus peab looma positiivse töökliima ja ergutama töötajaid infoturbesse isiklikku panust andma. Selle juurde kuuluvad muu hulgas järgmised aspektid:

- kasutusele tuleb võtta sobivad ja kasutajasõbralikud infoturbealased tooted;
- infoturbe kontseptsioonid ja direktiivid peavad olema realistlikud;
- infoturvet tuleb praktikasse juurutada juhatuse tasandil, et tagada selle kõrge aktsepteerimistase töötajate seas.

Koolitus ja tähelepanu juhtimine infoturbele

Järgmine ülesanne, mis peab kogu infoturbeprotsessiga kaasnema, on koolitusmeetmete ja infoturbele tähelepanu juhtimiseks vajalike meetmete organiseerimine ja elluviimine. Ettevõte või ametiasutus peaks välja töötama koolituse ja infoturbele tähelepanu juhtimise kontseptsiooni (vt B 1.13 Infoturbe teadlikkus ja -koolitus).

Töötajate osalemine

Töötajatele tuleb selgitada turvameetmete mõtet. Lisaks sellele tuleks töötajad kaasata aegsasti IT turvameetmete planeerimisse või organisatoorsete eeskirjade väljatöötamisse.

Personaalsed turvameetmed

On suur hulk personaalseid infoturbega seotud aspekte, mida tuleks kõikide ettevõttes ja väljaspool ettevõtet töötavate töötajate puhul silmas pidada. Sellega tuleb arvestada personali valides, uute töötajate juhendamisel ja töötajate lahkumisel (vt B 1.2 Personal).

Kontrollküsimused:

- Kas töötajaid kaasatakse infoturbealaste juhendite ja tööriistade juurutamisse ja kas neid informeeritakse sellest eelnevalt?
- Kas on olemas koolituse kontseptsioonid ja infoturbele tähelepanu juhtimise kontseptsioonid?

M 2.198 Personali teavitamine infoturbe küsimustest

Algatamise eest vastutab: infoturbespetsialist

Rakendamise eest vastutavad: infoturbespetsialist, ülemused

Paljude turvaintsidentide põhjus peitub ebapädevas käitumises. Töötajad võivad turvaintsidente esile kutsuda nii enda teadmatuse, väära käitumise kui ka teabe liiga kergekäelise edasiandmisega. Seetõttu tuleb tagada, et kõik töötajad oleksid piisavalt kursis nende töökohal kehtivate infoturbemeetmetega, et turvaintsidendid tuvastataks võimalikult kiiresti ja et töötajad suudaksid turvaintsidentide korral võtta asjakohaseid meetmeid ka omal algatusel. Infoturbehalduse oluline ülesanne on muu hulgas ka töötajate infoturbealase teadmistepagasi suurendamine.

Infoturbe teemad

Loetletud eesmärkide saavutamiseks tuleb töötajatele arusaadaval moel selgitada, miks ja millised infoturbe meetmed on olulised nii institutsiooni jaoks tervikuna kui ka erinevate konkreetsete tööülesannete täitmisel. Töötajad peavad tundma turbega seotud ohte, turvaintsidentide võimalikke tagajärgi, vajalikke turbemeetmeid ja turbe dokumentatsioonis kajastatud nõudeid (vt M 3.93 Teavitus- ja koolitusprogrammide sihtrühmade analüüs).

Teavitustöös tuleks käsitleda järgmisi teemasid:

- infoturbe alustõed,
- ülevaade kaitstavatest andmetest, ohtudest ja turbemeetmest seoses IT-seadmete kasutamisega ja ilma,
- asutuses kehtestatud infoturvet käsitlevate turvapoliitikate sisu,
- turbekontseptsiooni sisu ja eesmärgid,
- institutsiooni ülesanded, eesmärgid ja väärtused: väärtuste puhul on siin mõeldud nii materiaalseid väärtusi (nt andmeid, tootmisseadmeid, töötajaid, oskusteavet) kui ka vaimseid väärtusi (nt institutsiooni tegutsemisfilosoofia, käitumiskoodeks jmt).

Kõiki teemasid tuleks nende paremaks mõistmiseks toetada erinevate näidetega, mis peaksid olema võimalikult tihedalt seotud töötajate töökeskkonnaga. Eelnevalt loetletud teemade puhul on tegemist vaid ühe võimaliku valikuga. Teavitamismeetmete sisu tuleb alati kohandada institutsiooni konkreetsete oludega. Infoturbealase teadlikkuse pidevaks suurendamiseks ja sisseharjunud käitumismallide muutmiseks tuleb tagada, et teavitustöö ei oleks mitte juhuslik, vaid pidev õpiprotsess. Sealjuures on oluline, et pidevalt võetavate teavitamismeetmete sisu oleks kooskõlas nii töötajate töökeskkonna kui ka tööülesannetega.

Infoturbe teavitusmaterjalid

Töötajate infoturbealase teadlikkuse suurendamiseks tuleb infoturbest pidevalt erinevates suhtluskanalites ja -keskkondades juttu teha. Selleks võib kasutada juba institutsioonis olemasolevaid või ka uusi, spetsiaalselt selleks otstarbeks loodavaid keskkondi. Valdkonna teadvustamisele aitavad kaasa ka atraktiivsed reklaammaterjalid ja üritused. Selle alla kuulub nt infoturvet käsitlevate teadete ja juhtkirjade edastamine konkreetsetele sihtrühmadele. Hoidmaks vajalikku teavet pidevalt töötajate silmade ees, võib lühikesi infoturvet käsitlevaid suuniseid trükkida nt kalendritele või kohvitassidele. Efektiivne viis sõnumite edastamiseks on

ka plakatid. Plakatid tuleks üles riputada käidavatesse kohtadesse, nt sööklasse, lifti või koosolekuruumi ja plakateid tuleks ka regulaarselt vahetada. Asjakohaseid plakateid on võimalik hankida nt erinevatelt turvatoodete tootjatelt ja reklaammaterjalide tootjatelt. Infoturbe lööklaused võiksid olla lihtsad ja meeldejäävad ning olenevalt asutuse töökultuurist võib-olla isegi humoorikad, nt „Elu lühike, parool pikk", „Tänaseid varukoopiaid ära viska homse varna" või „Ära saada meili – avalikkus läheb leili".

Infoturbe teemade edastamiseks sobib kasutada nt järgmisi materjale:

- flaiereid ja uudisnupukesi asutuse juhtkonna sõnastatud infoturbealase olulise teabe ja selle põhitõdedega;
- teabebrošüüre erinevate teemade kohta, nagu nt töökoht, koosolekuruumid, käitumine töölähetustel;
- plakatid ja ekraanipimendid;
- infoturbetekstidega tassid, hiirepadjad jmt;
- infoturbemeeskonna saadetavad e-kirjad, milles teavitatakse värsketest intsidentidest ja tuletatakse meelde turbereegleid;
- erinevaid turbeteemasid käsitlevad videoklipid, nt kuidas käituda võõrastega, kellel puudub külastajapääse;
- lühiettekanded infoturbe teemadel asutusesiseste ürituste raames, nt osakonna koosolekutel või ette nähtud koolitustel;
- artiklite avaldamine töötajatele suunatud asutusesisestes uudiskirjades kõige värskemate turvaintsidentide kohta (juhul kui puudub intsidentide matkimise oht) jms.

Infoturbeteemade käsitlemiseks sobivad muu hulgas hästi ka interaktiivsed õpivormid, nagu töötoad ja rollimängud (vt M 3.47z IT-turbealased tegevus- ja rollimängud). Enne infoturvet puudutava teabe edastamist tuleb hoolikalt analüüsida, mis liiki teabematerjale ja teabekanaleid peavad töötajad kõige usaldusväärsemaks.

Turbealast teadlikkust suurendavate meetmete võtmine

Infoturbealaste teadlikkust suurendavate meetmete võtmist saab toetada ka koolitusprogrammidega. Seetõttu tuleks teavituskontseptsioonis arvestada ka nendega. Lisateavet asjakohaste koolituste kohta leiate meetmest M 2.557 Infoturbealase koolitusprogrammi kontseptsioon .

Selleks, et infoturve jõuaks kõikide töötajate teadvusesse, tuleb välja töötada pikkajaline koolitus- ja teavitusprotsess. Tuleb luua eeldused, et infoturvet käsitlevate teemadega mindaks järk-järgult süvitsi, et materjale ajakohastataks pidevalt ning et materjalid oleksid kogu aeg saadaval ja nähtaval. Teavitusmeetodid ja -materjalid peaksid viima töötajad infoturbe teemadega kurssi ning andma neile vajalikud taustateadmised ja looma eeldused individuaalseks tegutsemiseks.

Alljärgnevalt kirjeldatakse infoturbealase teavituskampaania nelja erinevat valdkonda (teadlikkuse suurendamine, koolitus, teadmiste kinnistamine ja suhtekorraldus). Järgmised valdkonnad sõltuvad küll teatud määral üksteisest, kuid alljärgnevalt kirjeldatavaid tegevusi ei pea ilmtingimata korraldama siin loetletud järjekorras.

Teadlikkuse suurendamine

Teadlikkuse suurendamise etapis antakse töötajatele taustateavet, et nad mõistaksid, miks on asutuses kehtestatud teatud turbenõuded, millised on turbega seotud ohud, milliste ohtudega seistakse silmitsi igapäevatöös ja millised võivad olla ohtude tagajärjed nii asutusele endale kui ka selle töötajatele. Taustateave peab töötajaid infoturbe temaatikaga tegelemiseks ette valmistama ja selgitama edasiste koolituste vajalikkust. Taustateabe edastamise meetodite ja materjalide näited: teavitusüritused, flaierid, brošüürid, plakatid, ekraanipimendid, hiirematid, videod jms.

Koolitus

Koolituste eesmärk on juhendada töötajaid, kuidas järgida turvakontseptsiooni nõudeid ja ennetada seeläbi kõikvõimalikke infoturbega seotud ohte. Erinevate sihtrühmade koolitusvajaduste väljaselgitamisel tuleb lähtuda turvakontseptsioonist ja sihtrühmade analüüsist (vt M 3.93 Teavitus- ja koolitusprogrammide sihtrühmade analüüs). Koolituse meetodite ja materjalide näited: kontaktkoolitused, olemasolevate koolituste täiendamine infoturbeteemadega, infolust, videod jms.

Teadmiste kinnistamine

Teadmiste kinnistamise eesmärk on hoida töötajate omandatud teadmisi ka pärast koolitusi võimalikult kaua kõrgel tasemel ja tagada, et töötajad tegeleksid infoturbe temaatikaga pidevalt edasi (vt M 3.95z Õppematerjali kinnistamine). Teadmiste kinnistamise meetodite ja materjalide näited: uudiskirjad, foorumid, auhinnamängud, värskenduskoolitused jms.

Suhtekorraldus

Suhtekorraldusega on võimalik esitleda asutuse infoturbealast teadlikkust nii sisse- kui ka väljapoole. Kõikvõimalikud artiklid, nt kongressidel või erialameedias, ja osalemine töörühmades, kus kajastatakse asutuses võetud teavitamismeetmeid, võib luua nii asutusele kui ka selle töötajatele positiivse turbeimago, aidates nii veelgi kaasa turbealase teadlikkuse suurendamisele. Suhtekorralduse meetodite ja materjalide näited: töötajatele suunatud ajalehed, valdkonnakesksed ajakirjad, pressiteated, osalemine kongressidel, töörühmades jms.

Kontrollküsimused:

- Kas on tagatud, et töötajate infoturbealast teadlikkust suurendatakse pidevalt ja piisavalt?

M 2.200 Infoturbearuanded juhtkonnale ja hinnangud infoturbele

Algatamise eest vastutavad: IT turvaosakond, IT-juht

Rakendamise eest vastutavad: IT turvaosakond, ametiasutuse/ettevõtte juhtkond

Infoturbe eest vastutava töötaja ülesannete hulka kuulub ametiasutuse või ettevõtte juhtkonna toetamine seoses kogu vastutusega, mida juhtkond infoturbe eest kannab. Vastuvõetavate otsuste põhiliseks aluseks on ülevaatlik ja adekvaatne informatsioon infoturbe hetkeolukorra kohta institutsioonis. Infoturbeprotsessi juhtimiseks ja käigus hoidmiseks peab vähemalt kord aastas andma infoturbele hinnangu. Infoturbele hinnangu andmise eesmärk on infoturbeprotsessi raames elluviidava edasise tegevusplaani kooskõlastamine juhtkonnaga. Juhtkonnale esitatavad aruanded on infoturbele antava hinnangu andmiseks vajalike otsuste tegemise aluseks. Infoturbele antavas hinnangus tuleb välja tuua ja fikseerida kõik muudatused, mida on vaja infoturbeprotsessis teha ja need peavad olema vormistatud näiteks infoturbealaste eesmärkide või infoturbe poliitikana. Infoturbealase hinnangu kõik tulemused tuleb dokumenteerida ja ülestähendused arhiveerida.

Aruanded juhtkonnale

Vahet tuleb teha kahe erineva aruandeliigi vahel.

Regulaarsed aruanded juhtkonnale

Regulaarsete infoturbearuannete esitamisega garanteeritakse, et juhtkond saab informatsiooni, mida ta vajab infoturbele hinnangu andmiseks. Infoturbele antav hinnang peaks sisaldama järgmist:

- millised infoturbe kontseptsioonis fikseeritud eeskirjad on ettevõttes või ametiasutuses juba olemas,
- kus esineb veel lünki ja seega hajutamata riske,
- milliseid turvaintsidente on esinenud, millised olid kahjud ja milliseid kahjusid suudeti ära hoida,
- milliseid tulemusi andsid ettevõttesisesed kontrollimised ja auditid (vt M 2.217 Teabe, rakenduste ja süsteemide hoolikas liigitamine ja käitlus),
- millisel määral vastab infoturbetase infoturbenõuetele ja institutsiooni ohustatuse astmele,
- kas raamtingimused on muutunud sellisel määral, et vajatakse uusi meetmeid,
- kas infoturbe raames läbi viidud tegevused olid edukad.

Parandusettepanekud

- kas infoturbealaste eesmärkide saavutamiseks võetud IT turvameetmed õigustasid ennast või peab meetmeid muutma või täiendama,
- milline oli klientidelt, äripartneritelt, töötajatelt või avalikkuselt infoturbe kohta saadud tagasiside,
- milliseid infoturbe ressursse kasutati.

Viimase infoturbele antud hinnangu järelseire

- kas ja kuidas täideti viimase infoturbele antud hinnangu otsuseid ja kas infoturbe raames läbi viidud tegevused olid edukad.

Ühtlasi tuleks esitada kogu organisatsiooni edasise arengu eeldatavad perspektiivid ja ära märkida, kas on olemas tehnilisi arenguid või meetodeid, mille abil võiks infoturbeprotsessi täiustada.

Vajadusepõhised infoturbearuanded

Ootamatult tekkivate infoturbeprobleemide korral või riskide tõttu, mis tulenevad uutest tehnilistest arengutest, võib tekkida vajadus koostada lisaks regulaarsetele infoturbearuannetele vajadusepõhiseid infoturbearuandeid. Nii on see eelkõige siis, kui selgub, et neid probleeme ei ole võimalik töökohal kõrvaldada, sest vajatakse nt lubatud raamidest väljuvaid materiaalseid ressursse või tuleb võtta ulatuslikumaid personaalseid meetmeid. Ikka ja jälle tõmbavad sellised turvaintsidendid nagu arvutiviiruste globaalsed ründed endale massimeedia tähelepanu. Ka nendel juhtudel on infoturbearuannete koostamine osutunud otstarbekaks, et selgitada välja, millisel määral need turvaintsidendid organisatsiooni tabasid. Ka siis, kui infoturbealane olukord muutub (nt uute ohtude, tehnoloogiate või seaduste tõttu), võib vajadusepõhise infoturbearuande koostamine olla mõistlik.

Lühike ja arusaadav

Infoturbearuannete koostamisel tuleks silmas pidada, et nende lugejad ei ole tavaliselt tehnikaeksperdid. Seetõttu peaks tekst olema võimalikult arusaadav ja lühike. Seega tuleks oluliste punktidena välja tuua eelkõige olemasolevad nõrgad kohad, kuid unustada ei tohiks ka saavutusi.

Otsuse projekt

Infoturbearuande lõpus, seda eelkõige vajadusepõhiste aruannete puhul, peaks meetmete osas esitama alati ka ettepanekud, mis sisaldaksid selgeid prioriteete ja eeldatavate rakenduskulude realistlikke hinnanguid. Nii garanteeritakse, et juhatus saab vajaliku otsuse teha ilma tarbetute viivitusteta.

Koostöö juhatusega

Kui vähegi võimalik, tuleks juhatusele esitatud infoturbearuannet levitada mitte ainult kirjalikus vormis, vaid seda võiks esitleda infoturbeosakonna töötaja isiklikult. Selline informatsiooni personaalne edastamine annab ühelt poolt võimaluse viidata olulistele raskustele, eelkõige olemasolevatele või tekkida võivatele puudustele infoturbe valdkonnas, neid seejuures eriliselt rõhutades. Teiselt poolt saab isiklikult kohal viibivale infoturbe eest vastutavale töötajale esitada küsimusi või paluda temalt täpsemaid selgitusi, mis omakorda kiirendab otsuste vastuvõtmise protsessi. Lõppude lõpuks pakub selline isiklik kontakt võimalust seada sisse „teatud hierarhia", mille olemasolust võib kiireloomuliste hädaolukordade korral olla väga palju abi. Alternatiivi või täiendusena infoturbearuande isiklikule esitlemisele tuleks mõelda sellele, kas ettevõtte või ametiasutuse juhatuse liige, kellel on vastav erialane taust ja huvi, võtab samuti sõna. Ka nii on võimalik juhatuse otsuseid paremini ette valmistada ja probleeme juba eelnevalt lahendada.

Infoturbealane hinnang

Infoturbealases hinnangus tehakse infoturbearuande põhjal otsused, mis puudutavad edasist tegutsemist seoses infoturbeprotsessiga. Võimaluse korral aitab

infoturbe eest vastutav töötaja seejuures ametiasutuse või ettevõtte juhatust. Infoturbealane hinnang peaks ette valmistama ja dokumenteerima otsuste tegemist järgmistes punktides:

- vajalikud tegevused infoturbe kontseptsiooni efektiivsuse tõstmiseks ja vajatavad ressursid,
- turbevajaduse aste ja hajutamata riski käsitlemine täiendavas riskianalüüsis,
- muudatused infoturbe seisukohalt olulistes protsessides, et olla valmis reageerima ettevõttesisestele või ettevõttevälistele intsidentidele, mis võiksid avaldada mõju infoturbe kontseptsioonile, pidades silmas nt muutusi
- ärilistes eesmärkides,
- infoturbenõuetes,
- äriprotsessides,
- ettevõttevälistes raamtingimustes (nt seadustes või lepingulistes kohustustes).

Dokumentatsioon

Infoturbeprotsessi pideva jälgimise eesmärgil tuleks kõik juhtkonnale esitatud infoturbearuanded ja infoturbele antud hinnangud koos langetatud otsuste kohta tehtud märgetega süstematiseeritult arhiveerida. See dokumentatsioon peaks olema vastutavatele töötajatele vajaduse korral kiiresti kättesaadav (vt M 2.201 Infoturbe protsessi dokumenteerimine).

Konfidentsiaalsus

Et juhtkonnale esitatavad infoturbearuanded sisaldavad üldiselt konfidentsiaalset informatsiooni olemasolevate turvaaukude ja hajutamata riskide kohta, tuleb nende konfidentsiaalsust kaitsta. Tarvitusele tuleb võtta vastavad kaitsemeetmed, et volitamata isikud ei saaks infoturbearuannete sisu teada.

Täiendavad kontrollküsimused:

- Kas infoturbearuanded sisaldavad olulist informatsiooni infoturbeprotsessi kohta?
- Kas infoturbearuannetele antakse adekvaatne hinnang ja kas need allkirjastatakse?
- Kas infoturbearuanded ja infoturbele antud hinnangud arhiveeritakse?

M 2.201 Infoturbe protsessi dokumenteerimine

Turvameetme kasutuselevõtmise eest vastutab: IT turvaosakond

Turvameetme rakendamise eest vastutab: IT turvaosakond

Arvestatavat infoturbetaset on võimalik saavutada üksnes siis, kui infoturbeprotsessi kohta on olemas arusaadav, nõuetele vastav, ajakohane ja pidevalt säilitatud dokumentatsioon ning süstematiseeritud dokumendihaldus. Infoturbeprotsessi kulg ja tähtsad otsused ning protsessi üksikutes etappides saavutatud töötulemused tuleks dokumenteerida. Selline dokumentatsioon on infoturbe toimimise oluline eeldus ja seega protsessi efektiivse arengus otsustava tähtsusega. See aitab leida ja kõrvaldada rikete ning valesti suunatud protsesside põhjusi. Seejuures on tähtis, et kunagi ei hoitaks käepärast ainult vastavate dokumentide konkreetset ajakohast versiooni, vaid võetaks ette ka eelmiste versioonide tsentraalne arhiveerimine. Alles nii tagatakse infoturbe valdkonnas arengu pidev jälgimine, mille puhul on võimalik vastuvõetud otsuste juurde tagasi pöörduda.

Dokumentide liigid

Lisaks infoturbe ja infoturbeprotsessi kohta käivatele dokumentidele on olemas veel muid infoturbe jaoks olulisi dokumente. Olenevalt objektist ja kasutusotstarbest eristatakse järgmisi liike:

Aruanded juhtkonnale

Et ametiasutuse või ettevõtte juhtkond saaks soovitaval tasemel infoturbe tagamiseks võtta vastu õigeid otsuseid, vajatakse asjakohast informatsiooni. Seetõttu peaks infoturbe eest vastutav töötaja või IT-osakond koostama regulaarselt infoturbearuandeid infoturbe olukorra kohta (vt M 2.200 Infoturbearuanded juhtkonnale ja hinnangud infoturbele).

Infoturbeprotsessi kohta käivad dokumendid

Infoturbeprotsessi kohta tuleks koostada järgmist liiki dokumente:

- infoturbe eesmärgid ja infoturbe-strateegia – juhtkond peab kindlaks määrama ja avaldama ametiasutuse või ettevõtte infoturbe poliitika, mis sisaldab muu hulgas infoturbe eesmärke ja infoturbestrateegiat.
- infoturbe kontseptsioon – infoturbe kontseptsioonis kirjeldatakse IT vajalikke turvameetmeid ja nende rakendamist.
- turvasuunised – infoturbe poliitikast lähtudes on olemas valdkonna- ja süsteemispetsiifilised turvasuunised ja nõuetele vastava ning turvalise IT kasutuse eeskirjad.
- infoturbeosakonna olulised tööd, sealhulgas nt koosolekute protokollid ja otsused, tuleks samuti dokumenteerida.
- auditite ja kontrollimiste tulemused (nt kontrollnimekirjad ja küsitluste protokollid).

Tööetappide dokumenteerimine

Tööetapid, organisatsioonilised eeskirjad ja IT tehnilised turvameetmed peavad olema dokumenteeritud nii, et teadmatusest või väärtegudest tingitud turvaintsidendid oleksid välistatud. Rikete või turvaintsidentide puhul peab olema võimalik

taastada IT turvameetmed soovitud normaalsel seisul. Seetõttu tuleb tehnilisi üksikasju ja tööetappe dokumenteerida nii, et taastamine oleks mõistliku aja jooksul võimalik.

Turvaintsidentide dokumenteerimine

Turvaintsidente tuleb dokumenteerida nii, et kõiki sellega seotud protsesse ja otsuseid oleks võimalik tagantjärele tõendada. Samuti peab see võimaldama dokumenteerimist, hädaolukordadeks ettenähtud strateegiate parandamist ja teadaolevate vigade vältimist. Lisaks sellele tuleb sellised turvaintsidentide töötlemiseks vajalikud tehnilised dokumendid nagu protokollid või intsidendi seisukohalt eriti olulised süsteemiteated salvestada ja arhiveerida. Kinni tuleb pidada andmeturbeeeskirjadest.

Tehniline dokumentatsioon

Infoturbe jaoks oluliste dokumentide sellesse rühma kuuluvad:

- installatsioonide ja konfiguratsioonide juhendid,
- juhendid infoturbe uuesti käivitamiseks pärast turvaintsidenti,
- testimise ja käikulaskmise meetodite dokumendid ja
- juhised rikete ja turvaintsidentide korral tegutsemiseks.

Juhised IT kasutajale

IT turvameetmed peavad olema IT kasutajale arusaadavalt dokumenteeritud. Seega peavad kasutaja käsutuses olema:

- kehtivad turvasuunised,
- ülevaatlikud infolehed IT-süsteemide ja rakenduste turvalise kasutamise ning turvaintsidentide korral ette nähtud tegutsemise kohta,
- rakendatud IT-süsteemide ja rakenduste käsiraamatud ja juhendid.

Erandite lubamise eeskirjad

Harvadel juhtudel võib ette tulla, et turvasuunise rikkumine on mõttekas ja vajalik. Sellisel rikkumisel peab aga igal juhul olema volitatud instantsi luba. Erandeid tohib lubada ainult pärast põhjalikku kontrolli ja ülimalt harvadel juhtudel. Lisaks tuleb koostada kirjalik põhjendus, mille vastutav töötaja peab allkirjastama.

Infotulv ja infokanalid

Infoturbeprotsessi toimimiseks on oluline, et kirjeldatud oleks infokanaleid ja infotulva korral tegutsemist, samuti tuleks tagada kiire uuendamine.

Formaalsed nõuded dokumentidele ja aruannetele

Dokumendid

Infoturbe eest vastutava töötaja või infoturbeosakonna ülesanne on tagada alati ajakohaste ja adekvaatsete infoturbealaste dokumentide olemasolu. Kõigi infoturbeprotsessi raames koostatavate dokumentide vormistamiseks peaks seega olema kehtestatud üks organiseeritud tegutsemisviis.

Siia kuuluvad nt järgmised punktid:

- Loetavus – dokumendid peavad olema arusaadavad, mis tähendab ka seda, et need peavad olema kujundatud sihtgrupi kohaselt. Juhatusele esitatavate aruannete koostamisele kehtivad teistsugused nõuded kui administraatoritele mõeldud tehnilistele dokumentidele.
- Ajakohane ja ülesleitav – dokumendid peavad olema ajakohased ja nende haldamiseeskirjad peavad olema fikseeritud. Dokumendid peavad olema tähistatud ja paigutatud nii, et vajaduse korral oleks võimalik neid kiiresti üles leida. Dokument peab sisaldama andmeid selle koostamiskuupäeva, versiooni, allikate ja autorite kohta. Aktuaalsuse kaotanud dokumendid tuleb ringlusest kõrvaldada ja arhiveerida.
- Muudatusettepanekute esitamiseks (kaasa arvatud uute dokumentide koostamiseks), hindamiseks ja vajaduse korral nende arvessevõtmiseks peaks olema kindel meetod.
- Lisaks informatsiooni kiirele edastamisele vastava õigusega isikutele tuleb tagada konfidentsiaalsus organisatsioonisisestes üksikasjades. Konfidentsiaalne informatsioon tuleb sellena ka klassifitseerida ning dokumente tuleb säilitada ja käidelda turvaliselt (vt M 2.217 Teabe, rakenduste ja süsteemide hoolikas liigitamine ja käitlus).

Suure hulga infoturbe seisukohalt oluliste dokumentide haldamisel võib abi olla dokumendihaldussüsteemist (vt M 2.259z Üldise dokumendihaldussüsteemi kasutuselevõtt). Dokumendid ei pea olema alati paberkandjal. Dokumendivormi võib valida vajaduse järgi. Dokumenteerimiseks võib kasutada ülevaatlikke diagramme (nt võrguplaani), lühikesi koosolekuprotokolle (nt ettevõtte juhatuse iga-aastane koosolek infoturbestrateegia arutamiseks), käsikirjalisi märkmeid või tarkvaralisi tööriistu (nt infoturbe kontseptsiooni dokumenteerimiseks).

Kontrollküsimused:

- Kas infoturbeprotsessi kõikide etappide kohta on olemas piisav hulk dokumente?
- Kas on kehtestatud eeskirjad, kuidas kaitsta dokumentide konfidentsiaalsust?
- Kas olemasolevad dokumendid on ajakohased?

M 2.204 Ebaturvalise võrkupääsu tõkestamine

Turvameetme kasutuselevõtmise eest vastutab: IT turvaosakond

Turvameetme rakendamise eest vastutab: IT turvaosakond

Arvestatavat infoturbetaset on võimalik saavutada üksnes siis, kui infoturbeprotsessi kohta on olemas arusaadav, nõuetele vastav, ajakohane ja pidevalt säilitatud dokumentatsioon ning süstematiseeritud dokumendihaldus. Infoturbeprotsessi kulg ja tähtsad otsused ning protsessi üksikutes etappides saavutatud töötulemused tuleks dokumenteerida. Selline dokumentatsioon on infoturbe toimimise oluline eeldus ja seega protsessi efektiivse arengus otsustava tähtsusega. See aitab leida ja kõrvaldada rikete ning valesti suunatud protsesside põhjusi. Seejuures on tähtis, et kunagi ei hoitaks käepärast ainult vastavate dokumentide konkreetset ajakohast versiooni, vaid võetaks ette ka eelmiste versioonide tsentraalne arhiveerimine. Alles nii tagatakse infoturbe valdkonnas arengu pidev jälgimine, mille puhul on võimalik vastuvõetud otsuste juurde tagasi pöörduda.

Dokumentide liigid

Lisaks infoturbe ja infoturbeprotsessi kohta käivatele dokumentidele on olemas veel muid infoturbe jaoks olulisi dokumente. Olenevalt objektist ja kasutusotstarbest eristatakse järgmisi liike:

Aruanded juhtkonnale

Et ametiasutuse või ettevõtte juhtkond saaks soovitaval tasemel infoturbe tagamiseks võtta vastu õigeid otsuseid, vajatakse asjakohast informatsiooni. Seetõttu peaks infoturbe eest vastutav töötaja või IT-osakond koostama regulaarselt infoturbearuandeid infoturbe olukorra kohta (vt M 2.200 Infoturbearuanded juhtkonnale ja hinnangud infoturbele).

Infoturbeprotsessi kohta käivad dokumendid

Infoturbeprotsessi kohta tuleks koostada järgmist liiki dokumente:

- infoturbe eesmärgid ja infoturbe-strateegia – juhtkond peab kindlaks määrama ja avaldama ametiasutuse või ettevõtte infoturbe poliitika, mis sisaldab muu hulgas infoturbe eesmärke ja infoturbestrateegiat.
- infoturbe kontseptsioon – infoturbe kontseptsioonis kirjeldatakse IT vajalikke turvameetmeid ja nende rakendamist.
- turvasuunised – infoturbe poliitikast lähtudes on olemas valdkonna- ja süsteemispetsiifilised turvasuunised ja nõuetele vastava ning turvalise IT kasutuse eeskirjad.
- infoturbeosakonna olulised tööd, sealhulgas nt koosolekute protokollid ja otsused, tuleks samuti dokumenteerida.
- auditite ja kontrollimiste tulemused (nt kontrollnimekirjad ja küsitluste protokollid).

Tööetappide dokumenteerimine

Tööetapid, organisatsioonilised eeskirjad ja IT tehnilised turvameetmed peavad olema dokumenteeritud nii, et teadmatusest või väärtegudest tingitud turvaintsidendid oleksid välistatud. Rikete või turvaintsidentide puhul peab olema võimalik

taastada IT turvameetmed soovitud normaalsel seisul. Seetõttu tuleb tehnilisi üksikasju ja tööetappe dokumenteerida nii, et taastamine oleks mõistliku aja jooksul võimalik.

Turvaintsidentide dokumenteerimine

Turvaintsidente tuleb dokumenteerida nii, et kõiki sellega seotud protsesse ja otsuseid oleks võimalik tagantjärele tõendada. Samuti peab see võimaldama dokumenteerimist, hädaolukordadeks ettenähtud strateegiate parandamist ja teadaolevate vigade vältimist. Lisaks sellele tuleb sellised turvaintsidentide töötlemiseks vajalikud tehnilised dokumendid nagu protokollid või intsidendi seisukohalt eriti olulised süsteemiteated salvestada ja arhiveerida. Kinni tuleb pidada andmeturbeeeskirjadest.

Tehniline dokumentatsioon

Infoturbe jaoks oluliste dokumentide sellesse rühma kuuluvad:

- installatsioonide ja konfiguratsioonide juhendid,
- juhendid infoturbe uuesti käivitamiseks pärast turvaintsidenti,
- testimise ja käikulaskmise meetodite dokumendid ja
- juhised rikete ja turvaintsidentide korral tegutsemiseks.

Juhised IT kasutajale

IT turvameetmed peavad olema IT kasutajale arusaadavalt dokumenteeritud.

Seega peavad kasutaja käsutuses olema:

- kehtivad turvasuunised,
- ülevaatlikud infolehed IT-süsteemide ja rakenduste turvalise kasutamise ning turvaintsidentide korral ette nähtud tegutsemise kohta,
- rakendatud IT-süsteemide ja rakenduste käsiraamatud ja juhendid.

Erandite lubamise eeskirjad

Harvadel juhtudel võib ette tulla, et turvasuunise rikkumine on mõttekas ja vajalik. Sellisel rikkumisel peab aga igal juhul olema volitatud instantsi luba. Erandeid tohib lubada ainult pärast põhjalikku kontrolli ja ülimalt harvadel juhtudel. Lisaks tuleb koostada kirjalik põhjendus, mille vastutav töötaja peab allkirjastama.

Infotulv ja infokanalid

Infoturbeprotsessi toimimiseks on oluline, et kirjeldatud oleks infokanaleid ja infotulva korral tegutsemist, samuti tuleks tagada kiire uuendamine.

Formaalsed nõuded dokumentidele ja aruannetele

Dokumendid

Infoturbe eest vastutava töötaja või infoturbeosakonna ülesanne on tagada alati ajakohaste ja adekvaatsete infoturbealaste dokumentide olemasolu. Kõigi infoturbeprotsessi raames koostatavate dokumentide vormistamiseks peaks seega olema kehtestatud üks organiseeritud tegutsemisviis.

Siia kuuluvad nt järgmised punktid:

- Loetavus – dokumendid peavad olema arusaadavad, mis tähendab ka seda, et need peavad olema kujundatud sihtgrupi kohaselt. Juhatusele esitatavate aruannete koostamisele kehtivad teistsugused nõuded kui administraatoritele mõeldud tehnilistele dokumentidele.
- Ajakohane ja ülesleitav – dokumendid peavad olema ajakohased ja nende haldamiseeskirjad peavad olema fikseeritud. Dokumendid peavad olema tähistatud ja paigutatud nii, et vajaduse korral oleks võimalik neid kiiresti üles leida. Dokument peab sisaldama andmeid selle koostamiskuupäeva, versiooni, allikate ja autorite kohta. Aktuaalsuse kaotanud dokumendid tuleb ringlusest kõrvaldada ja arhiveerida.
- Muudatusettepanekute esitamiseks (kaasa arvatud uute dokumentide koostamiseks), hindamiseks ja vajaduse korral nende arvessevõtmiseks peaks olema kindel meetod.
- Lisaks informatsiooni kiirele edastamisele vastava õigusega isikutele tuleb tagada konfidentsiaalsus organisatsioonisisestes üksikasjades. Konfidentsiaalne informatsioon tuleb sellena ka klassifitseerida ning dokumente tuleb säilitada ja käidelda turvaliselt (vt M 2.217 Teabe, rakenduste ja süsteemide hoolikas liigitamine ja käitlus).

Suure hulga infoturbe seisukohalt oluliste dokumentide haldamisel võib abi olla dokumendihaldussüsteemist (vt M 2.259z Üldise dokumendihaldussüsteemi kasutuselevõtt). Dokumendid ei pea olema alati paberkandjal. Dokumendivormi võib valida vajaduse järgi. Dokumenteerimiseks võib kasutada ülevaatlikke diagramme (nt võrguplaani), lühikesi koosolekuprotokolle (nt ettevõtte juhatuse iga-aastane koosolek infoturbestrateegia arutamiseks), käsikirjalisi märkmeid või tarkvaralisi tööriistu (nt infoturbe kontseptsiooni dokumenteerimiseks).

Kontrollküsimused:

- Kas infoturbeprotsessi kõikide etappide kohta on olemas piisav hulk dokumente?
- Kas on kehtestatud eeskirjad, kuidas kaitsta dokumentide konfidentsiaalsust?
- Kas olemasolevad dokumendid on ajakohased?

M 2.206 Lotus Notesi/Domino kasutuselevõtu planeerimine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator, infoturbespetsialist

Lotus Notesi/Domino kasutuselevõttu tuleb hoolikalt planeerida. Planeerimine ja selle tulemuste rakendamine peab olema järjepidev protsess, mitte ühekordne tegevus seoses esmakordse kasutuselevõtuga. Planeerimise detailsusaste ja erinevate aspektide hulk, mida tuleb planeerimisprotsessi vältel dokumenteerida, olenevad muu hulgas Lotus Notesi/Domino kasutuskeskkonna turbevajadusest. Planeerimisel tuleb kindlasti arvestada ka sobivust hindavate kriteeriumitega, nt institutsiooni suuruse ja kasutada olevate ressurssidega. Samuti tuleb kaaluda Lotus Notesi/Domino platvormis saada olevate teenuste kasutamist ja arvestada platvormi keerulise arhitektuuriga. Näiteks kui Lotus Notesi/Dominot soovitakse kasutusele võtta ainult sisemise ja välimise meiliplatvormina ja üleinstitutsioonilise koostööplatvormina (Workgroupi tugi), on arhitektuur enamasti lihtne ja planeerimine ei ole ülemäära töömahukas, kuid olukorras, kus neid ei soovita rakendada mitte ainult meili- ja koostööplatvormina, vaid tahetakse neile lisada ka ekstraneti- ja internetiliidesed ning kasutada suurt hulka internetiteenuseid, k.a Instant Messaging ja Web Services, on planeerimistööde maht juba tunduvalt suurem. Lotus Notesi/Domino kasutuselevõtu planeerimisel tuleb üldjuhul arvestada järgmiste aspektidega:

- süsteemiarhitektuur ja selle turbeaspektid;
- Lotus Notesi/Domino roll üleinstitutsioonilises identiteedihalduses;
- domeenide ja sertifikaatide hierarhia planeerimine;
- Lotus Notesi/Domino keskkonnas aset leidvate administratiivtegevuste planeerimine;
- Lotus Notesi/Domino platvormi olulisuse kindlaksmääramine üleinstitutsioonilises tööprotsesside tagamise ja hädaolukorraks valmisoleku planeerimises;
- Lotus Notesi/Domino keskkonna andmeside turvalisuse planeerimine.

Lotus Notesi/Domino platvormi saab kasutada serveri virtualiseerimistehnoloogia ja terminaliserveri tehnoloogiaga. Neil juhtudel tuleb planeerida, kuidas tagada Lotus Notesi/Domino platvormi ja rakendatava virtualiseerimisplatvormi parim võimalik koostöö. Olenevalt Lotus Notesis/Dominos kasutatavate tööprotsesside turbevajadusest võivad Lotus Notesi/Domino teenustele kehtida kõrgkäideldavusnõuded. Sel juhul tuleb planeerida, kuidas tagada Lotus Notesi/Domino platvormi ja rakendatava tehnoloogia koostööle kehtestatud kõrgkäideldavusnõuete täitmine, s.t lahendada küsimus, kuidas Lotus Notesi/Domino mehhanisme kõrgkäideldavuse jaoks konfigureerida (klasterdamine).

Süsteemiarhitektuur ja selle turbeaspektid

Kasutusvaldkonnast ja funktsioonidest tingitud ning IT-strateegiast lähtuvate nõuete kõrval tuleks Lotus Notesi/Domino platvormi arhitektuuri planeerimisel arvestada ka turbeaspektidega. Selleks võib järgida kas üldkehtivat turbepoliitikat või kasutada konkreetseid, institutsioonis spetsiaalselt selleks otstarbeks välja töötatud süsteemiarhitektuuri turvet käsitlevaid nõudeid. Lotus Notesi/Domino ar-

hitektuuri planeerimise jaoks oluline turbepoliitika, s.t süsteemiarhitektuuri turbeelemendid, tuleb muuta konkreetseks arhitektuuri planeerimise osaks. Näiteks tuleb arvestada institutsioonis ekstraneti või interneti üleminekutena toimivate Lotus Notesi serverite turvalise asukohavaliku ja nende võrguüleminekute planeerimise kohta kehtivate turbenõuetega. Langetades otsust, kui paljusid Lotus Notesi/Domino servereid erinevates punktides kasutada, tuleks lähtuda eelkõige Lotus Domino teenuste turbevajadusest. Lotus Domino teenuste puhul tuleb üldjuhul eesmärgiks seada turbe-eesmärkidel põhinev valikuline ja piiranguid kehtestav installatsioon. Kõikjal, kus see on vähegi võimalik, tuleks väga suure turbevajadusega teenused väiksema turbevajadusega teenustest süsteemiarhitektuuri tasandil lahutada. Nii tagatakse, et väiksema turbeastmega teenustes leiduvaid kitsaskohti ei saa ära kasutada suure turbevajadusega teenuste pärssimiseks. Näiteks võiks institutsioonis tsentraalselt toimiva meiliteenuse puhul kasutada liiasust ning seda teenust võiks käitada serverites, kus ei tööta teisi kitsaskohtade poolest riskantseid teenuseid.

Lotus Notesi/Domino roll üleinstitutsioonilises identiteedihalduses

Üleinstitutsioonilise identiteedihalduse sisseseadmiseks on Lotus Notesi/Domino platvormi funktsioonid üpris laialdased. Lotus Notesi/Dominot on võimalik tööle panna identiteedihalduse peasüsteemina, mis varustab teisi süsteeme liideste (nt LDAP-liideste) abil andmetega elektrooniliste identiteetide ja nendega seotud volituste kohta. Samuti on Lotus Notesi/Dominot võimalik tööle panna järelsüsteemina, mis saab vastavate liideste kaudu hoopis ise andmeid mõnelt peasüsteemilt. Seetõttu on institutsiooni jaoks oluline kindlaks määrata, milline on identiteedihalduse peasüsteem ja kuidas elektrooniliste identiteetide andmetega IT-maastikul ümber käiakse. Selle põhjal saab planeerida ka Lotus Notesi/Domino rolli. See roll mõjutab olulisel määral Lotus Domino teenuste ja Lotus Notesi/Domino infrastruktuurikomponentide turbevajadust.

Domeenide ja sertifikaatide hierarhia planeerimine

Lotus Notesi/Domino platvormi kasutuselevõtt eeldab domeenide ja sertifikaatide hierarhia planeerimist. Hierarhiat on kindlasti tarvis planeerida Lotus Notesi/Domino esmakordsel kasutuselevõtul, kuid samas tuleb seda ka iga kord kohandada, kui tehakse olulisi muudatusi organisatsiooni struktuuris, rakendatavates teenustes, süsteemiga liidetud partnerites jms. Kuna paljud turvet hõlmavad seadistused (nt tõkked ja turvet puudutavad replikeerimisparameetrid) toimivad domeeni tasandil, tuleb domeeni hierarhia planeerimisel ilmtingimata arvestada ka selle turbeaspektidega. Väikeste institutsioonide puhul võib täiesti piisata ühe domeeni kontseptsioonist (produktiivdomeen), kuid selliste keerulisemate struktuuride puhul nagu suuremad ametiasutused ja kontsernid tuleb ilmselt rakendada mitmikdomeeni kontseptsiooni. Domeeni hierarhia alla kuuluvad kõik Lotus Domino infrastruktuuri elemendid. Siia ei kuulu mitte üksnes Lotus Domino domeenid, vaid ka Lotus Domino struktuurid ja Lotus Domino võrgud (DNN, Lotus Domino Named Networks) ning kasutatav hierarhiline nimesüsteem (X.500 standardile tuginev). Domeeni hierarhia (mis reguleerib muu hulgas ka seda, milliste serverite ja kasutajate vahel võib toimuda kommunikatsioon) kehtestatakse sertifikaadihierarhiaga (PKI). Sertifikaadihierarhia planeerimine sõltub Lotus Notesi/Domino rollist üleinstitutsioonilises identiteedihalduses. Iga kord, kui identiteedihalduses tehakse olulisi muudatusi, tuleb planeerida ka muudatuste sisseviimine sertifikaatide hierarhiasse, mitte nendest tehniliste lahendustega mööda hiilida. Siinkohal tuleb arvestada, et haldama peab nii Lotus Notesi kui ka interneti sertifikaate (X.509 sertifikaate). Vajalikud struktuurid ja protsessid (nt sellised, nagu neid kirjelda-

takse X.509 standardites) tuleb defineerida juba sertifikaatide hierarhia planeerimise etapis. Siia alla kuulub näiteks sertifitseerimiskeskuse (certificate authority), registreerimiskeskuse (registration authority) ja sertifitseerimisprotsessi (CA-process) kindlaksmääramine. Muu hulgas tuleb otsustada, kas kasutusele võetakse mõne võõra teenusepakkuja või Lotus Domino sertifitseerimiskeskus. Kõiki sertifikaatide hierarhiat puudutavaid tehnilisi seadistusi ja selle haldamisega seotud tööprotsesse tuleb väga hoolikalt planeerida, kontseptsiooniliselt võimalikult detailselt välja töötada ja piisavas mahus dokumenteerida. Siinkohal tuleb arvestada, et alates versioonist Lotus Notes/Domino 8.5 saab tagasi võetud sertifikaate kontrollida ka OCSP-ga (Online Certificate Status Protocol, IETF-i RFC nr 2560). Sertifikaatide hierarhia planeerimisse tuleb sisse viia vastav uuendus.

Lotus Notesi/Domino keskkonnas aset leidvate administratiivtegevuste planeerimine

Lotus Notesi/Dominoga seotud administratiivtegevusi tuleb detailselt planeerida ning koostada nende jaoks kohustuslikud juhised (nt administraatorite kohustuslik tööjuhend). Planeerimistööde detailsusaste ja dokumentatsiooni maht olenevad Lotus Notesile/Dominole kehtestatud turbeastmest. Piisavat hoolt ja häid eriteadmisi eeldavad kriitilised administratiivsed tegevused, nt sertifitseerimisprotsessi haldus, aga ka kasutajate ja andmebaaside haldus ning komponentide ja teenuste installimine ja konfigureerimine. Kriitilise tähtsusega administreerimistegevuste piisavat dokumenteerimist tuleb nõuda administraatorite tööjuhistes ning selle nõude täitmist tuleb kontrollida. Oskamatult ja kohalekutsumise peale kiirelt ära tehtud või ebapiisavalt dokumenteeritud administreerimistegevustega kaasnevad ohud on oma tagajärgedelt võrdsed ettekavatsetud rünnete ja administraatorivolituste väärkasutusega. Need tegevused ei ole küll otseselt seotud Lotus Notesi/Dominoga, kuid need mõjutavad siiski oluliselt Lotus Notesi/Domino platvormile kehtestatud turbeastme saavutamist. Kuna Lotus Notesi/Domino platvorm on keeruline, ei piisa enamasti administraatoritele mõeldud üldiste juhiste rakendamisest, vaid arvestada tuleb ka platvormi eripäraga. Lotus Notesi/Dominoga seotud administratiivtegevuste planeerimisel tuleb muu hulgas kindlaks määrata, et nimetatud tegevusi jälgitaks ja kontrollitaks Lotus Notesi/Domino platvormi enda tehniliste võimalustega. Lotus Notesi/Domino platvormi olulisuse kindlaksmääramine üleinstitutsioonilises tööprotsesside tagamise ja hädaolukorraks valmisoleku planeerimises. Tööprotsesside ja nendega tugevalt seotud Lotus Notesi/Domino platvormi turvamehhanismide (nt andmetest varukoopiate tegemise ja andmete taastamise) planeerimine eeldab, et platvormi puhul tuleb välja selgitada selle koht tööprotsesside tagamise ja hädaolukorraks valmisoleku planeerimise üldraamistikus. Kui seda ei ole institutsioonis veel tehtud, tuleks Lotus Notesi/Domino platvormi olulisus tööprotsesside tagamise ja hädaolukorraks valmisoleku seisukohalt kindlaks määrata kas Lotus Notesi/Domino kasutuselevõtu või migratsiooni planeerimise raames. Ainult nii saab tagada, et suur hulk vajaminevaid turbemeetmeid, nt platvormi käideldavust tagavad meetmed, suudetakse planeerida võimalikult adekvaatselt.

Lotus Notesi/Domino keskkonna andmeside turvalisuse planeerimine

Lotus Notesi/Domino keskkonna struktuur on jaotatud osadeks, mistõttu on andmeside turvalisuse planeerimisel väga oluline roll platvormi üldise turbe tagamises. Selleks on soovitatav tegelda järgmiste andmeside turvet puudutavate teemadega:

- server-server-andmeside, s.t Lotus Domino serverite andmeside serverist serverisse (seda nii Lotus Notesi protokollide, internetiprotokollide kui ka andmebaasi replikeerimise kasutamisel);
- klient-server-andmeside, s.t Lotus Notesi klientide andmeside Lotus Domino serveritega (kõikide Lotus Notesi klienditüüpide kohta, kaasa arvatud administreerivad kliendid);
- võõraste klientide klient-server-andmeside, s.t võõraste klientide andmeside Lotus Domino serveritega (kasutades POP3- ja IMAP-protokolle);
- Lotus Domino serverite kaugpöörduse juurdepääsud ja spetsiifilised sissevalimisjuurdepääsud;
- push -teenuste kasutamine kaasaskantavates lõppseadmetes;
- ebaturvaliste ja -vajalike sideprotokollide (nt WebDAV) desinstallimine ja installimata jätmine;
- kitsenduste kehtestamine serveritevahelistele usaldussuhetele;
- teenuste ja liideste, nt LDAP-liideste kasutamine või nende kasutuse võimaldamine väljaspool Lotus Notesi/Domino keskkonda.

Siinkohal tuleb arvestada, et Lotus Notesis/Dominos on olemas ka eelkäijaversioonidest tuntud serveritevahelised modemiühendused, mis on tänapäeva mõistes juba aegunud ja võivad tekitada turvariske. Seetõttu tuleb andmeside turbe planeerimisel vajaduse korral ette näha selliste ühenduste eemaldamine ning vastavate liideste ja ühenduskomponentide desaktiveerimine.

Täiendavad kontrollküsimused:

- Kas Lotus Notesi/Domino platvormi arhitektuuri planeerimisel arvestatakse ka turbeaspektidega?
- Kas Lotus Notesi/Domino roll üleinstitutsioonilises identiteedihalduses on kindlaks määratud?
- Kas domeenide ja sertifikaatide hierarhia planeerimine on piisavalt hästi dokumenteeritud?

M 2.207 Lotus Notesi/Domino turvakontseptsioon

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: erialaspetsialist, infoturbespetsialist

Nii nagu iga teisegi tarkvaratoote puhul, mis terves institutsioonis kasutusele võetakse, tuleb ka Lotus Notesi/Domino jaoks koostada turvakontseptsioon. Olenevalt institutsiooni suurusest, ressurssidest ja töökorralduse struktuurist võib Lotus Notesi/Domino turvakontseptsioon koosneda kas ainult ühest lõppdokumendist (nt turvapoliitikast) või ka mitmest lõppdokumendist. Vajalike dokumentide edastamist nende sihtrühmadele hõlbustab suurel määral see, kui turvakontseptsioon koostatakse moodulite kaupa, nt Lotus Notesi/Domino platvormi rakenduste arendamist käsitleva suunistekogumiku saab sel juhul edastada ainult arendajatele ja administraatoritele. Allpool on esitatud turvakontseptsiooni punktid, mis tuleb eraldi läbi töötada ja mille tulemused dokumenteerida. Kui mõned Lotus Notesi/Domino turvakontseptsiooni punktid on institutsiooni jaoks kasutusvaldkonna eripära tõttu ebaolulised (nt kui Lotus Notesi/Domino platvormi rakenduste arendamisega ei tegelda), tuleb sellekohane teave turvakontseptsiooni üles märkida.

Lotus Notesi/Domino turvapoliitika

Turvapoliitika raames tuleb arvestada järgmiste aspektidega:

- Turvapoliitika peab olema kooskõlas institutsiooni üldise turvapoliitikaga (vt M 2.192 Infoturbepoliitika koostamine).
- Lotus Notesi/Domino turvakontseptsiooni koostamiseks tuleb defineerida sihtrühmad ning nende jaoks olulised kontseptsioonid ja suunised.
- Nimetatud alamkontseptsioonid tuleb kas turvapoliitikasse sisse kirjutada või kasutusele võtta viidatava materjalina. Siinkohal tuleb tagada, et viidatavate materjalide puhul oleks alati kättesaadav kontseptsiooni kõige uuem versioon.
- Kui institutsioonis pole kehtestatud nõuete järgimise kohustus üldtasandil reguleeritud, tuleb kõikide sihtrühmade puhul (nt Lotus Notesi kasutajad, Lotus Domino administraatorid, juhttöötajad, projektijuhid, tarkvaraarendajad, tarkvaraarhitektid) tagada, et turvapoliitika järgimine oleks kohustuslik.
- Kui institutsioonis on kasutusel mitu Lotus Notesi/Domino keskkonda (installatsiooni), tuleb turvapoliitika jaoks dokumenteerida ka nende keskkondade eripärad.
- Lotus Notesi/Domino kasutamise turvapoliitika peab olema institutsioonis kooskõlastatud ja kõikidele kasutajatele teatavaks tehtud. Siinkohal on soovitatav iga sihtrühma jaoks koostada lühike ja meeldejääv ülevaade kõikidest olulisematest aspektidest kas voldiku või veebilehena. Turbeettekirjutuste muutumisel tuleb kõiki kasutajaid sellest ka teavitada.

Lotus Notesi/Domino domeeni- ja sertifikaadihierarhia kontseptsioon

Lotus Notesi/Domino domeeni- ja sertifikaadihierarhia kontseptsioon on meetme M 2.206 Lotus Notesi/Domino kasutuselevõtu planeerimine läbitöötamise tulemus. Kontseptsiooni eest vastutav töötaja peab seda pidevalt ajakohastama

ja muudatuste korral kohandama. Lotus Notesi/Domino infrastruktuuri suuremate muudatuste korral tegelevad kohandamisega tavaliselt vastutavad projektijuhid ning süsteemi- ja tarkvaraarhitektid. Selles turbe seisukohalt üliolulises kontseptsioonis tehtavad muudatused peab heaks kiitma infoturbehalduse eest vastutav osakond.

Lotus Notesi/Domino enda turvamehhanismide kasutamise kontseptsioon:

krüpteerimine, ümberkäimine sertifikaatide ja Lotus Notesi ID-dega Lotus Notesis/Dominos on olemas erinevad krüpteerimismehhanismid nii liigutatavate andmete (andmesideühenduste, andmeside sisu) kui ka andmehulkade (nt andmebaaside, meilide) krüpteerimiseks. Tuleb kindlaks määrata, milliseid Lotus Domino mehhanisme hakatakse kasutama. Dokumenteerida tuleb nende kokkusobivus üleinstitutsioonilise üldise krüpteerimiskontseptsiooniga, s.t Lotus Notesi/Domino mehhanismidest tingitud kõrvalekalded. Lotus Notesi/Domino võtmehalduse sisseseadmisel tuleb lähtuda üleinstitutsioonilise krüpteerimiskontseptsiooni ettekirjutustest ning see peab vastama Lotus Notesi/Domino platvormi turbevajadusele. Selle kontseptsiooniga tuleb muu hulgas reguleerida ka sertifikaatide kasutamine, nt sertifikaatide uuendamine nende aegumise korral, cross- sertifikaatide koostamine. Tarvis on konkreetseid regulatsioone, mitte üldisi viiteid Lotus Notesis/Dominos olevatele mehhanismidele. Näiteks tuleb kindlaks määrata, millistel juhtudel on lubatud sertifikaadi uuendamiseks seda meiliga administraatorile saata ja millal mitte. Kuna Lotus Notesi ID-dega kaasneb nende ülekantavuse tõttu turvarisk, tuleb reguleerida ka seda, kus hoitakse nendest ID-dest andmete taastamiseks tehtud varukoopiaid ja kuidas peaksid Lotus Notesi ID-dega seotud protsessid toimima (nt sertifikaadi uuendamine, andmete taastamine varukoopiatest).

Alates Lotus Notesi versioonist 8.5 on Lotus Notesi ID-de haldamiseks kasutusele võetud eritööriist ID Vault, mis laiendab platvormi seniseid funktsioone ja lihtsustab nende kasutamist ning millega saab muu hulgas taastada Lotus Notesi kaotsi läinud ID-sid ja paroole ning sünkroniseerida Lotus Notesi/Domino platvormi enda vahenditega ID-de koopiaid. Seda tööriista on soovitatav kasutada. Kasutust tuleb hoolikalt planeerida ning selle põhjal tuleb kohandada ka Lotus Notesi/Domino enda turvamehhanismide kasutamise kontseptsiooni.

Lotus Notesi/Domino paroolisuunised

Lotus Notesis/Dominos on juba algusest peale olemas olnud omad parooli kvaliteedi hindamise mehhanismid. Seetõttu tuleb Lotus Notesi/Domino jaoks kasutusele võtta asjakohaste märkustega varustatud üleinstitutsioonilised paroolisuunised või kohandada need suunised spetsiaalselt Lotus Notesi mehhanismidega. Lotus Notesi/Domino paroolisuunised peaksid moodustama alati kindla osa Lotus Notesi/Domino turvapoliitikast. Kui sisselogimiseks kasutatakse Single-Sign-Onprotseduuri, tuleb see turvapoliitikas ka asjakohaselt ära märkida. Single-Sign-On-protseduuri jaoks kasutatavate paroolide kvaliteet peab vastama ühendatud rakenduste ja süsteemide kumulatiivsetele nõuetele.

Lotus Notesi/Domino logide koostamise ja analüüsimise kontseptsioon

Lotus Notesi/Domino platvormi jaoks on tarvis koostada kontseptsioon, mis peab olema kooskõlas institutsioonile kui tervikule kehtiva turbe jaoks oluliste andmete logimise ja analüüsimise kontseptsiooniga. Kui logimise ja logide analüüsimise kohta puuduvad üldkehtivad suunised või kui need suunised ei ole piisavalt detailsed, tuleb kontseptsiooni koostamise protsessis ette näha ka vajalikud koos-

kõlastused andmekaitsespetsialisti, töötajate esindaja ja teiste sellesse kontseptsiooni kaasatud osalistega. Turvapoliitika koostamisel tuleb arvesse võtta, et analüüsitavate andmete hulga kohta tehtavad ettekirjutused oleksid realistlikud ning et nõuete täitmiseks saadakse hakkama olemasolevate tööks kasutatavate ressurssidega. Kui institutsioonis kasutatakse juba mõnda tsentraalselt töötavat logimistööriista ja automaatselt toimivat logide analüüsimise mehhanismi, siis tuleks välja selgitada, kas nendega saaks logida ja analüüsida ka Lotus Notesi/Dominoga seotud tegevusi.

Lotus Notesi/Domino arhiveerimise kontseptsioon

Lotus Notesi/Domino platvormi puhul võib arhiveerimise kohustus kehtida väga erinevat liiki andmetele. Need võivad olla näiteks meiliandmed, arhiveerimiskohustusega workflow -elemendid, arhiveerimiskohustusega Lotus Notesi rakenduste ja teenuste andmebaasid. Kui Lotus Notesi/Dominot kasutatakse muu hulgas ka tsentraalse identiteedihalduse süsteemina, kuuluvad siia veel ka identiteedihalduse andmed. Seetõttu tuleb Lotus Notesi/Domino platvormi jaoks koostada valdkonna eripärasid arvestav tehniline arhiveerimise kontseptsioon ning seda ka rakendada või võtta aluseks üleinstitutsiooniline arhiveerimise kontseptsioon ja see Lotus Notesi/Domino keskkonna jaoks sobivaks kohandada.

Kõikide kasutatavate Lotus Notesi teenuste turvakontseptsioonid

Turvalisuse tagamise nõue kehtestatakse teenustele (sageli ka installitud moodulite tasandil) enamasti turvapoliitikas. Lotus Notesi/Domino puhul ei pea teenuste turvet tagavate meetmete dokumenteerimiseks ilmtingimata kasutama turvapoliitikat, sest sihtrühmaks on peamiselt administraatorid ja infoturbehaldusega tegelevad töötajad, mistõttu võib need sisse kirjutada ka käituskontseptsiooni. Lotus Notesi/Domino platvormi teenuste turvakontseptsioon peaks kajastama nii tehnilisi meetmeid (nn karastamine, serveri ja kliendi komponentide konfiguratsioon) kui ka töökorraldust puudutavaid meetmeid ja teavet teenuste kaitseks rakendatavate täiendavate turvakomponentide kohta. Lotus Notesi/Domino platvormi vanade turvet ohustavate rakendustega ümberkäimise ja nende rakenduste käitamiseks vajaminevate turvet ohustavate konfiguratsioonide kontseptsioon. Lotus Domino vanemad rakendused, mida ei õnnestu migreerida, võivad eeldada ebaturvalisi seadistusi, et neid saaks uuemates platvormides edasi kasutada. Kui nendest rakendustest pole võimalik loobuda, tuleb turvariskide minimeerimiseks kontseptsiooni üles märkida, kuidas toimub nende käitamine ja seire. Siinkohal tuleb tähelepanu pöörata eriti sellele, et ebaturvalisi parameetreid rakendataks platvormis ainult konkreetsel otstarbel, s.t ebaturvalisi parameetreid ei tohi kehtestada üleinstitutsioonilise standardina, tuues ettekäändeks, et nii tagatakse igapäevatööks vajalik ühilduvus vanade rakendustega.

Lotus Notesi/Domino platvormi rakenduste arendamise suunis

Lotus Notesis/Dominos on võimalik rakendusi arendada tootja enda senise tehnoloogiaga ning samas on loodud ka võimalused kasutada Eclipse'il põhinevat Java arenduskeskkonda. Ükskõik kumba rakenduste arendamise võimalust kasutatakse, mõlema puhul tuleb koostada asjakohased rakenduse arendamise suunised. Need suunised peavad sisaldama nii kasutatavate programmeerimiskeelte kodeerimisstandardeid kui ka arendamise head tava ja arendustegevuse protsessikirjeldust.

Lotus Notesi/Dominoga tehtava rakenduste integreerimise suunis

Lotus Notesi/Dominot kasutatakse aina enam serveri- ja kliendirakenduste integreerimise platvormina ja seda nii uue Lotus Notes Clienti tõttu, mida tootja reklaamib kui universaalset klientprogrammi, kui ka põhjusel, et platvorm võimaldab integreerida ka SAP-d. Et rakenduste integreerimine ei kujuneks turvaaukude allikaks, tuleb koostada Lotus Notesi/Domino platvormi eripäraga arvestavad integreerimissuunised.

Lotus Notesi/Domino kahjurvaravastane kaitse

Lotus Notesi/Domino kaitsmiseks kahjurvara kahjulike mõjude eest tuleb rakendada üldisi tervele institutsioonile kehtivaid kahjurvaravastast kaitset puudutavaid ettekirjutusi. Näiteks kuuluvad siia kahjurvaravastane kaitse võrguüleminekutes, kus Lotus Dominot rakendatakse kas veebi või meililüüsina, aga ka Lotus Domino andmebaaside (k.a meiliandmebaaside) nn järele paigutatud kaitse. Selles kontseptsioonis tuleb muu hulgas kirjeldada ka serverit ja klienti kaitsva standardina installitud tarkvara ning Lotus Notesi/Domino installitud komponentide koostööd.

Lotus Notesi/Domino karastamise kontseptsioon ja konfigureerimist puudutavad ettekirjutused

Need Lotus Notesi/Domino komponendid, mida soovitakse installida, tuleb nende turbevajaduse ja kasutusvaldkonna järgi ka karastada ja konfigureerida. Juba kasutatavate teenuste turvakontseptsioonis kirjeldatud turbemeetmeid tuleb kirjeldada nüüd kontseptsiooniliselt ka serveri tasandil. Lisaks tuleb kirjeldada seda, millised teenused jäetakse kasutusest kõrvale ja kuidas neid teenuseid selleks otstarbeks desinstallida või installimata jätta. Klientprogrammi karastamiseks ja tugeva konfiguratsiooni loomiseks vajalikke ettekirjutusi tuleb kontseptsiooniliselt kirjeldada kõikide kasutatavate klientprogrammi tüüpide (k.a brauseripõhiste klientide) puhul.

Push-teenuste kasutamise kontseptsioon

Lotus Domino meiliteenuse kasutamise seoses push -teenustega võib lahendada võõraste push -teenuste ühendamisega (nagu näiteks nutitelefonide puhul seda tehakse) või Lotus Notes Traveleri komponendiga. Push-teenuste kasutamisel on oluline, et teenuse turbega seotud teemad oleksid kontseptsioonilaadselt kirja pandud.

Kontrollküsimused:

- Kas Lotus Notesi kasutamise kohta on olemas ajakohane turvapoliitika?
- Kas kõik olulised institutsiooni turvet puudutavad ettekirjutused on Lotus Notesi puhul rakendatud?
- Kas Lotus Notesi uutest või muudetud turvareeglitest teavitatakse kõiki kasutajaid?

M 2.212 Organisatsioonilised eeskirjad puhastusteenindusele

Turvameetme kasutuselevõtmise eest vastutab: IT-turvaosakond

Turvameetme rakendamise eest vastutab: siseteenistus

Tavaliselt kasutatakse ruumide puhastamiseks väljastpoolt tellitud teenust. Eelkõige sellistes kõrgendatud turvanõuetega piirkondades, nagu seda on arvutuskeskused, serveriruumid, tehnikaruumid või kommunikatsioonikeskused võib see olla problemaatiline ning seetõttu võidakse vajada infoturbealaseid lisameetmeid. Juba riigihankes ja lepingu sõnastamisel tuleb arvestada tundlike piirkondade erilise käsitlusega. Näiteks arvutuskeskuste puhul tuleb lepingutesse juba sisse kirjutada ettevõttevälise personali kottide ja keskusesse transporditavate kaupade pisteline kontrollimine, mis toimub sisenemis- ja sissesõidualas.

Puhastusteenindajate instrueerimine

Et puhastusteenindajate puhul ei saa eeldada IT-alaste teadmiste olemasolu, tuleks neid kõigi äri seisukohalt kriitiliste IT-süsteemide osas põhjalikult instrueerida, eriti selles osas, milliste tegevuste tagajärjeks võivad olla IT-seadmete kahjustamine või probleemid IT käigushoidmisel. Sellised problemaatilised valdkonnad on alljärgnevalt ära toodud:

- Klaviatuuride puhastamisel võidakse kogemata siseneda serveritesse või teistesse tsentraalsetesse komponentidesse, mis kahjustab IT-kasutust.
- IT-süsteem võidakse kogemata välja lülitada.
- Tolmuimejat kasutades võidakse toite- ja kommunikatsioonikaableid vigastada või pistikutest välja tõmmata.
- Vee või puhastusvedeliku tõttu võidakse põhjustada riistvara komponentides lühiühendusi.

Puhastusteenindajate sissepääsu reguleerimine

Kui puhastusfirmat usaldatakse, tuleks puhastusteenindajate sissepääsemisel rakendada olemasolevat, sisenemise või uste sulgemise suhtes läbiviidavat kontrolli. Selleks võib kehtestada vaid efektiivseid turvameetmeid, nt kui töötõend või võti antakse puhastusfirma nimekirjas olevatele või selle teatud kindlatele töötajatele allkirja vastu ja ajalise piiranguga. Kokkuleppe sõlmimisel põhipersonali kasutamise kohta võib isiku tõendamise süsteemi abil saavutada tõhusa kontrolli lepingust kinnipidamise üle.

Puhastusfirma konsultandid

Töö koordineerimiseks ja esineda võivate probleemide lahendamiseks peab tellija ametisse nimetama objekti eest vastutava töötaja, kes peab olema kogu aeg kättesaadav. Tal peab olema õigus otsustada kasutatava personali üle (eelkõige personali üle, keda enam ei ole soovitatav kasutada). Selliseid kõrgendatud turbevajadusega ruume, nagu seda on arvutite ruum või andmekandjate arhiiv, tohib puhastada üksnes tellija poolt nimetatud vastutavate isikute juuresolekul või mõningatel juhtudel ka tööandja usaldusisiku juuresolekul, järgides nt nelja-silma-põhimõtet.

Täiendavad kontrollküsimused:

- Kas kontrollitakse, et volitatud puhastusfirma töötajad kasutavad neile väljastatud võtmeid või töötõendeid vastavalt lepingule?

- Kas puhastusteenindajaid on ITga ümberkäimise osas piisavalt informeeritud?
- Kas eriti tundlikes piirkondades teostatakse puhastusteenindajate töö üle järelevaatust?

M 2.213 Tehnilise infrastruktuuri hooldus

Turvameetme kasutuselevõtmise eest vastutab: tehnikaosakonna juhataja
Rakendamise eest vastutavad: tehnikaosakonna töötajad

Tootjate poolt soovitatud hooldusintervallidest ja -eeskirjadest tuleb tingimata kinni pidada. Lisaks normaalhooldusele tuleks põhjalikumalt kontrollida vanemaid seadmeid, millel otsitakse eelkõige kulunud detaile, mis vajavad väljavahetamist. See puudutab ennekõike hoone tehnika suuremaid agregaate, näiteks tsentraalseid kütte- ja kliimaseadmeid, samuti suure mehhaanilise koormusega seadmeid, nt arvutuskeskuste kaubalifte. Võimaluse korral tuleks kasutada tehnikaekspertide abi. Erilise koormuse või ebatavaliste ekspluatatsioonitingimuste tõttu võib tekkida vajadus lisahoolduse järele. Näiteks peab õhufiltreid ehitustööde ajal ja pärast nende lõppu tunduvalt lühemate intervallidega kontrollima.

Kontrollküsimused:

- Kas hoolduseeskirjadest peetakse kinni?
- Kas hooldusintervalle kohandatakse vastavalt seadmete erilisele koormusele?

M 2.214 IT-kasutuse kontseptsioon

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT-juht, IT turvaosakond

Rakendamise eest vastutavad: IT-juht, IT turvaosakond

Korrakohase ja turvalise IT-kasutuse tagamiseks on ülimalt oluline, et selle kohta oleks olemas kõikehõlmav kontseptsioon. Erinevate valdkondade IT-süsteemide ja IT-toodete kasutamiseks tuleb kehtestada reeglid ja nõuded, mis peavad olema omavahel tasakaalus ja peegeldama vastava ametiasutuse või ettevõtte turvaeesmärke.

IT-protsesside ja IT turvapõhimõtete suunised

Oluliste IT turvapõhimõtete kooskõlastamine

Kõik IT-planeerimise ja IT-kasutusega seotud organisatsiooni allüksused peavad omavahel kooskõlastama olulisemad turvapõhimõtted, mida tuleb rakendada kõikides valdkondades (nt paroolide nõuded). Autentimise ja õiguste andmise reeglid peavad olema kõikjal ühesugused (vt M 2.220 Pääsu reguleerimise suunised).

Vastutuspiiride kindlaksmääramine

Kõikide IT-komponentide kasutamisega seotud vastutus peab olema selgelt määratletud. Siia alla kuulub ka administraatorite ja kontaktisikute nimetamine, kelle poole kasutajad võivad pöörduda (vt M 2.79 Vastutuste määramine tüüptarkvara alal).

Uute komponentide integreerimine

Iga uue IT-komponendi soetamise aluseks peaks olema selle kasutuse kontseptsioon. Siinjuures tuleb arvestada ka komponendi integreerimisvõimalusi olemasolevasse IT-kooslusesse ja komponendi mõju olemasolevatele IT turvamehhanismidele, kuna see võib nõuda mehhanismide ümberkohandamist (vt M 2.216 IT-komponentide kinnitamise protseduur).

Uue riist- ja tarkvara testimine

Nii nagu IT-tellimustega seotud protseduurid, peab reguleeritud olema ka kohale toimetatud IT-komponentidega ümberkäimine (vt M 2.90 Kohaletoimetuse kontroll). Enne uute riistvarakomponentide või uue tarkvara kasutuselevõttu tuleb neid testida (vt M 4.65 Uue riist- ja tarkvara testimine).

Reguleeritud installeerimine ja konfigureerimine

Kõikide IT-komponentide installeerimise käigus tuleb järgida ametkonna või ettevõtte IT-turbe põhimõtteid ning installeerimisprotseduur peab olema reguleeritud. Olenevalt konkreetsetest IT-komponentidest ja nende turvanõuetest, tuleb siinkohal määratleda pääsuõigused, kasutajaõigused ja muud turvalisusega seotud konfiguratsioonid. Kõik installeerimistööd tuleb selgelt dokumenteerida (vt M 2.87 Tüüptarkvara installeerimine ja konfigureerimine).

Turvalise IT-kasutuse suunised

Tagamaks kõikide IT-süsteemide turvalist kasutamist, tuleb arvestada paljude erinevate teguritega. Seetõttu tuleb täpselt kirjeldada ja määratleda kõik nõuete-

kohase ja turvalise kasutamise tagamiseks vajalikud ülesanded. Muu hulgas puudutab see järgmisi aspekte:

- Süsteemide ja rakenduste kõikides faasides asetleidvad infotöötluse etapid tuleb pidevalt dokumenteerida (vt M 2.219 Infotöötluse pidev dokumenteerimine).
- Kõikide IT-süsteemide juurdepääs peab olema kaitstud, nt paroolidega.
- IT-komponentide funktsioonid, mille kasutamine pole vajalik või on keelatud, tuleb võimaluse korral sulgeda (vt M 4.95 Minimaalne operatsioonisüsteem).
- Logifaile tuleb regulaarselt kontrollida, et neis ei esineks anomaaliad (nt funktsioone, mida ei ole tegelikult üldse ette nähtud).
- Volitamata muudatuste võimalikult kiireks tuvastamiseks tuleks võimaluse korral kontrollida regulaarselt IT-süsteemide terviklust. Eriti kehtib see konfiguratsioonifailide puhul.
- Kõikides IT-süsteemides tuleks rakendada sobivaid andmevarundusmeetmeid.
- Regulaarselt tuleb kontrollida IT turvameetmete järgimist (vt M 2.182 IT-turvameetmete regulaarne läbivaatus).

Kasutatava riist- või tarkvarakomponentide tüüplahendused

Kasutage võimalikult ühesuguseid komponente

Mida suurem on institutsioon, seda tähtsam on kasutada IT-varustuses ja IT-kasutuses võimalikult ühesuguseid komponente. See puudutab nii riistvarakomponente (nt marsruuterid, printerid ja graafikakaardid) kui ka tarkvaratooteid (nt operatsioonisüsteemid, tekstitöötlusprogrammid ja rakendustööriistad). Vastasel korral võib terviksüsteemi administreerimine muutuda ühilduvusprobleemide ja süsteemi üha kasvava keerukuse tõttu võimatuks.

Majasiseste standardite defineerimine

Riist- ja tarkvarakomponentidele kehtivad majasisesed standardid, millega tuleb uute komponentide soetamisel arvestada, tuleks defineerida ja kirja panna. See võimaldab kasutada juba järeleproovitud lahendusi ja aitab vältida paljusid puudulikust koostalitlusvõimest või ühilduvusest tingitud probleeme. Lisaks vähendab see administratiivset koormust ja vajadust spetsiaalse oskusteabe järele. Paljudel juhtudel on niiviisi võimalik langetada ka kulumaterjalide ladustamisega seotud kulusid. Sidudes majasisesed standardid raamlepingute või hulgihindadega, tekib sageli ka täiendav rahaline kokkuhoid.

Ühilduvuse tagamine

Infotöötlusvallas toimuva kiire tehnilise arengu tõttu tuleb IT-komponentidele kehtestatud majasiseseid standardeid regulaarselt uuendada. Reeglina tekib selle tagajärjel olukord, kus paralleelselt on kasutusel majasiseste standardite erinevad „generatsioonid". Seetõttu tuleks majasiseste standardite uuendamisel pöörata suurt tähelepanu IT-komponentide ühilduvusele, et uusi ja vanu komponente oleks võimalik ka koos kasutada.

Töökohaarvutite majasisesed standardid

Eriti olulise majasiseste standardite kasutusvaldkonna moodustavad töökohaarvutid. Siinkohal tuleb majasisesed standardid kehtestada niihästi arvutite riistvarakomponentidele (nt protsessoritele, töömälule, graafikakaartidele jne) kui ka installeeritud tarkvarale ja tarkvara konfiguratsioonidele. Vastasel korral on arvutite mitmekülgsete konfiguratsioonivõimaluste tõttu oht kaotada ülevaade ja koos sellega ka administreerimise võimalus. Kohustuslike majasiseste standardite puudumisel muutub keskmise suurusega ametiasututes ja ettevõtetes juba ainuüksi operatsioonisüsteemide vajalike riistvaradraiverite hooldamine võimatuks. Töökohaarvutite majasisesed standardid lihtsustavad ka süsteemihaldustoodete kasutamist.

Teadmiseks: riistvara- või tarkvarakomponentide majasiseste standardite defineerimisel ei tohiks mitte mingil juhul keskenduda ainult kõige laiema levikuga tootele. Pigem tuleks kõnealuste toodete valikul lähtuda funktsionaalsuse nõuetest ja (IT-) turvanõuetest. „Monokultuur", st turu domineerimine ühe kindla toote poolt võib teatud asjaoludel kujuneda isegi turvariskiks. Sellistel juhtudel on ka toote tarkvara võimalikud turvaaugud väga laialt levinud, mis võivad, kui keegi neid ära kasutab, põhjustada suuri kahjusid. Arvutiviirused, Trooja hobused ja muud tahtlikud ründed on enamasti suunatud just suure levikuga toodete vastu.

Nime-, aadressi- ja numbriruumide konventsioonid

Ühe institutsiooni piires on tavaliselt kasutuses mitu erinevat nime- ja numbriruumi (namespace). Eriti populaarsed on sellised, mida kasutatakse ka väljaspool ametiasutust või ettevõtet, näiteks meiliaadressid, DNS-nimed, telefoninumbrid ja organisatsiooni allüksuste nimed. Kuid organisatsiooni ja IT-halduse jaoks on sageli olulise tähtsusega ka puhtalt asutusesisese nimeandmise konventsioonid, mis puudutavad nt inventarinumbreid, IP-aadresse ja isikutunnistuste numbreid.

Nime- ja numbriruumide üldkontseptsioon

Infotöötlusprotsessi ja kasutatava IT-administreerimise sujuvuse tagamiseks tuleb kasutatavate nime- ja numbriruumide jaoks luua üldkontseptsioon.

Kontseptsiooni puhul tuleb arvestada järgmiste aspektidega:

- Korraga tuleks kasutada ja töös hoida võimalikult vähe erinevaid nime- ja numbriruume.
- Kontseptsioon peab reguleerima nimede ja numbrite andmist, tühistamist, vajaduse korral sulgemist, samuti üksikute nime- ja numbriruumide omavahelist koostööd.
- Nimed ja numbrid, mida läheb tarvis ainult teatud allüksustes (organisatsiooni allüksustes, alamvõrkudes, kinnistutes, jne), tuleks võimaluse korral tuletada üldistest ametiasutuse või ettevõtte nime- või numbriruumidest.

Ebavajalike erandite vältimine

Kasutatud nime- ja numbriruumide struktuur peaks olema võimalikult lihtne, üldine ja ei tohiks sisaldada ebavajalikke erandeid ka siis, kui see toob kaasa nimetuste pikenemise (nt sisaldab rohkem numbreid). Vastasel korral tekib oht, et nimetusi hakatakse valesti tõlgendama või et levinud tooted ei suuda nendega töötada.

Varude planeerimine

Kontseptsioonis tuleb arvestada prognoositava keskmise lühiajalise kasvuga, millega nime- ja numbriruum peavad suutma kaasas käia. Kõikidel juhtudel tuleb planeerida piisavalt suur varu. Hilisem laiendamine või migratsioon suurematele nime- või numbriruumidele kulutab sageli liiga palju aega ja raha.

Konfliktide lahendamine

Kui süsteemis võib esineda konflikte, st sama nimetuse või numbri korduvat määramist üldise süsteemi poolt, tuleb kontseptsioonis kindlaks määrata ka konfliktide lahendamisviis. Oluline näide on meiliaadresside konventsioon eesnimi.perekonnanimi. Kontseptsioonis tuleb määratleda, milliseid asendusaadresse antakse siis, kui ametiasutuses või ettevõttes on kaks või enam sama ees- ja perekonnanimega töötajat.

Komponentide koostööd tagavate liideste definitsioonid

Infotöötlus toimib tavaliselt paljude väikeste tööetappidena, mida toetavad sobivad riist- või tarkvarakomponendid. Andmevahetus toimub nende komponentide vahel tavaliselt failide, andmebaaside või võrkude kaudu.

Liideste defineerimine ja dokumenteerimine

Sujuva IT-kasutuse tagamiseks on seega vajalik defineerida selgelt liidesed, mis peavad võimaldama üksikute komponentide koostööd. Kõik liidesedefinitsioonid tuleb dokumenteerida juhul, kui need pole kasutuses olevatest komponentidest lähtuvalt iseenesest mõistetavad.

Standardsete formaatide ja protokollide kasutamine

IT-komponentide vaheliste liideste definitsioonide olulised aspektid on näiteks faili- ja andmeformaadid ning võrguprotokollid. Võimalikult palju tuleks kasutada standardseid formaate ja standardseid protokolle, näiteks EDI, XML ja HTTP, mis võimaldavad üksikuid komponente vajaduse korral ilma probleemideta välja vahetada (investeeringukindlus) ja kasutada praktilises kasutuses testitud lahendusi.

IT-turbele avaldatava mõju kontrollimine

Kõik muudatused kasutatavate IT-komponentide liideste definitsioonides tuleb dokumenteerida, lisaks tuleb kontrollida nende mõju IT-koosluse turvalisusele. Vajaduse korral tuleb IT turvakontseptsiooni vastavalt täiendada või kohandada.

Kontrollküsimused:

- Kas IT turvapõhimõtete ja turvalise IT-töö tagamiseks on olemas suunised?
- Kas riist- ja tarkvarakomponentidele on kehtestatud majasisesed standardid?
- Kas nime-, aadressi- ja numbriruumide kasutamiseks on olemas üldine kontseptsioon?

M 2.215 Tõrkekäsitlus

Algatamise eest vastutavad: IT turvaosakond, IT-juht

Rakendamise eest vastutavad: kasutaja, administraator

Kõikide IT-süsteeme või sideühendusi puudutavate vigade kohta peavad ilmuma teated ning need peavad kajastuma logis. Siia alla ei kuulu loomulikult need veateated, mida kuvatakse vastavuskontrollide tagajärjel, nt kasutajate tehtud väärate sisestuste tõttu. Tuleb tagada, et tekkinud vead saaksid võimalikult kiiresti kõrvaldatud.

Kasutajate informeerimine

Vigade uurimise ja kõrvaldamisega peaksid tegelema ainult vastava koolitusega töötajad. Kõik kasutajad peavad teadma, kelle poole tuleb neil IT-süsteemide vigade või probleemide korral pöörduda. Lisaks tuleb kasutajaid informeerida vigadest, mis võivad mõjutada IT-süsteemide tööd, samuti nende kõrvaldamisest.

Logimine

Veateadete logid peavad sisaldama järgmist infot:

- probleemist puudutatud IT-süsteemi ja tarkvara nimetus ja versiooni number,
- veateate tekkimise aeg,
- kirjeldus, kas ja mil määral on vastavate IT-süsteemide edasine kasutamine piiratud,
- vigade kõrvaldamise eest vastutava töötaja nimi ning
- vea kõrvaldamise aeg.

Mõningatel juhtudel võib olla mõistlik või vajalik loobuda esinenud vigade kõrvaldamisest, nt kui puudub usaldusväärne paik (patch) või kui varuosa pole saada. Sel juhul tuleks logisse märkida, kas vastavat IT-komponenti on võimalik piiratud funktsioonidega edasi kasutada. Vastavaid logisid tuleks regulaarselt kontrollida, et veenduda, kas need kajastavad reaalset hetkeolukorda, ning kas kõik veateadetega kajastatud vead on kõrvaldatud.

Vigade hoolikas kõrvaldamine

Vigade korrigeerimine peab jääma selleks määratud vastutava töötaja ülesandeks. Vigade kõrvaldamise protseduur peab vastama institutsiooni IT turvasuunistele. Kui vigade kõrvaldamiseks on vaja paikasid või täiendeid, tuleb need muretseda otse tootja käest või usaldusväärsest kohast (vt ka M 4.107 Tootja ressursside kasutamine). Suuremaid korrektuure tuleb esmalt testida koguvõrgust lahutatud süsteemidel, sest nendega võivad kaasneda soovimatud kõrvalmõjud. Pärast vigade kõrvaldamist tuleb muudetud IT-süsteemid või komponendid võimaluse korral uuesti vastu võtta ja väljastada neile uued kasutusload (vt M 2.62 Tarkvara vastuvõtuprotseduurid).

Kontrollküsimused:

- Kas vigade kõrvaldamise protseduur on kindlaks määratud?
- Kas vigade kõrvaldamisega tegeleb eranditult erialaselt vastutav osakond?

M 2.216 IT-komponentide kinnitamise protseduur

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT-juht, IT turvaosakond

Rakendamise eest vastutavad: IT-juht, IT turvaosakond

Igat liiki IT-komponentide soetamine, installeerimine ja käitamine vajab koordineerimist ja kinnitamist. IT-komponentide vastuvõtmine, kasutusse andmine, installeerimine ja kasutamine peavad olema reguleeritud. See puudutab näiteks ka modemite, disketilugejate, tarkvara ja mobiiltelefonide kasutamist. Tüüptarkvara vastavat protseduuri on kirjeldatud moodulis B 1.10 Tüüptarkvara . Siinkohal tuleb arvestada tüüptarkvara täieliku kasutustsükliga: nõuete kataloogi koostamine, sobiva toote eelvalik, testimine, kasutuse kinnitamine, installeerimine, litsentsihaldus ja desinstalleerimine. Nimetatud moodulist võib lähtuda ka sarnase meetodi väljatöötamisel teistele IT-komponentidele.

Uute IT-komponentide kasutamise kinnituse protseduuri raames tuleb:

- kontrollida üldist funktsionaalsust (vt M 4.65 Uue riist- ja tarkvara testimine),
- hinnata funktsioonide turbeomadusi,
- kontrollida ja hinnata IT-komponentide turvariske ja need riskid võimalikult suures ulatuses kõrvaldada,
- kõik turbega seotud omadused (niihästi positiivsed kui ka negatiivsed) hoolikalt dokumenteerida,
- eelnevast lähtuvalt välja töötada installeerimisjuhendid.

Kõikide turvalisust puudutavate seadistuste dokumenteerimine

Kinnitusprotseduuri käigus tuleb lisaks välja töötada installeerimis- ja konfigureerimisjuhendid, milles peavad olema dokumenteeritud ka kõik turvalisust puudutavad seadistused. Ka pärast IT-komponentide esmakordset installeerimist tuleb nendega pidevalt edasi tegeleda (vt M 4.78 Konfiguratsioonimuudatuste hoolikas teostamine). Enne uute IT-komponentide kasutuselevõttu tuleb administraatoreid ja kasutajaid (vajaduse korral) koolitada komponentide kasutamises. Kasutuskinnituseta IT-komponentide installeerimine ja kasutamine tuleb keelata ja keelust kinnipidamist tuleb regulaarselt kontrollida.

Kontrollküsimused:

- Kas igat liiki IT-komponentide jaoks on olemas kasutusloa saamise ja registreerimise protseduurid?
- Kas IT-komponentide vastuvõtul ja kasutusse lubamisel tehtavad sammud dokumenteeritakse hoolikalt?

M 2.217 Teabe, rakenduste ja süsteemide hoolikas liigitamine ja käitlus

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT-juht, IT turvaosakond

Rakendamise eest vastutavad: IT-juht, IT turvaosakond

Loomulikult peavad kõik töötajad igasuguse infoga alati hoolikalt ümber käima. Lisaks leidub paljudes valdkondades erinevaid andmeid, millele kehtib kas kõrgendatud turbeaste või spetsiaalsed piirangud, nt isikuandmed, finantsandmed, konfidentsiaalsed või autoriõigusega kaitstud andmed. Olenevalt andmete kategooriatest kehtivad nende käitlemisele erinevad piirangud. Seega on oluline, et kõik töötajad tunneksid erinevate andmete kohta kehtivaid piiranguid (vt M 3.2 Uute töötajate kohustamine eeskirju järgima). Andmete turbevajadus mõjutab muidugi vahetult kõiki andmekandjaid, millele neid salvestatakse või millel neid töödeldakse.

Spetsiaalse turbevajadusega andmeid võib esineda erinevates kasutusvaldkondades, nt faksides või e-kirjades. Seega vajavad kõik valdkonnad reegleid, milles on muu hulgas näiteks määratletud, kes tohib vastavaid andmeid lugeda, töödelda või edasi anda (vt M 2.42 Võimalike suhtluspartnerite määramine). Selle alla kuuluvad ka andmete korrektsuse ja tervikluse kontrollimine (vt M 4.64 Ülekantavate andmete kontrollimine enne edastamist/peidetud info kõrvaldamine).

Edasiandmise piiramine

Mitmesugune info, kuid ka IT-rakendused võivad kuuluda kas autorikaitse alla või on neile kehtestatud edasiandmise piirangud („Ainult asutusesiseseks kasutuseks”). Kõiki töötajaid tuleb informeerida, et dokumentide, failide ja ka tarkvara kopeerimisel tuleb ilmtingimata arvestada autoriõiguseid kajastava informatsiooni või litsentsitingimustega.

Strateegilise info kaitse

Erilist tähelepanu tuleb osutada infole, mis on aluseks tööülesannete täitmisel. Siia alla kuuluvad kõik organisatsiooni toimimisega seotud andmed, seega nt andmed, mille kaotamisel muutub institutsioon tegutsemisvõimetuks, mis võivad mõjutada koostööd tegevate ettevõtete majandussuhteid või mille abil võib kolmas osapool (nt konkureeriv ettevõte) saada finantseelise. Igal ametiasutusel ja igal ettevõttel peab olema ülevaade sellest, millised andmed on strateegilise tähtsusega.

Lisaks üldisele kohustusele andmetega hoolikalt ümber käia võib vastavate andmete salvestamise, töötlemise, edasiandmise ja hävitamise suhtes kehtestada veel ka täiendavaid eeskirju ja reegleid. Strateegilise tähtsusega info peab olema kadumise, manipuleerimise ja võltsimise eest kaitstud. Pikemaks ajaks salvestatud või arhiveeritud andmete loetavust tuleb regulaarselt kontrollida. Ebavajalik info tuleb turvaliselt kustutada (vt M 2.167 Andmete kustutamine või hävitamine).

Kontrollküsimused:

- Kas töötajatele tuletatakse regulaarselt meelde, kuidas peab infoga hoolikalt ümber käima?
- Kas kogu info on liigitatud turbevajaduse alusel?

M 2.218 Andmekandjate ja IT-komponentide kaasavõtmise protseduurid

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhatus, IT-juht, infoturbeosakond

Rakendamise eest vastutavad: IT-juht, infoturbeosakond

IT-komponendid, mida kasutatakse oma asutuse kinnistu piires, on üldiselt tänu infrastruktuurilistele turvameetmetele kuritarvitamise ja varguse eest piisavalt kaitstud. Sageli tuleb IT-süsteeme või andmekandjaid aga kasutada väljaspool maja, nt ametireisidel või kaugtöös. Selleks, et ka neid piisavalt hästi kaitsta, peab andmekandjate ja IT-komponentide kaasavõtmine olema selgesti reguleeritud.

Reguleerimine

Reguleerimise all tuleb kindlaks määrata järgmised aspektid:

- Millised komponendid? – Milliseid IT-komponente või andmekandjaid tohib majast välja viia.
- Kes tohib? – Kes tohib IT-komponente või andmekandjaid majast välja viia.
- Mida tuleb silmas pidada? – Milliseid põhilisi IT turvameetmeid peab seejuures järgima (viirusetõrje, konfidentsiaalsete andmete krüpteerimine, säilitamine jne).

Väljaspool maja kasutatavate IT-komponentide puhul rakendatavate IT turvameetmete liik ja maht olenevad ühelt poolt nendele salvestatud IT-alaste rakenduste ja andmete kaitsmise vajadusest ja teiselt poolt nende kasutamis- ja hoidmiskohtade turvalisusest. Põhimõtteliselt tuleks kõikide väljaspool maja kasutatavate IT-komponentide väljaviimiseks hankida vastav luba. Suuremate institutsioonide korral, mille puhul ligipääsu kinnistule kontrollib uksehoidja või valveteenistus, tuleks kaaluda, kas nende ülesannete hulka peaks kuuluma pisteline kontroll, kuidas andmekandjate ja IT-komponentide kaasavõtmise korrast kinni peetakse. Väljaspool oma organisatsiooni kinnistuid vastutavad neile usaldatud IT kaitsmise eest selle kasutajad.

Nende tähelepanu tuleb juhtida sellele ja rakendatavatele ettevaatusabinõudele. Selle kohta kehtivad järgmised reeglid:

- **Hoidmine** – IT-süsteeme tuleb hoida alati turvalises kohas. Töölähetuses olles ei tohi neid jätta järelevalveta. Eelkõige tuleks vältida nende sõidukitesse jätmist (vt M 1.33 Kaasaskantavate IT-süsteemide hoidmine reisil).
- **Juurdepääsukaitse** – selliseid IT-süsteeme nagu sülearvuteid või mobiiltelefone ja nende rakendusi saab üldiselt kaitsta PIN-ide või paroolide abil. Neid tuleks ka kasutada.
- **Krüpteerimine** – IT-süsteemid või andmekandjad, mis sisaldavad konfidentsiaalseid andmeid, tuleks võimalikult komplektselt krüpteerida (vt M 4.29z Kaasaskantavatele IT-süsteemidele mõeldud krüpteerimistoote kasutamine).
- **Haldamine** – väljaspool maja kasutatavate IT-süsteemide haldamist, hooldamist ja edasiandmist tuleks reguleerida. Selleks võib luua näiteks vastavad andmestud (pools) (vt M 1.35z Kaasaskantavate IT-süsteemide ühisladustus ja M 2.190z Mobiilikogu sisseseadmine).

- **Protokollimine** – tuleks protokollida, millal ja kes milliseid IT-komponente väljaspool maja kasutas.

Kontrollküsimused:

- Kas on kehtestatud kindlad reeglid igat liiki IT-komponentide kaasavõtmise kohta?
- Kas väljaspool maja kasutatavate IT-komponentide kasutajatele tutvustatakse reegleid, millest nad peavad kinni pidama?
- Kas väljaspool maja kasutatavate IT-komponentide kasutajate tähelepanu juhitakse sellele, et komponente tuleb hoida nii, nagu on ette nähtud?
- Kas IT-komponentide kasutamisel väljaspool asutuse ruume rakendatakse neisse sisse ehitatud autentimismehhanisme?

M 2.219 Infotöötluse pidev dokumenteerimine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT-juht, IT turvaosakond
Rakendamise eest vastutavad: IT-juht, IT turvaosakond

Nõuetekohase IT-kasutuse tagamiseks tuleb infotöötlus kõikides etappides, rakendustes ja süsteemides pidevalt dokumenteerida.

Siia alla kuuluvad:

- **konfiguratsioon** – kõikide olemasolevate IT-süsteemide ja nende konfiguratsioonide pidev dokumenteerimine (vt M 2.25 Süsteemi konfiguratsiooni dokumenteerimine),
- **õiguseprofiilid** – IT-süsteemides loodud kasutajate ja nende õiguseprofiilide dokumenteerimine (vt M 2.31 Volitatud kasutajate ja õiguste profiilide dokumenteerimine), mis hõlmab ka IT-süsteemide kasutamispiirangute kirjeldusi ja põhjendusi (õigused ja ressursid),
- **muudatused** – süsteemi dokumentatsiooni tuleb kaasata ka sinna lisandunud riist- ja tarkvarakomponendid (vt M M 2.34 IT-süsteemi muutuste dokumenteerimine),
- **turvalisust puudutavad protseduurid** – kõikide turvalisust puudutavate protseduuride dokumenteerimine, nt andmevarundus (vt M 6.37 Andmevarunduse dokumenteerimine) või andmekandjate hävitamine,
- **hooldus** – hooldusmeetmete dokumenteerimine (vt M 2.4 Hooldus- ja remonditööde reeglid),
- **tõrkekäsitlus** – kõikide leitud ja kõrvaldatud vigade kirjeldamine (vt M 2.215 Tõrkekäsitlus),
- **kontaktisikud** – probleemide puhuks peab olema dokumenteeritud, kelle poole tuleb pöörduda ja kust saab asjakohast informatsiooni (vt M 6.59 Turvaintsidentide käsitlemise eest vastutavate isikute määramine). Kirjalikult peab toimuma ka süsteemi eest vastutavate töötajate ametisse nimetamine (vt M 2.26z Süsteemiülema ja ta asetäitja määramine), millest tuleb teavitada ka kasutajaid.

Kontrollküsimused:

- Kas infotöötluse kõik etapid, rakendused ja süsteemid on dokumenteeritud?
- Kas infotöötluse dokumenteerimise kohta on kehtestud reegleid?

M 2.220 Pääsu reguleerimise suunised

Algatamise eest vastutavad: IT-juht, IT turvaosakond
Rakendamise eest vastutavad: administraator, vastutav spetsialist

IT-süsteemide või süsteemikomponentide ja võrkude kasutamiseks, st nende abil info kättesaamiseks peab olema kehtestud pääsukontroll. Lisaks üksikute IT-komponentide pääsukontrollidele läheb tarvis ka kõikehõlmavat asjakohast suunist, millega lahendatakse lähteprobleemid. Pääsukontrollide reeglid peavad kajastama ametiasutuse või ettevõtte turbevajadusi. Eriti tuleb siinkohal viidata kehtivatele seadustele, eeskirjadele ja regulatsioonidele, seega nt andmekaitseseadusele, autoriõiguseseadusele ja litsentsitingimustele.

Standardne õiguseprofiil
Kasutusõigustega isikutele tuleks määrata standardsed õiguseprofiilid lähtudes nende töö funktsioonidest ja ülesannetest (vt M 2.8 IT-rakendustele ja andmetele pääsuõiguste andmine). Failide ja programmide juurdepääsude kasutajaõigused peavad olema defineeritud olenevalt vastavast töörollist, teadmistarbe printsiibist ja andmete tundlikkusest. Juhul kui pääsuõiguste jagamisel ületatakse standardit, tuleb täiendavate õiguste andmist ka põhjendada. Pääsukontrolli reguleerimise suunised peavad olema teada kõikidele IT-rakenduste eest vastutavatele isikutele. Sellele toetudes saab sisse seada üksikute IT-süsteemide juurdepääsuõigused.

Regulatsioonide kohandamine IT-süsteemidele
Iga üksiku IT-süsteemi ja iga IT-rakenduse jaoks tuleb luua dokumentatsioon, kus kajastuvad pääsuõigused ning kasutajate loomine ja pääsuõiguste sisseseadmine (vt M 2.30 Kasutajate ja kasutajarühmade määramise protseduurid). Siinkohal tuleb arvestada süsteemi ja rakendusvaldkonna spetsiifikast tulenevate eripärade ja turvanõuetega. Süsteemi ja rakendusvaldkonna spetsiifiliste nõuete koostamise ja uuendamise eest vastutavad IT eest vastutavad töötajad.

Piiratud õiguste andmine
Kui töötajatele on tarvis anda eriti laialdasi õigusi (nt administraatoritele), tuleks seda siiski piirata nii palju kui vähegi võimalik. Privilegeeritud kasutajate ring tuleb muuta võimalikult kitsaks ning töötajatele tuleb anda vaid need õigused, mis on vajalikud nende tööülesannete täitmiseks (vt M 2.38 Administraatorirollide jagamine). Nende ülesannete puhul, mida saab täita ilma laiendatud õigusteta, peaksid ka privilegeeritud õigustega kasutajad töötama standardsete õigustega kasutajakontode alt.

Autentimisega juurdepääs
Juurdepääs kõikidele IT-süsteemidele või teenustele peab olema kaitstud kasutaja või IT-süsteemi identifitseerimise ja autentimisega. Välisvõrkudest loodav juurdepääs peab alluma tugevatele autentimisprotseduuridele, ehk siis sellistele, mis põhinevad nt ühekordsete paroolide või kiipkaartide kasutamisel. Sisselogimisel ei tohi näidata infot IT-süsteemi või sisselogimise etappide kohta enne, kui sisselogimine on edukalt lõpuni viidud. Siinkohal tuleb viidata infole, et juurdepääs on lubatud ainult volitatud kasutajatele. Autentimisandmeid tohib kontrollida alles siis, kui need on täielikult sisestatud (vt M 4.133z Sobivate autentimismehhanismide valimine).

Kontrollküsimused:

- Kas pääsukontrolli jaoks on kehtestatud suunised?
- Kas erinevate funktsioonide või ülesannete jaoks on loodud standardsed õiguseprofiilid?

M 2.221 Muudatuste haldus

Algatamise eest vastutavad: IT-juht, IT turvaosakond
Rakendamise eest vastutavad: administraator, vastutav spetsialist

Töötavates süsteemides tehtavate väikestegi muudatustega võivad tänapäevaste IT-süsteemide keerukust arvestades kaasneda turvariskid, nt süsteemi ootamatu käitumine või tõrge. IT-turvalisusest lähtudes on muudatuste halduse ülesanne tuvastada uued turvanõuded, mis on tingitud IT-süsteemides asetleidnud muudatusest. Kui IT-süsteemis planeeritakse riistvara või tarkvara ulatuslikke muudatusi, tuleb uurida muudatuste mõju terviksüsteemi turvalisusele. IT-süsteemi muudatused ei tohi vähendada üksikute turvameetmete tõhusust ega ohustada ka üldist turvalisust.

Muudatuste sisseviimise suunised

IT-komponentide, tarkvara või konfiguratsiooniandmete muudatuste tegemiseks on vaja kindlaid suuniseid (vt M 4.78 Konfiguratsioonimuudatuste hoolikas teostamine). Kõik IT-komponentide, tarkvara või konfiguratsiooniandmete muudatused vajavad planeerimist, testimist, kinnitamist ja dokumenteerimist. Seega tuleb hoolt kanda, et kõikidele turvalisust puudutavatele muudatustele reageeritaks adekvaatselt.

Siia alla kuuluvad näiteks:

- IT-süsteemide muudatused (uued rakendused, uus riistvara, uued võrguühendused, kasutatava tarkvara modifikatsioonid, turvapaikade paigaldamine, riistvara täiendamine),
- muudatused püstitatud ülesandes või ülesande tähtsuses institutsiooni jaoks,
- kasutajate struktuuri muudatused (uued, näiteks välised või anonüümsed kasutajarühmad),
- tööruumi muudatused, nt pärast ümberkolimist.

Varulahendus

Enne muudatuste kinnitamist ja sisseviimist tuleb planeeritud tegevuste kontrollimise ja testimisega tagada, et soovitud turvalisuse tase säiliks nii muudatuste sisseviimise ajal kui ka pärast muudatusi. Kui riske ei õnnestu välistada, eriti kättesaadavuse puhul, tuleb planeerida varulahenduse kasutamine ja määrata kriteeriumid, mille alusel see lahendus kehtima hakkab.

Muudatuste dokumenteerimine

Kõik muudatused ja sinna juurde kuuluvad valikukriteeriumid tuleb dokumenteerida. See kehtib nii kasutuskeskkonna kui ka testimiskeskkonna kohta. Muudatuste halduse puhul on muudatuste teostamise oluline punkt õiguste kontseptsioon:

- Vastavate süsteemiosade pääsuõigused peaksid olema vaid neil töötajatel, kes on volitatud muudatusi süsteemi sisse viima.

- Vaja läheb mehhanisme, mis suudaksid tagada, et kõik olulised muudatused läbivad enne sisseviimist asjakohase kooskõlastusringi.

Teadmiseks: muudatuste tegemisel tuleks alati arvestada, et IT-süsteemi või selle kasutustingimuste muudatustega võib kaasneda

- IT turvaplaani rakendamise muutmine,
- IT uue turbekontseptsiooni koostamine või isegi
- vajadus kogu organisatsiooni IT turvapoliitika ümbertöötamiseks.

Suuremate muudatuste puhul tuleks seega protsessi kaasata ka IT turvaosakond.

Kontrollküsimused:

- Kas IT-komponentide, tarkvara või konfiguratsioonifailide muudatuste tegemiseks on olemas suunised?
- Kas kõik muudatused läbivad testimise ja kas need dokumenteeritakse?
- Kas suuremate muudatuste puhul on protsessi kaasatud ka IT turvaosakond?

M 2.223 Tüüptarkvara kasutamise turvaeesmärgid

Algatamise eest vastutavad: IT-juht, IT turvaosakond
Rakendamise eest vastutavad: administraator, kasutaja

Enamikes bürookeskkondades kasutatakse tüüpiliste bürooülesannete täitmiseks tüüptarkvara. Selle alla kuuluvad nt tekstitöötlusprogrammid (Word, WordPerfect, StarOffice), tabelarvutus, büroo sidesüsteemid, meiliprogrammid ja andmebaasid. Kuna need ostetakse sageli tervikuna ühe pakkuja käest, räägitakse siinkohal ka kontoripakettidest. Samalaadse tarkvara laia leviku tõttu võivad nende programmide turvaaugud olla üsnagi ulatuslike tagajärgedega, kuna neid saab erinevates IT-süsteemides ära kasutada ja kahjulikud programmid levivad väga kiirelt. Tüüpiline näide on siinkohal makroviirused (vt G 5.43 Makroviirused). Probleemide vältimiseks või vähendamiseks tuleks tüüptarkvara kasutamisele määrata seega turvasuunised.

Kasutaja informeerimine sobivusest ja turvafunktsioonidest

Üldjuhul ei ole tüüptarkvara väljatöötamisel lähtutud IT kõrgest turbetasemest. Seetõttu tuleb kõikide töötajate tähelepanu juhtida sellele, et standardsel töökohal ei tohiks eriti konfidentsiaalset infot töödelda ilma täiendavate infoturbemeetmeteta.

Paljud tüüptooted võimaldavad küll kasutada ka erinevaid infoturbefunktsioone, kuid need pakuvad sageli vähem kaitset kui eriotstarbelised turvatooted. Kasutajaid tuleb informeerida turvafunktsioonidest ja nende tõhususest (vt M 4.30 Rakendusprogrammide turvavahendite kasutamine). Siinjuures tuleb esmajoones veenduda, et kasutajad ei lähtuks petlikust kõrgest turvatundest ja et nende turvafunktsioonide kasutamine ei tekitaks juurde uusi turvaauke. Kasutajaid tuleb informeerida, et kontoritarkvaratooted ei sobi kõikideks otstarveteks. Lisaks pakuvad kontoripaketid sageli infovahetust kergendavaid funktsioone, mis tekitavad kahjuks juba oma olemuselt tõsiseid turvaprobleeme.

Näited:

- **Töökohtumiste ühiste kalendermärkmike kasutamine** - Töörühmade sisekoostöö koordineerimiseks saab enamikke elektroonilisi töökohtumisi kajastavaid kalendermärkmikke omavahel ühendada. Lisaks paljudele eelistele toob see endaga kaasa ka probleeme. Näiteks ei taha iga töötaja teha kõiki oma sissekandeid kolleegidele nähtavaks. Tootjad on sellele reageerinud ja pakuvad võimalust näidata teistele ainult sissekandeid kokkulepitud kohtumiste kohta või siis või vabu aegu. Kuid paljud töötajad arvavad esiteks, et neist jääb halb mulje, kui töökohtumisi kajastavas märkmikus on näha, et neil on palju vaba tööaega ja teiseks kardavad nad, et kolleegid hõivavad nende iga vaba minuti, täites kõik saadaolevad ajad töökohtumistega. Selle tulemusel blokeeritakse suured ajavahemikud juba igaks juhuks ette. Lisaks võib probleeme esineda näiteks liiga kergekäelise pääsuõiguste andmisega. Seega läheb tarvis suuniseid ühendatud töökohtumiste kalendermärkmike ja nendega seotud pääsuõiguste jaoks. Need tuleks juba varakult töötajate esindusega kooskõlastada. Töökohtumiste ühendatud kalendermärkmike kasutuselevõtu korral tuleb töötajatele õpetada nende õiget kasutamist.

- **CD-ROM-ide automaatne käivitamine** - Kõikides uuemates Windowsi operatsioonisüsteemides saab CD-ROM-e automaatselt tuvastada ja käivitada. Seeläbi võivad arvutisse pääseda kahjulikud programmid, nagu viirused või Trooja hobused. Seetõttu tuleks CD-ROM-i automaatne tuvastus välja lülitada.
- **OLE (object linking and embedding, teenus objektide ühendamiseks ja integreerimiseks)** - OLE-funktsioonide kaudu saab failidesse integreerida erinevaid objekte. Seda võimalust kasutavad mitmed kontoritarkvaratooted, et võimaldada ligipääsu teiste programmide infole. Näiteks saab Excelis koostatud tabeli integreerida Wordi dokumenti. Seeläbi ei kanta Wordi faili üle mitte ainult tabelilõigus leiduvat infot, vaid võidakse edastada ka kogu ülejäänud Exceli failis leiduvat infot. Kui vastav Wordi fail antakse edasi, saab vastuvõtja näha ja isegi muuta ka Exceli faili ning seda isegi siis, kui fail on lugemise või kirjutamise eest parooliga kaitstud. Selle vältimiseks tuleks Exceli tabel Wordi faili ümber kopeerida teksti kujul. Exceli algfaili võib integreerida mõnda teise faili ainult siis, kui see sisaldab vaid sellist informatsiooni, mida võib probleemideta edasi anda. Seda võib saavutada näiteks uue Exceli faili loomisega (vt M 4.64 Ülekantavate andmete kontrollimine enne edastamist/peidetud info kõrvaldamine).
- **PostScript** / **ghostscript** - PostScript-failides võib esineda sarnaseid probleeme nagu makroviiruste puhul. PostScripti vaatamisprogrammide puhul on tegu tõlgendajatega, mis töötlevad PostScript-keelt. Alates PostScript-spetsifikatsiooni tasemest 2.0 on olemas ka PostScript-käsud failide kirjutamiseks. See võimaldab luua PostScript-faile, mis suudavad tõlgendajapoolse töötlemise või ka juba ekraanile kuvamise ajal teisi faile muuta, kustutada ja ümber nimetada. Konkreetsed probleemid esinevad programmis ghostscript (gs). Unixi versioonides saab failide kirjutamisvõimalused välja lülitada funktsiooniga -dSAFER. Kuid see ei ole algseadistus. Teiste operatsioonisüsteemide versioonides on kõnealusel funktsioonil samuti sarnane nimi. Funktsiooni -dSAFER rakendamine on jäetud kasutaja valikuks. Selle tagajärjel rakendavad ka mitmed muud programmid, mis kasutavad programmisiseselt ghostscripti (gs), (nt Netscape, xdvi, xfig, xv jne) seda erinevalt. Funktsioon tuleks seega määrata vaikeseadeks. (vt M 2.35 Teabe hankimine turvaaukude kohta). Vanemate ghostscripti versioonide puhul võib esinda veel ka teisi PostScripti käske, mis võimaldavad faile modifitseerida. Kasutada tuleks ainult selliseid ghostscripti versioone, milles on vastavad probleemid lahendatud. Programm ghostview, millega saab vaadata PostScript-faile, pakub alates versioonist 1.5 funktsiooni -safer, mis aktiveerib ghostscripti turvafunktsioonid. Versioonile 1.5 eelnenud versioonid sellist kaitset ei paku ja need tuleks seetõttu asendada uuema versiooniga. Sarnane PostScript-failide vaatamise programm on gv. Selle programmi puhul tuleks dialoogväljal „Ghostscript Options” aktiveeida valik „Safer”. PostScripti vaatamisprogrammis GSview, mis on saadaval Windowsi ja OS/2 jaoks, peab olema sisse lülitatud failide kirjutamiskaitse funktsioon.
- **PDF (Portable Document Format)** - Ka PDF-failide puhul võib esineda sarnaseid probleeme juhul, kui failide vaatamiseks kasutatakse Acrobat Readeri vanemaid versioone. PDF-failidesse saab integreerida funktsioone, nagu nt programmi avamine, mis kujutab endast turvariski kohaliku IT-süsteemi failidele. Seega tuleks PDF-failide vaatamiseks kasutada vaatamisprogrammi, mis seda funktsiooni ei toeta või on varustatud sobivate turvamehha-

nismidega makrode käivitamisel (nt Acrobat Readeri uuemad versioonid). Vastasel korral esineb oht, et integreeritud funktsioonid käivitatakse juba dokumendi avamisel või dokumendis ringiliikumisel nn action trigger'i abil, ilma et lugeja sellest üldse teadlik oleks.

- **Kiirsalvestamine Wordis** - Wordis on olemas koostatud tekstide kiirsalvestamise funktsioon. Selle tulemusel salvestatakse ainult dokumendis tehtud uuemad muudatused. Kiirsalvestuse protseduur ei kuluta nii palju aega nagu täielik salvestamine, mille käigus salvestab Word ületöötatud dokumendi selle kogumahus. Täielik salvestamine nõuab siiski vähem kõvaketta ruumi kui kiirsalvestamine. Kiirsalvestamise otsustavaks puuduseks on asjaolu, et fail võib sisaldada tekstifragmente, mida dokumendi koostaja ei soovi teistele edastada. Seega tuleks kiirsalvestuse lubamise funktsioon välja lülitada. Lisaks tuleks aktiveerida varukoopia salvestamise funktsioon. Süsteemi tuleb ebavajalike varukoopiate kustutamisega regulaarselt puhastada.

Kui kasutaja otsustab siiski kiirsalvestuse kasuks, peab ta alati kasutama täieliku salvestamise funktsiooni järgmistes olukordades:

- Niipea kui dokumendi töötlemine on lõpetatud.
- Enne suurt mälumahtu nõudva ülesande teostamist, nt enne teksti otsimist või aineregistri koostamist.
- Enne dokumendi tekstiosa ülekandmist teise rakendusse.
- Enne dokumendi konverteerimist teise failiformaati.

Turvaauke puudutava info kogumine

Kontseptsiooni võimalikele nõrkadele külgedele ja ilmsiks tulnud turvaaukudele kiireks reageerimiseks peaks administraator või IT turvaosakond end vastavate probleemidega kursis hoidma (vt M 2.35 Teabe hankimine turvaaukude kohta).

Kontrollküsimused:

- Kas kasutajaid on rakendusprogrammide turvafunktsioonidest ja nende tõhususest informeeritud?
- Kas -dSAFER-funktsioon on kasutatavate PostScript-tõlgendajate puhul aktiveeritud?

M 2.224 Trooja hobuste tõrje

Algatamise eest vastutavad: IT-juht, IT turvaosakond
Rakendamise eest vastutavad: administraator, kasutaja

Trooja hobune on kahjutekitava funktsiooniga programm, mis on integreeritud mõnda teise programmi peidetud kujul. Trooja hobuste levitamiseks integreeritakse neid võimalikult „atraktiivsetesse" peremeesprogrammidesse, mida pakutakse näiteks allalaadimiseks või saadetakse e-kirja manustena. Lisaks otsese kahju tekitamisele võimaldavad Trooja hobused spioneerida niihästi üksikarvutite kui ka terve kohtvõrgu infot.

Kasutajaid tuleb korduvalt informeerida!

Trooja hobuste vastu on kaitset raske leida, kuna need võivad olla peidetud erinevatesse failidesse. Seetõttu on oluline teavitada kõiki kasutajaid ikka ja jälle Trooja hobustega seotud probleemidest.

Oluline on kinni pidada järgmistest käitumisreeglitest:

- Arvutiviiruste ja Trooja hobuste peamine levimisviis on internetist alla laaditud andmed ja programmid, mis võivad spioneerida, edasi suunata, muuta või kustutada kasutajaandmeid. Viiruseid ja Trooja hobuseid võivad sisaldada mitte ainult programmid selle otseses mõttes, vaid ka Office'i dokumendid (teksti-, tabeli- ja esitlusfailid) makrode näol.
- Tarkvara tuleb muretseda usaldusväärsest allikast. Tundmatust allikast pärit programmide installeerimine peab olema keelatud (vt M 2.9 Aktsepteerimata riist- ja tarkvara kasutuse keeld). Paljusid andmeid ja programme on võimalik saada erinevatest allikatest, nt interneti peegelserveritest või ajakirjade CD-ROMidelt. Andmeid ja programme tuleb laadida ainult usaldusväärsetelt lehekülgedelt, seega tuleks eelistada eriti just tootjate originaallehekülgi. Vajaduse korral tuleb saatja käest üle küsida.
- E-kirjade manuseid või muid sidepartnerite saadetud faile ei tohi avada, kui adressaat pole osanud neid oodata või kui need on imelike nimedega. Kahtluse korral tuleb sidepartnerilt küsida, kas vastavad saadetised on nende tõesti teele pandud või mitte. Teadmiseks: saabuvad e-kirjad on arvutiviiruste ja Trooja hobuste peamine sissepääsuvõimalus arvutitesse. Ka tuntud ja usaldusväärsest allikast saabunud e-kirjade puhul tuleb kontrollida, kas sõnumi tekst sobib saatjaga kokku ning kas manus oli ka oodatud. Võimaluse korral tuleb kontrollida suurust ja kontrollsummat.
- Pärast faili allalaadimist tuleb alati kontrollida infot faili suuruse kohta, samuti kontrollsumma andmeid, juhul kui need on kaasa pandud. Kui failide suuruses või kontrollsummas esineb kõrvalekaldeid seoses etteantud andmetega, on põhjust kahtlustada volitusteta muudatusi. Seetõttu tuleks niisugused failid kohe kustutada.
- Meilivahetuses tuleks sisu ehtsuse ja õiguse kontrollimiseks kasutada võimaluse korral digitaalallkirju (M 4.34z Krüpteerimise, kontrollsummade ja

digitaalallkirjade rakendamine).

- Kasutage värskendatud viiruseskannerit – kõik kolmandatelt osapooltelt saadud failid ja programmid tuleb enne aktiveerimist viiruseskanneriga üle kontrollida. Need kontrollivad ka seda, kas esineb (teadaolevaid) Trooja hobuseid (vt B 1.6 Viirusetõrje kontseptsioon).
- Kõik programmid tuleb enne paigaldamist ja kasutusse lubamist testsüsteemidel läbi kontrollida (M 4.65 Uue riist- ja tarkvara testimine).
- CERTide või muude turvalisust puudutavate infoteenuste puhul tuleb regulaarselt uurida, kas kasutatavad programmid on silma jäänud sellega, et edastavad kasutaja IT-süsteemist kasutaja teadmata andmeid (vt M 2.35 Teabe hankimine turvaaukude kohta). Lisaks mõnele Office'i programmile ja vabale lisatarkvarale on selles kontekstis silma jäänud ka programmiteegid (library), mis edastavad infot kolmandatele isikutele, ilma et see oleks neid kasutanud programmeerijatele teada.
- Programmide installeerimisel tuleb programmi juhised ja kasutajatingimused hoolikalt läbi lugeda. Sageli leidub juhendites (rohkemal või vähemal määral selgelt sõnastatud) viiteid sellele, et programmide kasutamisel kogutakse ja edastatakse andmeid kasutaja või süsteemi kohta.
- Ettevaatust aktiivsisudega – Trooja hobused võivad peituda ka veebilehtede aktiivsisus (Java, JavaScript ja eriti ActiveX) ning kuna need laetakse koos internetilehekülgega, jäävad need kasutajale sageli märkamata. Teatud kaitset saab saavutada ka sellega, kui jätta töösse ainult tõesti hädavajalikud protsessid ja programmid, (eriti oluline just võrgustatud töö puhul), kuna seeläbi saab arvuti või kõvaketta lubamatut tegevust kergemini märgata. Lisaks saab veebilehitseja seadistusvõimalusi põhjalikumalt tööle rakendada, näiteks selliselt, et aktiivsisu arvutisse laadimine oleks täielikult välistatud.
- Paroole ei tohi salvestada – sageli on Trooja hobuste eesmärk paroolide või muude pääsuandmete kogumine. Seetõttu ei tohi paroole mitte kunagi salvestada IT-süsteemidesse. Lisaks tasub kasutatud andmekandjaid regulaarselt kontrollida, kas seal esineb ootamatuid muudatusi (uusi või muudetud faile, ebatavalist käitumist).

M 2.225 Teabe, rakenduste ja IT-komponentide alaste vastutuste kinnistamine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT-juht, IT turvaosakond
Rakendamise eest vastutavad: vastutav spetsialist, administraator, töötaja

Kõikehõlmava turvalisuse saavutamiseks tuleb vajalike IT turbemeetmete võtmise kaasata organisatsiooni kõik töötajad. Info, rakenduste ja IT komponentide puhul tuleb kindlaks määrata, kes on nende eest vastutav ning kes peab vastutama nende turvalisuse eest. Vastutus peab olema selge, mistõttu tuleb vastutuse kandjaks nimetada alati keegi konkreetne isik (koos asendajatega), aga mitte abstraktne grupp. Keerukama info, rakenduste ja IT komponentide puhul peavad kõik vastutavad töötajad ja nende asendajad olema nimeliselt teada. Samuti peavad kõik töötajad loomulikult teadma, millise info, rakenduste ja IT komponentide eest nad millisel viisil vastutavad. Iga töötaja vastutab seejuures kõige selle eest, mis jääb tema mõjuvaldkonda, välja arvatud juhul, kui see on reguleeritud selgelt teisiti. Näiteks vastutab organisatsiooni juhtkond kõikide põhimõtteliste otsuste eest uue rakenduse kasutuselevõtmisel, IT-juht koos IT turvaosakonnaga turvapoliitika väljatöötamise eest, administraatorid selle korrektse rakendamise eest ja kasutajad kogu IT juurde kuuluva info, rakenduste ja süsteemide hoolika kasutamise eest.

Vastutavad spetsialistid peavad info ja rakenduste „omanikena" tagama, et:

- info, rakenduste ja IT komponentide turbevajadused oleksid õigesti määratud,
- vajalikud turvameetmed saaksid ellu rakendatud,
- infot ja rakendusi kontrollitaks regulaarselt (nt iga päev, nädal, kuu),
- turvameetmete rakendamise ülesanded oleksid selgelt defineeritud ja töötajate vahel ära jagatud,
- juurdepääs infole, rakendustele ja IT komponentidele oleks reguleeritud,
- turvalisust ohustavad kõrvalekalded saaksid kirjalikult fikseeritud.

Vastutavad spetsialistid peavad koos IT turvaosakonnaga otsustama, mida teha võimalike jääkriskidega.

M 2.226 Asutusevälise personali kasutamise protseduurid

Algatamise eest vastutavad: ametiasutuse või ettevõtte juhtkond
Rakendamise eest vastutavad: IT-juht, personalijuht

Vastava personaliressursi puudumisel kasutatakse ametiasutustes või ettevõtetes sageli ka väljastpoolt tulevaid abijõudusid. Ekstreemsetel juhtudel võib selle tagajärjel tekkida olukord, kus asutusevälist personali on palgatud asutuses nii kaua, et paljud oma töötajad ei tea enam täpselt, kelle puhul on tegu asutusesisese või -välise personaliga.

Seaduste ja eeskirjade järgimine
Asutuseväliselt personalilt, kes tegutseb pikema aja vältel organisatsioonis või organisatsiooni heaks ning võib ligi pääseda konfidentsiaalsetele dokumentidele ja andmetele, tuleb võtta kirjalik kinnitus, et nad kohustuvad järgima kehtivaid seadusi, eeskirju ja asutusesiseseid reegleid (vt M 3.2 Uute töötajate kohustamine eeskirju järgima).

Töö tutvustamine ja juhendamine
Asutusevälise personali kasutamisel tuleb lisaks muule alati tagada, et neid viidaks – sarnaselt oma töötajatele – tööülesannetega ka piisavalt kurssi (vt M 3.1 Uute töötajate esmane juhendamine ja väljaõpe). Asutuseväliseid töötajaid tuleb teavitada – nii palju, kui see on nende ülesannete ja kohustuste täitmiseks vajalik – IT turvalisust puudutavatest majasisestest reeglitest ja eeskirjadest ning üleorganisatsioonilisest turvapoliitikast. See kehtib eriti siis, kui nad tööülesannete täitmisel tööandja hoonetest ei lahku.

Asendamise korraldamine
Lisaks tuleb tagada, et töötajate asendamine oleks reguleeritud ka asutusevälise personali puhul (vt M 3.3 Asendamise korraldamine). Samuti peab olema tagatud, et asendustöötajad tunneksid oma tööks vajalikke IT-rakendusi ja suudaksid ümber käia ka vajalike turvameetmetega.

Töösuhte reguleeritud lõpetamine
Kui tellimus on täidetud peab töösuhte lõppemisele järgnema töötulemuste üleandmine ning töötajatele antud toimikute ja töövahendite reguleeritud tagastamine. Lisaks tuleb ära võtta või kustutada kõik välise personali jaoks sisse seatud pääsuõigused. Lisaks muule tuleb lahkuva töötaja tähelepanu juhtida sõnaselgelt sellele, et vaikimiskohustus jääb kehtima ka pärast töösuhete lõppu (vt M 3.6 Reguleeritud protseduur töösuhete lõpetamiseks). Lühiajaliselt või ajutiselt kasutatavat asutusevälist personali tuleb kohelda nagu külalist, mis tähendab näiteks ka seda, et tema viibimine turvalisust puudutavates tsoonides peaks olema lubatud ainult ametiasutuse või ettevõtte oma töötaja juuresolekul (vt M 2.16 Välispersonali ja külastajate valve ja saatmine).

Kontrollküsimused:

- Kas pikemaajaliste ülesannetega seotud asutusevälist personali kohustatakse kinni pidama kehtivatest seadustest ja eeskirjadest?
- Kas asutusevälise personali sissetöötamine on reguleeritud ja kas neid informeeritakse kehtivatest IT-turbereeglitest?
- Kas asutusevälistele töötajatele sisseseatud pääsuõigused võetakse ära või kustutatakse pärast töösuhte lõppemist?

M 2.229 Active Directory planeerimine

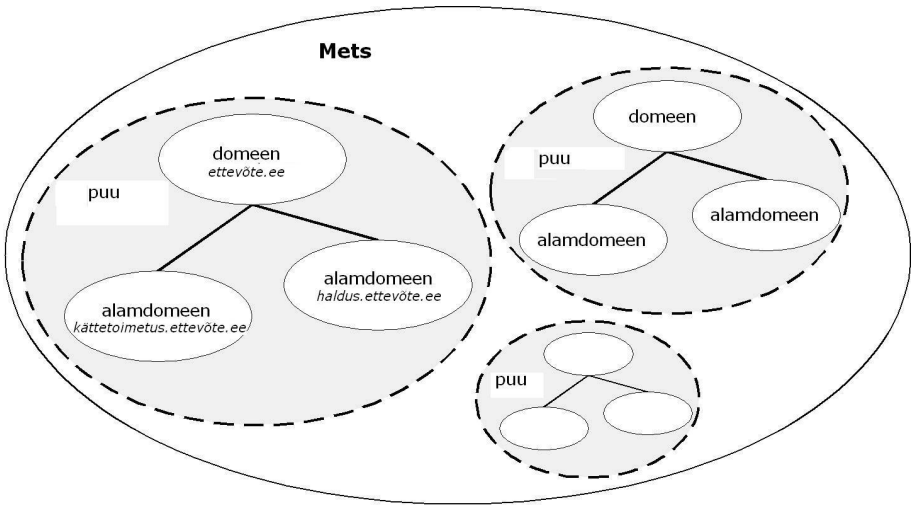
Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: administraator, IT-juht

Active Directory (AD) on kõikide haldusandmete keskne andmebaas Microsofti serverites. Abstraktselt vaadatuna moodustab AD hierarhiliselt ja puukujuliselt organiseeritud objektpõhise andmebaasi. See tugineb kataloogiteenuse standardile X.500, millelt pärineb sisemine struktuur ja ülesehitus. Sellele vaatamata ei ühildu see kataloogiteenusega X.500.

Domeenid
Domeenikontseptsioon: arvuti ja kasutajad koondatakse domeeni alla ja domeeni administraator saab neid hallata. Domeeni piir moodustab üldjuhul ka administratiivse piiri ning piirab ka volituste mõjuala. Lisaks nimetatud kontseptsioonile pakutakse võimalust domeene üksteisega siduda puustruktuuri alusel, et luua domeenide vahel „vanem-laps“ tüüpi seoseid. Lapsdomeeni nimetatakse ka alamdomeeniks, kuna laps-domeeni nimi tuleneb kõrgemalseisva domeeni nimest – sellele nimele lisatakse punktiga eraldatud domeeni nimi.

Näide:
vanem-domeeni nimi: ametiasutus.ee
Alamdomeeni nimi: haldus.ametiasutus.ee

Puustruktuur
Selliselt koostatud nimeruum on identne vastava DNS-i nimeruumiga ning teisiti ei ole seda võimalik koostada. Ühise nimetüvega domeenid moodustavad puu (ingl. Tree).



Joonis: metsaks (Forest) koondatud domeenipuud

Forest – metsastruktuur; Tree – puustruktuur; Domäne – domeenis; Sub-Domäne

– alamdomeenid; Domäne Unternehmen.de – domeenid ettevõte.de; Sub-Domäne expedition.unternehmen.de – alamdomeenid kättetoimetusosakond. ettevõte.de; Sub Domäne verwaltung.unternehmen.de – alamdomeenid haldus. ettevõte.de

Forest

Erinevatesse puudesse kuuluvaid domeene – seega erinevatesse nimeruumidesse kuuluvad domeene – saab siiski ühiselt hallata. Selliselt kokku koondatud domeenipuud moodustavad metsa (ingl. Forest). Üksik domeen moodustab samuti puu ja samal ajal ka metsa.

Forest-Root domeen

Metsas on alati üks eriline domeen, millel on teatud eristaatus. Tegu on esimesena loodud domeeniga, mida nimetatakse ka Forest-Root domeeniks (FRD, metsa juurdomeen). Eristaatus seisneb selles, et FRD administraatoritel on kogu metsas kehtivad volitused. Organisatsiooni administraatorirühma liikmete jaoks ei ole domeeni piirid administratiivseteks piirideks, sest neil on pääsuõigused kõikide domeenide jaoks. Windowsi domeenikogumi ülesehitamisel tuleb arvestada, et esimesena loodud domeen on alati FRD. Oluline on teada, et FRD rolli ei saa hiljem mõnele teisele domeenile üle kanda, seega tuleb vajadusel kogu domeenistruktuur soovitud kujul uuesti luua.

Active Directory objektid

AD koosneb erinevatest objektidest, Active Directory objektidest (ADO). Igal objektile on määratud tüüp, nt kasutaja objekt või arvuti objekt, mis koosneb selle tüübi erinevatest atribuutidest. Erinevad objektiatribuudid võivad omada erinevaid väärtuseid, nt telefoninumbreid või IP-aadresse. AD tunneb erinevaid eeldefineeritud objektitüüpe:

- Domeeni objekt: antud objekt on domeeni kõikide AD-objektide juur ja sisaldab infot domeenide kohta, nt nime. Domeeni objektide alla võivad kuuluda muud objektid.
- Rühmaobjektid: objektid teiste objektide rühmadesse liigitamiseks. Standardina on saadaval objekt „organiseerimisühik“ (Organizational Unit , OU). OU objekti alla võivad kuuluda edasised OU objektid, samuti arvuti, kasutaja ja kasutajarühmade objektid.
- Arvuti objekt: siia alla ei saa liigitada täiendavaid objekte. Active Directory on mõeldud ainult Windowsi arvutite haldamiseks, seega võivad arvuti objektid esindada eranditult vaid Active Directoryga koos töötavaid Windowsi arvuteid. Windows 98 jaoks saab kasutada nt Active Directory sisselogimiskomponente.
- Kasutaja objekt: antud objektiga esindatakse domeeni kasutajaid. Kasutaja objekti alla ei saa kuuluda muid objekte.
- Kasutajagruppide objektid: need nn turvagrupid esindavad Windowsi gruppe.

On erinevaid grupitüüpe, mille erinevused seisvad kehtivusalas (domeeni või kogu metsa piires) ja võimalikes grupi liikmetes (domeeni, metsa objektid). Siinkohal eristatakse kohalikke, domeenide kohalikke, globaalseid ja universaalseid gruppe. Turvagruppe kasutatakse volituste andmiseks. Windowsi süsteemis tuleb võrreldes varasemate süsteemidega arvestada oluliselt suurema gruppide arvuga (suuremate ettevõtete puhul mitukümmend tuhat), mistõttu tuleb kaaluda programmitoega haldust. Halduse võib lahendada nii isekirjutatud skriptide kui ka teis-

te firmade toodete abil. Kas ja millised programmid on vajalikud, tuleb otsustada sõltuvalt konkreetsest olukorrast.

AD üldist ülesehitust võib kirjeldada järgnevalt:

- Domeeni objekt moodustab domeeni AD-puu juure.
- Domeeni objekti alla luuakse OU-objektid, et arvuti, kasutaja ja kasutajagruppide objekte oleks võimalik struktureeritult kokku koondada. Kuna OU-objekte saab üksteise suhtes allutada, tekib organisatsiooni spetsiifikat järgiv puustruktuur.

Kohandamine administratiivsete oludega

Pärast standardset installeerimist on olemas lihtne ja tasapinnaline AD-struktuur, mille loob Windows ja mida tuleb vastavalt AD planeerimisele muuta. Kuna AD on mõeldud peamiselt Windowsi süsteemi haldamiseks, tuleb AD struktuuri ülesehitamisel jälgida, et struktuur viidaks vastavusse administratiivsete oludega. Kui selle asemel püütakse jäigalt ametiasutuse või ettevõtte organisatsioonilist struktuuri kuni iga väikseima detailini taasluua, võivad tagajärjeks olla haldusprobleemid.

AD skeem

Niinimetatud AD skeem kehtestab AD-objektide võimalikud kombinatsioonid, st määrab, milline objekt tohib teisi objekte sisaldada, millised on olemasolevad atribuudid ja millistest atribuutidest objektid koosnevad. Microsofti poolt määratud AD skeemi saab ka muuta. Kuid muutmise puhul on tegu tõsise sekkumisega, mida tohib teha ainult hoolikalt ette planeerides. Skeemi muutmine mõjutab kõiki ühiselt hallatavaid domeene, st metsa (Forest). Kuna skeemi muutmine on kriitiline operatsioon, saab seda teha ainult ühes kindlas arvutis, nn Scheme Master 's, kasutajarühma Scheme Admins liikmete abil. Skeemimuudatuste tühistamine võib olla võimatu. Antud kasutajarühma kuulumist tuleb jagada ülimalt piiratult ning seda tuleb rangelt kontrollida

Global Catalog

ADd hoitakse domeenikontrolleritel ja sünkroniseeritakse nendevahelise tiražeerimise teel. Domeeni AD sisaldab ainult domeeni puudutavat infot. Et leida metsas kiirelt infot kogu metsa kohta, moodustatakse nn Global Catalog (GC). Globaalne kataloog koosneb AD objektide osainfost ja tiražeeritakse kogu metsa vahel nõnda, et domeeni GC kaudu on võimalik vahetult ligi pääseda ka teiste domeenide infole.

Sites

Lisaks kirjeldatud puulaadsetele ja hierarhilistele struktuuridele tekitab Windows automaatselt ka täiendava ja ortogonaalse struktuuri. Ruumiliselt üksteisele lähedal asuvad arvutid – Windows tuvastab seda võrguaegade abil – koondatakse kokku nn asukohtadeks (ingl. Sites). Sites abil juhitakse muuhulgas ka domeenikontrollerite tiražeerimisstruktuuri. Ühe asukoha kohta peab olema vähemalt üks arvuti, mis sisaldab Global Catalogi -i koopiat. Kasutaja logimisprotsessi raames tuleb esitada päring Global Catalog -ile, mis tähendab, et sisselogimisel peab alati mõni Global Catalog -i server olema saadaval. Windowsi automaatselt koostatud asukohastruktuuri tuleks kohandada vastavalt ametiasutuse või ettevõtte sisestele oludele, nt asukohtadele erinevates linnades või riikides. Kuna see mõjutab AD tiražeerimissuhteid, tuleb selleks luua sobiv kontseptsioon.

AD planeerimise raames tuleb arvestada järgnevate aspektidega:

- Milline AD-struktuur tuleks valida domeenidesse jaotamise jaoks ja kuidas koondada domeene puudesse ja metsadesse?

- Millised kasutajad ja arvutid tuleks erinevatesse domeenidesse kokku koondada?

Iga domeeni puhul tuleb otsustada:

- millised OU objekte läheb tarvis, kuidas neid hierarhiliselt paika seada ja milliste objektide alla peavad need kuuluma,
- milliseid turvagruppe läheb tarvis ja kuidas neid OU-desse koondada,
- millist administratiivset mudelit tuleks rakendada (tsentraliseeritud/detsentraliseeritud haldust),
- kas administratiivsete ülesannete delegeerimine on vajalik ja kellele võib delegeerida,
- millised turvaseadistused tuleb kehtestada eri tüüpi arvutitele ja kasutajarühmadele,
- millised seadistusi läheb tarvis grupeerimissuuniste puhul ja millise kontseptsiooni järgi tuleb grupeerimissuuniseid jaotada (vt M 2.231 Windowsi grupipoliitika planeerimine ja M 2.326 Windows Vista ja Windows 7 grupeerimissuuniste planeerimine),
- millised usaldussuhted loob Windows automaatselt ja millised täiendavad usaldussuhted (nt väliste Kerberose realm-idega) tuleb sisse seada,
- millisele AD infole tohib erinevate AD liideste (nt ADSI, LDAP) kaudu ligi pääseda ja kes tohib ligi pääseda,
- millised AD objektid peavad kuuluma nn Global Catalog -i, millega peab saama ühendust kõikjalt metsast,
- millises režiimis tuleb domeene käitada: kui domeenis tuleb käitada veel ka Windowsi varukoopia-domeenikontrollereid (BDCs), peab domeen töötama režiimis „Mixed-Mode“. Kui BDC-d puuduvad, võib domeen töötada režiimis „Native-Mode“.

Üldjuhul tuleb planeeritav AD struktuur dokumenteerida, kuna see suurendab oluliselt stabiilsust, tagab järjekindla administreerimise ja tõstab seega ka süsteemi turvalisust. Eriti soovitatav on dokumenteerida tehtavad skeemimuudatused. Sealjuures tuleb dokumenteerida ka muudatuse põhjused.

Iga AD objekti puhul tuleb dokumenteerida:

- nimi ja asukoht AD puustruktuuris (nt “asukoht Tallinn”, isa-objekt: OU “filiaalid-Eesti”)
- mis on objekti eesmärk (nt RAS juurdepääsuga kasutajarühm RAS serveril nr 1)
- millised administratiivsed pääsuõigused tuleb määrata objektile ja selle atribuutidele (nt täielikult hallatud “Admin1” poolt)
- kuidas seadistada AD-õiguste pärimist, nt õiguste pärimise blokeerimine (vt M 2.230 Active Directory halduse planeerimine ja M 3.27 Koolitus Active Directory haldamiseks)
- millised grupeerimissuuniste objektid antud objekti mõjutavad (vt M 2.231 Windowsi grupipoliitika planeerimine)

AD administreerimise planeerimise ja rakendatava administratiivse mudeli planeerimise näol on tegemist tähtsate ülesannetega. Asjakohased soovitused on kokku võetud meetmesse M 2.230 Active Directory halduse planeerimine .

AD planeerimise turvalisust puudutavad põhiaspektid on kokkuvõetult:

- Domeenid on administratiivseteks piirideks - Domeenid piiravad administraatorite administratiivset võimu. Administraatorid saavad seega haldusoperatsioone teostada ainult ühe domeeni piires, mistõttu ei ulatu nende haldusvolitus tavaliselt üle domeeni piiri. Eriti kehtib see mitme domeeniga kooslustes (puu, mets), seega jääb ära tavaliste administraatorikontodega sageli esinev mure, et standardina transitiivse usaldusmudeliga on võimalikud ka domeenipiire ületavad volitused.
- Domeeniülesed juurdepääsud - Domeeniülene juurdepääs eeldab selgete pääsuvolituste määramist teisest domeenist pärit pöörduja jaoks vastavas sihtdomeenis. Standardses lahenduses pole seega domeeniülesed juurdepääsud võimalikud. See tähendab, et puustruktuuris või metsas saab domeeni „A“ administraator ainult siis suvalisele teisele domeenile „B“ administratiivsetes ülesannetes ligi pääseda, kui domeeni „B“ administraator on andnud domeeni „A“ administraatorile selleks selged volitused.
- Organisatsiooni administraatorid - Kasutajarühma organisatsiooni administraatorid liikmed on eristaatusega, kuna neil on kogu metsastruktuurile kehtivad AD administreerimisõigused. Kui juurdepääsu loob organisatsiooni administraator, ignoreeritakse seeläbi eriti just AD objektidele määratud pääsuõigusi. Organisatsiooni administraatorite kasutajarühma kuuluvust tuleb seega määrata võimalikult limiteeritult ja range täpsusega kontrollida. Tuleb arvestada, et organisatsiooni administraator on vajalik näiteks alamdomeenide loomiseks.
- Administratiivsete õiguste delegeerimine - Administratiivsete õiguste delegeerimiseks määratakse pääsuõigused AD objektidele ja nende atribuutidele. Pääsuõiguste jaotamine peab toimuma vastavalt administratiivsele mudelile. AD pääsuõiguste mehhanismide abil (pärimine, pärimise kontrollimine, juurdepääsuseadistuste mõjuala) on võimalik luua ülikeerukaid volitusstruktuure. Keerukate struktuuride puhul võib ülevaatlikkus ja haldusvõime kergesti kaduda, mistõttu on võimalik, et vale konfigureerimise tagajärjel tekivad AD-s turvaaugud. Seega tuleks eelistada võimalikult lihtsat volitusstruktuuri.

Skeemimuudatuste hoolikas planeerimine

Skeemimuudatused on kriitilise tähtsusega operatsioonid ja neid tohivad teha ainult vastava volitusega administraatorid pärast põhjalikku planeerimist. Lõpetuseks olgu öeldud, et AD planeerimises ja rakenduse aluseks olevates kontseptsioonides tehtud vigu saab pärast installeerimist kõrvaldada ainult suure vaevaga. Kui AD struktuuri on tarvis hiljem muuta, nt domeenide asetust puudes ja metsades, võib see endaga kaasa tuua olukorra, kus domeenid tuleb täielikult algusest peale uuesti üles ehitada.

Kontrollküsimused:

- Kas AD planeerimine on läbiviidud?
- Kas kõik osapooled on planeerimisse kaasatud?
- Kas vajadustest lähtuv AD volituste kontseptsioon on koostatud?

- Kas administratiivsete õiguste delegeerimine toimub koos piiravate ja nõuetekohaste volituste andmisega?

M 2.230 Active Directory halduse planeerimine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator, IT-juht

Active Directory (AD) koosneb erinevatest, puulaadse struktuuri alusel organiseeritud objektidest. Iga objekt koosneb teatud atribuutidest, mis salvestavad objekti infot. Objektide läbi toimub Windows süsteemi haldamine, mis on volitustega administraatori ülesanne. Kõikide AD objektide jaoks saab määrata volitused, mis juhivad objektide juurdepääse. Sellega saab määrata, millisel viisil võivad erinevad kasutajad erinevaid objekte muuta, näiteks kasutajaid luua või kasutajate paroole taastada. Windows standardse variandi installeerimise puhul on ainult administraatoritel õigus objekte muuta ja seega ka domeene hallata. Kasutajatel on üldjuhtudel maksimaalselt ainult lugemisõigus. Üldiselt kehtib ka Windows all väide, et domeeni piiriga lõpeb ka domeeni administraatorite administratiivne võim. Ainult grupi organisatsiooni administraatorid liikmetel on metsa igas domeenis täielik juurdepääs kõikidele AD objektidele, ja seda olenemata nende objektide jaoks määratud pääsuõigustest. Standardina on selleks metsa juurdomeeni (FRD) administraatorite kasutajarühma liikmed.

Administratiivsete ülesannete delegeerimine

Suurtes domeenides on soovitatav administratiivseid tööülesandeid delegeerida nii, et administratiivne koorem oleks jaotatud mitme administraatori vahel, või et vajadusel saaks rakendada ka töörollide eraldamist. Administratiivsete ülesannete delegeerimiseks tuleb ADs määrata vastavate administraatori kasutajarühmade AD-objektidele vastavad pääsuõigused. AD õiguste struktuur võimaldab õigusi määrata väga täpselt. Seadistuste abil saab näiteks administraatoril lubada kasutajakontosid luua ja kasutajate paroole taastada, kuid samas saab ka keelata kasutajakontode kustutamist või teistesse organisatsiooniüksustesse (OU - Organizational Units) ülekandmist. Lihtsustamaks sama tüüpi õiguste määramist terve puuosa piires, on lisaks võimalik pärandada objekti õigusi alampuu objektidele. Kuna alati pole soovitav, et alampuu teatud objektid saavad endale päritud õigused, saab ülevõtmist objekti kaupa ka blokeerida, mistõttu võivad tulemuseks olla volituste jaotamise keerukad stsenaariumid (vt M 3.27 Koolitus Active Directory haldamiseks).

Turvalisuse vaatepunktist tuleb AD halduse planeerimisel arvestada järgmiste punktidega:

- **Piiratud õiguste andmine** - Õiguste delegeerimisel tuleb anda ainult sellised hädavajalikud õigused, mis on vajalikud delegeeritavate administratiivsete operatsioonide teostamiseks.
- **Delegeerimismudeli dokumenteerimine** - Delegeerimismudel ja sellest tulenev õiguste andmine tuleb dokumenteerida. Administratiivsed tegevused tuleb delegeerida selliselt, et ülesannete kattumine oleks võimalikult välistatud. Vastasel korral võivad kaks administraatorit teha üksteisele vastukäivaid muudatusi. Niisugune olukord põhjustab tiražeerimiskonflikte, mis lahendatakse Windows poolt automaatselt, mis tähendab, et üks kahest muudatusest jääb igal juhul püsima. Niisuguste olukordade eest süsteem kahjuks ei hoiata. Seetõttu on alati soovitatav kavandada selline administratsioonimudel, kus vastutusalad võimalusel ei kattuks. Sel moel on võima-

lik vähendada tiražeerimiskonfliktide ohtu. Kui esineb oht tiražeerimiskonfliktide tekkeks või kui neid on juba esinenud, tuleb regulaarselt või pärast olulisi muudatusi käsitsi kontrollida, kas kehtima jäänud väärtused on õiged. Kas Active Directory nimiandmete tõendibaasi pidamine on organisatoorselt mõttekas, tuleb otsustada iga üksikjuhu puhul eraldi.

- **Keerukuse vähendamine** - Kui AD haldamisel soovitakse kasutada õiguste delegeerimist, tuleb selleks määrata AD piires vastavad pääsuõigused. Puustruktuuri osaks olevate objektide haldamiseks kasutatakse siinjuures tavaliselt pärimismehhanismi. Delegeerimisel ja õiguste pärimisel tuleks siiski ilmtingimata vältida keerukaid stsenaariume, sest vastasel korral on turvaaugud kerged tekkima. Näiteks võib juhtuda, et ühele kasutajale on antud liiga vähe või liiga palju õigusi.
- **Kasutajarühma kuulumise kontseptsiooni loomine** - Erinevatesse administratiivsetesse kasutajarühmadesse kuulumise kohta tuleb koostada visandlik kontseptsioon. Siinjuures tuleb kõigepealt defineerida need volitused ja protseduurid, mis määravad, kas, millal ja kui kauaks teatud kasutaja või kasutajarühm mõnda administratiivsesse rühma võetakse. Eriti tuleb hoolt kanda selle eest, et kuuluvus organisatsiooni administraatorite kasutajarühma oleks piiratud ja kontrollitud. Kui organisatsiooni protseduur seda võimaldab, võib kaaluda kõikide selle kasutajarühma liikmete eemaldamist pärast domeenistruktuuri loomist ja lisada vastavaid liikmeid edaspidi ainult vajadusel, pidades seejuures kinni nelja-silma-printsiibist. Siiski tuleb arvestada ka asjaoluga, et organisatsiooni administraatorite kasutajarühma liiget läheb alati tarvis siis, kui metsastruktuuris on tarvis luua uus domeen.
- **Administraatorite informeerimine ja koolitamine** - Muudatuste kooskõlastamata jätmisest tingitud turvaaukude välistamiseks tuleb administraatoreid AD struktuuri ja nende administratiivseid tegevusi puudutavate protseduuride osas informeerida ja koolitada. Näiteks võib olla vajalik, et uue kasutaja loomisel tuleb ta kaasata teatud turvarühmadesse või luua isegi täiendav uus erinimega turvarühm. Antud nõudmiste unustamisel võivad kasutajad saavad valed volitused.
- **Tööriistade kasutamine** - Suurte domeenide puhul tasuks mõelda haldusprogrammide kasutamisele. AD haldamise kergendamiseks on saada erinevaid nii tasulisi kui ka tasuta tööriistu. Nende kasutamist tasub kaaluda. Vastavate tööriistade kasutamisel tuleb tagada, et AD haldamine toimuks eranditult vaid nende tööriistade abil.

Kontrollküsimused:

- Kas AD halduse administratiivsed kasutajarühmad on planeeritud?
- Kas delegeerimismudel välistab ülesannete kattumise?
- Kas kõik administratiivsed valdkonnad ja volitused on dokumenteeritud?
- Kas administraatorid on koolituste läbi AD haldamiseks ettevalmistatud?

M 2.231 Windowsi grupipoliitika planeerimine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator, IT-juht

Grupeerimissuunised on Active Directorys selleks, et rakendada objektide rühmale konfiguratsiooni seadete kogumikku, mille hulka kuuluvad eriti just ka turvaseadistused. Nn grupeerimissuuniste objekt (inglise keeles Group Policy Object, GPO) hõlmab etteantud konfiguratsiooniparameetrite kogumiku (standardina üle 700). Igale parameetrile saab määrata konkreetse väärtuse, mis võib sõltuvalt olukorrast pärineda ainult piiratud väärtusskaalast. Üldiselt saab alati valida ka väärtuse defineerimata , seega kehtivad vastava parameetri jaoks automaatselt Windowsi standardseadistused.

Arvuti ja kasutajate seadistused

Grupeerimissuunise objekti piires on parameetrid kokku kogutud kas puulaadse struktuuri alusel või failisüsteemi stiilis teemade kaupa. Siinkohal tekib kõige kõrgemal tasandil üldine jaotus niihästi arvuti kui ka kasutaja seadistustes.

Turvalisuse aspektist on eriti tähtsad seadistused need, mis asuvad järgnevates asukohtades:

- Computer settings\Windows settings\Security settings
- Computer settings\Administrative settings \
- Windows components\Windows Installer
- Computer settings\Administrative Templates\System\Group Policy
- User Preferences\Administrative Templates
- Windows components\Microsoft Management Console
- User Preferences\Administrative settings\
- Windows components\Windows Installer

Hetkel kehtivate seadistuste arvutamine

See arvutamine on vajalik, kuna parameetrite seadistuste andmed võivad olla defineeritud erinevate objektide kaudu ning grupeerimissuuniste objektid võivad üksteisega kattuda.

Defineerida saab järgnevaid grupeerimissuuniste objekte:

1. Igal arvutil on lokaalselt määratletud grupeerimissuunise objekt. See võimaldab defineerida parameetriseadistusi arvutil lokaalselt, nt võrguühenduse puudumisel.
2. Grupeerimissuuniste objekte saab defineerida Windows asukohtade (Sites) abil. Sellega saab seadistusi kohandada sõltuvalt asukohast.
3. Active Directory struktuuri piires saab defineerida domeeniobjekti grupeerimissuuniste objekte selliselt, et nendega saab juhtida arvuti ja kasutaja parameetriseadistusi kogu domeeni piires.
4. Igale OU objektile saab määrata grupeerimissuuniseid, mille seadistused mõjuvad kõikidele arvutitele ja kasutajatele vastava OU objekti alluvuses.

LSDO järjestus

Konkreetse arvuti või kasutaja jaoks kehtivate parameetrite seadistuste arvutamiseks kasutatakse järgnevat arvutus-/kattuvusskeemi [kohalik (local) site) domain) organisational Unit), LSDO]: esmalt arvestatakse kohalike seadistustega (L, lokaalne). Siis kaetakse need seadistused vastavas asukohas defineeritud grupeerimissuuniste objekti seadistustega (S, asukoht). Seejärel kaetakse vastavas domeeniobjektis defineeritud grupeerimissuuniste objektiga (D, domeen). Lõpuks rakendatakse OU objektide grupeerimissuuniste objekte sellises järjekorras, nagu need on defineeritud domeeniobjektist OU objektini kulgevas ahelas, mis sisaldab vastavat arvutit või kasutajat (O, organisatsiooni allüksus).

Kattuvuse blokeerimine ja kohustamine

Kattuvust saab mõjutada valikutega blokeeri/kohusta. Kui seadistused blokeeri ja kohusta on üksteisega konfliktis, jääb kehtima seadistus kohusta. Lisaks saab OU tasandil defineerida ühe OU objekti jaoks mitu grupeerimissuuniste objekti. Seejuures toimub kattuvus vastavalt kindlaksmääratud järjekorrale. Lisaks saab igat üksikut grupeerimissuuniste objekti OU objekti jaoks aktiveerida või desaktiveerida. Grupeerimissuuniste objekte saab Active Directorys määrata ainult OU objektidele, kuid mitte üksikutele arvutitele või kasutaja objektidele. Lokaalselt defineeritud grupeerimissuuniste objekti Active Directorys ei salvestada. Kui arvuti objekte koondav, vastavalt OU objektile defineeritud grupeerimissuuniste objekt ei tohi mõjuda kõikidele olemasolevatele arvuti objektidele on võimalik rakendust siduda konkreetse arvuti objektiga, määrates pääsuõigused grupeerimissuuniste objektile. Selleks tuleb arvuti objektilt ära võtta grupeerimissuunise objekti pääsuõigus rakenda.

Seosed GOP-de ja OU-de vahel

Seni kasutatud kirjeldus grupeerimissuuniste objektide defineerimisest OU objektide jaoks oli siiski lihtsustatud: grupeerimissuuniste objektid salvestatakse Active Directorys eraldi ja need moodustavad objektide kogumi. Igat defineeritud grupeerimissuuniste objekti saab siduda ühe või ka mitme OU objektiga. Sel juhul on tegu lingiga (Link). Sõltuvalt lingi märgistusest, aktiivne või mitteaktiivne, rakendatakse OU objekti arvutamisel vastavat grupeerimissuunise objekti, või ei rakendata (vt eespoolt). Iga grupeerimissuunise objekti jaoks saab omaduste dialoogiaknas määrata, milliste OU objektidega on Link seotud, st millistele objektidele võivad nad oma mõju avaldada.

Turvalisuse vaatepunktist tuleb grupeerimissuuniste objektide planeerimisel ja nendega ümberkäimisel arvestada järgnevate aspektidega:

- Hoidke GPO kontseptsioon võimalikult lihtne - Grupeerimissuuniste kontseptsioon peab jääma võimalikult lihtsaks. Mitmekordsete kattuvustega keerukaid struktuure tuleb vältida. Grupeerimissuuniste objektidele pääsuõiguste andmist tuleks kasutada ainult erandolukorras. Grupeerimissuuniste kontseptsioon peab olema selliselt dokumenteeritud, et erandid oleks kergesti äratuntavad.
- OU grupeerimisel arvestage GPO kontseptsiooniga - Grupeerimissuuniste kontseptsioon ja OU objekti struktuur mõjutavad üksteist olulisel määral, kuna grupeerimissuuniste objekte saab Active Directorys rakendada ainult OU objektidele, aga mitte arvuti või kasutaja objektidele. Seega tuleb OU

gruppide moodustamisel jälgida, et OU objektidesse või alataseme OU objektidesse koondataks ainult sama GPO seadistusega objektid.

- Kus määratletakse milline parameeter? - Õiguste arvutamisega saab parameetrite seadistuste haldamist jaotada erinevate „kohtade“ peale (lokaalne, asukoht, domeeni objekt, OU objektid). Seega tuleb iga parameetri puhul otsustada, kus see defineeritakse. Seejuures tuleb arvestada, et teatud parameetrid aktiveeruvad ainult siis, kui neid defineeritakse teatud kindlates „kohtades“. Näiteks saab parooli seadistusi defineerida ainult domeeni objektidele.
- GPO-de kaitsmine - Grupeerimissuuniste objekte tuleb kaitsta volitamata muudatuste eest. Ühest küljest tuleb selleks Active Directorys anda vastavad volitused (vt M 2.230 Active Directory halduse planeerimine ja M 3.27 Koolitus Active Directory haldamiseks) ning teisest küljest saab kasutajal keelata vastavate haldustööriistade nagu nt MMC-grupeerimissuuniste, Snap-In'de või registritöötlusprogrammide kasutamise.
- Turvalisust puudutavate parameetrite määramine - Eriti oluline on kindlaks määrata turvalisust puudutavate parameetrite seadistused grupeerimissuunise objekti raames. Lisaks antud seadistustele võivad sõltuvalt kasutusest turvalisuse jaoks olulised olla ka muud parameetrid. Nende hulka kuuluvad ka nt Internet Exploreri seadistused. Erinevate grupeerimissuuniste objektide seadistused peavad üldjuhul lähtuma ettevõtte või ametiasutuse turvasuunistest ja neid ka rakendama.

Järgnevalt on toodud mõningad turvaseadistuste näited, mida saab kasutada grupeerimissuunise turvaseadistuste alusena. Näidetes kasutatud väärtused tuleb ilmtingimata vastavalt kohalikele tingimustele ümber kohandada. Grupeerimissuuniste kontseptsiooni raames tuleb üksikud väärtused erinevate grupeerimissuuniste objektide vahel ära jaotada ja kasutusotstarbele (nt GPO serverile, GPO töökohaarvutile) sobivaks kohandada. Seeläbi on sissekannete puhul võimalikud ka erinevad väärtused.

Paroolisuunis
Suunis
Seadistus arvutis
paroolide ajaloo kohustamine
6 salvestatud parooli
paroolid peavad vastama keerukusnõuetele.
aktiveeritud
paroolide salvestamine kõikide domeenikasutajate jaoks reversiivse krüpteeringuga
desaktiveeritud
parooli maksimaalne vanus
90 päeva
parooli minimaalne pikkus
6 märki
parooli minimaalne vanus
1 päev
Konto blokeerimise suunised
Suunis
Seadistus arvutis
konto blokeerimise lävi

3 kehtetut sisselogimiskatset
konto blokeerimise kestvus
0 (märkus: konto on blokeeritud kuni administraator blokeeringu tühistab)
konto blokeerimisloenduri nullimiseks peab mööduma
30 minutit
Kerberose suunis
Suunis
Seadistus arvutis
kasutajate sisselogimise piirangute kohustus
aktiveeritud
kasutajapileti maksimaalne kehtivusaeg
8 tundi
teenusepileti maksimaalne kehtivusaeg
60 minutit
maksimaalne tolerants arvuti töötakti sünkroniseerimiseks
5 minutit
maksimaalne aeg, mille jooksul saab kasutajapiletit uuendada
1 päev
Seiresuunis
Suunis
Seadistus arvutis
Active Directory juurdepääsude seire
edukas, ebaõnnestunud
sisselogimissündmuste seire
edukas, ebaõnnestunud
sisselogimiskatsete seire
edukas, ebaõnnestunud
kontode halduse seire
edukas, ebaõnnestunud
objektidele juurdepääsukatsete seire
ebaõnnestunud
protsessi jälgimise seire
seiret ei toimu
õiguste kasutamise seire
ebaõnnestunud
suuniste muudatuste seire
edukas, ebaõnnestunud
süsteemisündmuste seire
edukas, ebaõnnestunud
Kasutajaõiguste andmine
Suunis
Seadistus arvutis
teenusena sisselogimine
defineeritud, kuid tühi
süsteemiaja muutmine
administraatorid
aja planeerimise prioriteedi tõstmine
administraatorid
kvootide tõstmine
administraatorid

sisselogimine pakktöötlustellimusena
defineeritud, kuid tühi
pakktöö tellimusena sisselogimisest keeldumine
defineerimata
teenusena sisselogimisest keeldumine
defineerimata
arvutile ligipääsemine võrgust
kõik,
administraatorid,
autenditud kasutajad,
varunduse operaatorid
läbiotsiva kontrolli ärajätmine
kõik
programmide debug
defineerimata
kasutamine operatsioonisüsteemi osana
defineeritud, kuid tühi
arvuti eemaldamine dokkimisjaamast
administraatorid
arvuti- ja kasutajakontode usaldamine delegeerimisotstarbeks
administraatorid
Token 'i asendamine protsessitasandil
defineeritud, kuid tühi
saalimisfaili loomine
administraatorid
süsteemivõimsuse profiili loomine
administraatorid
üksikprotsessi profiili loomine
administraatorid
Token' i -objekti loomine
defineeritud, kuid tühi
püsivalt ühiskasutusse antud objektide loomine
defineeritud, kuid tühi
väljalülitamise sundimine kaugsüsteemiga
administraatorid
turvakontrollide loomine
defineeritud, kuid tühi
süsteemi väljalülitamine
administraatorid
töökohtade lisamine domeeni
defineeritud, kuid tühi
seadmedraiverite lisamine ja eemaldamine
administraatorid
lokaalne sisselogimine
administraatorid,
varunduse operaatorid
lokaalse sisselogimine keelamine
defineerimata
failide ja kataloogide varundamine
varunduse operaatorid

andmebaasi lehekülgede sulgemine
defineeritud, kuid tühi
kataloogiteenuse andmete sünkroniseerimine
defineeritud, kuid tühi
Teadmiseks: vastavalt Ressource-Kit dokumentatsioonile ei ole antud seadistus praeguse Windows 2000 all enam kasutuses.

failide ja objektide omandamine	administraatorid
püsivara keskkonna muutujate muutmine	administraatorid
seire- ja turvalogide haldamine	administraatorid
failide ja kataloogide taastamine	administraatorid
juurdepääsu keelamine võrgust arvutile	defineerimata

Turvavalikud
Suunis
Seadistus arvutis
administraatori ümbernimetamine
defineerimata
kasutajalt parooli muutmise nõudmine enne parooli kehtivusaja lõppemist
7 päeva
printeridraiverite installeerimise keelamine kasutaja jaoks
aktiveeritud
eelmiste logimiste vahesalvestamise arv (juhuks kui domeenikontroller pole saadaval)
0 sisselogimist
virtuaalse töömälu saalimisfaili kustutamine süsteemi väljalülitamisel
aktiveeritud
NTFS draivide väljastamise lubamine
administraatorid
kasutaja automaatne väljalogimine, kui sisselogimisaeg on ületatud (lokaalne)
aktiveeritud
kasutaja automaatne väljalogimine pärast sisselogimisaja lõppemist
aktiveeritud
kliendi side digitaalne allkirjastamine (alati)
desaktiveeritud
kliendi side digitaalne allkirjastamine (võimalusel)
aktiveeritud
varundamis- ja taastamisõiguste kasutamise kontrollimine
desaktiveeritud
külaliskonto ümbernimetamine
defineerimata
süsteemi väljalülitamine sisselogimiseta
desaktiveeritud
LAN halduse autentimistasand
saada ainult NTLMv2 vastuseid\keeldu LM’st
tegevusevaba ajavahemik kuni sessiooni lõpetamiseni
15 minutit

viimast kasutajanime ei näidata sisselogimisdialoogis
aktiveeritud
teated kasutajatele, kes tahavad sisse logida
defineerimata
teadete pealkiri kasutajatele, kes tahavad sisse logida
defineerimata
serveri side digitaalne allkirjastamine (alati)
desaktiveeritud
Turvavalikud (jätk)
Suunis
Seadistus arvutis
serveriside digitaalne allkirjastamine (võimalusel)
aktiveeritud
serveri operaatoritel planeeritud ülesannete sisseseadmise võimaldamine (ainult domeenikontrollerile)
defineerimata
turvaline kanal: turvalise kanali andmete digitaalne allkirjastamine (võimalusel)
aktiveeritud
turvaline kanal: turvalise kanali andmete digitaalne krüpteerimine (võimalusel)
aktiveeritud
turvaline kanal: turvalise kanali andmete digitaalne krüpteerimine või allkirjastamine (võimalusel)
desaktiveeritud
turvaline kanal: vajab tugevat seansivõtit (Windows 2000 või kõrgem)
desaktiveeritud (Teadmiseks: aktiveerida täielikes Windows 2000 keskkondades)
globaalsete süsteemiobjektide standardvolituste võimendamine (nt sümbolilised kiirvalikud)
aktiveeritud
CTRL+ALT+DEL nõude desaktiveerimine sisselogimiseks
desaktiveeritud (Teadmiseks: st CTRL+ALT+DEL on vajalik)
süsteemi kohene väljalülitamine, kui turvakontrolle ei saa enam logida
desaktiveeritud
arvutikonto parooli süsteemihoolduse keelamine
desaktiveeritud
krüpteerimata parooli saatmine, et luua ühendus kolmandate tootjate SMB serveritega
desaktiveeritud
käitumine allkirjastamata failide installeerimisel (välja arvatud draiverid)
hoiata, kuid võimalda installeerimist
käitumine allkirjastamata draiverite installeerimisel
hoiata, kuid võimalda installeerimist
käitumine Smartcard'de eemaldamisel
arvuti sulgemine
anonüümsete ühenduste täiendavad piirangud
juurdepääsu keelamine, kui puudub selge anonüümne volitus
taastamiskonsool: automaatsete administratiivsete sisselogimiste lubamine
desaktiveeritud
taastamiskonsool: diskettide kopeerimise ja kõikidele lugejatele ja kataloogidele juurdepääsemise lubamine

desaktiveeritud
CD-ROMi lugejatele juurdepääsu piiramine lokaalselt sisselogitud kasutajatele
aktiveeritud
disketiseadmetele juurdepääsu piiramine lokaalselt sisselogitud kasutajatele
aktiveeritud
globaalsete süsteemiobjektidele juurdepääsu kontrollimine
desaktiveeritud
Sündmuste logi
Suunis
Seadistus arvutis
rakenduste logi säilitamine . . . päevaks
defineerimata
rakenduslogi säilitusmeetod
vajadusel sündmused üle kirjutada
turvalogi säilitusmeetod
vajadusel sündmused üle kirjutada Teadmiseks: suurt turvalisust nõudvas keskkonnas tuleb valida järgnev seadistus: sündmuste ülekirjutamise keelamine (logi puhastamine käsitsi)
süsteemilogi säilitusmeetod
vajadusel sündmused üle kirjutada
külaliskonto juurdepääsu piiramine rakenduslogile
aktiveeritud
külaliskonto juurdepääsu piiramine turvalogile
aktiveeritud
külaliskonto juurdepääsu piiramine süsteemilogile
aktiveeritud
rakenduslogi maksimaalne suurus
30 080 kilobaiti
turvalogi maksimaalne suurus
100 992 kilobaiti
süsteemilogi maksimaalne suurus
30 080 kilobaiti
turvalogi säilitamine . . . päevaks
defineerimata
süsteemi väljalülitamine turvalogi maksimaalse suuruse saavutamisel
desaktiveeritud (Teadmiseks: aktiveerida kõrget turvalisust nõudvates süsteemides)
süsteemilogi säilitamine . . . päevaks
defineerimata

Kontrollküsimused:

- Kas GPO kontseptsioon loodi vastavalt vajadusele?
- Kas kõik GPOd on piiravate pääsuõigustega kaitstud?
- Kas kõikides GPOdes on GPO-parameetrite jaoks kehtestatud nõuded?

M 2.232 Windows CA-struktuuri plaaneerimine

Algatamise eest vastutavad: IT-turvaosakond, IT-juht

Rakendamise eest vastutavad: administraator, IT-juht

Windowsi tarnitakse oma enda PKI komponentidega, mis võimaldavad üleorganisatsioonilise sertifikaadihierarhia ülesehitamist. PKI (Public Key infrastruktuuri) tuumaks on nn sertifitseerimisüksus (Certificate Authority, CA), mis väljastab sertifikaate. CA kasutamine ei ole Windowsi tööks küll hädavajalik, kuid kohustuslik siis, kui läheb tarvis teatud funktsioone, nt kiipkaardiga sisselogimist või turvalist sidet Windowsi süsteemikomponentide vahel SSL-i kaudu.

Windows pakub ühe CA kaht versiooni:

1. Stand-alone-CA (eraldiseisev sertifitseerimisüksus) ja
2. Enterprise-CA (organisatsiooniülene sertifitseerimisüksus).

Nende kahe CA versiooni peamine erinevus seisneb selles, et Enterprise-CA on integreeritud Active Directorysse ja saab Active Directoryst kasu, rakendades seda kataloogiteenusena. Näiteks avalikustatakse sertifitseerimiskohad Active Directorys ja sertifikaate saab väljastada ja jaotada automaatselt suures mahus. Stand-alone-CA puhul kontrollib sertifitseerimistaotlust alati vastav CA administraator. Administraator peab sertifikaadi loomise käsitsi aktiveerima. Standalone-CA -d saab installeerida ja käitada ka arvutis, mis pole võrku ühendatud, Enterprise-CA saab seevastu kasulikult töötada ainult võrku ühendatud arvutis.

Enterprise-CA puhul saab sertifitseerimismalle individuaalselt kohandada. Mõlemad CA versioonid sobivad sertifitseerimishierarhia loomiseks ja võivad seega töötada ka allutatud CA-dena. Enterprise-CA sobib LANi paljude infrastruktuuriliste eesmärkide jaoks paremini ja seda tuleks tavaolukorras eelistada. Eriti just organisatsiooniüleste PKI planeerimisel tuleb jälgida, et kõik kasutusvõimalused ja sellega seotud rakendused oleks teada. Tehnilise teostatavuse hindamiseks on soovitatav kõik kasutatavad komponendid eelnevalt koostalitlusvõime osas üle kontrollida.

Sobivate sertifitseerimisüksuste kasutamise planeerimise organisatsioonilised aspektid

Vastutusalade reguleerimine

- PKI planeerimine vajab aega. Tavaliselt tuleb kehtestada spetsiaalsed organisatsioonisisesed vastutusalad ja luua vastavad eeskirjad.
- Sertifikaatide kasutusotstarve on CA-struktuuri planeerimisel olulise tähtsusega.

Seega kaasneb üldise, organisatsiooniülese sertifitseerimisinfrastruktuuri ülesehitamisega tihti rohkem probleeme, kui rakendusest lähtuva PKI ülesehitamine. Rakendusest lähtuvat PKId saab kasutada näiteks siis, kui võrgupõhise rakenduse raames on tarvis usaldusväärselt identifitseerida ainult asjassepuutuvaid töötajaid.

Näitena võib välja tuua puhkuseavalduste elektroonilise esitamise ja

töötlemise, mille käigus peavad erinevad isikud andma järgemööda avaldustele digitaalallkirja.

- Kui sertifikaate kasutatakse ainult ametiasutuse või ettevõtte piires, peavad neid väljastama ainult CAd, mis väljastavad eranditult vaid sisekasutuseks mõeldud sertifikaate. Sellised sisesed CAd ei tohi sertifikaate väljastada „väljapoole“, nt inimestele või seadmetele, mis ei kuulu ametiasutuse või ettevõtte alla. Sisekasutuse CA ei tohi olla väljapoolt Interneti kaudu ligipääsetav, seepärast ei saa see kontrollida ka väljapoole väljastatud sertifikaate.

Kasutussuuniste dokumenteerimine

- Väliselt kasutatavate sertifikaatide ja väljastatavate CAde jaoks tuleb määratleda ja dokumenteerida kasutussuunised. Seejuures tuleb hoolikalt jälgida, et identiteedikontrolli kvaliteedile kehtestataks sobivad nõuded ja tagataks ka nende rakendamine.
- Sertifikaatide sulgemiseks tuleb juurutada sobivad protsessid. Siinkohal on tarvis arvestada sulgemisega tegeleva organisatsiooniüksuse kättesaadavuse ja käideldavusega, töötajatele väljastatavate sulgemisvolitustega, sulgemisega tegelevate töötajate isiku usaldusväärse identifitseerimisega ning sulgemisprotsessi dokumenteerimisega.
- Võtmete kaotsiminekul või kompromiteerimisel ja sellele järgneva sertifikaadi sulgemise korral läheb töötajatel tarvis uut sertifikaati, et nad saaksid oma tööga jätkata. Tööprotsesside taastamiseks tuleb välja töötada asjakohased protsessid, mis toimiksid võimalikult kiiresti, eriti nendel juhtudel, kus võtmeid talletatakse kiipkaartides ja lubades (tokens). Selleks tuleb näiteks tagada juba varem valmis varutud ja isikustatud kiipkaartide hoidmine turvalistes kohtades ning nende turvaline väljastamine.

Sobivate sertifitseerimisüksuste kasutamise planeerimise tehnilised aspektid

Puudulik koostalitlusvõime

- Tarvis on planeerida, milliseid krüptograafilisi protseduure ja algoritme ning millise pikkusega võtmeid tuleks kasutada (vt M 2.162 Krüptoprotseduuride ja -toodete vajaduse määramine).

CA-de hoolikas kaitse

- CA sertifikaatide usaldusväärus sõltub olulisel määral nende turbeastmest. Seetõttu tuleb turvalisuse seisukohast olulisi sertifikaate väljastavate CA-de puhul eriti hoolikalt jälgida füüsilist ja tarkvaratehnilist turvalisust. Turvalisuse seisukohast on eriti olulised need sertifikaadid, millel on palju kasutajaid või mille õigsusest sõltuvad muud turvalisuse seisukohast olulised rakendused.
- Erineva turbevajadusega sertifikaatide jaoks tuleks kasutada erinevaid CA-sid.

- CA hierarhiate kasutamisel tuleb määrata kehtivusmudel. Seejuures on oluline määrata, kuidas käsitleda järgsertifikaate, kui nt juur-CA sertifikaat tuleb sulgeda (mis põhjusel see ka ei juhtuks).
- Erinevatele sertifikaaditüüpidele (nt Root-CA sertifikaadile, kasutaja meilisertifikaadile) tuleb määrata maksimaalne kehtivusaeg. Üldjuhul on mõistlik, kui sertifikaatide kehtivusaeg ei ületa väljaandva CA sertifikaadi kehtivusaega. Siinkohal eksisteerivad erinevad kehtivusmudelid (nt nn „ahelmudelid“ ja „kestmudelid“).

Pikendusvõimalused

- Tuleb kehtestada võimalused ja protseduurid, mis kehtivad pärast sertifikaadi kehtivuse lõppemist. Kas sertifikaati on näiteks võimalik pikendada või tuleb väljastada uued sertifikaadid?
- Erinevate kasutusvaldkondade jaoks tuleb sisse seada ja kasutusele võtta asjakohased sertifikaadimallid. Siinkohal tuleb tähelepanu pöörata piirangute rakendamisele, eriti kasutuspiirangule Certificate Usage, et välistada sertifikaatide väärkasutus (nt alam-CA-de sisseseadmine). Alates versioonist Windows Server 2008 on sertifikaadimallidel varasemast rohkem parameetreid, millega piiranguid kehtestada, kuid neid saab kasutada vaid juhul, kui sama hierarhia piires ei kasutata ühtki vanema operatsioonisüsteemiga töötavat CA-d.
- Andmevarundusprotsessi peab olema kaasatud ka CA sertifikaadiandmebaas. Lisaks PKI planeerimisele on tähtis tagada üksikute PKI komponentide turvalisus nende käitamise ajal. Sertifitseerimisüksuse kaitse peab vastama selle rakenduse kaitsevajadusele, milles sertifikaate kasutatakse. Sellekohased soovitused leiate IT etalonturbe abivahendist.

CA versioonist sõltuvad planeerimisaspektid

Sertifikaatide jaotamine:

- Auto-Enrollment - sertifikaatide tellimise ja väljastamise protseduur (lühidalt: jaotamine) võib toimuda automaatselt (ilma kasutajapoolse sekkumiseta) või käsitsi. Sertifikaatide automaatne jaotamine (Auto-Enrollment) põhineb Active Directoryl ja grupeerimissuunistel (M 2.231 Windowsi grupipoliitika planeerimine). Auto-Enrollment on võimas tööriist, mis lihtsustab oluliselt organisatsioonis teatud rakenduste jaoks määratud kasutajate ja arvutite sertifikaatide haldamist. Sagedaseks näiteks on Encrypting File System (EFS) krüpteerimissertifikaatide jaotamine klientidele. Sertifikaadi Enrollment toimub ainult autenditud klientidele ja tuleb varustada vastavate turvamehhanismide ja volitustega. Seadistused leiab grupeerimissuuniste objektide redaktoris järgnevate valikute alt:
- Computer Configuration | Windows Settings | Security Settings | Public Key Policies | Autoenrollment
- User Configuration | Windows Settings | Security Settings | Public Key Policies | Autoenrollment

Standardina nõuavad automaatselt arvutisertifikaati ainult domeenikontrollerid. Mõned valikulised Windowsi komponendid nõuavad samuti automaatselt sertifikaati, nt saab iga aktiivse EFS-iga klient automaatselt EFS-sertifikaadi. Auto-Enrollment -i tuleks kasutada ainult reaalselt vajalikul määral, kuna vastasel korral muutub haldamine keerulisemaks ja esineb ka võtmete kinnipüüdmise oht. Planeeritud rakenduste või Windowsi komponentide baasil tuleb kaaluda, milliseid sertifikaadi tüüpe tuleks erinevatele kasutajatele ja arvutitele lubada ning kuidas peaks toimuma nende jaotamine. Vastavalt äsja mainitud põhimõtetele tuleb planeerida ka grupeerimissuuniseid ja sertifitseerimisteenuste volitused.

Privaatvõtmete arhiveerimine:
privaatvõtmete arhiveerimine sertifitseerimisüksuses tuleks aktiveerida ainult siis, kui PKI halduseks vajalik töörollide jaotuse kontseptsioon on välja töötatud ja ellu rakendatud. Arhiveerimine võib küll vähendada üksikute kasutajate võtmekaotuse ohtu, kuid see suurendab väärkasutuse riski. Seepärast ei saa selle kasutamist soovitada. Sobiv strateegia sõltub kasutatavatest rakendustest ja komponentidest ning tuleks kehtestada läbi PKI planeerimise ja IT-turvasuuniste.

Rollijaotus:
Rollijaotuse elluviimine rollijaotus tähendab, et PKI mitut või kõiki kriitilisi haldusrolle ei jäeta ühe isiku või kasutajakonto kanda. Selleks peab töörollide jaotus olema määratletud organisatsiooni tasandil (vt eespoolt). Tehnilisest vaatepunktist saab töörollide jaotamist ka süsteemi abil sundida.
Neli töörolli on:

- sertifitseerimiskeskuse administraator
- sertifikaadi haldaja
- varunduse operaator
- kontrollija

Kasutajakonto, mille alla kuulus enne kas kaks või mitu nimetatud rolli, eraldatakse töörollide jaotusega kõikidest CA haldustegevustest. Töörollide jaotus tuleb administraatoril uuesti kindlaks määrata. Töörollide jaotuse väära seadistuse korral ei saa CAd enam kasutada. Juhul kui töörollide jaotamise funktsiooni soovitakse kasutama hakata, tuleb esmalt välja töötada sobiv volituste kontseptsioon, mida tuleb omakorda eelnevalt proovikasutuses testida.

Täiendavad kontrollküsimused:

- Kas vajadustest lähtuv PKI planeerimine on juba läbi viidud?
- Kas CA hierarhia on koos kõikide vastutusalade ja kasutustingimustega dokumenteeritud?
- Kas kõik sertifitseerimiskeskused ja sertifitseerimisteenused on kaitstud vastavalt rakenduste kaitsevajadustele?
- Kas on kindlaks määratud, millised sertifikaate tohib erinevatele kasutajatele väljastada?
- Kas kõik parameetrid, muuhulgas nt sertifikaaditüüpide kehtivus, on defineeritud?
- Kas haldusrollide lahutamiseks vajalik volituste kontseptsioon on välja töötatud?

M 2.241 Kaugtöökoha nõuete analüüsi sooritamine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: IT-turvaosakond, administraator

Enne kaugtöökoha sisseseadmist oleks mõistlik läbi viia nõuete analüüs. Nõuete analüüsi eesmärgiks on määratleda kõik võimalikud kasutusvaldkonnad ja tuvastada, milliseid riist- ja tarkvarakomponente läheb tarvis kodutöökoha ühendamiseks töökohaga. Selle käigus võivad selguda spetsiaalsed nõudmised, mis võivad eeldada teatud kindlate süsteemide ja/või tarkvara kasutamist (vt B 4.4 Virtuaalne privaatvõrk (VPN) ja B 4.5 IT-süsteemi kohtvõrguühendus ISDN kaudu).

Dokumenteerimine ja kooskõlastamine

Nõuete analüüsi tulemused tuleb dokumenteerida ja IT-turbespetsialistiga kooskõlastada. Nõudmiste analüüsi käigus tuleb muuhulgas välja selgitada järgmised punktid:

- Millise konfidentsiaalsusastmega andmeid tohib töödelda kaugtöökohas, st väljaspool ametiasutuse või ettevõtte „kaitsvaid seinu“?
- Millisel otstarbel hakatakse kasutama juurdepääsu tööandja institutsioonile (andmete saamiseks, informatsiooni seadistamiseks, programmide kasutamiseks)?
- Kui suur võib olla kodutöökoha ja tööandja vaheline andmevahetus?
- Kas kodutöökoha kasutajal on tarvis juurdepääsu tööandja intraneti võrgule? Kui jah, kas ühendus on tarvis sisse seada kogu Interneti, st kõikide seal olevate andmete ja teenuste kasutamiseks või ainult teatud intraneti valdkondade jaoks?
- Kas kaugtöötaja jaoks on ette nähtud ka Interneti kasutamine? Kui jah, kas kaugtöötajal on isiklik Internetiühendus või luuakse ühendus läbi tööandja intraneti võrgu?

Edastuskanalite kinnitamine

Sõltuvalt andmete konfidentsiaalsusastmest võib olla vajalik kehtestada tööandja ja kaugtöökoha vahel kindlad edastuskanalid. Selle käigus oleks mõttekas teatud edastuskanalite kasutamine kas välistada või seada neile vastavad miinimumnõuded. Näiteks võib kaugtöötajale teha ettekirjutuse, et konfidentsiaalset infot sisaldavaid paberdokumente tohib tööandja juurest kaugtöökohta transportida ainult otseteid pidi, kasutades lukustatud transpordikaste. Samuti võib töötajat kohustada kasutama erineva konfidentsiaalsusastmega info edastamisel erinevaid krüpteerimisprotseduure. Sarnaseid meetmeid tuleks kaaluda ka siis, kui kaugtöö raames töödeldavat informatsiooni on ilmtingimata tarvis kaitsta ka manipulatsioonide eest.

Täiendavad kontrollküsimused:

- Kas kaugtöökoha puhul on läbi viidud nõuete analüüs?
- Kas kaugtöökoha jaoks väljatöötatud nõudmised kooskõlastati ka IT eest vastutava töötajaga (administraatoriga või mõne muu tehnilise personali liikmega)?

- Kas kaugtöö raames töödeldava info puhul on tuvast atud ja dokumenteeritud selle kaitsevajadus?

M 2.242 Elektroonilise arhiveerimise eesmärkide määratlemine

Algatamise eest vastutavad: IT turvaosakond, ametiasutuse/ettevõtte juhtkond
Rakendamise eest vastutavad: IT turvaosakond

Elektroonilise arhiveerimise juurutamiseks tuleb institutsiooni raames sõnastada arhiveerimisega seotud eesmärgid. Selleks tuleb protsessi kaasata ka organisatsiooni juhatajad. Vajaduse korral tuleb tööd koordineerida ka struktuuris kõrgemal asuvate organisatsiooniüksustega.

Eriti oluline on kindlaks määrata:

- milliseid andmeid tuleb eri valdkondades arhiveerida,
- milline turbeaste on tarvis saavutada,
- millised on soovitud funktsioonid ja selleks vajaminev jõudlus ning
- kes on vastutav.

Eesmärkide dokumenteerimine arhiveerimiskontseptsioonis
Tulemused tuleb dokumenteerida arhiveerimise kontseptsioonis (vt M 2.243 Arhiveerimiskontseptsiooni väljatöötamine).

Milliseid andmeid tuleb arhiveerida?
Arhiveeritavate andmeliikide määratlemist on tarvis arhiveerimissüsteemi tehniliste nõudmiste piiritlemiseks. Nõudmiste piiritlemine peaks olema siiski võimalikult üldistav ja jätma tehnilise teostuse jaoks piisavalt mänguruumi, sest tuleb arvestada, et vajadused võivad aja jooksul muutuda.

Üldistav lähenemine on eriti oluline juhtimistasandi puhul, näiteks:

- kõik ühe osakonna andmed/dokumendid,
- kõikide töö- ja äriprotsesside andmed/dokumendid,
- kõik töö- ja äriandmed,
- kõik raamatupidamisandmed,
- kõik kliendiandmed ja
- kõik tundlikud andmed.

Turbeastmega arvestamine
Erineva kaitsevajadusega andmete arhiveerimisel soovitatakse määratleda arhiveerimise eesmärgid ja nõuded iga vastava turbekategooria kohta eraldi. Arhiveerimise erinevad turbekategooriad võivad moodustuda näiteks dokumentide liigitusest, nagu avalik kasutus, sisekasutus ja salastatud.

Millist turbeastet soovitakse saavutada?
Juhatuse tasandil on arhiveerimisel eesmärgiks seatavat turbeastet võimalik määratleda järgmiselt:

- seadustest tulenevate ja organisatsioonisiseste andmekaitsenõuete täitmine nii andmete arhiveerimisel kui ka muudes valdkondades (nt andmekandjate utiliseerimisel),
- andmekaitseprotsesside manipuleerimiskindlus,
- kasutatava arhiveerimissüsteemi vastupanuvõime salvestatud andmete ja IT-süsteemide vastu suunatud sisemistele ja väljast tulevatele rünnetele.
- Esitatud klassifikatsiooni võib kasutada ka andmete ja dokumentide salastamise puhul turbeastmete täpsemaks eristamiseks.

Milliseid funktsioone ja millist jõudlust soovitakse kasutada?
Elektrooniliseks arhiveerimiseks vajalikud funktsioonid ja jõudlus võivad organisatsioonide lõikes suuresti erineda.

Juhatuse tasandil seatakse üldjuhul eesmärgiks järgmiste nõuete täitmine:

- arhiveerimise integreerimine olemasoleva IT-süsteemi keskkonnaga,
- arhiveerimise integreerimine olemasolevate IT- ja dokumendihaldusprotsessidega,
- andmetele kehtestatud (seadustest tulenevate ja organisatsioonisiseste) salvestus- ja kustutustähtaegade järgimine,
- väljavahetamise tingimused ja hankekorraldusnõuete järgimine.

Eriti on sellest puudutatud avalik haldus, sest olenevalt tegevusalast võib asutusel olla kohustus saata ühiskondlikult, poliitiliselt või ajalooliselt olulised andmed teatud säilitusaja möödudes edasi vastutavale arhiivile. Andmed võib lõplikult kustutada alles pärast seda, kui arhiivilt on saadud kinnitus, et kõnealuseid andmeid ei ole tarvis arhiveerida. Paljudel juhtudel saab andmete arhiveerimisväärtuse üle otsustada alles pärast säilitusaja möödumist, mis tähendab, et säilitusaja möödumisel ei ole andmeid alati võimalik automaatselt töödelda.

Migreerimisvõime

- arhiveerimissüsteemi migreerimisvõime, kui nõuded ja mõjufaktorid peaksid muutuma.

Vastutusala
Elektroonilise arhiveerimise ülesehitamiseks ja käitamiseks tuleb määrata töötajate vastutusalad. Üldjuhul määrab juhatus arhiveerimise eest vastutavaks kas IT-osakonna või selle juhi. Vastutuse määramisel peab arvestama, et töötajaid tuleb teavitada ka seatud eesmärkidest, neile tuleb anda tööks vajalikud volitused ning tagada piisav personali- ja finantsressurss. Ülesannete delegeerimine tuleb määratleda organisatsioonisiseste eeskirjade kohaselt ja fikseerida kirjalikult arhiveerimiskontseptsioonis.

Kontrollküsimused:

- Kas arhiveerimiskontseptsioonis on loetletud kõik arhiveerimisele kuuluvad andmeliigid?
- Kas arhiveeritavate andmete puhul eesmärgiks seatud turbeaste on määratletud?
- Kas elektrooniliseks arhiveerimiseks vajalikud funktsioonid ja jõudlus on määratletud?
- Kas arhiveerimise vastutusalad on määratud ja kirjalikult fikseeritud?

M 2.243 Arhiveerimiskontseptsiooni väljatöötamine

Algatamise eest vastutavad: IT turvaosakond,
Rakendamise eest vastutavad: IT turvaosakond, arhiivi haldaja

Arhiveerimissüsteemi ülesehitust tuleb hoolikalt planeerida. Siinkohal tuleb ühelt poolt arvestada paljude mõjuritega (nt organisatsioonisiseste või seadustest tulenevate ettekirjutuste või tehniliste ja organisatoorsete raamtingimustega) ning teiselt poolt seista silmitsi tõsiasjaga, et elektroonilise arhiivi loomiseks võib kasutada väga palju erinevaid tehnilisi lahendusi. Seetõttu tuleks esmalt välja töötada kontseptsioon, mis looks ülevaate kõigist mõjuritest ja kriteeriumitest, mille alusel konkreetset arhiveerimissüsteemi luua ja selleks vajalikke tooteid soetada, samuti peaks kontseptsioon arvestama kuludega ja olema võimalikult ökonoomne. Arhiveerimiskontseptsiooni aluseks on meede M 2.242 Elektroonilise arhiveerimise eesmärkide määratlemine .

Arhiveerimiskontseptsioon peab määratlema arhiveerimissüsteemi tehnilise ja organisatoorse kasutuse, näiteks:

- pädevused ja vastutusalad,
- kasutajarollide määramine (nt arhiivi haldaja, administraatorid, kasutajad, tehnilised kasutajad),
- pääsuõiguste määramine ja tingimuste sõnastamine õiguste andmisteks,
- arhiveerimisele kuuluvate andmete piiritlemine,
- arhiveeritud andmete turve, nt krüpteerimine ja digitaalsed allkirjad,
- soovitatav süsteemiga ühendamise viis ehk arhiveerimiskomponentide kasutustingimused,
- arhiivisüsteemi tehniline teostus,
- arhiivisüsteemi käitamine, nt teenusetasemelepete (service level agreement) kirjeldus.

Kontseptsioon tuleb kirjalikult dokumenteerida
Tulemused tuleks dokumenteerida selliselt, et neid oleks võimalik värskendada ja täiendada. Arhiveerimiskontseptsiooni tuleks säilitada kõikides rakendatud versioonides. Töötajaid tuleb kontseptsioonist nende vastutusalade piires teavitada. Teavitamine tuleks dokumenteerida, et seda oleks võimalik üle kontrollida.

Järgnev arhiveerimiskontseptsiooni sisukord on toodud näitena kontseptsiooni ühe võimaliku ülesehituse kohta:
Arhiveerimiskontseptsiooni sisukord
1. Dokumendi kontekst

- Reguleerimisala
- Pidev mugandamine
- Rakendamise korraldus

2. Definitsioonid

- Arhiveerimine, dokumentide mõisted
- Pikaajaline arhiveerimine, arhiveerimine auditi tarbeks
- Rakendusvaldkonna ja arhiveerimissüsteemi kirjeldus

3. Vastuvõtlikkus ohtudele ja motivatsioon

- Institutsiooni sõltuvus andmete kättesaadavusest
- Loetelu tüüpilistest ohtudest, nagu andmekadu, rekonstrueerimisvead jt
- Institutsiooni puudutavate kahjude põhjused
- Näiteid seni esinenud kahjudest

4. Organisatsioonisisese turvasuunise määratlemine

- Vastutusalade defineerimine
- Eesmärgipüstitus: turbeaste

5. Mõjufaktorite kirjeldus

- Arhiveeritavate andmete identifitseerimine
- Andmete konfidentsiaalsusnõuded
- Andmete tervikluse nõuded
- Andmete autentsuse nõuded
- Andmete kättesaadavuse nõuded
- Seadustest tulenevad raamtingimused
- Arhiveerimistähtajad (salvestiste minimaalne, vajaduse korral ka maksimaalne hoiuaeg)
- Jõudlusele esitatavad nõudmised andmete sisselugemisel, lugemisel; rekonstrueerimise keerukus
- Andmemaht ja muutmise maht
- Andmeliigid (formaadid)
- Arhiveeritud andmete juurdepääsude liigid (kohapeal või jagatud koht- või laivõrgus)
- Kohustuslikud normid ja standardid
- Vajaminevad funktsioonid
- Vajalik personaliressurss
- Kulutused koos täiendavate kuludega (hooldus, haldamine, täiendid jms)
- Kasutajatelt eeldatavad teadmised ja spetsiaalsed IT-kvalifikatsioonid

6. Kasutusala defineerimine

- Arhiveerimissüsteemi liik
- Arhiveerimissüsteemi kasutustingimused
- Kasutusaeg
- Vastutavate töötajate nimetamine
- Teenusetasemelepete määratlemine

- Personali puudutavate meetmete rakendamine (koolitamine, asendamise korraldamine, kohustused, rollijaotus)
- Kasutustingimuste ja konfiguratsiooni dokumenteerimine
- Koostalitlusvõime, standardne ühilduvus, investeeringukindlus
- Regulaarne andmevarundus
- Viirusetõrje
- Krüptoprotseduuride rakendamine

7. Arhiveerimise raamtingimused

- Lepingutingimused
- Salvestite värskendustsüklid
- Inventari loetelu
- Andmete kustutamine
- Defektsete andmekandjate hävitamine
- Funktsioneerivate lugemisseadmete varu hoidmine

8. Pistelised taastamisharjutused
Kõnealuse kontseptsiooni mõningaid aspekte käsitletakse veel ka järgmistes meetmetes:

- M 2.242 Elektroonilise arhiveerimise eesmärkide määratlemine
- M 2.244 Elektroonilise arhiveerimise tehniliste tegurite väljaselgitamine
- M 2.245 Elektroonilise arhiveerimise õiguslike tegurite väljaselgitamine
- M 2.246 Elektroonilise arhiveerimise organisatsiooniliste tegurite väljaselgitamine

Arhiveerimise kontseptsiooni regulaarne läbitöötamine
Elektrooniline arhiveerimine ei ole mitte ühekordne ettevõtmine, vaid pigem dünaamiline protsess. Seetõttu tuleb arhiveerimiskontseptsiooni regulaarselt ajakohastada.

Kontrollküsimused:

- Kas arhiveerimiskontseptsioon on siduvalt määratletud?
- Kas olemasolev arhiveerimiskontseptsioon kajastab hetkeolukorda?
- Kas töötajaid on nende vastutusalade piires kontseptsioonist teavitatud?
- Kas kontseptsiooni ajakohasust kontrollitakse regulaarselt?
- Kas mõjurite muudatused integreeritakse esimesel võimalusel?

M 2.244 Elektroonilise arhiveerimise tehniliste tegurite väljaselgitamine

Algatamise eest vastutavad: IT turvaosakond
Rakendamise eest vastutavad: IT turvaosakond, arhiivi haldaja

Enne otsuste langetamist konkreetsete arhiveerimisprotseduuride või -toodete kasuks tuleb välja selgitada terve hulk erinevaid tehnilisi mõjureid. Selleks tuleb muu hulgas konsulteerida ka arhiveeritavate andmete omanikega ehk siis näiteks üksikute IT-süsteemide ja IT-rakenduste eest vastutavate töötajatega ning süsteemi administraatoritega. Tulemused tuleb dokumenteerida loetaval kujul arhiveerimise kontseptsioonis (vt M 2.243 Arhiveerimiskontseptsiooni väljatöötamine).

Elektroonilise arhiveerimise jaoks oluliste tehniliste mõjurite hulka kuuluvad muu hulgas järgmised tegurid:

- eeldatavalt tekkiv andmehulk,
- arhiveeritavate dokumentide failiformaadid,
- muudatuste maht ja versioonimine,
- dokumentide säilitusaeg,
- juurdepääsude arv ja liigid,
- olemasolev IT-kasutuskeskkond ning
- kohustuslikud normid ja standardid.

Alljärgnevalt on ära toodud äsjaloetletud mõjufaktorite detailsemad kirjeldused.
Eeldatavalt tekkiv andmehulk

Eeldatavalt tekkiva andmehulga prognoosimine
Elektrooniliste arhiveerimissüsteemide oluline valikukriteerium on arhiveeritavate failide suurus ja tulevikus oodatav andmete hulk. Enamasti on seda võimalik hinnata ainult umbkaudselt. Dokumendifailide suurus sõltub aga suuresti ka failiformaadi valikust ja tõlgenduse (rendition) ulatusest (vt allpool).

Arhiveeritavate dokumentide failiformaadid
Olenevalt arhiveerimissüsteemi valikust võib neis üldjuhul kasutada kõiki levinud failiformaate, nagu nt kontoritöös enimlevinud formaate (DOC, PDF, RTF, ASCII, ZIP jms) või ka graafika- ja helifaile (JPG, GIF, WAV, MPEG jms). Arhiveerimise puhul on olulised failiformaadid, mis võimaldavad pikaajaliselt stabiilselt säilitada dokumendifailides kasutatud süntaksit ja semantikat (nt SGML, XML või ka HTML) ning pildifailid, mis võimaldavad varasemast paberdokumendist loodud kujutist täpselt edasi anda (nt TIFF). Erinevate failiformaatide täpsema kirjelduse leiate meetmest M 4.170 Dokumentide arhiveerimiseks sobivate andmevormingute valimine .

Dokumente tuleb arhiveerida erinevates formaatides
Elektroonilise arhiveerimise raames on suutnud ennast õigustada erinevad failiformaadid, mille sobilikkus tulevikus kasutamiseks on siiski erinev. Tihti ei ole tule-

vast kasutusotstarvet kas võimalik määrata või taheta selle määramisega tekitada liigseid piiranguid. Sellistel juhtudel ei ole võimalik ette ennustada, milline on parim failiformaat tuleviku tarbeks. Tihti eksisteerivad ka juba andmete salvestamise hetkel failiformaadi valiku puhul konkureerivad nõudmised, mis tulenevad andmete erinevatest kasutuseesmärkidest. Seetõttu on osutunud otstarbekaks, eriti just pikaajalise arhiveerimise puhul, andmete arhiveerimine korraga erinevates failiformaatides. Arhiveeritavad dokumendid tuleb selleks eelnevalt konvertida. Seda tegevust nimetatakse tõlgenduseks. Tõlgenduse käigus tuleb tingimata jälgida, et protseduur dokumenteeritaks täpselt. Originaalformaati kajastav info tuleb arhiveerida koos dokumendiga. Dokumentide tõlgendamine ja nende salvestamine mitmes failiformaadis mõjutab otseselt arhiveerimiseks vajalikku mäluruumi.

Muudatuste maht ja versioonimise ulatus
Dokumentide arhiveerimise puhul tuleks kaaluda, milliseid muudatusi võib dokumentatsioonis aja jooksul ette tulla, kui tihti tuleks muudatustega arvestada ja kuidas nendega ümber käia. Arhiveeritud dokumentide muutmiseks on järgnevad võimalused:

- Algse dokumendi asendamine muudetud dokumendiga.
- Versioonimine – dokumendi uue versiooni arhiveerimine paralleelselt algdokumendiga (versioonimine), mille puhul võidakse kehtestada piiranguid dokumendi erinevate arhiveeritud versioonide arvule (arhiveerimisulatusele). Dokumentide versioonimise vajadus võib tekkida organisatsioonisisestest või seadustega ettekirjutatud nõuetest (vt M 2.245 Elektroonilise arhiveerimise õiguslike tegurite väljaselgitamine ja M 2.246 Elektroonilise arhiveerimise organisatsiooniliste tegurite väljaselgitamine). Versioonimist võib tekitada ka salvestusvahendi valikuga (nt ainukirjutusega andmekandja).

Dokumentide säilitusaeg
Arhiveerimissüsteemi jaoks hädavajalikku mäluruumi kalkuleerides on arhiveeritavate dokumentide säilituskohustuse hindamine vältimatu. Säilituskohustuse miinimum- ja kohati ka maksimumnõuded tulenevad kas seadustest või organisatsioonisisestest eeskirjadest ning neid tuleb järgida. Säilitusaja pikkus ei mõjuta mitte ainult arhiveerimissüsteemi mäluruumi, vaid ka andmekandja valikut ning selle utiliseerimist pärast säilitusaja lõppemist.

Juurdepääsude arv ja liigid
Arhiivisüsteemi juurdepääsude arv ja liigid mõjutavad arhiveerimisserveri konfiguratsiooni ja salvestuskomponentide valikut.

Seetõttu tuleb välja selgitada järgnevad mõjurid:

- Kui palju luuakse arhiivisüsteemiga ühendusi teatud kindlas ajavahemikus?
- Kui suure osakaalu moodustavad loodud ühendustest kirjutuspääsud ja lugemispääsud?
- Milline on eesmärgiks seatud reaktsiooniaeg?
- Kas kasutaja- või klientsüsteemidest luuakse ühendused arhiivisüsteemiga otse või läbi hierarhias kõrgemal asetseva dokumendihaldussüsteemi?

- Kas arhiivisüsteem peab suutma erinevate juurdepääsude vahel vahet teha või tegelevad sellega hoopis hierarhias kõrgemal asetsevad komponendid?

Klientide teenindamis-võime (multi-client capability)

- Kas arhiivisüsteem peab suutma hallata mitut üksteisest lahutatud arhiivi (multi-client capability)?

IT-kasutuskeskkond

Üldjuhul on arhiivisüsteemid integreeritud keerukamatesse IT-kooslustesse. Sellest tulenevalt tekivad spetsiaalsed tehnilised nõuded:

- võrguühendusele,
- võrguprotokollidele (nt kui sideühendus kulgeb läbi tulemüüride, peab teada olema protokollide definitsioon),
- ühilduvusele seoses teiste programmide ja IT-süsteemidega,
- ühendamisvõimele süsteemihalduskeskkonnaga, seda nii arhiivisüsteemi administreerimiseks kui ka seireks,
- administreerimis- ja kasutusliidestele ning
- arhiivisüsteemi reaktsiooniaegadele.

Kohustuslikud normid ja standardid

Arhiveerimisalased standardid keskenduvad järgmistele valdkondadele:

- failiformaadid ja pakkimisprotseduurid,
- andmekandjad ja nende salvestusprotseduurid ning
- dokumendihalduse tarkvara.

Planeerimise ja investeeringukindlus

Standardiseerimisprotsessi raames tootjate liideste kohta avaldatud info annab süsteemitootjatele võimaluse omavahel ühilduvate süsteemikomponentide, liideste ja andmeformaatide loomiseks. Arhiivisüsteemide valimisel tuleks arvesse võtta standardeid, sest nendega on võimalik suurendada planeerimisprotsessi ja investeeringu garantiisid. Moodulis soovitatud meetmete puhul on arvestatud hetkel kehtivate standarditega. Kasutaja jaoks toob standardite tundmine endaga kaasa väiksema sõltuvuse konkreetsetest tootjatest, süsteemi tarnijatest ja teenusepakkujatest. Standardite tundmine on arhiivisüsteemide puhul oluline ka süsteemi pika kasutusea tõttu, kuna pikemas perspektiivis ei ole tootearengut võimalik kindlalt ette ennustada. Probleeme võib tekkida nt ühe kindla tootja salvestuskomponentide eelistamisel, kuna tootja võimaliku maksejõuetuse puhul ei ole süsteemi enam võimalik senisel moel uute andmekandjate ja salvestuskomponentide juurde ostmisega laiendada. Suure arhiveerimisvajadusega ametiasutustes ja ettevõtetes võib niisugune olukord tähendada, et kiirkorras tuleb algatada üleviimine. Standardsete komponentide puhul seevastu saab sarnases olukorras lihtsalt üle minna mõne teise tootja osakomponentide kasutamisele. Standardite puhul tuleb siiski jälgida, et kehtivad standardid võivad aja jooksul tänu tehnika arengule muutuda ning vajaduse korral asendatakse ka vanad standardid uutega. Mõnikord

võivad väliselt ainult erineva versiooninumbriga tähistatud standardid olla oma sisu poolest täiesti erinevad. Lisaks on erinevad standardiseerimiskomiteed ja tootjad omavahel pidevas konkurentsivõitluses eesmärgiga saavutada võimalikult suur turuosa ning seetõttu leidub ka omavahel konkureerivaid standardeid.

Hooldus ja tugi

Arhiveerimist on põhimõtteliselt võimalik sisse seada ka ilma konkreetseid standardeid järgimata, kasutades mõne kindla tootja faili- ja salvestusformaate, eeldusel, et tootja pakub kogu arhiveerimisaja vältel piisavas mahus hooldust ja tuge ning garanteerib liideste ümberkorraldamise, kui nõuded peaksid muutuma.

Eespool nimetatud põhjustel on arhiivisüsteemide planeerimisel siiski soovitatav lähtuda võimalikult täpselt kehtivatest standarditest ja failiformaatidest. Üleviimisvajadusega tuleks arvestada juba arhiivisüsteemi planeerimisfaasis, sest andmete pikaajalise salvestamise käigus võivad aeg-ajalt muutuda nii tehnika kui ka nõuded. Erilist tähelepanu tuleks seetõttu pöörata liideste, failiformaatide ja indeksiandmebaaside valikule ning asjaolule, et langetatud otsused saaksid arusaadavalt dokumenteeritud.

M 2.245 Elektroonilise arhiveerimise õiguslike tegurite väljaselgitamine

Algatamise eest vastutavad: IT turvaosakond
Rakendamise eest vastutavad: IT turvaosakond, arhiivi haldaja

Andmete säilitamist reguleerivad mitmed seadused, mille eiramine võib endaga kaasa tuua nii tsiviil- kui ka karistusõiguslikke tagajärgi. Seetõttu peaksid vastutavad töötajad välja selgitama, milliseid õiguslikke eeskirju tuleb järgida konkreetse projekti puhul. Eeskirjadest tulenevad erinevad nõudmised, mida peab järgima elektroonilise arhiveerimise juurutamiseks vajamineva arhiveerimise kontseptsiooni koostamisel.

Muu hulgas on sellest puudutatud järgnevad valdkonnad:

- maksudest, eelarvest või muudest tingimustest sõltuv minimaalse säilitusaja pikkus,
- andmekaitsenõuetest tulenev maksimaalse säilitusaja pikkus,
- välistele osapooltele, nt maksuametile antavad pääsuõigused ning
- digitaalallkirjade kvaliteet.

Seadustest tulenevad eeskirjad tuleb välja selgitada iga juhtumi puhul eraldi. Olenevalt organisatsiooni eripärast võivad kehtida veel ka muud seadustest tulenevad või organisatsioonisisesed eeskirjad (nt sotsiaalkindlustusele, haiglatele, farmaatsiatööstusele, sõjaväele või pangandusele kehtivad eeskirjad), mis tuleb iga konkreetse juhtumi puhul eraldi välja selgitada. Olulisemate reguleeritud valdkondade alla kuuluvad tavaliselt säilitusaja pikkus ning konfidentsiaalsus- ja terviklusnõuded, kusjuures kahe viimase puhul käsitletakse lisaks tugevusele ka kaitsevajaduse kestvust. Avaliku halduse jaoks kehtib lisaks eelmainitule seadusest tulenev kohustus, et vastutavatele arhiividele tuleb olemasolevaid dokumente pakkuda ka digitaalsel kujul (pakkumiskohustus).

M 2.246 Elektroonilise arhiveerimise organisatsiooniliste tegurite väljaselgitamine

Algatamise eest vastutavad: IT turvaosakond

Rakendamise eest vastutavad: IT turvaosakond, arhiivi haldaja

Elektroonilist arhiveerimist mõjutab terve hulk organisatsioonilisi tegureid, millega peab arhiveerimise kontseptsiooni koostamisel arvestama. **Muu hulgas kuuluvad nende hulka järgmised:**

- arhiivisüsteemi kasutusaeg,
- arhiveeritava materjali säilitusajad,
- andmete konfidentsiaalsusnõuded,
- andmete käideldavusnõuded,
- andmete terviklusnõuded,
- andmete autentsusnõuded,
- vastuvõetavate reaktsiooniaegade määramine,
- rekonstrueerimise keerukus,
- vajalik personaliressurss,
- kasutajatelt eeldatavad teadmised ja spetsiaalsed IT-kvalifikatsioonid,
- arhiivisüsteemi ergonoomilisus ja kasutajasõbralikkus,
- standardite järgimine ja
- finantsilised raamtingimused.

Alljärgnevalt on ära toodud äsjaloetletud mõjurite detailsemad kirjeldused.

Arhiivisüsteemi kasutusaeg

Komponentide kasutusiga

Arhiivisüsteemi kasutusiga tuleb planeerida arhiveerimise kestvusest eraldi. Väljavalitavale süsteemile tuleb anda hinnang, kui kaua peaks vastav süsteem olema kasutamisvõimeline, ning selle hinnanguga tuleb arvestada komponentide valikul, et langetada otsus just selliste komponentide kasuks, mis peaksid suutma tagada vajaliku kasutusea. Pikk arhiveerimine eeldab, et valik langetatakse pika kasutuseaga IT-komponentide ning vajalike teenindus- ja tarnelepingute kasuks, mis on üldjuhul tavatingimustega võrreldes kallimad. Lühike arhiveerimisaeg tähendab, et arhiiv tuleb suhteliselt lühikese aja möödudes uuele arhiivisüsteemile üle viia.

Arhiveeritava materjali säilitusajad

Arhiveerimissüsteemi jaoks hädavajalikku mäluruumi kalkuleerides on arhiveeritavate dokumentide säilituskohustuse hindamine vältimatu. Säilituskohustuse miinimum- ning kohati ka maksimumnõuded tulenevad kas seadustest või organisatsioonisisestest eeskirjadest ning neid tuleb järgida. Säilitusaja pikkus ei mõjuta mitte ainult arhiveerimissüsteemi mäluruumi, vaid ka andmekandja valikut ja selle utiliseerimist pärast säilitusaja lõppemist.

Andmete konfidentsiaalsusnõuded

Konfidentsiaalsusnõuete määramisel tuleb ennekõike arvestada asjaoluga, et arhiveerimise jooksul võivad konfidentsiaalsusnõuded muutuda. Tegu võib olla nt

majanduslike või juriidiliste mõjuritega. Reeglina võib siiski oletada, et aja möödudes arhiveeritava materjali konfidentsiaalsusnõuded vähenevad. Vajadus tagada pikaajaline konfidentsiaalsus mõjutab arhiveerimiskontseptsiooni organisatoorset poolt (vt M 2.264 Krüpteeritud andmete regulaarne regenereerimine arhiveerimisel) ja tehniliste komponentide valikut.

Andmete käideldavusnõuded

Elektroonilist arhiveerimist rakendatakse üldjuhul andmete ja dokumentide pikaajaliseks säilitamiseks. Üks peamisi nõudeid on siinkohal juba eelnevates punktides nimetatud arhiveeritud dokumentide säilituskohustuse pikkus. Lisaks säilitusajale tuleb määrata täiendavad käideldavusnõuded, milleks on nt arhiivisüsteemi rikkekindlus ja kasutatavate andmekandjate stabiilsus.

Andmete tervikluse nõuded

Elektrooniliselt arhiveeritud dokumentide terviklus peab üldjuhul olema tagatud ka pärast pika arhiveerimisaja lõppemist, samuti peab terviklust olema võimalik kontrollida. Siinkohal tuleb arvestada eriti sellega, et kontrollimise ajaks ei pruugi ei algdokumente ega ka täiendavat kontekstiinfot enam olemas olla, mistõttu peab tervikluse tagama arhiivisüsteem ise. Lisaks terviklusele esitatavate nõuete klassifitseerimisele (nt madal kuni keskmine, kõrge või kõrgeim) tuleb määrata, millise aja jooksul peab olema võimalik terviklust kontrollida.

Andmete autentsusnõuded

Sarnaselt terviklusega tuleb määrata ka autentsuse tagamise vajadus ja aeg, mille vältel peab olema võimalik kontrollida dokumentide autentsust. Ka selle valdkonna puhul võib eeldada, et pikema arhiveerimisaja möödudes ei pruugi ei algdokumente ega ka täiendavat kontekstiinfot enam olemas olla. Autentsuse kontrollimisvõimalus tuleb seega tagada arhiveerimisprotsessiga.

Vastuvõetavate reaktsiooniaegade määramine

Arhiivisüsteemile esitatud päringu ja sellele vastuse saamise vahel tekib teatud viivitus (reaktsiooniaeg). Tavaliselt määratakse nimetatud viivituse pikkus kindlaks eesmärgiks seatava keskmise ja maksimaalselt lubatud reaktsiooniaja defineerimisega.

Reaktsiooniaja määramisel tuleb arvestada erinevate teguritega, muu hulgas järgmistega:

- arhiivisüsteemi päringule reageerimiseks kuluv aeg,
- arhiivisüsteemi salvestuskinnitusele kuluv aeg ning
- soovitud dokumendi täielikuks klientsüsteemi ülekandmiseks kuluv aeg.

Vajalik reaktsiooniaeg sõltub suurel määral konkreetsest kasutusvaldkonnast. Näiteks reisijate teenindamisel lennujaamades võib aktsepteeritav reaktsiooniaeg jääda mõne minuti piiresse. Kinnistusraamatu vanade arhiiviandmete päringu puhul seevastu võib vastuvõetav reaktsiooniaeg jääda tööpäevadel nt tunni piiresse.

Subjektiivsed nõuded

Üldjuhul tekivad reaktsiooniaegadele ka teatud subjektiivsed nõuded. Näiteks päringute või arhiveeritud dokumentide puhul võidakse pikka reaktsiooniaega pidada palju ebameeldivamaks võrreldes sama pika reaktsiooniajaga, mis kulub arhiivile edastatud dokumentide salvestuskinnituse saamiseks. Reaktsiooniaegadele seatavad nõuded tuleb välja selgitada ja dokumenteerida.

Rekonstrueerimise keerukus

Tuleb määrata, milline aja ja tehniliste ressursside kulu on vastuvõetav arhiveeritud dokumentide leidmiseks ja kasutusvalmis seadmiseks. Need nõuded sõltuvad arhiveeritud andmete liigist ja struktuurist, seega konkreetsest kasutusvaldkonnast.

Vajalik personaliressurss

Arhiivisüsteemi käitamiseks vajaliku personali suurus on arhiivisüsteemi valimisel määrava tähtsusega. Organisatsiooni põhjal tuleks välja selgitada, kui palju on võimalik palgata täiendavat personali ning kui palju on iga töötaja võimeline taluma töökoormuse kasvu, mis oleks seotud arhiveerimisega. Nimetatud tegur mõjutab otseselt personali planeerimist, sest olenevalt olukorrast võib arhiveerimiseks vaja minna täiendavat personali. Ametisse tuleb nimetada töötajad, kes täidaksid vähemalt järgmisi töörolle: arhiivi haldaja, arhiivi administraator ja (tehniline) kasutaja. Piisava personaliressursi puudumisel tuleb puuduvad töötajad kompenseerida väliste hooldus- ja teenusetasemelepingutega.

Kasutajatelt eeldatavad teadmised ja spetsiaalsed IT-kvalifikatsioonid

Arhiivisüsteemi sobivate kasutajaliideste valikut mõjutavad muu hulgas ka planeeritavate kasutajate eelteadmised. Tuleks uurida, millised on kasutajate IT-alased teadmised. Teadmised mõjutavad ka arhiveerimisega veidi kaudsemalt seotud teenuste kujundamist, nt kasutajatoe (helpdesk) organiseerimist.

Kasutajate koolitamine

Väärkasutustest tingitud kahjude minimeerimiseks peavad kõik kasutajad läbima ilmtingimata arhiivisüsteemi kasutamist käsitleva koolituse. Lõpphinna kalkuleerimisel tuleb seega arvestada ka vajalike koolituste maksumusega.

Arhiivisüsteemi ergonoomilisus ja kasutajasõbralikkus

Kasutajasõbralikkus on määrava tähtsusega arhiivisüsteemi aktsepteerimiseks kasutajate poolt ning aitab tagada arhiivisüsteemi korrakohast kasutamist.

Pilootprojektid ja installeerimine testimise eesmärgil

Lisaks töökoha ergonoomilisuse seadustest tulenevatele nõuetele tuleb arvestada ka kasutajate subjektiivse muljega. Subjektiivsete omaduste väljaselgitamiseks võib tulevaste kasutajate hulgas korraldada näiteks küsitluse, kuid samas tuleks arvestada ka arhiivisüsteemi komponentide pilootprojektide ja testimiste raames saadud kogemustega.

Standardite järgimine

Investeeringukindlus

Toodete ja organisatsiooniliste tööprotsesside koostalitusvõime tagamiseks tuleks tähelepanu pöörata sellele, et valitaks niisugused arhiivisüsteemi komponendid, millel oleks kehtivate standardite tugi. Vaatamata sellele, et standardite eluiga

ei ole väga pikk, kuna tehnilise arengu tõttu kehtestatakse üha uusi standardeid, peetakse levinud standardite tuge siiski investeerigu garantiiks. Loomulikult sõltub see ka konkreetsest kasutusvaldkonnast ja -keskkonnast. Seetõttu tuleks iga juhtumi puhul eraldi uurida, millised on olulisemad standardid. Mõningaid olulisi tehnilisi standardeid käsitletakse meetmetes M 4.169 Sobiva arhiveerimisandmekandja valimine ja M 4.170 Dokumentide arhiveerimiseks sobivate andmevormingute valimine .

Finantsilised raamtingimused

Arhiivisüsteemi juurutamist ja vajaliku organisatoorse raamistiku loomist mõjutavad harilikult järgmised kulud:

- ühekordsed investeeringud,
- jooksvad kulud, kaasa arvatud personalikulud,
- litsentsitasud.

Arhiivisüsteemi käitamise planeerimine käib seetõttu käsikäes finantside planeerimisega. Siinkohal tuleb arvestada organisatsioonisiseste eeskirjadega (eelarve planeerimine, kulude jaotamine jms). Arhiveerimisega seotud kulutuste lõppsumma kalkuleerimisel tuleb sisse planeerida ka kasutajate ja administraatorite koolitusega seotud kulud.

M 2.247 Exchange/Outlook 2000 kasutamise planeerimine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: IT-turvaosakond, administraator

Enne Exchange/Outlook 2000 juurutamist tuleb otsustada, millistes valdkondades hakatakse süsteemi kasutama. Kasutusvaldkonnast sõltub vajamineva serveri valik, nt kas Exchange 2000 Enterprise Server või Exchange 2000 Conferencing Server , samuti määrab see planeerimistööde liigi ja mahu. Planeeritavast kasutusvaldkonnast sõltub suuresti ka kehtestatav turvasuunis. Tugevalt üldistades võib siinkohal eristada kolme Exchange-serverite kasutusvaldkonda:

- Intranet-server ja juurdepääs Outlook 2000 klientide abil. Antud variandi puhul on peamiseks rakenduseks sisekasutus büroo kommunikatsiooni (meilivahetuse, töökohtumise kokkuleppimise, rühmatöö koordineerimise) tagamiseks.
- Intranet-server ja juurdepääs Web-Clients abil. Antud valdkonna peamine rakendusala on brauserite kasutamine juurdepääsuks Exchange-serverile. Kuna Exchange-serveri Web-liidese puhul rakendatakse täiesti teistsuguseid turvamehhanisme, käsitletakse Web-liidese turvalist konfigureerimist eraldi kasutusvaldkonnana.
- Rakendamine demilitariseeritud tsoonis Exchange-serverit võib rakendada ka demilitariseeritud tsooni avaliku juurdepääsuga infoserveri funktsioonides. Antud kasutusvaldkond nõuab serveri paljastatud oleku tõttu suurt tähelepanu süsteemi konfigureerimisel.

Loetletud kasutusvaldkondade raames saab omakorda täiendavalt täpsustada, millist Exchange funktsiooni, mille alla kuulub näiteks sisekasutuse meiliteenus, konverentsifunktsioon, Instant Messaging , LDAP-server või HTML-server, soovitakse kasutama hakata. Loetletud eristamist siinkohal täpsemalt ei käsitleta. Üldjuhul kehtib siiski reegel, et sõltumata funktsiooni valikust tuleb läbi viia eraldi planeerimine, mille käigus arvestatakse ka turbeaspektidega. Mõningate funktsioonide puhul saab rakendada juba olemasolevaid IT-etalonturbekataloogide üldiseid mooduleid, nt B 5.3 Rühmatarkvara . Kasutusvaldkonna planeerimise puhul tuleb üldjuhul arvestada järgmiste aspektidega:

- Integreerimine Active Directory alla - Exchange 2000 on integreeritav Windows 2000 Active Directory (AD) alla. Seetõttu tuleks Exchange 2000 planeerimine kooskõlastada Active Directory planeerimisega (vt M 2.229 Active Directory planeerimine). Exchange 2000 installeerimise käigus toimub Active Directory skeemi täiendamine. Sellega mõjutab Exchange-i installeerimine Active Directory-t püsivalt, mistõttu tuleb protsessi ilmtingimata kaasata ka Windows 2000 süsteemi skeemiadministraator. Lisaks peavad planeerimises osalevatel inimestel olema piisavad teadmised Windows 2000/XP üldise ülesehituse kohta, eriti aga domeenikontrollerite jaotumise ja nn Global Catalog Server-i juurdepääsetavuse kohta.

- Marsruutimisrühmade loomine - Exchange 2000 ja Outlook 2000 kasutuse planeerimisel tuleb otsustada, kas rakendada ka nn marsruutimisrühmade (Routing Groups) loomist. Tegu on Exchange-serverite koondamisega, mis suhtlevad omavahel spetsiaalse ülikiire ühenduse abil. Seda kasutatakse Exchange 5.5 Site-Concept -i (asukohakontseptsiooni) asemel. Lisaks tuleb otsustada ka Exchange-serverite jaotamise üle eraldi administreerimisgruppidesse.
- Partitsioonide loomine - Meiliandmebaasid võib panna erinevatele partitsioonidele ja seeläbi erinevate Exchange-serverite vahel ära jagada. Seeläbi on võimalik erineva kaitsevajadusega meiliandmeid jagada vastaval moel füüsiliselt kaitstud serverite vahel. Vajadustest lähtuv planeerimine võib samas suurendada ka jõudlust ja rikkekindlust. Sama kehtib ka meiliandmebaaside koopiate rakendamisel, mida võib kasutada rikkekindluse suurendamiseks.
- Turvasuunise koostamine - Paralleelselt kavandatava kasutusvaldkonna planeerimisega ja Exchange-serveri jaotamisega tuleb koostada turvasuunised, mis käsitlevad spetsiaalselt Exchange aspekte. Olulised teemakohased aspektid on kokku võetud meetmesse M 2.248 Exchange/Outlook 2000 turvapoliitika määratlemine .
- - Exchange-süsteemi konfigureerimisel lähtutakse Windows 2000/XP süsteemi- ja grupeerimissuunistest. Vastavad seadistused tuleb kooskõlastada Windows 2000/XP üldiste suuniste seadetega (vt l M 2.231 Windowsi grupipoliitika planeerimine ja M 2.326 Windows XP, Vista ja Windows 7 grupeerimissuuniste planeerimine).
- Konnektorite planeerimine - Exchange-süsteemi ühendamiseks võõraste E-Mail/Messaging -süsteemidega, nt X.400 või ccMail-iga saab kasutada nn konnektoreid (connectors), mis on loodud erinevate meilisüsteemide omavaheliseks ühendamiseks. Sujuva meilivahetuse tagamiseks on tarvis konnektorite kasutamist hoolikalt planeerida.
- Bridgehead serverite turvaline käitamine - Võimaldamaks meilide edastamist sisseseatud marsruutimisrühmade kaudu, tuleb planeerida nn Bridgehead Server -ite rakendamine. Kuna reeglina peavad vastavad serverid suhtlema võõraste võrkudega, peaks nende asukoht olema kas demilitariseeritud tsoonis või vähemalt tulemüüri taga (vt B 3.301 Turvalüüs (tulemüür)).
- Klientide juurdepääsuvõimaluste määramine - Outlook 2000 klientide kasutamine, nende juurdepääsuvõimalused Exchange-süsteemile ning vastavate juurdepääsude turvamine on aspektid, mis vajavad planeerimist. Samuti tuleb selgitada, kas MAPI-Client ühendusviisi soovitakse või mitte. Minevikust on teada palju juhtumeid, kus MAPI-liidest kasutati kurjasti ära kahjutekitavate programmide (viiruste, usside jms) levitamiseks.
- Planeerida tuleb Exchange/Outlook 2000 süsteemi administreerimine. Ülesanded ulatuvad siinkohal alates töötajate vastusalade määratlemisest koos organisatsioonisiseste asendamise korraga kuni sobilike administraatorirollide väljatöötamiseni. Vastavates domeenides tuleb sisse seada sobilike õigustega varustatud kasutajarühmad.

- Planeerida tuleb organisatsioonis kasutatavad meilikontod ja uudistegrupid.

- Viirusetõrje - Planeerida tuleb Exchange/Outlook 2000 süsteemi integreeritud viirusetõrjeprogrammi kasutamine. Siinkohal on tarvis otsustada, kas vastavat programmi rakendatakse serveri ja/või kliendi poolel.

- Aktiivsisuga ümberkäimine - Planeerida tuleb järjekindel aktiivsisuga ümberkäimine. Selleks tuleb pärast valdkonnaga seotud eeliste ja puuduste kõrvutamist koostada terve organisatsiooni jaoks ühesed tegutsemisjuhised.

- Eemalviibimistega ümberkäimine - Tuleb otsustada, kuidas kasutatakse „ out-of-office “ teateid, kuna antud funktsiooni kasutamisega on seotud oht, et teatega võidakse väljapoole edastada liiga palju organisatsioonisisest isikutega seotud infot, nt mõne konkreetse töötaja eemalviibimise kohta.

- Planeerida tuleb meilifiltrite kasutamine, mis peaks kaitsma soovimatute meilide (spam mail -ide) eest

- Kalendrifunktsiooni ja ülesannete nimekirja kasutamise puhul tuleb sõltuvalt olukorrast määrata võõraste kasutajate juurdepääsuvõimalused nendele funktsioonidele.

- Planeerimise käigus tuleb arvestada, millised Outlooki kasutajad peavad kasutama ühist arvutit. Sellest sõltuvalt tuleb vastavates arvutites luua kasutajaprofiilid ja need üksteise eest turvaliseks muuta.

- Vajadusel tuleb organisatsioonisiseselt planeerida Chat- , Instant Messaging- , audio- või videokonverentsiteenuste kasutamine.

- Audit ja logimine - Auditeerimise ja logimise kohta tuleb koostada vastav kontseptsioon. Selleks tuleb kindlaks määrata, kuidas soovitakse hakata kasutama Exchange-süsteemi auditeerimist ja logimist. Kui mõni üleettevõtteline auditeerimis- või logimissüsteem on juba kasutuses, tuleb otsustada, kas ja kuidas oleks võimalik Exchange sellega integreerida. Planeerimisse tuleb võimalikult varakult kaasata ka andmekaitse eest vastutav töötaja ning töötajate esindaja, kuna seireprotsesside käigus võidakse kokku puutuda ka isikuandmetega.

- Exchange-süsteemi jaoks tuleb planeerida varunduse (backup) kontseptsioon ja hädaolukorraks valmisoleku kontseptsioon. Selle käigus tuleb ette näha integreerimisvõimalus juba olemasolevate kontseptsioonidega.

- Kui Exchange-süsteemi juurdepääsuks kasutatakse HTTP-d (HyperText Transfer Protocol -i), tuleb arvestada spetsiaalsete turvaaspektidega. Varasemast on teada mitmeid juhtumeid, kus nn OWA-funktsiooni (Outlook Web Access) kasutati (eriti versiooni Exchange 5.5 puhul) ründe sihtmärkidena. Seetõttu peab selle turvalisuse tagamisele ja konfigureerimisele eelnema eriti põhjalik planeerimistöö. Võttes arvesse OWA-funktsioonide turvariske, peab ettevõte või ametiasutus esmalt vastama põhimõttelisele küsimusele, kas vastavat brauseripõhist juurdepääsu tuleks üleüldse kasutada.

-

Otsustades OWA-funktsiooni rakendamise kasuks, tuleb üldjuhul arvestada järgnevaga:

- Tuleb otsustada, millisele infole võimaldatakse juurdepääs, nt avalikele kaustadele (public folders), uudistegruppidele (newsgroups) või ka personaalsele Inbox -ile.
- Exchange -serveri ülesseadmine - Internetist ligipääsetava Exchange-serveri ülesseadmine tuleb hoolikalt planeerida. Siinkohal tuleb pöörata tähelepanu piisavale varjamisele nii seest kui ka väljast. Enamikel juhtudel tuleks väljastpoolt ligipääsetav Exchange-server paigaldada nn demilitariseeritud tsooni.
- Tuleb arvestada, et ilma krüpteerimiseta, näiteks ilma SSLita, võivad kliendi ja serveri vahel liikuvad teated olla kolmandatele osapooltele loetavad. Kliendi ja serveri mõlemapoolse turvalise autentimise tagamiseks tuleb SSLi kasutamine hoolikalt planeerida.

Exchange/Outlook -süsteemi planeerimise võib lõppenuks lugeda alles siis, kui ka niinimetatud roll-out on detailides paika pandud. Viimase puhul määratakse muuhulgas iga Exchange-serveri ja kõikide Outlook-klientide installeerimisjärjekord.

Täiendavad kontrollküsimused:

- Kas rakendatava Windows 2000/XP süsteemi planeerimisel on arvestatud piisavalt vajadustega?
- Kas Exchange-süsteemi planeerimisse on kaasatud ka skeemiadministraator?
- Kas Exchange/Outlook-tarkvara paigaldamiseks on plaan olemas?

M 2.248 Exchange/Outlook 2000 turvapoliitika määratlemine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: IT-turvaosakond, administraator

Sarnaselt kõikide teiste klient-server-süsteemidega, mida asutustes või ettevõtetes juurutatakse, tuleb ka Exchange 2000 serveritele ja Outlook 2000 klientidele koostada omad turvasuunised. Kuna Exchange 2000 on väga suures mahus integreeritav Windows 2000 keskkonda, täpsemalt Windows 2000 Active Directory alla, tuleb siinkohal arvestada Windows 2000 turvasuunisega (vt l M 2.229 Active Directory planeerimine). Exchange/Outlook 2000 turvasuunistega tuleb määratleda:

- Millised on kasutajate pääsuõigused seoses erinevate serveritega ning millised kasutajad ei tohi erinevatele serveritele ligi pääseda (keelunimekirjad).
- Millised on erinevate kasutajate õigused erinevatele meiliandmebaasidele (Mail Store) ligipääsuks.
- Millised ülejäänud serverid võivad luua ühendusi Exchange-serveritega.
- Meilandmebaaside kopeerimistingimused.
- Milliseid meilandmebaaside koostisosi lubatakse kopeerida ning
- Millistest kohtadest tohib Exchange-serveritele ligi pääseda.

Turvasuuniste kehtestamise raames tuleb lisaks arvestada ka järgnevate aspektidega:

- Exchange/Outlooki turvasuunised peavad olema kooskõlas ettevõtte või ametiasutuse üldiste turvasuunistega.
- Tuleb määratleda, millistel juhtudel on tarvis sideühendusi, nt võrgu- või meilisidet turvata (nt brauseri kaudu toimival juurdepääsul või alati kõikide Interneti kaudu toimivate juurdepääsude puhul). Lisaks tuleb määrata, milliseid mehhanisme on turbeks tarvis kasutada.
- Planeerida tuleb Exchange-i administreerimisrühmad, marsruutimisrühmad (Routing Groups), rühmadevahelised juurdepääsuõigused (kasutaja- ja serveripõhised õigused) ning meiliandmebaaside kopeerimine.
- Väljapoole suunatud sideühendustele tuleb kehtestada eraldi turvasuunised. Siinkohal tuleb luua kooskõla juba olemasolevate organisatsiooni füüsiliste või loogiliste piiride kaitseks loodud suunistega.

Turvasuunised tuleb teatavaks teha kõigile kaudselt ja otseselt antud valdkonnaga seotud töötajatele ning kõige sobilikum oleks selleks kasutada organisatsioonisisest koolitust.

Täiendavad kontrollküsimused:

- Kas kõiki olulisi turvasuuniseid on võimalik Exchange/Outlook 2000 valdkonnas ellu rakendada?

- Kas olemasolevaid turvasuuniseid on tarvis muuta?
- Kas uutest või muudetud turvareeglitest informeeritakse kõiki kasutajaid?

M 2.249 Exchange 5.5 serverite Exchange 2000-le üleviimise planeerimine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: IT-turvaosakond, administraator

Praktikas tuleb tihti ette, et täiemahulise reinstalleerimise vältimiseks viiakse olemasolev meilisüsteem hoopis üle uuele süsteemile. Exchange 5.5 on laialt levinud meili- ja sõnumsidesüsteem (messaging system), mistõttu tuleb Exchange 5.5 üleviimist Exchange 2000-le käsitelda tähtsa kasutustsenaariumina.

Laiaulatuslik välimuse muutus

Exchange 5.5 üleviimine Exchange 2000-le tähendab märgatavat hüpet peaaegu kõikides puudutatud valdkondades. Seetõttu ei ole tegemist mitte tarkavara täiendusega, vaid pigem laiaulatusliku muutusega toote välimuses. Üleviimisest ei ole puudutatud mitte ainult Exchange-tarkvara, vaid ka kasutuse aluseks olev operatsioonisüsteem Windows 2000. Exchange 2000 käitamise süsteemieeldusena peab olema installeeritud Windows 2000 server. Seetõttu kaasneb Exchange 5.5 üleviimisega Exchange 2000-le tihti ka Windows NT 4 operatsioonisüsteemi asendamine operatsioonisüsteemiga Windows 2000 ning Active Directory juurutamine.

Integreerimine Active Directory alla

Exchange 2000 on loodud selliselt, et seda oleks võimalik integreerida Windows 2000 Active Directory'ga. Exchange 2000 installeerimise käigus toimub Active Directory niinimetatud skeemi täiendamine. Skeemi muutmine tähendab tõsist sekkumist Active Directory töösse, mida ei ole võimalik tühistada. Seetõttu on ülimalt tähtis, et üleviimise planeerimisse kaasataks Windowsi süsteemiadministraator ja spetsiaalselt ka Active Directory-skeemiadministraator. Active Directory kasutamisel läbi Exchange 2000-e on järgmised mõjud:

- Pääsuloendid (ACL-id) - Pääsuloendid (Access Control Lists) on rakendatavad nii iga üksiku ressursi puhul, nt üksikute avalike kataloogide Item -ite kui ka nende omaduste puhul (Properties).
- Erinevalt Exchange 5.5-st ei kasuta Exchange 2000 enam rollijaotusi, sest turvalisuse aluseks ei ole enam otseselt Information Store. Selle asemel jagatakse Exchange-serveri administreerimisõigused Active Directory vahendusel.
- Security Identifiers - Kasutaja- ja rühmaobjektide SID-sid (Security Identifiers) kasutatakse vastavate Exchange-objektide pääsuloendites. Anonüümsed pääsuõigused seotakse spetsiaalse anonüümse Logon -kontoga. Iga kasutajarühm saab pääsuõigusteks standardsed seadistused.
- Kasutaja-, objekti ja omadustepõhiseid õigusi saab selgelt keelata. Keeldusid kajastavatel seadistustel on õigusi jagavate seadistuste suhtes eesõigus.
- Kerberos - Võrgus kasutatavaks autentimisprotokolliks on Kerberos 5.

Marsruutimisrühmad

Exchange 5.5 puhul veel tavaline Exchange-serverite Site -grupeerimisviis on Exchange 2000 puhul asendatud nn marsruutimisrühmadega (Routing Groups). Sellisel moel kokku koondatud Exchange-serverid võimaldavad suure ribalaiusega andmevahetust. Exchange 2000 puhul rakendatakse varasema RPC (Remote Procedure Calls -i) asemel standardina SMTP-d (Simple Mail Transfer Protocol -i).

Samuti on muudetud Exchange-serveri administreerimist: kui varasemalt piirdus see NT-domeeniga, siis nüüd võimaldatakse vastavate administreerimisõigustega koguni domeeniülest administreerimist terve ühe metsastruktuuri raames.

Partitsioonide ja koopiate loomine

Meiliandmebaaside partitsisoonide loomise ja koopiate tegemise ülesande võtab täielikult enda kanda Active Directory. Juhul kui soovitakse suurendada jõudlust, tuleb siinkohal siiski läbi viia vajaduste planeerimine. Võõrad meilisüsteemid nagu nt X.400 või ccMail ühendatakse Exchange-süsteemiga nn konnektorite abil. Siinkohal vaadeldud üleviimiseks pakutakse ka spetsiaalset konnektorit Exchange 5.5 süsteemi ühendamiseks Active Directory-ga.

Üleviimine tuleb planeerida ja dokumenteerida

Üleviimise üksikud etapid tuleb planeerida võimalikult detailselt, eesmärgiks seatud üleviimisprotsess tuleb dokumenteerida ning muuta kõikidele osapooltele juurdepääsetavaks. Üleviimisprotsessi ülevaate loomiseks võib välja tuua järgmised kohustuslikud etapid:

- Exchange 5.5-süsteemi varukoopia tegemine
- Exchange 2000 tarkvara proovikasutus testimiseks loodud kasutusvaldkonnas
- Windows 2000 Active Directory installeerimine domeenikontrolleritele
- Windows 2000 võrgu ja soovitud teenuste (DNS, DHCP, jne) sisseseadmine
- Windows 2000 Server installeerimine uutele arvutitele (Exchange 2000 serverite kasutamiseks)
- Uute (Exchange 2000 serverite kasutamiseks) mõeldud arvutite lubamine soovitud domeenide liikmeteks
- Exchange 2000 tarkvara installeerimine selleks ette nähtud Windows 2000 serveritele
- Outlook 2000 klientide jaotamine
- Meilifunktsioonidega kasutajakontode loomine
- Vanade meiliandmete paigaldamine. Selle võimaldamiseks võib Exchange 5.5 Serveri jaoks sisse seada vastava konnektori.

Üleviimise planeerimisel tuleb turbeaspektidest lähtuvalt leida vastused järgmistele küsimustele ning järgida järgmisi soovitusi:

- Millised meilikontod ja avalikud kaustad (public folders) tuleb üle viia?
- Kas olemasolev turvasuunis võetakse üle, muudetakse või täiendatakse?
- Kas Active Directory kasutamise kontseptsiooniga on arvestatud ning kas seda on vajadusel täiendatud?
- Milliseid võõraid meilisüsteeme on tarvis ühendada?
- Millised marsruutimis- ja administreerimisrühmad tuleb luua?
- Olemasolevat Exchange 5.5-t tuleks turvata ja vähemalt senikaua kasutuses hoida, kuni Exchange 2000 süsteem on turvaliselt kasutusse võetud.
- Uut tarkvara tuleks testida eraldiseisvas testimisvõrgus.

Terminoloogia muutumine

Üldise tähelepanekuna tuleks arvestada, et Exchange 5.5-e objektide terminoloogia erineb osaliselt Exchange 2000-e terminoloogiast. Näiteks on mõiste Mailbox asendatud mõistega Mail-Enabled User, Distribution List mõistega Distribution or Security Group, Custom Recipient mõistega Contact ning on veel teisigi muudatusi.

Täiendavad kontrollküsimused:

- Kas üleviimise planeerimisse kaasati ka Windows 2000 süsteemiadministraator?
- Kas Active Directory puhul vajalikud eesseisvad skeemimuudatused on dokumenteeritud?
- Kas üleviimise raames on planeeritud ka süsteemi ja andmete varukoopia tegtegemine?

M 2.250 Väljasttellimise strateegia määramine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond
Rakendamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, spetsialist

Koostöö välise teenusetarnijaga on pikaajaline ning alguses kindlasti seotud ka suuremate kulude ja riskidega. Väljasttellimise põhjalik planeerimine on seega ülimalt oluline. Lisaks majanduslikele, tehnilistele ja organisatoorsetele raamtingimustele tuleb siinkohal arvestada ka turvalisust puudutavate aspektidega.

Kaaluda tuleks järgnevaid punkte:

- ettevõtte strateegia (paindlikkus, sõltuvus teistest, edasised plaanid),
- teostatavuse uuring ja raamtingimuste koostamine,
- majanduslikud aspektid ja tasuvusanalüüs.

Pärast esmaseid strateegilisi kaalutlusi tuleb selgeks teha, milliste ülesannete ja IT-rakenduste puhul võiks väljasttellimist kaaluda.

Vastutus
Üldjuhul vastutab teenuste ja toodete kvaliteedi eest klientide või ametiasutuste ees siiski teenuse pakkuja, olenemata asjaolust, et osad tema pakutavad teenused tellitakse väljast.

Üldised turvaaspekid
Vaatamata tõsiasjale, et IT turvalisusel on nendes protsessides keskne tähtsus, jäetakse see planeerimise alguses sageli unarusse. See kehtib nii tehniliste kui ka organisatoorsete turvaaspektide puhul, mis on väljasttellimisel otsustava tähtsusega.

Üldjuhul tuleb arvestada järgnevaga:

- Väljasttellimise kasuks langetatud otsusest ei ole tavaliselt lihtne taganeda. Koostöölepe välise teenusetarnijaga võib olla sõlmitud väga pikaks ajaks.
- Teenusetarnijal on juurdepääs tellija andmetele ja IT-ressurssidele. Teenuse tellija ei ole seega enam ainus osapool, kellel on kontroll oma andmete ja ressursside üle. Olenevalt väljasttellimisele seatud eesmärkidest võivad puudutatud olla ka kõrge turbevajadusega andmed.

Andmeedastus

- Väljasttellimise tehniline teostus eeldab, et tellija ja teenusetarnija vahel leiab aset andmevahetus. Sellega kaasneb automaatselt ka suurem ohupotentsiaal.

- Reeglina peavad ka välise teenusetarnija töötajad või allhankefirmad (seega oma ettevõtte jaoks võõrad) vähemalt ajutiselt töötama tellija ruumides. Ka sellega kaasneb suurem ohupotentsiaal.
- Väljasttellimise raames tuleb kavandada, kasutusele võtta ja ellu viia uued protsessid ja töömeetodid. Tuleb välja selgitada ja prognoosida, millised võivad olla vajalike muudatuste tagajärjed.

Iga välise teenusetarnija puhul tekib tahes-tahtmata huvide konflikt, mida ei tohi alahinnata: ühest küljest tuleb teenuse osutamisel kulutusi kokku hoidma, et suurendada oma kasumit, teisest küljest ootab tellija jällegi maksimaalset kvaliteeti, paindlikkust ja kliendisõbralikkust. Kogemused näitavad, et seda punkti alahinnatakse kõige rohkem. IT-juhid on tavaliselt küll väga kriitilise meelega, hinnateadlikud ning tootjafirmade ja nõustajate lubaduste puhul ülimalt skeptilised, kuid väljasttellimisel on olukord sageli hoopis vastupidine. Tellijad lasevad ennast liiga kergesti mõjutada teenusetarnija reklaamlausetest, jäädes optimistlikult lootma, et niimoodi suudetakse oma IT-kulusid märkimisväärselt langetada. Praktika näitab siiski, et edaspidi osutatakse parimal juhul ainult neid teenuseid, mis on algusest peale lepingus fikseeritud. Kui selgub, et teenuse kvaliteet pole piisav, sest tellija vajab ka selliseid teenuseid, mida ta pidas erinevalt välisest teenusetarnijast iseenesest mõistetavaks, kaasnevad kvaliteedi parandamisega tavaliselt suured lisakulutused. Iga IT-juht, kes kaalub väljasttellimist, peaks esmalt põhjalikult arvutama, milliste hindadega peab teenusetarnija kokkulepitavat teenust tarnima, et lepinguline suhe oleks kasulik nii tellijale kui ka teenusepakkujale. Selle arvutuse tulemusel võib selguda, et kvaliteetse teenuse sisseostmine on lubatud madalate hindade juures ülimalt ebatõenäoline.

Iseseisev turvaanalüüs

Väljasttellimisstrateegia koostamisel tuleb seega viia alati läbi iseseisev turvaanalüüs. Ainult niimoodi on võimalik kindlaks määrata, kuidas olemasolevaid IT-süsteeme või IT-kooslusi piirata ja lahutada, et nende osi mõnda teise kohta ümber suunata. Varajases projektifaasis kirjeldab turvakontseptsioon loomulikult ainult raamtingimusi ja ei sisalda detailseid meetmeid. IT turvaanalüüs tuleb läbi viia IT etalonturbe protseduuris kirjeldatud metoodika alusel:

- IT väljasttellimise planeerimisel tuleb läbi viia IT struktuurianalüüs.
- Seejärel määratakse vajalik turbeaste.
- Mõningatel juhtudel saab juba järgmise sammuna läbi viia ka IT etalonturbeanalüüsi, et määrata edasised vajalikud tegutsemissammud ja tuvastada rakendatavate meetmete kulud. Tulemused saab kaasata väljasttellimise hindamisse, eriti majandusliku tasuvuse hindamisse.

Kui oluliste süsteemide või rakenduste turbevajadus on suur või kui IT-koosluse modelleerimisel ei ole võimalik lähtuda IT etalonturbest, tuleb viia läbi täiendav turvaanalüüs (nt riskianalüüs). Pärast turvalistust puudutavate ohtude analüüsimist saab määrata, kas ja kuidas tuleks nendega edasi tegutseda. Võimalik jääkrisk jääb tellija enda kanda. Turvaanalüüsi tulemusi saab kasutada vahetult tasuvusanalüüsi jaoks.

Strateegilised kaalutlused

Juhtkond ei tohi eduka, pikaajalise väljasttellimise strateegia planeerimise puhul lähtuda ainult kulude kokkuhoiust. Tuleb arvestada ka mõjuga, mida väljasttellimine võib avaldada ülesannete täitmisele, ärimudelile ja teenuste või toodete portfooliole. Kas väljast soovitakse tellida standardprotseduuride või tuumprotsesside täitmist? Selles kontekstis on oluline säilitada piisav isiklik kontroll IT-nõuete määramise ja kontrollimise üle. Eriti tuleks mõelda enda väljatöötatud IT-süsteemide ja rakenduste edasiarendamisele. Järgnevad juhised selgitavad väljasttellimise eeliseid ja puudusi, lähtudes IT-turvalisuse vaatepunktist.

- Eelis: võimalus juurutada uusi teenuseid (nt täiendada või laiendada tootevalikut), kuid selle tagajärjel tuleb algselt kehtestatud turbeastet rakendada ka lisandunud teenuste puhul.
- Eelis: suurenenud paindlikkus, näiteks saab süsteeme, ressursse või personalivajadust kiiremini kohandada/täiendada, kuna väliselt teenusetarnijalt saab neid vajaduse korral kiiresti juurde osta. Seeläbi saab püsikulusid muuta muutuvkuludeks. Tagajärjena võivad tekkida uued, täiendusest (nt IT-süsteemidele tehtud täiendustest) tulenevad turvaprobleemid.
- Eelis: ideaaljuhul võimaldab väljasttellimine saavutada paremat IT turbeastet, kuna teenusetarnija juures töötavad oma ala spetsialistid ja see võimaldab käitada ka uusi, suuremat turvalisust nõudvaid rakendusi. IT turvalisuse tagamine nõuab suurt ajakulu ja põhjalikke tehnilisi teadmisi, et säilitada pidev ülevaade turbeinfo, turvabülletäänide, täienditeadete ja programmivigade raportite infotulva üle, hinnata nende olulisust ja vajaduse korral kiiresti sobilikult tegutseda. Pakutavate riist- ja tarkvaralahenduste suurenev keerukus, üha lühemad andmetöötlustsüklid, kasvav võrguühenduste arv ja kasutajate suurenevad nõudmised muudavad turvalisuse ja lisafunktsioonide vahelise tasakaalu leidmise väga raskeks.
- Eelis: väikese IT-osakonnaga ettevõtetes või ametiasutustes sõltub väga palju üksikust töötajast. Kui töötajad pole ajutiselt kättesaadavad (haigusel, puhkusel) või lahkuvad asutusest, võivad võrdväärse asendaja puudumisel tekkida tõsised turvaprobleemid. Teenusepakkujatel on seevastu reeglina kasutada mitu võrdväärse kvalifikatsiooniga spetsialisti, kes suudavad üksteist asendada.
- Eelis: mõnede asutuste jaoks võib väljasttellimine olla ainuke võimalus IT-süsteeme ja rakendusi töötajate vastuseisust hoolimata vajalikul moel ümber kujundada. Väljasttellimise raames tuleb heterogeenne süsteemikeskkond korrastada ja standardiseerida.
- Puudus: kui välise teenusetarnija rakendatavate spetsialistide teadmised pole piisavad, võivad tagajärjena tekkida tõsised IT turvaaugud. Kui ka institutsioonisiseselt puuduvad eriteadmised, et kontrollida välise teenusetarnija poolt tagatavat turbeastet, on võimalik, et vastavad turvaaugud jäävad koguni avastamata.
- Puudus: pakutavate teenuste laiendamine ja IT-süsteemide täiendamine ei ole enam töid tellinud institutsiooni juhtkonna ainupädevuses. Vastavatesse aruteludesse tuleb alati kaasata ka väline teenusetarnija. Teenusetarnijad hakkavad üsna sageli lepingu sõlmimisel määratud soodsaid tingimusi enda jaoks kompenseerima, esitades hiljem tellijale erisoovide või uute nõudmiste eest kõrged arved. Sellest tuleneva hinnasurve tagajärjeks on sageli kokkuhoid IT turvalisuse arvelt.

- Puudus: teenusetarnimise kvaliteedi kontrollimisele tehtavaid kulutusi ei tohi alahinnata. Kui kontrollimisel tuvastatakse puudujääke, võib nende kõrvaldamine olla keeruline ja väga ajamahukas, eriti siis, kui tellija ja teenusepakkuja vahel tekivad erimeelsused. Kui IT turvalisust puudutavatele küsimustele ei leita kiiret lahendust, võivad tagajärjeks olla turvaaugud.

Tasuvusanalüüs

Iga väljasttellitava projekti strateegilise ja majandusliku edu aluseks on põhjalik tasuvusanalüüs. Seega tuleb tunda kõiki parameetreid ja osata neid õigesti hinnata.

Väljasttellitava projekti raamtingimustes tuleb hinnata järgmiste ressursside strateegilist väärtust:

- oskusteave (know-how),
- töötajad,
- IT-süsteemid ja rakendused.

Tasuvusanalüüsi puhul võivad väärtuslikku infot pakkuda ka teiste institutsioonide uuringud ja kogemused.

Valitud strateegia dokumenteerimine

Planeerimise lõpus tuleb väljasttellimise strateegia dokumenteerida. Dokumentatsioonis tuleb selgelt kirjeldada väljasttellimise eesmärke, võimalusi ja riske. Lisaks on väljasttellimise strateegia dokumentatsiooni soovitatav kaasata ka võimaliku käimasoleva väljasttellimise projekti raames saadud kogemused. Seejuures tuleks viidata ka varasemates otsustes tehtud vigadele ja nendest otsustest tuletatud soovitustele.

Kontrollküsimused:

- Kas kõik ettevõttesisesed ja seadustest tulenevad raamtingimused on teada?
- Kas IT turbega on piisavalt arvestatud?

M 2.251 Väljasttellimisprojektide turvanõuete spetsifitseerimine

Algatamise eest vastutavad: IT turvaosakond, IT-juht

Rakendamise eest vastutavad: IT turvaosakond, IT-juht, administraator

Pärast väljasttellimise strateegia koostamist tuleb välja töötada IT-turbe nõuded, mis peavad olema piisavalt konkreetsed, et leida nende alusel sobiv teenusepakkuja. Turvanõuded tuleb siinkohal koostada nii välisele teenusetarnijale, tema kasutatavale tehnikale (kaasa arvatud sidekanalitele ja sideteenustele) kui ka enda organisatsioonile. Eelnevalt sõnastatud nõuetel põhineva ja teenusetarnija valimisele suunatud detailse turvakontseptsiooni koostamist on kirjeldatud meetmes M 2.254 Väljast tellitud projektile infoturbekontseptsiooni loomine .

Tuleb arvestada, et IT turvanõuete koostamine on järkjärguline protsess:

- Esmalt täpsustab tellija, millised on tema eesmärgiks seatud IT turvanõuded.
- Seejärel võrreldakse pakkumisfaasis, kuidas suudab teenusepakkuja soovitud IT turvanõudeid täita (vt M 2.252 Väljasttellitava teenuse sobiva tarnija valimine).
- Kui teenusepakkuja on valitud, tuleb IT turvanõudeid omavahelises koostöös jätkuvalt täiendada (nt kasutatud operatsioonisüsteemide või turvamehhanismide alusel).

Kooskõlastamisprotsessi lõppfaasis tuleb täpsustada juba konkreetse teostuse turvanõuded.

Üldjuhul on väljasttellimise kasutusvaldkondade minimaalsed turvanõuded järgmised:

IT etalonturbe rakendamine

- IT etalonturbe rakendamine on mõlemale väljasttellimise osapoolele kehtiv miinimumnõue. Lisaks sellele peab nii väljasttellimise tarnijal kui ka tööde tellijal olema koostatud ja ellu rakendatud oma IT turvakontseptsioon.
- Olulised IT-kooslused tuleb täpselt piiritleda (nt erialase ülesande, äriprotsessi, IT-süsteemi alusel), et kõik liidesed oleksid identifitseeritavad. Selle alusel saab liidestele kehtestada omad vastavad tehnilised turvanõuded.
- IT-süsteemide ja rakenduste kohta tuleb läbi viia hetkeolukorra struktuurianalüüs (vt M 2.250 Väljasttellimise strateegia määramine).
- Lähtudes konfidentsiaalsusest, terviklusest ja käideldavusest (nt rakenduste, süsteemide, kommunikatsiooniühenduste, ruumide puhul), tuleb määrata kaitsevajadus (vt M 2.250 Väljasttellimise strateegia määramine).

Loomulikult tuleb järgida ka asjassepuutuvaid seadusi ja eeskirju. See võib olla äärmiselt töömahukas, eriti neis olukordades, kus tellija või teenusetarnija tegutseb korraga mitmes riigis või ülemaailmselt.

IT turvanõuete koostamise raames tuleb kindlaks määrata, millised õigused (nt pääsuõigused andmetele ja süsteemidele) annab tellija välisele teenusetarnijale. Tuleb kirjeldada nõudeid infrastruktuurile, organisatsioonile, personalile ja tehnikale. Sageli piisab, kui tarnijat kohustatakse täitma turbeastet, mis vastab IT etalonturbele. Kui nõudmised ületavad IT etalonturvet, tuleb neid detailselt kirjeldada. See sõltub olulisel määral turvastrateegiast ning olemasolevatest süsteemidest ja rakendustest.

Väljasttellitava projekti puhul võib näiteks täpsustada järgmisi punkte:
Organisatsioonilised reeglid ja protsessid

- Turvalisuse seisukohast kriitiliste organisatoorsete protsesside (nt teavitusplaanide ajapiirangud) täpsustamine.
- Teatud töörollidele esitatavate erinõuete kehtestamine. Näiteks võib nõuda, et välise teenusetarnija juures nimetataks ametisse eriteadmistega (nt hosti puudutavate teadmistega) IT-turbe eest vastutav töötaja.

Riist- ja tarkvara

- Väliselt teenusetarnijalt võib nõuda sertifitseeritud (nt Common Criteria või ITSEC-i tingimustest lähtuvate) toodete kasutamist.
- Võib esitada nõudeid teenuste ja IT-süsteemide käideldavusele. Näiteks võib selles kontekstis määrata koormuse jaotamise astme ja meetodi (nt kliendijuurdepääsuga veebiserverile, millel on palju kliente).
- Klientidega seonduvad nõuded (multi-client capability), samuti selleks vajalik riistvara ja tarkvara lahutamine. Näiteks võib kehtestada nõude, et ühtki tellija IT-süsteemi ei tohi paigaldada ruumidesse, milles asuvad teenusepakkuja mõne teise kliendi süsteemid.

Kommunikatsioon

- Täpselt määratud eriprotseduurid kommunikatsiooni tagamiseks teenusetarnija ja tellija vahel, näiteks krüpteerimis- ja allkirjaprotseduuride kasutamine (vt B 1.7 Krüptokontseptsioon ja B 4.4 Virtuaalne privaatvõrk (VPN)).

Kontrollid ja kvaliteedi tagamine

- Kehtestada võib üldised turvalisuse, kvaliteedi või ka protseduuride ja organisatoorsete reeglite kontrolli- ja mõõtmisnõuded, nt kontrollimise intervallid, vastutusalad.
- Soovitud kontrolli- ja seireprotseduurid või mehhanismid, nt ette teatamata kohapealsed kontrollid, auditid (vajaduse korral ka sõltumatu kolmanda osapoole teostatud).
- Võib kehtestada nõuded logimisele ja logifailide analüüsile.

Üldjuhul on kindlaksmääratud IT-turvanõuded üks kindlaid eeldusi sobiva välise teenusetarnija valimisel. Spetsiaalseid IT turvanõudeid tuleb vajaduse korral kohandada teenusepakkuja rakendatava IT turbeastme jaoks.

Kontrollküsimused:

- Kas nõuete nimekirja lähtemiinimumiks on võetud IT etalonturve?
- Kas kõiki väljasttellitava projekti IT turvanõudeid on piisavalt täpselt kirjeldatud?

M 2.252 Väljasttellitava teenuse sobiva tarnija valimine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT-juht, IT turvaosakond.
Rakendamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT-juht, IT turvaosakond

Välise teenusetarnija valimisel on olulised edutegurid võimalikult detailne nõuete profiil ja sellel põhinev kohustuste nimekiri. Need on eelduseks nõuetekohase hanke läbiviimiseks, kui soovitakse, et sellele kandideeriks sobivad teenusepakkujad.

Hanke kutse peab sisaldama järgmisi punkte:
Üldine kirjeldus

- väljasttellitava projekti kirjeldus (ülesannete kirjeldus ja jaotus), samuti
- nõutud kvaliteeditaseme kirjeldus, mis ei pruugi ilmtingimata vastata tellija tasemele.

Turvanõuded
Lisaks tuleb potentsiaalsetele teenusepakkujatele edastada võimalikult täpselt

- IT-turvet puudutavad nõuded ja
- teenuse kvaliteedi ja selle turvalisuse mõõtmise kriteeriumid (vt M 2.251 Väljasttellimisprojektide turvanõuete spetsifitseerimine).
- Erijuhtudel võib osutuda vajalikuks, et turvalisuse detailseid nõudeid väljastataks teenusepakkujatele ainult vastava konfidentsiaalsuskokkuleppe alusel, sest nõuded võivad sisaldada infot olemasolevate või planeeritavate turvamehhanismide kohta.

Nõuete profiil sõltub olulisel määral väljasttellitavast projektist. Teenusetarnija ja tema personali olulised üldised hindamiskriteeriumid võivad olla järgmised:
Nõuded välisele teenusetarnijale

Välise teenusetarnija päritolu

- Välismaiste teenusetarnijate puhul tuleb arvestada mõningate lisaaspektidega. Nende alla kuuluvad näiteks võõra riigi seadused, teistsugused vastutuskohustused, spionaaži oht, teistsugune turvakultuur, partnerettevõtte või konkreetse riigi seadusandlusega lubatud ja kasutatavad turvamehhanismid.

Teenusetarnija suurus

- Teenusetarnija ettevõtte suurus võib olla valimisel oluline. Väikeste ettevõtete puhul võib maksevõimetuse oht olla suurem. Suurte ettevõtete puhul tuleb seevastu arvestada, et suurettevõttel on üldjuhul palju tellijaid ja palju projekte, seega on tellija kõigest üks paljudest ning tal pole võimalik saavutada eelispositsiooni.

Soovitused

- Teenusetarnija peaks suutma nimetada soovitajaid sarnaste projektide kohta. Seejuures tuleb jälgida, et poleks huvide konflikte, mis võivad tekkida ärisuhetest tellija konkurentidega ja sõltumatusest teatud tootjatest (nt tarnijatest, kes on tellija konkurendid)

Omanikustruktuur ja organisatsiooni vorm

- Teenusepakkuja organisatsiooni vorm võib olla oluline näiteks põhjusel, et see võib mõjutada vastutuspiire. Tuleks uurida omanikustruktuuri, et võimalikud mõjutegurid oleksid juba varakult teada.

Kliendistruktuur

- Kliendistruktuur võib viidata sellele, millises majandussektoris asuvad teenusetarnija tugevad küljed.

Sertifitseerimine

- Mõistlik on oleks nõuda kvaliteeditõendit või sertifikaati, nt IT etalontube alusel ISO 27001 või ISO 9000.

Maksevõime

- Koguge infot teenusetarnija hetke majandusolukorra ja äri võimaliku edasise arengu kohta.

Töötajatele esitatavad nõuded

Ka teenusetarnija personalile tuleb esitada erinevaid nõudeid (vt M 2.226 Asutusevälise personali kasutamise protseduurid ja M 3.33z Personali taustakontroll).

Kvalifikatsioonide profiil

- Hankele laekunud pakkumiste hindamisest moodustab tähtsa osa ka loetletud personali kvalifikatsiooni hindamine. Pärast projekti kinnitamist tuleb kontrollida, et pakkumises loetletud personal ka reaalselt projektis osaleks.

Ressursside planeerimine

- Tuleb hinnata, kui palju personali on teenusepakkujal kasutada. Seejuures tuleb kontrollida, kuidas on reguleeritud töötajate asendamine ja tööajad.

Suhtluskeel

- Välismaiste partnerite puhul tuleb määrata ühine keel oma personali ja teenusepakkuja personali vahelise suhtluse jaoks. Siinkohal tuleks välja selgitada, kas teenusepakkuja ja tellija töötajate keeleoskus on piisav ka keerukamate probleemide lahendamiseks. Kogemused näitavad, et paljud inimesed eelistavad tähtsamate küsimuste puhul pigem vaikida, sest kardavad häbisse jääda, kuna arvavad, et nende keeleoskus ei ole piisav.
-

Taustakontroll

- Olenevalt väljasttellitava projekti jaoks vajalikust turbeastmest tuleb hankele laekunud pakkumisi analüüsides selgitada, kas teenusepakkuja on teinud oma personalile ka taustakontrolli või kas seda oleks võimalik teha.
-

Kontrollküsimused:

- Kas teenusetarnija valiku jaoks on olemas hindamise mõõdupuu koos hindamiskriteeriumitega?
- Kas hindamiseks loodud mõõdupuus on arvestatud turvanõuetega?
- Kas hindamise mõõdupuu sobib konkreetsele väljasttellitavale projektile?

M 2.253 Välise teenusepakkujaga sõlmitava lepingu koostamine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT turvaosakond, IT-juht

Rakendamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT turvaosakond, IT-juht

Kui välise teenusetarnija valik on langetatud, tuleb kõik väljasttellitava projekti aspektid kirja panna ja reguleerida teenusetasemeleppega (service level agreement, SLA). Alljärgnevalt kirjeldatud aspektid on mõeldud abivahendina ja kasutamiseks lepingu koostamise kontrollnimekirjana. Lepinguliste kokkulepete liik, maht ja detailsuse aste sõltub alati konkreetsest väljasttellitavast projektist.

Mida suurem on väljasttellitavate IT-süsteemide ja rakenduste kaitsevajadus, seda hoolikamalt ja detailsemalt tuleb sõnastada tellija ja teenusetarnija vahel sõlmitav leping. Teenusetarnijat tuleb kohustada IT etalonturbest ja tellija määratud turvanõuetest kinni pidama (vt M 2.251 Väljasttellimisprojektide turvanõuete spetsifitseerimine). See tähendab loomulikult ka seda, et väline teenusetarnija kohustub looma IT turvakontseptsiooni koos hädaolukorraks valmisoleku kontseptsiooniga ja dokumenteerib turvameetmed, süsteemid ja rakendused. Lisaks teenuste üldisele kirjeldusele on soovitatav alati lepinguliselt fikseerida ka teenuste kvantitatiivne kirjeldus, nt käideldavuse nõuded, reageerimisajad, arvutusvõimsus, saadaolev salvestimaht, personali arv, tugiteenuste kasutamise ajad.

Enamasti võib üldisest IT etalonturbe järgimiskohustusest küll piisata, kuid kasulikum oleks alati kõik kokkulepitud teenused võimalikult täpselt ja üheselt mõistetavalt lepingus fikseerida. Sellega saab hiljem vältida osapooltevahelisi tülisid. Lepingu tagantjärele täpsustamine ja täiendamine, mis osutub vajalikuks kirjeldatud teenuste erineva tõlgendamise tõttu, tähendavad tellijale sageli kulutuste märgatavat suurenemist. Ka IT turvakontseptsiooni koostamine peaks olema lepingus fikseeritud. Eriti tuleb selgitada, kes vastutab erialase sisu eest ja millised on tellijapoolsed osaluskohustused. Järgnevalt on ära toodud temaatiline nimekiri aspektidest, mis peaksid olema turvalisuse põhjustel reguleeritud.

Lisainfot asjakohaste detailide kohta leiate IT etalonturbe kataloogi vastavatest meetmetest:

Infrastruktuur

- teenusetarnija infrastruktuuri kaitse (nt juurdepääsukontroll, tuleohutus)

Organisatsioonilised reeglid/protsessid

- kommunikatsioonikanalite ja kontaktisikute määramine
- protsesside, tööprotsesside ja vastutusalade kindaksmääramine
- probleemide lahendamisel kasutatav protseduur, vajalike volitustega kontaktisikute nimetamine
- regulaarsed läbirääkimised kooskõlastamiseks
- andmekogumite arhiveerimine ja kustutamine (eriti lepinguliste suhete lõpetamisel)

- teenusetarnija juurdepääsuvõimalused tellija IT-ressurssidele: kellele antakse erinevate süsteemide juurdepääsuõigused? Kuidas on määratud vastutusalad ja õigused?
- teenusetarnija personali juurdepääsuõigused ja pääsuõigused seoses tellija ruumide ja IT-süsteemidega
- tellija personali juurdepääsuõigused ja pääsuõigused seoses teenusepakkuja ruumide ja IT-süsteemidega

Personal

- välispersonali töökohtade kujundamine (arvutiga töökohale kehtivatest suunistest kinnipidamine)
- töötajate omavahelise asenduskorra määramine ja kooskõlastamine
- täiendõppemeetmete rakendamise kohustus

Valmisolek hädaolukorraks

- kategooriad vigade ja häirete liigitamiseks nende liigi, raskusastme ja pakilisuse järgi
- vajalikud tegevused häireolukorra esinemisel
- reageerimisajad ja eskalatsiooniastmed
- tellija osaluskohustus hädaolukordade lahendamisel
- regulaarsete ja adekvaatsete hädaolukorra õppuste liigid ja toimumise ajaline järjestus
- andmevarunduse liik ja maht
- kokkulepe, kas ja millised süsteemid peavad olema liiasusega
- eriti olulised võivad olla vääramatut jõudu puudutavad regulatsioonid. Näiteks tuleks kokku leppida, kuidas tagada andmete ja süsteemide käideldavus juhul, kui teenusetarnija personal on otsustanud hakata streikima. Eriti ootamatult võivad sellised sündmused tabada tellijat juhul, kui teenusetarnija ja tellija tegutsevad kas erinevates valdkondades või asuvad erinevates riikides.

Vastutus, juriidilised raamtingimused

- Lepingus peavad olema fikseeritud kohustused järgida kehtivaid norme, seadusi, kokkulepitud turvameetmeid ja muid raamtingimusi. Samuti tuleb lepinguliselt fikseerida konfidentsiaalsuslepped (non-disclosure agreements).
- Reguleerida tuleb kolmandate osapoolte, teenusetarnija tütarettevõtete ja allhankefirmade kaasamine projekti. Üldjuhul pole mõistlik neid automaatselt kõrvale jätta, selle asemel tuleks kehtestada mõistlikud reeglid.
- Süsteemide, tarkvara ja liideste puhul tuleb kokku leppida omandi- ja autoriõigused. Tuleb saavutada kokkulepe, kas teenusetarnija võtab üle olemasolevad kolmandate osapooltega sõlmitud lepingud (tarkvaraga varustamine, teenusetasemelepingud, tarkvaralitsentsid jne).

- Teenusetarnijaga tuleb kokku leppida, kuidas toimitakse juhul, kui teenuse sisseostmine tahetakse lõpetada, kuid teenuseosutaja kasutatud tööriistu, protseduure, skripte ja pakkprogramme soovitakse edasi kasutada.
- Täpsustada võiks tingimusi, mis kehtivad väljasttellimisprojekti lõppemisel, nt teenusetarnija vahetuse või maksejõuetuse puhul. Tuleb jälgida, et tellijale jääks õigus katkestada lepingulisi suhteid piisavalt paindlikult.
- Teenusetarnijat tuleb kohustada pärast tellimuse lõppemist tagastama kogu tellijale kuuluva riist- ja tarkvara, kaasa arvatud salvestatud andmed. Kõik olemasolevad andmed ja nende varukoopiad tuleb tagastada või (olenevalt kokkuleppest) hävitada.
- Tuleks mõelda riskide jaotamisele tellija ja teenusetarnija vahel.
- Tuleks määrata, milline on poolte vastutus kahjude korral.
- Tuleb määrata, millised sanktsioonid või kahjunõuded kaasnevad teenuse ebapiisava kvaliteediga. Kahjutasude maksmisi ja juriidilisi tagajärgi ei tohiks siinkohal ülehinnata. Arvestada tuleb nimelt järgmiste punktidega:

1. Millist olukorda käsitletakse kahjuna?

- Kuidas mõõdetakse näiteks mainele tekitatud kahju?
- Kuidas hinnata kohustuste jämedat eiramist, millele vaid juhuse tahtel ei järgnenud tõsiseid kahjustusi?

2. Teenusepakkuja maksejõuetus

- Kahjutasude nõudmise õigus on väärtusetu, kui see ületab teenusepakkuja maksevõimet ja teenusepakkuja kuulutab välja maksejõuetuse. Minimaalsed kulutused, millega sellisel juhul tuleb arvestada, on vähemalt uue teenusepakkuja juurde kolimise kulud.

3. Katastroofilised kahjud

- Leppetrahviga on hiljaks jäädud, kui tellija jääb kahjustuse ulatuse tõttu ilma oma äritegevuse alusest ja muutub halvimal juhul maksevõimetuks.

4. Tõendatavus

- Kas kahju on tõendatav ja põhjustaja tuvastatav (nt spionaaži või manipulatsioonide tõestamine)?

Alati tuleb arvestada, et kahjunõuete esitamine on kõige viimane meede ja kahjunõuete tingimused ei tohi viia selleni, et kulude kokkuhoidmise nimel jäetakse muud, kahjunõudega koormamata turvameetmed unarusse. Juriidilised vahendid ei sobi turvalisuse saavutamiseks.

Klientide haldamisvõimekus

- Tuleb kokku leppida, et erinevate klientide IT-süsteemid ja rakendused oleksid üksteisest vajalikus mahus lahutatud.
- Tuleb tagada, et teenusepakkuja ülejäänud klientide probleemid ei segaks tellija protseduure ja süsteeme.

- Tuleb tagada, et tellija andmed ei oleks mitte mingil juhul ligipääsetavad välise teenusetarnija teistele klientidele.
- Vajaduse korral tuleb kokku leppida füüsiline lahutamine (st eraldiseisva riistvara kasutamine).
- Vajaduse korral tuleb kehtestada nõue, et teenusetarnija projekti kaasatud personal ei töötaks teiste tellijate jaoks. Lisaks võib olla mõistlik rakendada ka vaikimiskohustust, et konkreetse tellija projektiga seotud personal ei vahetaks infot teenusepakkuja ülejäänud personaliga.

Muudatuste haldamine ja testimisprotseduurid

- Tuleb välja töötada tingimused, mis võimaldaksid tellijal alati uute nõuetega kohanduda. Eriti kehtib see näiteks seadustest tulenevate ettekirjutuste muutmise korral. Tuleb määrata, kuidas reageerida süsteemi täiendamisvajadustele, suurenenud nõudmistele või ammenduma hakkavatele ressurssidele.
- Selles kontekstis tuleks reguleerida ka juba olemasolevate süsteemide hooldamine ja edasiarendamine. Üsna sageli võtab teenusetarnija tellija enda väljaarendatud süsteemi või tarkvara üle ja tellija kaotab sellega võimaluse neid oma äranägemise järgi edasi arendada. Seetõttu peavad süsteemide arendusteed olema reguleeritud.
- Teenuse kvaliteedi ja IT turbeastme pidev edasiarendamine peaks olema fikseeritud juba teenusetasemeleppes.
- Tuleb määrata vigade kõrvaldamiseks lubatud aeg.
- Tuleb kokku leppida uue tarkvara ja riistvara testimisprotseduurides.

Siinkohal tuleks kaasata järgmised punktid:

- Täiendite ja süsteemi kohandamiste reeglid
- Testimis- ja tootmissüsteemide lahutamine
- Vastutusalad testimiskontseptsioonide koostamisel
- Kasutatavate testimismudelite määramine
- Tellija ja teenusetarnija vastutusalad testide läbiviimisel (nt tellija koostöö või abi, vastuvõtu- ja kinnitamisprotseduurid)
- Informeerimiskohustus ja kooskõlatamine enne süsteemi olulisemat muutmist (negatiivne näide: teenusepakkuja installeerib serverile uue operatsioonisüsteemi. Ootamatute vigade tõttu häiritakse oluliste rakenduste kasutamist, ilma et tellija oleks saanud end selleks ette valmistada)
- Läbiviidavate testide kinnitamisprotseduurid
- Testimisega kaasneva talutava kvaliteedilanguse määramine (nt käideldavuse langus)

Kontrollid

- Teenuse kvaliteeti ja IT-turvalisust tuleb regulaarselt kontrollida. Tellijal peavad olema selleks vajalikud info-, ülevaatlikkuse ning juurdepääsu- ja pääsuõigused. Kui soovitakse, et auditid või jõudlustestid viiks läbi sõltumatu kolmas osapool, peab see olema juba lepingus reguleeritud.

- Kõikidele institutsioonidele, kes peavad tellija juures kontrolle sooritama (nt järelevalveametitele), tuleb võimaldada kontrollida ka välist teenusetarnijat (nt anda vajalikud pääsuõigused, volitused andmeid kontrollida).

Kontrollküsimused:

- Kas kõik kokkulepped on kirjalikult fikseeritud?
- Kas leping sisaldab teenuste üheselt mõistetavaid ja mõõdetavaid kirjeldusi?
- Kas lepingu lõppemine on täpselt reguleeritud?

M 2.254 Väljast tellitud projektile infoturbekontseptsiooni loomine

Algatamise eest vastutavad: IT-juht, IT turvaosakond

Rakendamise eest vastutavad: IT turvaosakond, administraator, IT-juht

Iga väljasttellitud projekti jaoks tuleb koostada vastav IT turvakontseptsioon. See võib olla koostatud näiteks IT etalonturbe kataloogide alusel. Väljasttellitud projektide iseloomustav tunnus on asjaolu, et paljud tehnilised ja organisatsioonilised detailid selguvad alles planeerimise ja süsteemide üleviimise käigus.

IT turvakontseptsioon, mis töötatakse välja alles pärast teenusetarnija poole pöördumist, on seega harva kohe täielik ja lõplik ning seda tuleb üleviimise käigus kõikide osapooltega edasi arendada ja täpsustada. Üleviimine on seega olulise tähtsusega kogu projekti edu tagamiseks ning seda on kirjeldatud meetmes M 2.255 Turvaline üleviimine väljast tellitud projektides . Väljasttellitavate projektide IT turvakontseptsioonide ja organisatsiooni enda käitatavate IT-süsteemide IT turvakontseptsioonide vahel ei ole üldjuhul suuri erinevusi. Siiski on mõningad eripärad, millega tuleb arvestada järgnevate punktidega.

Tehnilisest vaatepunktist lähtudes osalevad väljasttellitavates projektides kolm erinevat osapoolt:

1. Teenuse tellija
2. Väline teenusetarnija
3. Võrguteenuse pakkuja

Võrguteenuse pakkuja loob ühenduse väljasttellitava teenuse osapoolte vahel. Vastutus võrguühenduse tagamise eest jääb seejuures tavaliselt välisele teenusetarnijale. Iga osapool peab enda jaoks looma oma IT turvakontseptsiooni ja rakendama seda konkreetse väljasttellitava projekti kohaselt.

Seetõttu tuleb koostada eraldi IT turvakontseptsioonid järgmistele valdkondadele:

- välise teenusetarnija mõjuvaldkond,
- tellija mõjuvaldkond ning
- liidesed ja kommunikatsioon nende valdkondade vahel.

Lisaks üksikutele kontseptsioonidele tuleb luua ka terviksüsteemi käsitlev IT turvakontseptsioon, mis vaatleb turvalisuse alusel üksikute süsteemide koostööd. Erinevad osakontseptsioonid tuleb tellija ja teenusetarnijate vahel kooskõlastada. Tellija ei pea välise teenusetarnija IT turvakontseptsiooni koostamises vahetult osalema, kuid peaks auditi raames kontrollima, kas see on olemas ja piisav. Auditi jaoks võib tellija siinkohal kasutada kolmanda osapoole teenuseid. IT turvakontseptsiooni aluse moodustavad meetmed M 2.251 Väljasttellimisprojektide turvanõuete spetsifitseerimine ja M 2.253 Välise teenusepakkujaga sõlmitava lepingu koostamine . Lähtudes meetmetes kirjeldatud olulistest nõuetest, tuleb luua detailne IT turvakontseptsioon, mille loomise käigus toimub näiteks nimetatud meetmetes kajastatud nõuete konkretiseerimine ja kontaktisikute nimeline määramine.

Testimisfaasi turvakontseptsioon

Kogemused näitavad, et tellija ülesannete ja IT-süsteemide üleviimine (migratsioon) välisele teenusetarnijale on projekti faas, mille käigus tuleb eriti suurel määral arvestada turvaintsidentidega. Sel põhjusel peab turvakontseptsioon käsitlema ka üleviimise tingimusi ja meetmeid, mida kajastatakse täpsemalt meetmes M 2.255 Turvaline üleviimine väljast tellitud projektides . Järgnevalt on loetletud mõned aspektid ja teemad, mida tuleks IT-turvakontseptsioonis võimalikult detailselt kirjeldada. Kuna IT turvakontseptsiooni üksikasjad sõltuvalt alati konkreetsest väljasttellitud projektist, on kõnealune nimekiri mõeldud üldise soovitusena ja ei pretendeeri täielikkusele. Lisaks ohuastmete ülevaatele, mis peaks motiveerima turvameetmete kasutamist ning ohutusmeetmetele, mis puudutavad tööde organiseerimist, infrastruktuuri ja töötajaid, võib olla kasulik rakendata turbemeetmeid ka veel järgmistes valdkondades:

Organisatoorne külg

- andmete ja kaitsmist väärivate töövahenditega (nt printeripaber ja andmekandjad) ümberkäimine, eriti aga ettekirjutused koopiate tegemise ja kustutamise/hävitamise kohta
- tegevuse määramine, mille puhul tuleb rakendada kahemehereeglit

Riist- ja tarkvara

- tugevdatud operatsioonisüsteemide kasutamine, et muuta rünnakud võimalikult raskeks
- sissetungi tuvastamissüsteemide (IDS-ide) kasutamine, et rünnakuid varakult tuvastada
- failitervikluse kontrollsüsteemide kasutamine, et tuvastada muudatusi, nt pärast asetleidnud ründeid
- süsteemilogi- ja ajaserverite kasutamine, et võimaldada võimalikult põhjalikku logimist
- kaskaad-tulemüürisüsteemide kasutamine piirsüsteemide kaitse suurendamiseks teenusetarnija poolel
- hoolikas kasutajatunnuste määramine, grupi-ID-de keelamine teenusepakkuja personali puhul

Kommunikatsioon

- kommunikatsiooni turvamine (nt krüpteerimine, elektrooniline allkiri) teenusetarnija ja tellija vahel, et kaitsta tundlikke andmeid
- autentimismehhanismid
- täiendavate võrguühenduste detailsemad kokkulepped (vt M 5.87 Leping kolmandate poolte võrkudega ühendamise kohta)
- andmevahetuse detailsemad kokkulepped (vt M 5.88 Lepingud andmevahetuse kohta kolmandate pooltega).

Kontrollid ja kvaliteedi tagamine

- turvalisuse, teenuse kvaliteedi, protseduuride ja organisatoorsete reeglite kontrolli ja mõõtmise detailsed kokkulepped (nt ootamatud kohapealsed kontrollid, ajaintervallid, vastutusalad, detailsus)

Valmisolek hädaolukorraks

- Ootamatuste ennetamise kontseptsiooni on kirjeldatud meetmes M 6.83 Väljasttellimise avariiplaan .

Kontrollküsimused:

- Kas on koostatud turvakontseptsioonid erinevate osapoolte ja osade (tellija, teenusepakkuja, liidese) kohta?
- Kas teenusepakkuja IT turvakontseptsiooni on kontrollinud tellija või sõltumatu kolmas isik?
- Kas kõik IT turvakontseptsioonid on üksteisega kooskõlastatud ja harmoneeruvad?

M 2.255 Turvaline üleviimine väljast tellitud projektides

Algatamise eest vastutavad: IT-juht, IT turvaosakond
Rakendamise eest vastutavad: IT turvaosakond, IT-juht, administraator

Ohud

Pärast välisele teenusetarnijale tellimuse esitamist tuleb esmalt luua esialgne IT turvakontseptsioon, kus käsitletakse väljasttellitava projekti osana ka vajalikku testimis- ja juurutamisfaasi. Esiteks on selle faasiga seotud paljud ettevõttevälised isikud, teiseks tuleb juurutada protseduurid, anda üle tööülesanded ja seada uuesti sisse või kohandada vastavad süsteemid. Hoolikalt läbiviidud testimisfaas on seega ülimalt tähtis. Testimiseks ja suure töökoormusega faasideks kiputakse meelsasti valima „paindlikke" ja „lihtsakoelisi" lahendusi, mis pole enamasti eriti turvalised. Seetõttu tuleb tagada, et tootmisandmeid ei kasutataks testimisel ilma, et oleks rakendatud spetsiaalseid kaitsemeetmeid. IT turvakontseptsioon peab sellised võimalused välistama. Enne väljasttellitava projekti osaks muutuva üleviimise kontseptsiooni koostamist peab tellija juures olema moodustatud spetsiaalselt üleviimisfaasis IT turvalisusega tegelev meeskond. Meeskonna ülesanne on tegelda üleviimisfaasi turbeprobleemidega ja võtta sobivad kaitsemeetmed juba enne üleviimisfaasi algust, et üleviimise ajal oleks tagatud IT turvaline kasutamine.

IT-turbega tegeleva meeskonna suurus sõltub väljasttellitava projekti suurusest, minimaalselt võib selle ülesandega tegeleda ka ainult üks turbekspert.

IT-turbega tegeleva meeskonna ülesanded

Üleviimise kontseptsioonis peavad olema fikseeritud erinevad reeglid ja nõudmised, mis on tuletatud järgmistest IT-turbega tegeleva meeskonna tööülesannetest:

- Tellija ja välise teenusetarnija personalist tuleb moodustada ühine meeskond. Erialase kompetentsi tõstmiseks võib meeskonda kaasata ka kolmandate osapoolte spetsialiste.
- Üleviimisfaasi jaoks tuleb koostada IT turvakontseptsioon.
- Tuleb määrata migratsioonifaasi eest vastutavad töötajad ja nendevahelised alluvussuhted. Seejuures on oluline, et mõlemad osapooled looksid selged juhtstruktuurid ja määraks konkreetsed kontaktisikud. Lisaks tuleb mõlemal osapoolel määrata ka oma juhtivtöötajate vastutused. Ainult nii on võimalik tagada, et kahtluse korral tegutsetakse piisava kindlusega.
- Vajalikud testid tuleb planeerida ja ellu viia, vastuvõtuprotseduurid välja töötada ja planeerida enne tootmise/kasutamise alustamist.
- Testimis-, juurutamis- ja hilisema tööfaasi jaoks tuleb valida sobiv personal. Muidugi võib ka lepinguliselt määrata, et tellija osaleb välise teenusetarnija personali valimisel.
- Tellija personali tuleb koolitada, kuidas toimida üleviimisfaasi ajal ja pärast üleviimisfaasi. Tavalisel puutub personal selle käigus kokku uute ja tundmatute kontaktisikutega. Sellega kaasneb manipuleerimisvõtete (social engineering) oht (nt kõne isikult, kes väidab, et on teenusetarnija turvaosakonna töötaja).

- Teenusetarnija peab täpselt tundma õppima tellija olulisi protseduure, rakendusi ja IT-süsteeme ja saama vajalikud asjakohased juhised.
- Tõrgeteta töö tuleb tagada ressursside täpse planeerimise ja testidega. Siinjuures ei tohi unarusse jätta tootvaid süsteeme. Selleks tuleb eelnevalt kontrollida, kas vajalik personal on saadaval. Lisaks tuleb arvestada, et vajalike testidega võivad kaasneda tõrked.
- Teenusepakkuja vastutusalasse ülekantavad rakendused ja IT-süsteemid peavad olema piisavalt täpselt dokumenteeritud. Siinkohal tuleb mõelda ka dokumentatsiooni tervikluse kontrollimisele ning olemasoleva dokumentatsiooni kohandamisele väljasttellitud projektiga kaasnevate raamtingimuste muutumise kohaselt. Seejuures peab olema tagatud ka uute süsteemide või alamsüsteemide dokumenteerimine.
- Üleviimise ajal tuleb pidavalt kontrollida, kas teenusetasemeleppeid või ettenähtud IT turbemeetmeid on tarvis muuta.

Ootamatuste ennetamise kontseptsioon
Ootamatuste ennetamise kontseptsioon vajab suuremat tähelepanu väljasttellitava projekti juurutamisfaasis ja töö alguses. Seni, kuni kõik osalised pole kõikide tööetappidega harjunud, näiteks rikete ja turvalisust puudutavate sündmuste käsitlemisega, tuleb tavalisest suuremat tähelepanu pöörata personali valmisolekule ilmuda vajaduse korral kiiresti kohale.

Turvakontseptsiooni uuendamine ja täpsustamine
Pärast üleviimise lõppemist tuleb tagada IT turvakontseptsiooni uuendamine, sest kogemused näitavad, et üleviimisfaasiga kaasnevad alati muudatused. Erilist tähelepanu vajavad siinkohal järgnevad aspektid:

- Kõik turvameetmed tuleb üle täpsustada.
- Kontaktisikud ja vastutusalad tuleb dokumenteerida koos nimede ja vajalike kontaktandmetega (telefon, kättesaadavuse aeg, võimalikud vajalikud määratlusmõisted, nagu kliendinumbrid).
- Dokumenteerida tuleb süsteemi konfiguratsioonid ning seejuures tuleb kirja panna ka turvalisust puudutavad parameetrid.

Koolitus

- Personal tuleb koolitusmeetmete abil tööks ette valmistada.

Viimase ülesandena tuleb väljasttellitav projekt pärast üleviimisfaasi viia üle turvalisse tavakasutusse (vt M 2.256 Infoturbe planeerimine ja käigushoidmine väljasttellimise tegevuste ajal). Eelkõige tuleb siinkohal jälgida, et kõik erandkorras kehtestatud reeglid, mis olid vajalikud üleviimisfaasis, nt laiendatud pääsuõigused, saaksid tühistatud.

Kontrollküsimused:

- Kas üleviimisfaasi jaoks on loodud IT turvakontseptsioon?
- Kas üleviimise kontseptsioon sisaldab kõiki vajalikke turvalisust puudutavaid meetmeid?

- Kas on tagatud, et kõik üleviimise ajal erandkorras kehtestatud reeglid tühistatakse pärast üleviimisfaasi lõppemist?
- Kas nii tellija kui ka välise teenusetarnija personal on üleviimiseks piisavalt ette valmistatud?

M 2.256 Infoturbe planeerimine ja käigushoidmine väljasttellimise tegevuste ajal

Algatamise eest vastutavad: IT turvaosakond, IT-juht
Rakendamise eest vastutavad: IT turvaosakond, IT-juht, administraator

Kui väljasttellimise projekt on juurutatud, peab ka igapäevatöös olema tagatud IT turvalisus. Seepärast tuleb väljasttellimise projekti jaoks planeerida käitamise kontseptsioon, milles arvestataks ka turvaaspektidega. Väljasttellitava projekti IT-d puudutavad ülesanded on enamasti samad, mida tuleb planeerida ja teostada siis, kui ühtki väljasttellitavat projekti ei ole parajasti töös (vt M 2.217 Teabe, rakendus-te ja süsteemide hoolikas liigitamine ja käitlus). Erinevused tekivad asjaolust, et ülesanded on jaotatud mitme osapoole vahel, mis tekitab juurde lisaülesandeid (nt kooskõlastamisi ja kontrolle).

Muu hulgas tuleb tegeleda järgnevaga:

- Dokumentatsioone ja suuniseid tuleb regulaarselt uuendada.
- Turvakontseptsioonide ajakohasus – kõikide osapoolte kehtivaid turvakontseptsioone tuleb kontrollida, et veenduda, kas need on omavahel kooskõlastatud ja tagavad soovitud turbeastme. Väline teenusetarnija peaks tellijat ilmtingimata informeerima oma mõjuvaldkonnas toimuvatest olulistest muudatustest.

Kontrollid
Regulaarselt tuleb kontrollida järgmisi aspekte:

- kokkulepitud auditite teostamine
- kokkulepitud IT turvameetmed
- süsteemide ja rakenduste hooldusseisund
- teenusetarnija määratud õigused (õiguste kuritarvitamine)
- töötajate rakendamine, kellest pole tellijale teatatud, nt asendajad
- jõudlus, käideldavus, kvaliteedi tase
- andmete varundamine

Kommunikatsioon
Regulaarselt tuleb kooskõlastada järgmisi punkte:

- Osapooled peavad vahetama infot (nt personalimuutuste, organisatoorsete reeglite, seadusemuudatuste, planeeritud projektide, ettenähtud testimiste ja süsteemimuudatuste kohta, mis võivad kahandada teenuse kvaliteeti).
- Probleemid tuleb tuvastada ja läbi analüüsida.
- Oluline on vastastikune tagasiside ja potentsiaalsete täiendusvõimaluste leidmine. Kaastöötajate motiveerimiseks võib esile tuua positiivseid näiteid õnnestunud koostööst.
- Muudatuste haldus: muutmissoovidest (riistvara, tarkvara, teenuseportfoolio täiendamine, vajadus suuremate ressursside järele) tuleks rääkida võimalikult vara.

Testid ja harjutamine
Regulaarselt tuleb harjutada ja testida järgnevaid valdkondi:

- reageerimine süsteemikatkestustele (osaline/täielik avarii)
- andmevarunduste taaspaigaldamine
- toimetulek turvaintsidentidega

Kontrollküsimused:

- Kas väljasttellitava projekti juurutamise ajaks on olemas igapäevatöö kontseptsioon?
- Kas igapäevatöö kontseptsioon sisaldab protseduure ja meetmeid, mis tagavad töö ajal soovitud turbeastme?
- Kas vajalikke kontrolle tehakse regulaarselt?
- Kas turvakontseptsioonid on ajakohased?
- Kas lepingupartnerite vahel toimub regulaarne infovahetus?

M 2.257 Arhiveerimis-andmekandja salvestusressursside seire

Algatamise eest vastutavad: IT-juht, arhiivi haldaja
Rakendamise eest vastutavad: IT-juht, arhiivi haldaja, administraator

Teavitamine ja hoiatused
Arhiveerimisandmekandjate vabast salvestusmahust peab olema pidev ülevaade. Kui vaba salvestusmaht langeb alla määratud piirväärtuse, peab süsteem teavitama administraatorit või vajaduse korral saatma vastava info edasi süsteemihalduse keskkonda. Kui salvesti maht langeb edasi alla kriitilise piirväärtuse, peaks süsteem andma vastava hoiatuse. Hoiatusteadete puhul tuleb eelkõige jälgida seda, et need ei oleks seotud mitte konkreetse inimese, vaid tööülesandega. Sellega tagatakse hoiatuse kohaletoimetamine ka siis, kui konkreetne töötaja on parajasti haige või puhkusel.

Läviväärtuse ja piirväärtuse määramine
Läviväärtus, piirväärtus ning eskalatsiooniprotseduurid ja -meetodid tuleb määrata organisatsiooni eripärade põhjal. Piirväärtuste kindlaksmääramisel tuleb aluseks võtta kasutatud arhiveerimisandmekandjad ja arhiveeritavate andmete keskmine maht. Pärast kriitilise hoiatuse andmist peab piisava aja jooksul olema jätkuvalt tagatud keskmise andmehulga arhiveerimine. Tavaliselt määratakse läviväärtuseks 15% andmekandja kogumahust ja kriitiliseks piirväärtuseks 10% andmekandja kogumahust.

Tühjade andmekandjate varu hoidmine
Vältimaks olukordi, kus oleks kiiresti vaja andmekandjaid, aga tarnimine viibib, tuleb tuntud hoiukohas hoida käepärast piisavas koguses tühje andmekandjaid. Siinkohal tuleb kinni pidada ka klimaatilistest ja füüsilistest ladustamistingimustest (vt M 1.60 Arhiivi-andmekandjate asjakohane säilitus). Hoiatusteadete kohta tuleb dokumenteerida, millisel moel ja millise aja jooksul tuleb neile reageerida. Kui arhiivisüsteemi käitab kolmas osapool, tuleb see näiteks kirja panna teenusetasemeleppesse (service level agreement). Vajaduse korral peab seire tagama lisaks salvesti vabale ruumile ka ülevaate operatsioonisüsteemi või rakenduste piirangutest. Sellega seoses tuleb kontrollida vastavaid programmidokumentatsioone. Kahtluse korral või kui dokumentatsioonis puuduvad vastavad andmed, tuleb pöörduda tootja poole. Näiteks on oht ületada kataloogi kohta maksimaalselt lubatud failide arvu või andmebaasi sissekannete arvu, mille tagajärjel ei saa andmekandjale enam andmeid salvestada.

Kontrollküsimused:

- Kas seirega on tagatud pidev ülevaade olemasolevast salvestimahust?
- Kas hoiatusteadete piirväärtused on määratud ja dokumenteeritud?
- Kas tühje andmekandjaid on teadaolevas kohas piisavas koguses käepärast?

M 2.258 Dokumentide järjekindel indekseerimine arhiveerimisel

Algatamise eest vastutavad: IT-juht, arhiivi haldaja
Rakendamise eest vastutavad: IT-juht, arhiivi haldaja, administraator

Arhiivi kasutamisel on oluline luua kõikide dokumentide ja andmekogumite jaoks ühesed viited, et neid saaks hiljem arhiivist probleemideta üles leida. Lisaks pakuvad arhiivisüsteemid ka päringuvõimalust. Kuna täistekstiotsing võib olenevalt arhiveeritud andmete liigist ja mahust kesta väga kaua, salvestavad arhiivisüsteemid oma spetsiaalsesse otsinguandmebaasi iga dokumendi kohta eraldi indekseerimisinfo.

Indeksiandmete struktuuri ja andmemahtu saab üldjuhul ise seadistada ja neil peaksid olema järgmised omadused:

- Üheselt mõistetavad: dokumendi tähised peavad olema üheselt mõistetavad.
- Ootuspäraste päringuvõimaluste tugi: kontekstiandmed peaksid suutma hilisemaid päringuid kiirendada. Kuna hilisemad otsingukontekstid pole ette teada, võib tulevasi otsinguid ainult aimata ja püüda kontekstiandmed kujundada võimalikult selgeks.
- Väike andmemaht: indeksiandmete väiksem maht kiirendab hilisemat otsingut, kuid liiga väike otsinguindeksite maht võib päringuid ka takistada, st muudab dokumentide leidmise keerulisemaks. Kontekstiandmete maht sõltub eeldatavast andmete kogumahust. Üldjuhul tuleb need parameetrid määrata juba enne arhiivi kasutuselevõttu. Sellele vaatamata võib kasutuse käigus olla tarvis teha ka muudatusi. Olenevalt indeksiandmete mahust ja muudatuste liigist võib sellega kaasneda väga keeruline arhiivi andmekogude ümberindekseerimine. Arhiveeritavate dokumentide konkreetseid kontekste saab luua mitmel erineval moel. Eristatakse kolme meetodit:
- Käsitsi loomine: dokumendihaldussüsteemi tasandil luuakse iga dokumendi jaoks indeksiandmed, milleks tuleb täita vastav sisestusblankett. Suurte andmehulkade puhul esineb selle meetodi puhul suur ebaühtlaste indeksite loomise oht.
- Poolautomaatne loomine: poolautomaatsed meetodid automatiseerivad indeksiandmete määramise, kuid võimaldavad neid käsitsi kontrollida ja korrigeerida.
- Täisautomaatne loomine: selle meetodi puhul määratakse dokumendiindeksid täiesti automaatselt ja neid ei saa muuta.

Meetodi valik sõltub andmemahu eeldatavast suurusest. Kui üksikuid dokumente arhiveeritakse ebaühtlaste ajavahemike tagant, piisab käsitsi toimivast meetodist, kus konteksti loomine põhineb konkreetsetel ettekirjutustel. Kui regulaarselt arhiveeritakse suuri andmemahte, tuleks indeksiandmete loomiseks kasutada poolautomaatset meetodit. See annab võimaluse infot käsitsi kontrollida ja vajaduse korral ka parandada enne, kui dokument lisatakse koos indeksiga arhiivi, kus selle muutmine võib osutuda võimatuks. Indeksiandmete täisautomaatsel loomisel ei saa vigu tuvastada ega ka korrigeerida. Arhiveeritavate andmete võimalik valesti määramine, nt äriprotsesside hulka, ei ole selle meetodi puhul ei tuvastatav

ega ka välistatav. Seetõttu tuleks seda meetodit kasutada ainult siis, kui kõikide dokumentide struktuur suudab garanteerida kõikide indeksiandmete ühesuguse tuletamise.

Kontrollküsimused:

- Kas kasutajate arvu ja andmete hulga põhjal oleks mõeldav rakendada käsitsi toimuvat indekseerimist?
- Kas määratud tunnuseid saab kontrollida?
- Kas indekseerimise struktuur on dokumenteeritud ja kõigile edastatud?

M 2.259z Üldise dokumendihaldussüsteemi kasutuselevõtt

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: IT-juht, administraator

Elektroonilise arhiveerimise käigus peavad kõik dokumendid olema üheselt identifitseeritavad ja taastatavad. Kuna üldjuhul tuleb hallata suuri andmekogumeid, soovitatakse kasutada dokumendihaldussüsteemi (edaspidi DHS-i) ning seda ka väikeste ja keskmiste ametiasutuste ja ettevõtete puhul.

Dokumendihaldussüsteem

DHS moodustab liidese kasutaja (programmide) ja arhiivisüsteemi vahel ning tagab elektrooniliste dokumentide ühtlase haldamise, versioonimise ja indekseerimise.

Indeksiandmebaasi hooldamine

DHS hoolitseb regulaarselt ka indeksiandmebaasi hooldamise eest, hallates koos elektrooniliste dokumentidega arhiveeritavat kontekstiinfot ja täiendades seda vajaduse korral DHS-i komponentidega. Seejuures eristatakse süsteeme, mille puhul asuvad andmebaasis lisaks indeksitele ka dokumendid ise ja süsteeme, mille andmebaasides asuvad ainult viited vastavas salvestisüsteemis hoitavatele dokumentidele. Esimeste süsteemide andmebaasi maht on piiratud ja need ei sobi suurte andmehulkade arhiveerimiseks.

Pääsuõigused ja klassifikatsioon

Dokumendihaldussüsteem peab võimaldama määrata arhiveeritud dokumentide ja indeksiandmebaasi juurdepääsuõigusi. DHS peaks toetama ka dokumentide jaotamist eri klassidesse. Võimalik peab olema määrata profiile ja viitetabeleid, mille alusel saab dokumente liigitada ja tähistada märksõnadega. DHS-i omadused peavad pikaks ajaks tagama, et arhiveeritud dokumendid oleksid üheselt identifitseeritavad, et need oleksid kaitstud ja taastatavad.

Sidumine organisatsiooni tööga

Dokumendihaldussüsteeme tuleb sobival moel kasutada ja siduda organisatsiooni tööprotsessidega. Selleks tuleb defineerida vastavad organisatsioonilised protsessid, need dokumenteerida ja ametiasutuses või ettevõttes ellu viia. Reguleerimist vajavad muu hulgas järgnevad töövaldkonnad:

- dokumentide loomine DHS-is,
- DHS-i kasutamine dokumentidega ümberkäimisel,
- DHS-i kasutamise ja käitamise vastutus,
- õiguste määramine ja sellekohased volitused ning
- DHS-i käitamisnõuded (teenusetasemelepped).

Lõpuks tuleks organisatsiooni tööprotsessidega tagada, et dokumendi haldust kasutataks ettenähtud moel ja et sellest ei oleks võimalik mööda minna. Ainult nii on võimalik tagada organisatsioonis kasutatavate elektrooniliste dokumentide ja info täielik ja järjepidev arhiveerimine.

Standardiseerimine

Turustatavad dokumendihaldus- ja arhiivisüsteemid ei ühildu kõik omavahel. Selle põhjus võib olla nii kasutatud tehnoloogiad kui ka kasutatud andmekandjate ja andmesalvestuse formaadid. Probleemi lahendamiseks teevad enamlevinud DHS-ide tootjad omavahel koostööd eesmärgiga ühtlustada dokumendihalduse aluseks olevaid dokumentide salvestamis- ja taastamistehnoloogiaid. DHS-i valimisel tuleb arvestada asjakohaste standarditega, et DHS-i ja arhiivi komponente saaks pikka aega kasutada.

Olulisemad grupid/standardid on järgmised:

ODMA – rakenduste liidesed. AIIM-i (Association for Information and Image Management) juures tegutseb standardiseerimiskomiteena ODMA-grupp (Open Document Management API). ODMA tähistab standardiseeritud liidest dokumendihaldussüsteemi ja kasutaja rakenduste vahel. See lihtsustab rakendustega sidumist. Suurem osa tootjatest kasutab seda standardit.

DMA – erinevate DHS-ide integreerimine. AIIM moodustas DMA (Document Management Alliance) eraldi projektigrupina.See tekkis kolme samuti DHS-i valdkonnas töötanud standardiseerimiskomitee liitumisest:

1. ISO-grupp Document Filing and Retrieval – ISO 10166
2. Document Enabled Networking
3. Shamrock Document Management Coalition

- DMA juurutab standardit, mille abil saab lihtsalt integreerida erinevate platvormide ja süsteemide dokumendikogumeid ja andmete haldustarkvara. Kasutajal tekib seeläbi ühtne ülevaade kõikidest dokumenditüüpidest, olenemata salvestamise või loomise kohast. Seda standardit kasutavad peaaegu kõik juhtivad tootjad. Siiski tuleb igal konkreetsel juhul kontrollida, kas standardit on järgitud.
- WfMC – erinevate tööplaneerimistoodete koosmõju. WfMC (Work flow Management Coalition, Belgias) töötab töövoogude standardiseerimisorganisatsioonina. Eesmärk on luua tarkvaraspetsifikatsioonid, mille abil luua erinevates keskkondades ühtsed eeldused erinevate töövoo planeerimist võimaldavate toodete (workflow products) ja komponentide koostööks. Peaaegu kõik tuntud tootjad teevad selle komiteega koostööd.

Kontrollküsimused:

- Kas on välja selgitatud, kui suur vajadus on dokumendihaldussüsteemi kasutamise järele?
- Kas DHS-i käitamise ja kasutamise vastutusalad on dokumenteeritud ja töötajatele teada?
- Kas DHS-i kasutamine on muudetud organisatsioonis kohustuslikuks ning kas vastav kohustus on dokumenteeritud?
- Kas DHS võimaldab töörollide ja pääsuvolituste määramist ja kontrolli?
- Kas DHS toetab kehtivate standardite kasutamist?

M 2.260 Arhiveerimisprotseduuri regulaarne auditeerimine

Algatamise eest vastutavad: IT turvaosakond, audiitor
Rakendamise eest vastutavad: IT turvaosakond, audiitor, arhiivi haldaja

Arhiveerimisprotsess peab läbima regulaarse auditi, et oleks võimalik veenduda selle õigsuses ja nõuetekohases toimimises ning hinnata arhiivisüsteemi salvestatud dokumentide õigsust ja autentsust. Selleks tuleb meetmes M 2.243 Arhiveerimiskontseptsiooni väljatöötamine kirjeldatud kontseptsiooni kohaselt töötada välja sobiv auditeerimisprotseduur ja dokumenteerida see kontrollnimekirja vormis.

Vastav kontrollnimekiri peaks sisaldama vähemalt järgnevaid punkte:

Küsimused vastutusalade kohta

- Kas vastutavad isikud on nimetatud ja kas neile on nende ülesandeid selgitatud? Kas see on dokumenteeritud?
- Kas kõikidele vastutavatele isikutele on määratud asendajad?

Organisatsiooni tööprotsessi kajastavad küsimused

- Kas elektroonilise arhiveerimise rakendamise kohta on olemas tervet organisatsiooni hõlmavad reeglid?
- Kas terve organisatsiooni ulatuses on reguleeritud ja dokumenteeritud, millised dokumendid tuleb arhiveerida? Kas vastavad reeglid on piisavalt laiaulatuslikud ja täielikud?
- Kas kõik dokumentidele kehtestatud turvanõuded on dokumenteeritud?
- Kas tervet organisatsiooni hõlmavaid reegleid kohandatakse regulaarselt hetkeoludega?
- Kas kõik reeglite ümbertöötamised dokumenteeritakse ja arhiveeritakse regulaarselt ning nõuetekohaselt?

Arhiveerimist kajastavad küsimused

- Kas arhiveerimise kohta on olemas selged reeglid, millistele dokumentidele kehtib arhiveerimiskohustus?
- Kas arhiveeritavate dokumentide kontekstiandmete koostamise kohta on olemas dokumenteeritud reeglid, näiteks dokumendi kategooriate määramise reeglid?
- Kas arhiveeritavad dokumendid arhiveeritakse täies mahus ja kas neid on võimalik taastada?
- Kas arhiveeritavate dokumentide puhul järgitakse konfidentsiaalsusnõudeid?
- Kas arhiveeritavate dokumentide puhul järgitakse autentsusnõudeid?
- Kas arhiveeritavate dokumentide puhul järgitakse terviklusnõudeid?

- Kas arhiveeritavate dokumentide puhul järgitakse käideldavusnõudeid?
- Kas arhiveerimisel järgitakse seadustest tulenevaid eeskirju?
- Kas kõik kasutajad ja administraatorid on saanud oma rollile ja tööülesannetele vastavad koolitused ja juhised? Kas see on dokumenteeritud?

Arhiiviandmete liiasust kajastavad küsimused

- Kas arhiiviandmed salvestatakse piisava liiasusega, nt liiasust võimaldavate arhiivisüsteemide abil või varukoopiatena eraldi andmekandjatele?
- Kas arhiivisüsteeme ja vajaduse korral ka arhiiviandmeid varundatakse regulaarselt?
- Kas andmete varundamine toimub kooskõlas vastavate nõuetega?
- Kas varundatud arhiiviandmed on täielikud ja loetavad?
- Kas viimase auditiga võrreldes on esinenud andmekadu? Kui jah, siis kui sagedad ja kui tõsised olid need juhtumid?
- Kas arhiveeritud dokumentide taastamisel esineb vigu? Kui jah, siis kui sageli seda esines ning kas vead olid kõrvaldatavad?

Haldamist kajastavad küsimused

- Kas arhiivi andmekandjate puhul järgitakse kehtivat värskendustsüklit (refresh)?
- Kas ebavajalikud, täiskirjutatud arhiveerimise andmekandjad hävitatakse ja kas neid käideldakse nõuete kohaselt?
- Kas lugemisseadmeid ja andmekandjaid on varutud piisavas koguses?

Arhiivisüsteemi tehniline hindamine

Arhiivisüsteemi audit peaks sisaldama ka komponentide ja kasutatud failiformaatide tehnilist hindamist. See aitab õigel ajal rakendada tehnilisi edasiarendusi ja võimaldab viia ennast varakult kurssi tootjate planeeritavate arhiivisüsteemi tehniliste muudatustega. Auditi käigus võib selguda, et arhiivisüsteemi tehnilisi komponente on tarvis muuta. Sellises olukorras tuleb tagada, et väljavahetatud komponendid, nt kettaseadmed, andmekandjad ja operatsioonisüsteemi tarkvara suudaksid töötada veatult koos kõikide teiste komponentidega ja säilitaksid tööks vajalikud funktsioonid. Auditite tulemused tuleb samuti arhiveerida, rakendades samu nõudeid, mis kehtivad arhiveerimisprotsessile.

Kontrollküsimused:

- Kas arhiveerimisprotsessi auditeeritakse regulaarselt?
- Kas auditite läbiviimise protseduur on dokumenteeritud?
- Kas auditite tulemused arhiveeritakse?

M 2.261 Regulaarsed arhiivisüsteemide turu-uuringud

Algatamise eest vastutavad: IT-juht, arhiivi haldaja
Rakendamise eest vastutavad: IT-juht, arhiivi haldaja

Arhiiviandmete nõutav säilitamisaeg on tavaliselt mitu korda pikem kui elektroonilise arhiivi üksikute komponentide keskmine oodatav kasutusiga. See kehtib nii riistvara- kui ka tarkvarakomponentide puhul. Pikaajalise arhiveerimise kõigi vajalike funktsioonide tagamisel tuleb lähtuda sellest, et üksikuid riistvarakomponente, terveid mooduleid või ka tarkvarakomponente võib olla tarvis olenevalt asjaoludest isegi korduvalt vahetada. Siinkohal on oluline säilitada regulaarne ülevaade pakutavatest toodetest. Seeläbi saab võimalikke muudatusi õigel ajal märgata.

Muudatused võivad olla muu hulgas järgnevad:

- salvestusformaatide senise standardi muutmine või uue standardi kasutuselevõtt,
- kasutatud arhiivisüsteemi tootja algatatud muudatused või muudatused tema salvestikomponentides (uue süsteemiplatvormi kasutuselevõtt, vana tooteseeria tootmise ja toe lõpetamine, andmekandjate tootmise lõpetamine, tootja maksevõimetus),
- turvaaukude või nõrkade kohtade ilmsikstulek, nt kasutatud krüpteerimisalgoritmides.

Kontakti loomine tootjaga

Kõikide asjassepuutuvate tootjatega on soovitatav luua regulaarne kontakt, nt infofoorumites, uudistegruppides ja meililistides, kus edastatakse regulaarselt uut infot kasutusesoleva arhiivisüsteemi kohta.

Info kogumine ja hindamine

Ülalmainitud info regulaarse hankimise eest peaks vastutama vähemalt üks konkreetne isik, kes peaks kasutatud arhiivisüsteemi konteksti alusel hindama vastava info olulisust ja soovitama vajaduse korral ka vajalikke meetmeid. Selleks tuleb kindlaks teha, kuidas algatada vajaduse korral süsteemi üleviimist. Selles kontekstis kogutud info peab kajastuma arhiveerimisprotsessi regulaarsetes auditites (vt M 2.260 Arhiveerimisprotseduuri regulaarne auditeerimine).

Kontrollküsimused:

- Kas on määratud konkreetne isik, kes vastutab info kogumise eest?
- Kas osaletakse regulaarselt vastavates infofoorumites?
- Kas on määratud, kuidas algatatakse arhiivisüsteemi üleviimine?

M 2.262 Arhiivisüsteemide kasutamise reguleerimine

Algatamise eest vastutavad: IT-juht, arhiivi haldaja
Rakendamise eest vastutavad: IT-juht, arhiivi haldaja, administraator

Arhiivisüsteemi nõuetekohase kasutamise tagamiseks arhiveerimiskontseptsiooni järgi (vt M 2.243 Arhiveerimiskontseptsiooni väljatöötamine) tuleb kehtestada vajalikud reeglid. Selleks tuleb koostada arhiivisüsteemi kasutamist ja administreerimist reguleerivad suunised. Suunised tuleb juurutada institutsiooni väljakujunenud tööprotsessidesse ja teha kõigile teatavaks. Välispersonali rakendamisel tuleb ka neid kohustada vastavaid suuniseid järgima.

Haldusalased suunised

Haldusalased suunised peaksid sisaldama vähemalt järgnevaid punkte:

- arhiivisüsteemi käitamise ja haldamise eest vastutavate töötajate määramine,
- kokkulepe arhiivisüsteemi jõudlusparameetrite kohta (teenusetasemelepped), eriti oluline juhul, kui administreerimine või käitamine toimub väljaspool institutsiooni,
- arhiivisüsteemi ja arhiivi andmekandjate juurdepääsu- ja pääsuõiguste määramise reeglid,
- arhiivi pakutavate teenuste kasutamist võimaldavate pääsuõiguste määramise reeglid,
- reeglid arhiveeritud andmete ja arhiveerimis-andmekandjatega ümberkäimiseks,
- arhiivisüsteemi ja arhiivi andmekandjate keskkonnatingimuste jälgimine,
- rakendatava arhiivisüsteemi tarkvarakomponentide andmevarunduse reeglid,
- arhiivisüsteemi sündmuste logimine.

Kasutajatele mõeldud suunised

Kasutajatele mõeldud suunised peaksid sisaldama vähemalt järgnevat:

- selgitus elektroonilise arhiveerimise eesmärkide ja arhiveeritud dokumentide hoiutähtaegade kohta,
- arhiivisüsteemiga seotud töötajate vastutusalade määramine,
- arhiivisüsteemi kohustuslike rakendusvaldkondade määratlemine,
- arhiivi pakutavate teenuste kasutamist võimaldavate pääsuõiguste määramise reeglid,
- töötajatele esitatavad koolitusnõuded, mis on aluseks arhiivi kasutamise lubamiseks,
- arhiveeritud dokumentidele kontekstiinfo lisamise reeglid, vt M 2.258 Dokumentide järjekindel indekseerimine arhiveerimisel ,

- kohustus arhiivist otsitud dokumentidega hoolikalt ümber käia, arvestades info võimalike kasutuseesmärkidega,
- reeglid dokumentidega ümberkäimiseks pärast määratud arhiveerimisaja lõppemist,
- reeglid, mis keelavad kasutada andmeid, mis tuleb teatud aja möödudes kohutuslikus korras kustutada vaatamata tõsiasjale, et andmed võivad olla tehniliselt veel täiesti kasutuskõlblikud,
- reeglid isikuandmetega ümberkäimiseks,
- arhiivisüsteemi kaitsemehhanismide kasutamine, võimaldamaks hilisemat dokumentide tervikluse ja autentsuse kontrollimist, samuti vajaliku konfidentsiaalsuse tagamist,
- kohustus kontrollida dokumentide terviklust ja autentsust enne nende edasikasutamist,
- juhised failide kohta, mille terviklust ei suudetud kontrollida, nt ebaõnnestunud allkirjakontrolli tõttu,
- arhiivisüsteemi kasutajatega seotud sündmuste logimine,
- arhiivisüsteemi kasutamise tasuarvestuse reeglid, kui arhiivi kasutab mitu organisatsiooniüksust.

Reeglid peavad olema dokumenteeritud, samuti peab olema kirjalikult fikseeritud administraatorite ja kasutajate reeglitest teavitamine.

Kontrollküsimus:

- Kas arhiivisüsteemi kasutamise reeglid on dokumenteeritud ja kas nende rakendamine on ametiasutuses/ettevõttes kohustuslik?

M 2.263 Arhiveeritud andmeressursside regulaarne regenereerimine

Algatamise eest vastutavad: IT-juht
Rakendamise eest vastutavad: IT-juht, arhiivi haldaja

Nõuetekohase arhiveerimise tagamiseks tuleb arhiveerimisel kindlustada järgmiste punktide täitmine:

- kasutatud failiformaat peab vastama kaasaja tehnilistele nõuetele ja olema rakenduste jaoks kasutatav nii praegu kui ka tulevikus,
- salvestatud andmed peavad olema loetavad ka tulevikus ja taastatavad selliselt, et säiliks semantika ja tõendusvõime,
- kõik rakendatavad komponendid peavad suutma töödelda andmekandjal kasutatud failisüsteemi,
- andmekandjad peavad alati olema füüsiliselt vigadeta loetavad,
- rakendatavad krüptograafilised ja digitaalallkirja kasutamise protseduurid peavad vastama kaasaja tehnilistele nõuetele ning
- kõiki salvestusüksuse komponente (andmekandjaid, kettaseadmeid, andmekandja valimisseadmeid ning juhttarkvara) peab olema võimalik välja vahetada ja hooldada.

Kui on oht, et mõnda loetletud nõuet ei suudeta lähitulevikus enam tagada, tuleb sellest puudutatud süsteemid välja vahetada. Siinkohal tuleb arvestada, et protseduuri käigus uuele andmekandjale kopeeritav arhiveeritud andmete maht võib olla väga suur.

Ühilduvuse testimine
Krüpteeritud või allkirjastatud dokumentide regenereerimise kohta leiate infot meetmetest M 2.264 Krüpteeritud andmete regulaarne regenereerimine arhiveerimisel ja M 2.265z Digitaalallkirjade õige kasutamine arhiveerimisel .

Kontrollküsimus:

- Kas andmekandjate säilitamise ja sellest tulenevate tööjuhiste kohta, mis reguleerivad andmete ümberkopeerimist uutele andmekandjatele, on olemas vastav dokumentatsioon?

M 2.264 Krüpteeritud andmete regulaarne regenereerimine arhiveerimisel

Algatamise eest vastutavad: IT-juht, IT turvaosakond

Rakendamise eest vastutavad: IT-juht, IT turvaosakond, administraator

Krüptoprotseduuride tehnoloogia vananeb pidevalt, kuna aja jooksul tulevad arendustöö käigus ilmsiks matemaatilised või tehnilised puudujäägid, mida protseduuride valimise hetkel kas ei tuntud või mis olid ebaolulised. Kui andmeid on tarvis säilitada kümme aastat või kauem, tuleb krüpteeritud või allkirjaga varustatud andmete usaldusväärsuse ja tervikluse tagamiseks vastavad andmed korduvalt uute võtmete ja vajaduse korral ka uute algoritmidega ümber krüpteerida.

Krüptograafilise arengu jälgimine

Algoritmi usaldusväärsuse ja piisava turvalisuse hindamiseks tuleb krüptograafiavaldkonnas toimuvaid arenguid pidevalt jälgida. Lisaks tuleb pidevalt uurida usaldusväärseid infoallikaid, et näha, kas on avastatud võimalusi olemasolevate protseduuride kompromiteerimiseks.

Õigeaegne korduvkrüpteerimine/allkirjastamine

Kui kasutatud krüptograafilised protseduurid iganevad ja ei suuda enam krüpteeritud andmete usaldusväärsust või terviklust tagada, tuleb andmed uuesti krüpteerida või allkirjastada.

Ümberkrüpteerimisel tuleb arvestada järgmiste aspektidega (vt B 1.7 Krüptokontseptsioon):

- Kasutada tuleb hetkeoludes turvaliseks peetavat krüpteerimisalgoritmi, mille puhul võib eeldada, et see tagab pikaajalise turvalisuse.
- Krüpteerimiseks ja võtmete jagamiseks tuleb valida protseduur, mis sobib arhiveerimiseks kasutatavatele rakendustele kehtivate nõuetega.
- Uute krüpteerimisprotseduuri võtmete edastamine kasutajatele peab toimuma turvaliselt.
- Krüpteerimisvõtmed tuleb autentida (nt elektroonilise sertifikaadi abil).
- Esialgne fail tuleb pärast krüpteerimist hävitada, WORM-andmekandjate puhul hävitada kogu andmekandja.
- Kui korduvkrüpteerimise käigus sorteeritakse mõned andmekandjad välja, tuleb ka need turvaliselt utiliseerida.
- Lisaks peamistele andmekandjatele tuleb ka varukoopiate andmekandjaid turvaliselt käidelda või vanad failid turvaliselt kustutada.

Võtmeid võib jagada kahel erineval moel. Kui võtmete genereerija on sõltumatu usaldusväärne organ, tuleb tagada, et võtmed edastataks konfidentsiaalselt ja võltsimata kujul dokumendi esialgsele omanikule. Kui krüpteerimisel kasutatakse asümmeetrilisi meetodeid, võib dokumendi omanik ka ise uue võtmepaari genereerida ja edastada avaliku võtme arhiveerimisega tegelevale osakonnale.

Etteplaneerimine ja ajakulu

Tuleb arvestada, et korduvkrüpteerimine vajab alati teatud etteplaneerimist: tegevusest tuleb teavitada andmete ja võtmete omanikke, lisaks tuleb genereerida

ja jaotada uued vajalikud võtmed. Kui erinevaid omanikke on palju ja andmehulgad suured, tuleb planeerida suuremamahulisteks töödeks vajalik aeg. Uue, eeldatavasti võimalikult pika usaldusväärusega krüpteerimisprotseduuri valimisel tuleks kaaluda mõnda nüüdisaegset ja tunnustatud turvalisusega algoritmi. Kui hetkel kasutuses olevale algoritmile pole head alternatiivi, tuleks kontrollida, kas ajutise lahendusena võiks kõne alla tulla võtmepikkuse suurendamine.

Varukoopia-andmekandjad

Pärast korduvat krüpteerimist ja arhiveerimist tuleb vanad andmekogumid turvaliselt hävitada. Kui algfailid olid arhiveeritud WORM-andmekandjatele, tuleb vana krüpteeringuga failide andmekandjad turvaliselt hävitada. Korduvkirjutusega andmekandjatelt tuleb andmed turvaliselt kustutada (vt M 2.167 Andmete kustutamiseks või hävitamiseks sobivate lahenduste valik). Ka varukoopia-andmekandjatel asuvad andmed tuleb uuesti krüpteerida ja vanad varukoopia-andmekandjad vajaduse järgi kas kustutada või hävitada.

Kontrollküsimused:

- Kas jälgitakse krüptograafia valdkonnas toimuvaid arenguid?
- Kas korduvkrüpteerimise vastutusalad on selgelt määratud?
- Kas vanad andmekandjad hävitatakse turvaliselt?
- Kas korduv krüpteerimine hõlmab ka andmete varukoopiaid?

M 2.265z Digitaalallkirjade õige kasutamine arhiveerimisel

Algatamise eest vastutavad: IT-juht, IT turvaosakond

Rakendamise eest vastutavad: IT-juht, IT turvaosakond, arhiivi haldaja, administraator

Digitaalallkirjad kujutavad endast elektroonilisel arhiveerimisel suurt väljakutset, kuna tehnilistel põhjustel pole nende kasutusiga eriti pikk ja kasutusea pikkus pole alati ette teada. Teisest küljest on need aga arhiveerimisel vajalikud elektrooniliste dokumentide tõendamisvõime säilimiseks. Digitaalallkirjade kaalukus sõltub olulisel määral nende tõlgendamisest kontrollimise hetkel, seega nn kehtivusmudelist. Kuna digitaalallkirju rakendatakse reaalselt alles mõni aasta, puuduvad digitaalselt allkirjastatud dokumentide arhiveerimise kohta pikaajalised kogemused.

Kehtivus ja tõendamisvõime

Nimetatud kahte digitaalallkirja omadust defineeritakse tavaliselt järgmiselt: digitaalallkiri on kehtiv järgnevatel asjaoludel:

- allkiri on matemaatiliselt õige ja
- allkirja andmise hetkel oli kehtiv ka vastav allkirjavõti.

Digitaalallkiri on tõendamisvõimeline järgnevatel asjaoludel:

- kui allkiri oli kontrollimise hetkel kasutatud kehtivusmudeli kohaselt kehtiv ja
- kui juurdekuuluv allkirjavõti pole kompromiteeritud.

Digitaalallkirjade kaalukus

Digitaalallkirju saab kasutada erineval otstarbel, muu hulgas

- failide tervikluse tõendamiseks,
- krüptograafiliste võtmete või elektrooniliste dokumentide autentsuse tõendamiseks,
- autentimiseks.

Digitaalallkirja kasutamine ja kaalukus tuleb määrata rakenduse põhjal vastava turvapoliitika (policy) raames. Poliitikas tuleks muu hulgas määratleda järgnevad punktid:

- millised on digitaalallkirja loomise eeldused,
- kus toimub digitaalallkirjade loomine (sertifikaatide allkirjastamisel nt neutraalne usalduskeskus (trust center),
- milline on rakenduse puhul kasutatav kehtivusmudel,
- kas ja milliseid digitaalallkirju saab vajaduse korral tühistada ning
- milline on allkirja olulisus, st mida sellega kinnitatakse (nt ajatempli puhul dokumendi olemasolu teatud ajahetkel).

Poliitika tuleb kirjalikult dokumenteerida ja arhiveerida, et allkirja hilisemal kontrollimisel oleks selge, milline on allkirja sisu (st mida allkiri tõendab). Lisaks tuleb poliitika sobival kujul avaldada, et kõik allkirjade usaldamisest sõltuvad osapooled saaksid seda infot kasutada.

Digitaalallkirjade kasutusiga

Digitaalallkirjade kasutusiga piirab riistvara ja tarkvara tehniline areng, samuti edusammud krüptograafia valdkonnas (vt G 2.79 Arhiivisäilikute digitaalsignatuuride regenereerimise puudused ja G 4.47 Vananenud krüptomeetodid). Üldjuhul võib eeldada, et digitaalallkirjad vananevad umbes viie aastaga, kuna nende kaalukus väheneb. Seega tohiks usalduskeskus väljastada võtmesertifikaate ja ajatempleid ainult maksimaalselt viieks aastaks. Vajaduse korral saab nende kehtivuse tühistada ka enne kasutusperioodi lõppemist. Seda nimetatakse sulgemiseks.

Võtmesertifikaatide sulgemine

Kui sertifitseerimisorgan sulges võtmesertifikaadi, nt kompromiteeritud allkirjavõtme tõttu, tuleb kiirelt tegutseda. Sellest hetkest alates on kõik vastava võtmega antud allkirjad sisutühjad (nt pole enam kasutatavad tõendamiseks). Allkirjade kehtivus sõltub siiski ka kehtivusmudelist. Erinevalt kestmudelist ei ole ahelmudeli võtmete kompromiteerimisel edasised sammud ilmtingimata kohe vajalikud. Otseselt võib olla mõjutatud arhiveeritud dokumentide kaalukus. Kui asjassepuutuvad arhiveeritud dokumendid on allkirjastatud kehtetu võtmega, ei ole see allkiri olenevalt kehtivusmudelist enam tõendamisvõimeline.

Soovitus

Digitaalselt allkirjastatud dokumentide arhiveerimisel puuduvad hetkel testitud standardid, mille kasutamisega oleks võimalik tagada allkirjade pikaajalist kehtivust ja tõendamisvõimet. Seni kuni vastavaid standardeid veel pole, tuleks pikaajalise arhiveerimisega kaasnevate ohtudega arvestamisel lähtuda järgmistest soovitustest:

- Allkirjade ja sertifikaatide kaalukus tuleb dokumenteerida vastavas poliitikas. Ka poliitika ise tuleb arhiveerida.
- Võtmesertifikaatide ja ajatemplite genereerimiseks tuleks kasutada sõltumatu usalduskeskuse teenuseid.
- Kõik dokumendi juurde kuuluvad allkirjad, ajatemplid, sertifikaadid ning allkirja/sertifikaadi kontrollimiseks vajaminevad võtmed tuleb samuti arhiveerida. See võib toimuda kohapeal või tsentraliseeritult läbi usalduskeskuse.
- Olenevalt allkirjade kaalukuse nõudest tuleb muu hulgas arhiveerida täiendav kontekstiinfo. Allkirjastamise seaduse kohaselt kuulub kvalifitseeruvate allkirjade puhul siia alla näiteks sertifitseerimisteenuse pakkuja kataloogiteenuse info.
- Digitaalallkirjaga dokumentide arhiveerimisel on soovitatav nii dokument ise kui ka kõik selle dokumendi juurde kuuluvad allkirjad, ajatemplid, sertifikaadid ja kehtivuskinnitused kaitsta räsitud ajatemplitega. Kui kaitsmiseks moodustatud ajatemplites kasutatud räsifunktsioon hakkab nõrgenema, tuleb kogu protsessi korrata, st kaitsta nii dokument ise, sertifikaadid, kehtivuskinnitused, ja ajatemplid (sh kaitsmiseks mõeldud ajatemplid) uuel ja turvalisemal räsifunktsioonil põhinevate ajatemplitega.
- Digitaalallkirja kontrollimine ebaõnnestub kohe, kui dokumendi või selle allkirja kasvõi üksainus bitt on muudetud. Seega on allkirja kehtivuse tagamiseks ilmtingimata oluline, et arhiveerimine toimuks bitise täpsusega. Sel põhjusel tuleb digitaalselt allkirjastatud dokumentide salvestamisel rakendada vastavaid veakorrektuurimeetmeid.

- Elektroonilise arhiveerimise eest vastutavad töötajad peavad end pidevalt digitaalallkirjade valdkonnas toimuvaga kursis hoidma.

Arhiveerimismudelid

Alljärgnevalt kirjeldatakse erinevaid mudeleid, mida kasutatakse digitaalselt allkirjastatud dokumentide arhiveerimisel. Esialgu jätame siinkohal käsitlemata võtmehalduse info (näiteks sertifikaatide või keelunimekirjade) arhiveerimise. Seni kuni kirjeldatud mudeli puhul pole oluline, kas originaaldokument sisaldab ühte või mitut allkirja, räägitakse ühest originaalallkirjast. Mitut originaalallkirja mainitakse ainult siis, kui see muudab arhiveerimisfunktsioone. Mudelite kirjelduse struktuur on kujundatud järgnevate punktide alusel:

- vajalik infrastruktuur
- allkirjastatud dokumendi arhiveerimisprotseduur
- arhiivi dokumendipäringu protseduur
- arhiveerimisel tekkinud lisaallkirjade semantika, st mida need allkirjad kinnitavad?
- originaalallkirja tõendamisvõime kontrollprotseduur
- arhiveerimises osalevate organite vajalik usaldamine

Kirjeldusele järgneb lühike mõtteavaldus erinevate mudelite kohta.

Mudel nr 1: laekumistempliga arhiveerimisorgan

- **Infrastruktuur** – usaldusväärne arhiveerimisorgan, mis pakub ka sertifitseerimisteenuseid (trust center).
- **Arhiveerimisprotseduur** – dokument arhiveeritakse arhiveerimisorganis koos dokumendi laekumise hetke märkiva infoga.
- **Päringuprotseduur** – arhiveerimisorgan allkirjastab dokumendi allkirjastamispäringu laekumise hetkel digitaalselt koos infoga dokumendi laekumise kohta. Arhiveerimisorgani allkiri tõendab dokumendi autentsust ja kaitseb dokumendi terviklust.
- **Arhiveerimisorgani digitaalallkirja semantika** – dokumendipäringule antava allkirjaga kinnitab arhiveerimisorgan, et vastav dokument on laekunud ja arhiveeritud näidatud hetkel.
- **Originaalallkirja tõendamisvõime kontrollimine –** dokumendi autentsuse ja tervikluse verifitseerimiseks kontrollitakse esmalt arhiveerimisorgani allkirja. Originaalallkiri on tõendamisvõimeline vaid juhul, kui see oli dokumendi arhiveerimisorganisse laekumise hetkel tõendamisvõimeline. Vastava kontrolli peab läbi viima kasutaja. Vajalikud sertifikaadid võib kasutaja saada kas sellelt samalt arhiveerimisorganilt koos dokumendiga või tuleb tal esitada vastav avaldus mõnda teise sobivasse kohta.
- **Usaldusmudel** – arhiveerimisorganit usaldatakse allkirjastatud dokumentide terviklikus salvestamises ja dokumendi laekumise aja õigsuses. Kui ründe läbiviijal õnnestub muuta dokumendi saabumise aega, mõjutab ta sellega dokumendi tõendamisvõimet. Hilisema ajahetke määramisega on võimalik dokumendi tõendamisvõimet tühistada. Teisest küljest saab kehtiva, kuid tõendamisvõimetu allkirjaga varustatud dokumendi puhul teeselda tõendamisvõimet, määrates laekumise hetke tegelikust varasemaks. Dokumendi

laekumise aja korrektne salvestamine ja säilitamine tuleb tagada sobivate kaitsemeetmetega. Selleks võib kasutada digitaalallkirju nagu ka mudelite nr 3 ja nr 4 puhul.

Mudel nr 2: kinnitustempliga arhiveerimisorgan

- **Infrastruktuur** – usaldusväärne arhiveerimisorgan, mis pakub ka sertifitseerimisteenuseid (trust center).
- **Arhiveerimisprotseduur** – dokumendi laekumisel arhiveerimisorganisse kontrollitakse dokumendi originaalallkirja tõendamisvõimet. Dokument arhiveeritakse ainult siis, kui kontrollimise hetkel on võimalik kinnitada selle tõendamisvõimet. Mitme originaalallkirja puhul kontrollitakse nende tõendamisvõimet ükshaaval. Dokument arhiveeritakse koos üksikute allkirjade tõendamisvõimet kajastavate andmetega, kui vähemalt üks originaalallkirjadest on tõendusvõimeline.
- **Päringuprotseduur** – päringu hetkel väljastab arhiveerimisorgan dokumendile digitaalallkirja, vajaduse korral ka koos andmetega originaalallkirjade tõendamisvõime kohta. Arhiveerimisorgani allkiri tõendab dokumendi autentsust ja kaitseb dokumendi terviklust.
- **Arhiveerimisorgani digitaalallkirja semantika** – arhiveerimisorgani allkiri kinnitab originaalallkirja tõendamisvõimet. Mitme originaalallkirja puhul kinnitatakse nende kaasatulnud tõendamisvõime andmed ükshaaval.
- **Originaalallkirja tõendamisvõime kontrollimine** – arhiivi vastuse autentsuse ja tervikluse verifitseerimiseks kontrollitakse esmalt arhiveerimisorgani allkirja. Originaalallkirja tõendamisvõime tuleneb kaasatulnud andmetest või arhiveerimisest endast.
- **Usaldusmudel** – arhiveerimisorganit usaldatakse allkirjastatud dokumentide terviklikus salvestamises ja arhiveerimisele eelneva dokumendi tõendamisvõime kontrollimises. Kui ründajal õnnestub varem kehtinud allkirja võtmest märkamatult jagu saada ja ta suudab arhiivi sisse viia võltsitud allkirjadega dokumente, käsitletakse neid tõendamisvõimeliste dokumentidena. Seega tuleb sobivate meetmete abil tagada, et allkirjastatud dokumentide tõendamisvõimet kontrollitaks enne arhiivi lisamist ja et andmekogum oleks andmete volitamata lisamise eest kaitstud.

Mudel nr 3: ajatempli teenusega usalduskeskus (trust center)

- **Infrastruktuur** – omavahel suhtleva arhiveerimisorgani ja usaldusväärse ajatempli teenuse (usalduskeskuse) lahutamine.
- **Arhiveerimisprotseduur** – arhiveerimisorganisse laekuva dokumendi originaalallkirja tõendamisvõime kinnitatakse usalduskeskuse ajatempliga ja originaalallkirja tõendusvõime lõppeb koos templi tõendamisvõime lõppemisega. Enne viimase ajatempli tõendamisvõime lõppemist annab usalduskeskus regulaarselt kogu dokumendile, st dokumendile koos kõikide allkirjadega uue templi.
- **Arhiveeritud dokumendi struktuur** – arhiveeritud dokument sisaldab vähemalt allkirjastatud originaaldokumenti ja seda dokumenti kajastavat ajatemplit. Struktuur pikeneb aja jooksul täiendavate ajatemplite tõttu, mis mää-

ratakse allkirjastatud originaaldokumendi kaudu koos kõikide seniste ajatemplitega.

- **Päringuprotseduur** – dokument koos kõikide ajatemplitega saadetakse teele kõige värskemas olekus.
- **Ajatempli semantika** – ajatempliga märkimisel kinnitatakse spetsiaalselt selleks otstarbeks ettenähtud usalduskeskuse allkirjaga, et dokument oli ajatemplis näidatud hetkel olemas.
- **Originaalallkirja tõendamisvõime kontrollimine** – viimase ajatempli tõendamisvõimet kontrollitakse vahetult. Kõiki teisi ajatempleid kontrollitakse, verifitseerides nende tõendamisvõimet vastava järgneva ajatempli suhtes (rekursiivne verifitseerimine). Originaalallkirja tõendamisvõime kontrollimine toimub hetkel, mis on märgitud esimeses ajatemplis.
- **Usaldusmudel** – arhiveerimisorganit usaldatakse dokumentide terviklikus salvestamises. Usalduskeskuse puhul usaldatakse pakutavat ajatempli teenust. Ajatemplite ahela abil saab originaalallkirja tõendamisvõimet tõendada ilma lünkadeta.

Mudel nr 4: arhiveerimistempli teenusega usalduskeskus (trust center)

- **Infrastruktuur** – omavahel suhtleva arhiveerimisorgani ja usaldusväärse arhiivitempli teenuse (usalduskeskuse) lahutamine.
- **Arhiivitempli funktsioon** – kui dokument märgistatakse arhiivitempliga esimest korda, vastab see protseduur ajatempliga märgistamisele: dokument märgistatakse ajatempliga. Kui dokument on aga arhiivitempli teenuse juba ühe korra läbinud ja ajatempliga varustatud, kontrollitakse arhiivitempliga uuesti märgistamisel esmalt ajatemplit. Dokument koos ajatempliga allkirjastatakse spetsiaalse arhiiviallkirjaga ainult siis, kui ajatempel on tõendamisvõimeline. Kui dokument sisaldab juba arhiiviallkirja, kontrollitakse arhiivitempliga uuesti märgistamisel esmalt arhiiviallkirja. Seni kehtinud arhiiviallkiri asendatakse uuema arhiiviallkirjaga ainult siis, kui senine arhiiviallkiri on tõendamisvõimeline.
- **Arhiveerimisprotseduur** – arhiveerimisorganisse laekuva dokumendi originaalallkirja tõendamisvõime kinnitatakse usalduskeskuse arhiivitempliga ja originaalallkirja tõendusvõime lõppeb koos lisatud ajatempli tõendamisvõime lõppemisega. Regulaarselt enne ajatempli või viimase arhiiviallkirja tõendamisvõime lõppemist peab usalduskeskus märgistama dokumendi uue arhiivitempliga.
- **Arhiveeritud dokumendi struktuur** – arhiveeritud dokument koosneb vähemalt allkirjastatud originaaldokumendist ja seda kajastavast ajatemplist. Pärast ajatempli tõendamisvõime lõppemist saab dokument lisaks täpselt ühe arhiiviallkirja. See allkiri genereeritakse allkirjastatud originaaldokumendi ja ajatempli alusel.
- **Päringuprotseduur** – dokument koos kõikide allkirjadega saadetakse teele kõige värskemas olekus.
- **Arhiiviallkirja semantika** – arhiiviallkiri kinnitab ajatempli tõendamisvõimet. Ajatempel omakorda kinnitab originaaldokumendi olemasolu sellel ajahetkel.

- **Originaalallkirja tõendamisvõime kontrollimine** – esmalt verifitseeritakse arhiiviallkirja tõendamisvõime ja seejärel originaalallkirja tõendamisvõime ajatemplis näidatud hetkel.
- **Usaldusmudel** – arhiveerimisorganit usaldatakse dokumentide terviklikus salvestamises. Usalduskeskuses tuleb tingimata rakendada usaldusväärset arhiivitempli teenust. Arhiivitempli teenus peab kontrollima eelneva allkirja tõendamisvõimet. Kui ründaja suudab kontrolli takistada ja varustada võltsitud allkirjastatud dokumendid arhiiviallkirjaga, peetakse neid dokumente jätkuvalt tõendamisvõimelisteks. Seega tuleb sobivate meetmete abil tagada, et enne arhiiviallkirja uuendamist või lisamist kontrollitaks senise allkirja tõendamisvõimet.

Mõtteavaldus mudelite kohta

Mida väiksem on kasutajate silmis arhiveerimisorgani usaldusväärsus, seda suuremat hoolt tuleb kanda digitaalselt allkirjastatud dokumentide tõendamisvõimelise arhiveerimise tagamise eest. Kui arhiveerimisorganit usaldatakse täiel määral, saab rakendada mudelit nr 2. Kasutaja jaoks on see mudel kõige „mugavam", kuna arhiveeritud dokumendi päringul edastatakse kasutajale ka infot originaalallkirja tõendamisvõime kohta. Kasutaja eeldab, et arhiveerimisorgani andmed on usaldusväärsed. Kuid kontrollimisvõimalust tal pole. Kui kasutaja tahab kolmandat osapoolt veenda originaalallkirja tõendamisvõimes, saab ta viidata ainult arhiveerimisorganilt laekunud vastusele ja organi arhiveerimispoliitikast tulenevale usaldusväärsusele.

Mudeli nr 1 puhul peab kasutaja päringudokumendi originaalallkirja tõendamisvõimet ise kontrollima. Arhiveerimisorgan edastab kasutajale vaid info hetke kohta, millal dokument laekus organisse. Sarnaselt kasutajale saab tõendamisvõimet kontrollida ka kolmas osapool, kuid tal tuleb usaldada arhiveerimisorgani väljastatud ajainfo õigsust. Mõlema mudeli eeliseks on asjaolu, et arhiveerimisorgani organisatoorse töö maht on viidud miinimumini: pärast arhiveerimist ei ole dokumenti vaja edasi töödelda. Arhiveerimisprotseduur pitseerib originaalallkirja kogu arhiveerimise ajaks. Seepärast on arhiivi andmekogumi terviklus siinkohal kriitilise tähtsusega. Andmete volitusteta lisamine võib tähendada võltsitud allkirjade tunnistamist tõendamisvõimelisteks.

Mudelites nr 3 ja 4 on arhiveeritud andmete terviklus kaitstud digitaalsete allkirjadega. Sellega takistatakse volituseta arhiivi lisatud võltsitud allkirjastatud dokumentide tõendusvõimelisteks tunnistamist. 3. ja 4. mudeli täiendav usaldust suurendav meede seisneb võimaluses jaotada dokumendi salvestamine ja allkirja pitseerimine erinevate organite vahel: arhiveerimisorgani ja usalduskeskuse vahel. Arhiveerimisorgani vajalik usaldamine piirdub sellisel juhul nagu ka iga tavalise arhiveerimise puhul ainult dokumentide salvestamisega. Lisaks eeldab digitaalselt allkirjastatud dokumentide edukas arhiveerimine regulaarset sidet usalduskeskusega. Esmalt peab iga üksik dokument saama usalduskeskuse ajatempli, kuna dokumendi laekumise hetk arhiveerimisorganisse on oluline hilisemal tõendamisvõime kontrollimisel.

Mudelis nr 4 kinnitab usalduskeskus regulaarselt nõuetekohast arhiveerimist kuni käesoleva hetkeni seeläbi, et verifitseerib dokumendi senise arhiiviallkirja tõendamisvõimet ja asendab selle allkirja uue arhiiviallkirjaga. Ajavahemik ajatempli tõendusvõime lõppemise ja viimase arhiivitempliga märgistamise vahel suureneb seeläbi pidevalt. Seega kinnitab arhiiviallkiri ajatempli tõendamisvõimet

ainult seni, kuni on tagatud, et usalduskeskuses toimub arhiivitempliga märgistamine nõuetekohaselt. Eriti puudutab see senise arhiiviallkirja tõendamisvõime kontrollimist. Ilma selle kontrollita võib arhiveerimisorganile arhiivitempliga märgistamiseks esitada võltsitud allkirjastatud dokumente ja need dokumendid muutuksid seeläbi tõendamisvõimeliseks. Kasutaja peab seega usaldama, et usalduskeskuses toimub arhiivitempliga märgistamine nõuetekohaselt. Mudeli nr 3 puhul saab kasutaja kontrollida, kas regulaarses allkirja pitseerimises esineb lünki. Usalduskeskuse teenusena on tarvis kasutada ainult ajatempliga märgistamist. Ajatempliga märgistamine ei puuduta otseselt arhiveerimist ning selle käigus ei toimu kontrollimist. Dokument märgistatakse ilma eelneva kontrollimiseta, st „pimesi", käesoleva ajaga ja allkirjastatakse. Seega on üldiselt lihtsam realiseerida usaldusväärset ajatempliga märgistamist kui samavõrd usaldusväärset arhiivitempliga märgistamist.

Mudelid nr 3 ja 4 pakuvad küll võrreldes mudelitega 1 ja 2 suuremat usaldusväärsust, kuid kasutajatel on nende puhul palju keerulisem kontrollida originaalallkirja tõendamisvõimet. Lisaks originaalallkirja tõendamisvõimele esimese ajatempli määramise ajahetkel tuleb mudelis nr 3 kontrollida terve ajatemplite ahela tõendamisvõimet, kuid mudelis nr 4 seevastu ainult arhiiviallkirja tõendamisvõimet.

Digitaalallkirjade pikaajaliseks arhiveerimiseks pole veel standardeid, mis oleksid suutnud ennast tõestada. Ühtsed kontseptsioonid ja standardid on siin alles loomisel, seega peavad elektroonilise arhiveerimise eest vastutavad töötajad ennast valdkonnas toimuvate arengutega pidevalt kursis hoidma. Eelnevalt kirjeldatud mudelid on seega ainult näited, st digitaalselt allkirjastatud dokumentide arhiveerimiseks saab kindlasti kasutada ka teisi lahendusi.

Kontrollküsimused:

- Kas arhiveerimisel kasutatavate digitaalallkirjade rakendamise kohta on olemas vastav kontseptsioon ja turvasuunised?
- Kas olemasolev kontseptsioon ja turvasuunised on ajakohased?
- Kas personal on teadlik kontseptsiooni vastavatest osadest, mis neid otseselt puudutavad ja kas see on tõestatav?
- Kas kontseptsiooni ajakohasust kontrollitakse regulaarselt?

M 2.266 Arhiivisüsteemi tehniliste komponentide regulaarne asendamine

Algatamise eest vastutavad: IT-juht, arhiivi haldaja
Rakendamise eest vastutavad: IT-juht, arhiivi haldaja, administraator

Tehniline areng

Arhiivisüsteeme tuleb hoida pika aja jooksul tehnika arengule vastaval tasemel. Arhiveerimise pikkade ajavahemikega võrreldes on senised infotehnoloogia riistvara- ja tarkvarastandardid, samuti digitaalse salvestamise andmeformaadid olnud vaid üsna lühiajalise kasutuseaga. Seetõttu võib eeldada, et olukord ei muutu tulevikus palju, kuna tehnika areng mõjutab olulisel määral ka standardeid.

Kulumisnähud

Riistvarakomponendid kuluvad ja seetõttu tuleb neid regulaarselt hooldada ning vajaduse korral ka välja vahetada. Lisaks tuleb arvestada võimalusega, et tootja võib ootamatult lõpetada olemasolevate süsteemide toe või pole näiteks maksevõimetuse tõttu enam suuteline pakkuma pikaajalist tuge. Seega tuleb arvestada arhiivi komponentide regulaarse uuendamisvajadusega ja sellest tuleneva võimaliku vajadusega viia kogu andmekogum üle uuele arhiivisüsteemile. Nimetatud protsess on tihedalt seotud meetmega M 2.261 Regulaarsed arhiivisüsteemide turu-uuringud .

Ühilduvuse testimine

Uut riist- ja tarkvara tuleb enne töötavasse arhiivisüsteemi paigaldamist alati põhjalikult testida, et mitte ohustada olemasoleva süsteemi stabiilsust (vt M 4.65 Uue riist- ja tarkvara testimine). Uute andmekandjate ja kettaseadmete paigaldamisel tuleb jälgida, et need ühilduksid olemasolevate süsteemide ja andmekandjatega. Enne uute komponentide kasutuselevõttu või uute andmeformaatide rakendamist tuleb luua kontseptsioon, milles kirjeldatakse kõiki muudatusi ja testimisi. Arhiveerimiskontseptsiooni (vt M 2.243 Arhiveerimiskontseptsiooni väljatöötamine) tuleb vajaduse korral kohandada. Suuremate muudatuste puhul tuleb uuesti läbi teha moodulis kirjeldatud planeerimisfaas. Formaatide muutmisel tuleb kontrollida, kas vanade andmete konverteerimisel uude formaati tuleb andmed seadustest tulenevate nõuete tõttu arhiveerida lisaks ka algses formaadis.

Kontrollküsimused:

- Kas kõikidel arhiivikomponentidel (tarkvara, riistvara ja andmekandjad) on piisav tootja või mõni muu võrdväärne tugi?
- Kas enne uute komponentide paigaldamist tuleb kohustuslikus korras testida nende ühilduvust?

M 2.272z Veebitoimetajate meeskonna loomine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtorgan

Rakendamise eest vastutavad: IT-juht, vastutav spetsialist

Veebileht nõuab regulaarset hooldamist. Eriti kiiresti kasvab vajadus hooldamise järele siis, kui veebilehel pakutakse infot või teenuseid, mida tuleb tihti muuta. Veebilehe kontseptsioonis (vt M 2.172 Veebilehe kasutamise kontseptsiooni väljatöötamine) tuleb nimeliselt loetleda töötajad, kes hakkavad vastutama veebilehe hooldamise erinevate aspektide eest. Kui veebilehe maht ja sellega seotud hooldusvajadus ületab teatud piiri, võib parema koordineerimise tagamiseks olla otstarbekas luua iseseisev veebitoimetajate rühm. Vastav lahendus eristab veelkord selgesti töötajate vastutusalasid ja muudab need organisatsiooni struktuuris nähtavaks.

Tsentraalne algpunkt

Veebitoimetajate rühma sisseseadmine loob keskse koha, kuhu saab esitada kõik veebilehte puudutavad küsimused. Tihti on sellise toimetusüksuse abil ka palju lihtsam rakendada tõhusaid koostööprotsesse veebilehe info värskuse ja õigsuse tagamiseks (nt teatud kinnitusprotsesse või nelja-silma-printsiipi) võrreldes olukorraga, kus sarnaseid protsesse tuleks koordineerida korraga läbi erinevate organisatsiooniüksuste. Toimetusse peaksid kuuluma vähemalt need isikud, kes on WWW-kontseptsioonis loetletud vastutavate töötajatena. Sageli tasub toimetusse kaasata ka täiendavaid isikuid. Veebitoimetusse peaksid kuuluma järgnevad liikmed:

- peatoimetaja, kellel lasub koguvastutus veebilehe sisu ja sellega pakutavate teenuste eest,
- erialaselt pädev toimetaja iga veebilehe eraldi valdkonna jaoks,
- veebilehe optilise välimuse (veebidisaini) eest vastutav töötaja,
- „tehniline veebimeister“, kes vastutab veebiserveri töö tehniliste aspektide eest.

Kui veebiserveris kasutatakse mahukaid veebirakendusi, peab veebitoimetuse hulka kuuluma ka nende rakenduste eest vastutav kontaktisik. Erialaselt pädevad toimetajad, veebidisainer ja tehniline veebimeister on lisaks toimetuse tööle ka vastavate valdkondade kontaktisikuteks (vahelülideks toimetuse ja osakondade vahel). Lisaks tavapärastele veebitoimetusega seotud protsessidele on tarvis toimetuse piires määrata ka protseduurid ja vastutusalad, kuidas käituda probleemide korral, et tagada toimetuse kiire ja tõhus reageerimine turvaintsidentidele (vt M 2.173 Veebiserveri turbestrateegia väljatöötamine).

M 2.273 Turvalisust mõjutavate paikade ja värskenduste kiire paigaldamine

Algatamise eest vastutavad: IT-juht, infoturbespetsialist

Rakendamise eest vastutavad: infoturbespetsialist, administraator

Sageli avastatakse tarkvaratoodetes vigu, mis võivad mõjutada turvalisust IT-süsteemides, millesse need tooted on installeeritud. Avastatud puudused tuleb võimalikult ruttu kõrvaldada, et ründajad nii seest kui ka väljast ei saaks hakata neid ära kasutama. Eriti oluline on see siis, kui puudutatud süsteemid on ühendatud internetiga. Lahendusena avaldavad operatsioonisüsteemide või tarkvarakomponentide tootjad tavaliselt turvapaiku või uuendusi, mis tuleb vigade kõrvaldamiseks installeerida vastavasse IT-süsteemi.

Aktuaalsus

Süsteemiadministraatorid peavad end regulaarselt informeerima, kas tarkvaras on avastatud turvaauke (vt M 2.35 Teabe hankimine turvaaukude kohta).

Allikate tundmine, tervikluse ja autentsuse kontrollimine

Nagu igasuguse tarkvara puhul, on ka siin oluline, et paigad ja täiendid pärineksid usaldusväärsetest allikatest. Iga kasutatava süsteemi ja tarkvaratoote kohta peab olema teada, millisest allikast tuleb hankida vastavad paigad ja täiendid. Lisaks on oluline kontrollida juba paigaldatud toodete, samuti paigaldatavate turvatäiendite ja -paikade terviklust ja autentsust (vt M 4.177 Tarkvarapakettide tervikluse ja autentsuse tagamine) ja seda juba enne täiendi või paiga installeerimist. Samuti tuleb need enne installeerimist viirusetõrjeprogrammiga üle kontrollida. Viirusekontroll tuleb teha ka sellistele tarkvarapakettidele, mille terviklus ja autentsus on eelnevalt juba kindlaks tehtud.

Täiendite ja paikade testimine

Turvatäiendeid ja -paiku ei tohi rakendada enneaegselt, enne installeerimist tuleb neid kontrollida. Kui teiste kriitiliste komponentide või programmidega peaks tekkima konflikt, võib vastava täiendi installeerimine põhjustada hoopis süsteemi avarii. Vajaduse korral tuleb asjassepuutuvat süsteemi kuni testide lõppemiseni kaitsta teistsuguste meetmetega.

Varukoopia

Enne täiendi või paiga installeerimist tuleb süsteemi andmed alati varundada, et probleemide korral oleks võimalik taastada originaalseisund. Eriti kehtib see neil juhtudel, kus põhjalikku testimist ei ole võimalik kas aja või sobiva testsüsteemi puudumisel läbi viia.

Dokumentatsioon

Kõikidel juhtudel tuleb dokumenteerida, millal, kelle poolt ja mis põhjusel paigad ja täiendid installeeriti (vt M 2.34 IT-süsteemi muutuste dokumenteerimine). Dokumentatsiooni alusel peab saama igal ajal tuvastada, millised paikade versioonid on hetkel süsteemi paigaldatud, et nõrkuste ilmsikstulekul oleks võimalik kindlaks teha, kas süsteem on ohus või mitte. Kui tuvastatakse, et turvatäiend või paik ei sobi kokku mõne muu olulise komponendi või programmiga või põhjustab probleeme, tuleb hoolikalt kontrollida, mida edasi teha. Kui otsustatakse, et tuvastatud probleemide tõttu turvapaika ei installeerita, tuleb vastav otsus kindlasti

dokumenteerida. Lisaks tuleb sellistel juhtudel kirjeldada, milliseid asendusmeetmeid võetakse, et vältida nõrkade kohtade ärakasutamist.

Turvalisust puudutavat otsust ei tohi administraatorid langetada üksi, vaid peavad selle kooskõlastama ülemuste ja IT turvalisuse eest vastutava töötajaga.

Kontrollküsimused:

- Kas administraatorid kontrollivad regulaarselt, kas kasutatavate toodete, operatsioonisüsteemide ja rakenduste juures esineb turvaauke?
- Kas uuendused ja paigad hangitakse usaldusväärsetest allikatest?
- Kas uuendusi ja paiku testitakse enne väljastamist?
- Kas on kindlustatud, et pärast ebaõnnestunud uuendust on võimalik algne süsteemiseisund taastada?
- Kas dokumenteeritakse, millal, mis põhjusel ja kelle poolt millised muudatused süsteemis läbi viidi?

M 2.274 Asendamise korraldamine meilivahetuse alal

Algatamise eest vastutavad: IT-turvaosakond, administraator

Rakendamise eest vastutavad: kasutaja, administraator

Nii nagu kõikide muude tööülesannete puhul, tuleb ka meilide haldamise osas määrata igale töötajale asendaja. Plaanipärase eemalviibimise ajaks peab kasutaja sisse seadma meilide edasisuunamise asendajale või võimaldama juurdepääsu oma postkastile. Ootamatu eemalviibimise nagu nt haiguse puhul saab meilide õigeaegse läbivaatuse jaoks kasutada muid regulatsioone. Näiteks võib puudutatud osakonna kontaktisik informeerida IT-turvalisuse eest vastutavaid töötajaid, kes omakorda korraldavad meiliserveris edasisuunamise. Antud tegevust võib lubada muidugi ainult juhul, kui on selgelt reguleeritud, et meiliteenust tohib kasutada ainult ametiasjus. Lisaks tuleb kasutajaid teavitada meili teel edasisuunamisest. Niipea kui töötajad on tööle naasnud, peavad nad IT-turvalisuse eest vastutavale töötajale teatama, et meilide edasisuunamise võib tühistada. Alternatiivse lahendusena võib sisse seada ka konkreetsete ülesannetega seotud meiliaadressid. Loomulikult tuleb ka sellise variandi puhul tagada, et saabuvate meilidega tegeletaks võimalikult kiiresti.

Automaatne vastus / eemaloleku teade

Mitmed meilikliendid võimaldavad enne pikemat äraolekut aktiveerida teenuse (Autoreply, Outlookis Eemaloleku teade), mis saadab eemalviibimise ajal saabuvale meilile vastuteate, mis informeerib saatjat töötaja ajutisest eemalolekust. Antud lahendus võib pakkuda küll erinevaid eeliseid, kuid tihti kaasneb sellega kõrvalmõju, et kasutaja ja organisatsiooni kohta levib liiga palju infot väljapoole. Lisaks jääb meili saatjale sellise teadete puhul tavaliselt selgusetuks, mida tema saadetud meiliga edasi tehakse. Tekib küsimus, kas meil jääb esialgu tähelepanuta või edastatakse see mõnele asendajale. Seetõttu peavad kõik kasutajad jälgima, et nad ei edastaks oma eemalviibimist kajastavates teadetes ei täpset eemaloleku aega ega ka siseinfot nagu telefoninumbreid või organisatsiooni allüksuseid puudutavat infot. Niisugust infot on võimalik ära kasutada manipulatsioonideks (vt G 5.42 Inimestega manipuleerimine (Social Engineering)). Kõikidel juhtudel tuleks pikema eemaloleku ajaks nimetada asendajad. Eemaloleku teate abil võib asendustöötajatest informeerida ka organisatsioonivälised isikuid, teavitamaks, et nende meil on kohale jõudnud ja sellega tegeletakse.

Teadmiseks: suurem osa Autoreply funktsiooniga varustatud meiliprogrammidest võimaldavad teavitamist ka juhtida, kasutades selleks kasutaja poolt määratud kriteeriume. Selle abil saab näiteks määratleda, et organisatsioonisisesele meilile saadetakse vastuseks teistsuguse sisuga meil kui väljastpoolt organisatsiooni saabunud meilile. Kuid reeglina läheb selleks vaja juba täpsemaid teadmisi meilikliendi kohta. Kui automaatvastuse funktsioonide juhtimiseks soovitakse kasutada erinevaid kriteeriume, peaksid administraatorid tegema kasutajate jaoks vastavad ettevalmistused.

Täiendavad kontrollküsimused:

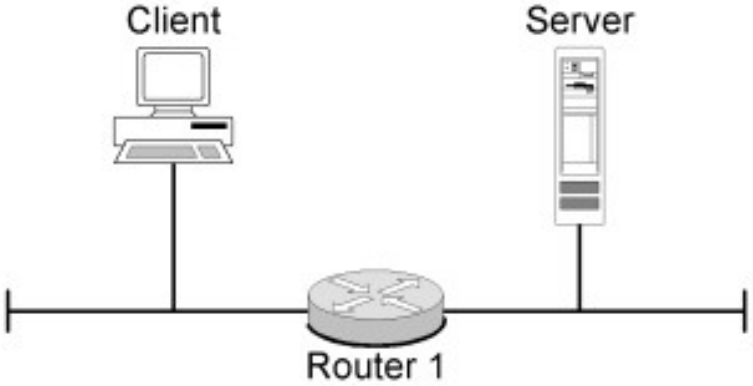
- Kas asenduste puhul on selge, kuidas hallata asendatava töötaja meile?
- Kas kõik kasutajad teavad, kuidas aktiveerida meiliklientides asendusfunktsiooni?

M 2.276z Marsruuteri funktsionaalne kirjeldus

Algatamise eest vastutavad: IT-turvaosakond, IT-juht

Rakendamise eest vastutavad: administraator

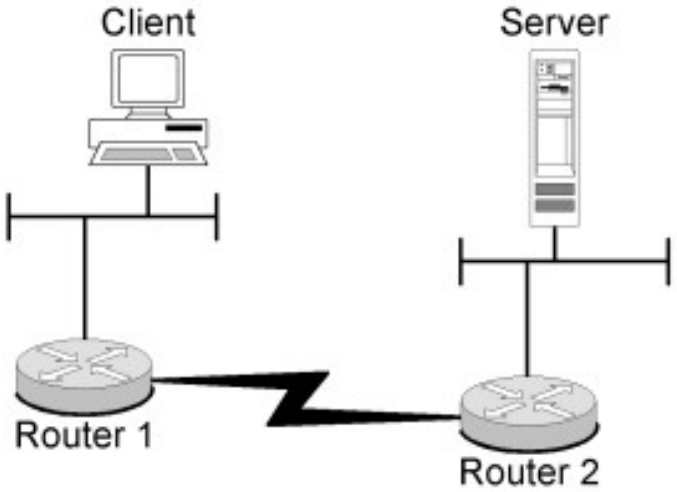
Suurtes võrkudes on marsruuterite kasutamisest loobuda praktiliselt võimatu. Marsruutereid kasutatakse nii kohtvõrkudes kui ka laivõrkudes (vt B 4.4 Virtuaalne privaatvõrk (VPN)). Ilma marsruuterite kasutamiseta ei saaks kasutada Internetti. Marsruuterid võivad samaaegselt toetada erinevaid protokolle (nt IP, IPX) ja topoloogiaid (nt Ethernet, Token Ring, FDDI, ATM, Frame Relay, ISDN). Seeläbi suudavad marsruuterid ühendada kohtvõrke laivõrkudega. Interneti kiire areng oli muuhulgas võimalik ka just tänu marsruuterite nimetatud funktsioonile. Marsruuter täidab peamiselt kahte ülesannet. Esiteks luuakse sobiv ühendus lähtesüsteemi/lähtevõrgu ja sihtsüsteemi/sihtvõrgu vahel ja teiseks edastatakse selle ühenduse kaudu andmepakette. Kui sihtsüsteem (sihtvõrk) on ühendatud otse marsruuteriga, st marsruuter ja sihtsüsteem asuvad samas alamvõrgus, edastatakse lähtesüsteemist teelesaadetud andmepakett otse sihtsüsteemi.



Joonis: marsruutimine

Next Hop

Kui sihtsüsteem (sihtvõrk) pole marsruuteriga otseses ühenduses, saadab marsruuter andmepaketi mõnesse naabruses asuvasse marsruuterisse, mis on sihtsüsteemile (sihtvõrgule) lähemal, nn Next Hop -i. Sellise ahela viimane marsruuter on alati ühendatud otse sihtvõrku ja saadab andmepaketi sihtvõrku.



Joonis: marsruutimine

Client – klient; Server – server, Router – marsruuter

Marsruuteri ülesandeks on toimetada saabuvad andmepaketid kas otse adressaadile või suunata need järgmisesse võrku. Selle, millisesse võrku andmepakett saadetakse, kui otsene kohaletoimetamine ei ole võimalik, otsustab nn marsruuteri meetrika. Meetrika on mõõtühik, mis näitab ühenduse kvaliteeti saatja/marsruuteri ja paketi sihtkoha vahel. Selle abil langetab marsruuter valiku, millisele Next Hop -ile andmepakett edastada. Marsruuteri meetrika ei pruugi lähtuda ainuüksi saatja ja vastuvõtja vahele jääva tee pikkusest, vaid suudab kaasata ka muude mõjufaktorite omadusi nagu nt kaablite kvaliteeti, ribalaiust või koormust. Milliseid kriteeriumeid parasjagu kasutatakse, sõltub marsruutimisprotokollist.

Marsruutimistabelid

Marsruutimisinfot hallatakse nn marsruutimistabelites. Marsruutimistabelid sisaldavad infot, milliseid läheduses asuvaid marsruutereid võiks rakendada teatud sihtmärkide Next Hop -idena. Marsruuterid teevad valiku, millisele Next Hop -ile vastuvõetud andmepaketti edastada, eranditult marsruutimistabelite alusel. Seega on eriti oluline kaitsta neid tabeleid manipulatsioonide eest. On teada terve rida ründeid, mille korral manipuleeritakse marsruutimistabelitega. Järgnevalt on toodud näide marsruutimistabeli sisu kohta.

Sihtkoht	Next Hop	Hop -ide arv
210.23.125.98	210.23.122.4	3
	127.200.45.123	5
	203.2.67.187	8

Tabel: marsruutimistabeli näide

Selles näites saadaks marsruuter andmepaketi, mille sihtaadressiks on 210.23.125.98 edasi Next Hop -ile 210.23.122.4. Niinimetatud Hop Count (Hop -ide arv) näitab, mitu vahejaama peab pakett veel läbima, et jõuda vastava Next Hop -i kaudu oma sihtmärgini. Kui teatud sihtmärgi jaoks saab Next Hop -idena kasutada mitut naabruses asuvat marsruuterit, võib Hop Count -i kasutada marsruutimismeetrikana, et tuvastada „soodsaim“ Next Hop. Hop Count -i kasutatakse marsruutimismeetrikana ka marsruutimisprotokollis RIP.

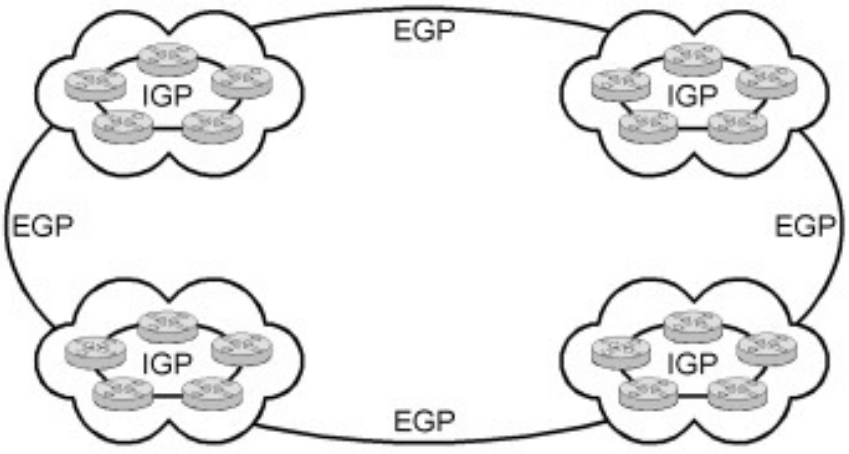
Staatiline ja dünaamiline marsruutimine

Marsruutimisel eristatakse staatilist ja dünaamilist marsruutimist. Nende meetodite erinevus seisneb marsruutimistabelite haldamises. Staatilise marsruutimise käigus kontrollitakse tabeleid süsteemikäskude abil käsitsi. Dünaamilise marsruutimise käigus toimub marsruutimistabelite hooldamine automaatselt. Selleks kasutatakse marsruutimisprotokolle. Siinkohal eristatakse omakorda Interior Gateway protokollide (IGP) ja Exterior Gateway protokollide (EGP) vahel. IGP-d kasutatakse võrkudes, mille administreerimine toimub omal vastutusel. Omal vastutusel administreeritavate võrkude kogumit nimetatakse ka marsruutimisdomeeniks. EGP abil vahetatakse erinevate marsruutimisdomeenide vahel marsruutimisinfot.

Järgnev joonis kujutab nende vastastikust seost.

EGP – välislüüsi protokoll (Exterior Gtaeway Protocol);

IGP – siselüüsi protokoll (Interior Gateway Protocol)



Joonis: marsruutimisinfo vahetamine

Marsruutimisprotokollid

Tuntuimad ja standardiseeritumad marsruutimisprotokollid on Routing Information Protocol (RIP), Open Shortest Path First (OSPF) ja Border Gateway Protocol

(BGP), kusjuures Border Gateway Protocol -i puhul on tegu Exterior Gateway protokolliga. Neid protokolle täiendavad veel ka erinevate tootjate poolt loodud marsruutimisprotokollid. Tuntuimad protokollid on Interior Gateway Routing Protocol (IGRP) ja Enhanced Interior Gateway Routing Protocol (EIGRP) tootjalt Cisco. Kuna marsruutimisprotokollid automatiseerivad marsruutimistabelite haldamist, on ründajatele nende protokollide turvaaugud juba ammu selged ja nad oskavad nende abil marsruutimistabeleid muuta, et seeläbi andmepakette ümber juhtida või kogu võrku halvata (vt G 5.51 Marsruutimisprotokollide väärkasutus). Võrkudevahelise dünaamilise marsruutimise kasutamisel tuleb esmajoones tegeleda marsruutimisprotokollide turbefunktsioonide rakendamisega (vt M 5.112 Marsruutimisprotokollide turvaaspektide arvestamine). Administraator peab eriliselt tähelepanu pöörama naabruses asuvate marsruuterite turvalisele autentimisele marsruutimistabelite andmevahetusel. Kasutada tohib ainult selliseid marsruutimisprotokolle, mis võimaldavad marsruutimistabelite andmevahetuses rakendada kodeeritud autentimist. Marsruutimistabelite käsitsi hooldamine on liialt töömahukas, seega ei ole keerukates võrkudes võimalik dünaamilisest marsruutimisest loobuda. Enne dünaamilise marsruutimise kasutuselevõtmist tuleb hinnata selle turvalisust.

Dünaamilise marsruutimise vältimine kõrge turbevajaduse korral

Dünaamilist marsruutimist ei tohiks üldjuhul kasutada kõrge turbevajadusega võrkudes. Kui dünaamilisest marsruutimisest ei ole võimalik olulistel põhjustel loobuda, tuleks vähemalt kasutada vaid selliseid marsruutimisprotokolle, mis suudavad tagada osalevate seadmete turvalise autentimise ja marsruutimisinfo turvalise edastamise. Moodul M 2.278 Marsruuterite ja kommutaatorite kasutamise tüüpstsenaariumid kajastab veel ühte kasutusvaldkonda, mille puhul soovitatakse marsruutimisprotokollidest loobuda.

Marsruuter paketifiltrina

Paljusid marsruutereid saab kasutada ka andmepakettide filtreerimiseks, st marsruuterit kasutatakse paketifiltri funktsioonides (vt B 3.301 Turvalüüs (tulemüür)). Marsruuter ei edasta tavaliselt erinevate selle külge ühendatud võrkude vahel liikuvaid leviedastuspakette (broadcast). Marsruuter jaotab ühenduses olevad võrgud erinevateks leviedastus-domeenideks. Reeglina on marsruuteritel siiski ka veel täiendavad filtrifunktsioonid. Näiteks saab konfigureerida nn pääsuloendeid (Access Control Lists (ACL)). Antud loendite alusel reguleerib marsruuter andmevahetust sides osalevate võrkude vahel. Pääsuloendite täiendavaid turbeaspekte on kirjeldatud M 5.111 Marsruuterite pääsuloendite konfigureerimine . Andmevahetuse kontrollimiseks erineva kaitsevajadusega võrkude vahel ei piisa ainuüksi paketifiltritest. Lisainfot leiate B 3.301 Turvalüüs (tulemüür) ja näiteks meetmetest M 2.73 Sobiva turvalüüsi (tulemüüri) põhistruktuuri väljavalimine ja M 2.74 Sobiva paketifiltri valimine .

Marsruuter VPN-lüüsina

Mõningad saadaolevad marsruuterid toetavad funktsiooni Virtual Private Network (VPN). Selliseid marsruutereid kasutatakse eriti just siis, kui võrgu kaudu on tarvis edastada tundlikke andmeid. VPN-funktsioonidega varustatud marsruuterite kasutamise eeliseks on asjaolu, et rakendusepoolel ei ole tarvis eraldi krüpteerimismehhanisme. Krüpteering on kommunikatsioonipartnerite jaoks läbipaistev. Sellele vaatamata toimub kommunikatsioon kuni esimese krüpteeritud võrguühenduselemendini ilma krüpteerimata ja kujutab endas seega jääkriski. Autentimine on antud variandi puhul võimalik ainult ühenduselementide vahel. Tegelike kommunikatsioonipartnerite autentimist ei toimu (M 5.68 Krüpteerimisprotseduuride kasutamine võrgusuhtluses).

M 2.277z Kommutaatori funktsionaalne kirjeldus

Algatamise eest vastutavad: IT-turvaosakond, IT-juht

Rakendamise eest vastutavad: administraator

Sissejuhatus

Algselt töötasid kommutaatorid vaid OSI kihis nr 2, kuid nüüdseks on saadaval juba erinevate funktsioonidega kommutaatorid. Tootjad märgistavad kommutaatoreid tavaliselt OSI-kihiga, mida seade toetab. Seeläbi on tekkinud mõisted 2. kihi, 3. kihi ja 4. kihi kommutaator, kusjuures 3. kihi ja 4. kihi kommutaatorite funktsioone arvestades on tegu juba marsruuteritega. Kommutaatorite ja marsruuterite algselt lahutatud funktsioonid ühendatakse ühte seadmesse. Seadmetüüpide eristamine (kommutaator või marsruuter) on seeläbi raskendatud. Antud seadmete olulised erinevused on loetletud B 3.302 Marsruuterid ja kommutaatorid sissejuhatuses.

Esimesed kommutaatorid tekkisid sildadest, mille ülesandeks oli sarnaselt tänapäevastele moodsatele kommutaatoritele suurte LAN-segmentide jaotamine mitmeks väikeseks segmendiks (kollisioonidomeeniks). Sillad töötavad tavaliselt Store-and-Forward -tehnoloogial. Vastuvõetud Etherneti kaader loetakse sisse ja seejärel otsustatakse sihtaadressi alusel, kas see edastatakse teisele LAN-segmendile. Kui tegu on kohaliku tasandi andmevahetusega, siis edastamist ei toimu ja kaader jõuab ainult kohalike võrkude tugijaamadesse. Niimoodi piiratakse kohaliku tasandi liiklus üksikutele segmentidele, mis võib soodsa paigutuse korral oluliselt vähendada võrgu koormust. Väiksemate segmentide puhul langeb lisaks kollisioonide osakaal ja paraneb jõudlus. Kui kaader tuleb saata mõnda teise segmenti, talletatakse see silla vahemälusse ja edastatakse seejärel sihtpordile. Lisaks saab Store-And-Forward tehnoloogia abil CRC-kontrollsummale toetudes kontrollida vastuvõetud kaadri terviklust. Rikkis kaadrid jäetakse kõrvale, mille tulemuseks on veelgi tõhusam võrgukoormuse vähendamine. Kommutaatoritel on lisaks Store-and-Forward-Switching mehhanismile ka Cut-Through-Forward-Switching mehhanism, mille puhul loetakse ainult sihtaadressi, st kaadri kuut esimest baiti. Seeläbi vähendatakse oluliselt viivitust saatja- ja vastuvõtjapordi vahel. Kahjuks ei ole seeläbi võimalik välja filtreerida kaadreid, mille andmeterviklus on rikutud. Rikutud kaadrite asjatu edasisaatmine võib aga põhjustada protsesside aeglustumist. Lahendusena saab kasutada kommutaatori adaptiivset käitumist, mille puhul kontrollitakse kaadreid edastuse käigus. See ei filtreeri küll vigaseid kaadreid välja, kuid võimaldab kommutaatoril jälgida kaadri kvaliteeti. Kui vigaste kaadrite protsent ületab eelnevalt seadistatud väärtuse, lülitab kommutaator vastava pordi Store-and-Forward funktsioonile ümber, et kaadreid hakataks filtreerima.

Kommuteerimistabelid

Järgneval joonisel on näha nn kommuteerimistabeli näidis. Sellesse tabelisse salvestatakse andmed, millise pordiga on ühendatud teatud jaam koos oma vastava MAC-aadressiga. Kommutaator tuvastab vastavad seosed dünaamiliselt. Erinevalt jaoturist (hub) saadab kommutaator Etherneti kaadri alati ainult sellisesse porti, millel on ühendus sihtarvutiga. Seeläbi ei mõjutata ribalaiust, mida seade saab kasutada sides ülejäänud vahejaamadega. Lisaefektiks on asjaolu, et kahe vahejaama vahelist sidet ei saa ühestki teisest jaamast pealt kuulata. Erandiks on leviedastused (broadcasts) ja multiedastused (multicasts), mis saadetakse kõikidele ühendatud vahejaamadele. Samuti saadetakse kõikidele portidele edasi ka tundmatu siht-MAC-aadressiga kaadrid.

Sihtkoha MAC-aadress	Sihtkoha kommutaatoriport
0001.02c4.fdca	Fast Ethernet0/4
0001.026d.d412	Fast Ethernet0/8
0008.a345.12f3	Fast Ethernet0/12
0060.97ac.de59	Fast Ethernet0/16
...	...

Tabel: kommuteerimistabel

Kaader, mis on suunatud vahejaama MAC-aadressiga 0001.02c4.fdca, suunatakse kommutaatori poolt edasi ainult porti 01. Kuna kommuteerimistabelit kasutatakse andmevoo juhtimiseks, tuleb seda kindlasti kaitsta manipulatsioonide eest. On teada mõningad ründemeetodeid, mis ohustavad nende tabelite terviklust ja käideldavust (vt G 5.112 ARP-protokolli tabelitega manipuleerimine). 3. kihi ja 4. kihi kommutaatorid töötavad analoogselt vastavas kõrgemas OSI-kihis.

Täispuu

Keeruka topograafiaga kohtvõrgus, kus on mitu kommutaatorit, võib juhtuda, et kahe seadme ühendamiseks eksisteerib mitu erinevat võimalust. Kommuteerimine töötab aga ainult siis, kui alati on selge, millisele pordile tuleb pakett edastada. Vastasel korral võivad võrgus tekkida silmused (Loops), st pakette hakatakse saatma ringikujuliselt, ilma et need iial jõuaks oma tegelikku sihtpunkti. Seepärast pakuvad kommutaatorid võimalust „leppida kokku“ automaatselt omavaheline loogiline võrgustruktuur (nn võrgu täispuu (Spanning Tree)), et töö võiks kulgeda probleemivabalt. Sel eesmärgil kasutatakse nn täispuuprotokolli (Spanning Tree Protocol (STP, IEEE 802.1d)). Võrgu üleliigsed ühendused desaktiveeritakse automaatselt ja aktiveeritakse ainult siis, kui STP poolt tuvastatav peaühendus pole enam saadaval. Selle toimimiseks tuleb igale kommutaatorile määrata prioriteediinfo ja MAC-aadress, lisaks peab igal kommutaatoril olema multiedastuse aadress ning iga port peab olema ID abil selgesti tuvastatav.

VLAN

Piiramaks „kommuteeritud“ võrgu leviedastusliiklust, on võimalik luua virtuaalvõrgud (VLANid). Selleks luuakse füüsilises võrgus loogiline võrgustruktuur, kus funktsionaalselt kokkukuuluvad tööjaamad ja serverid ühendatakse omavahel ühtseks virtuaalvõrguks. VLANi loomise põhjused võivad tulla organisatoorsetest või tehnilistest vajadustest. Ettevõtte struktuurist lähtuvalt on näiteks võimalik ühte võrgugruppi kokku koondada kõik ühe osakonna töötajad ja seda ka siis, kui nende töökohad asuvad erinevatel korrustel. Töö organiseerimise aspektist lähtuvalt saab ühte võrgugruppi kokku koondada kõik ühisprojektiga tegelevad töötajad ja seda ka siis, kui nad kuuluvad erinevate osakondade alla. Iga VLAN moodustab eraldiseisva leviedastusdomeeni. VLAN ei pea olema piiratud üksiku kommutaatoriga, see võib ulatuda üle kogu kommuteeritud võrgu. Sellisel juhul ei kuulu võrgukasutajad mitte enam kindlasse võrgusegmenti oma asukoha alusel, vaid koondatakse intranetis ühte gruppi koos teiste kasutajatega, sõltumata nende füüsilisest asukohast. Eristatakse portidel ja hostidel põhinevaid VLANe. Portidel põhinevate VLANide puhul määratakse kommutaatori üksikud ühendused (pordid) otseühendusse VLANidega. See tähendab, et määratud ühendus on püsivalt seotud teatud VLANiga, sõltumata ühendatud vahejaamast. Hostidel põhinevate VLANide puhul määratakse VLANi kuuluvus näiteks ühendatud vahejaama MAC-aadressi või IP-aadressi alusel. Hostidel põhinevate VLANide puhul saab kasutaja oma

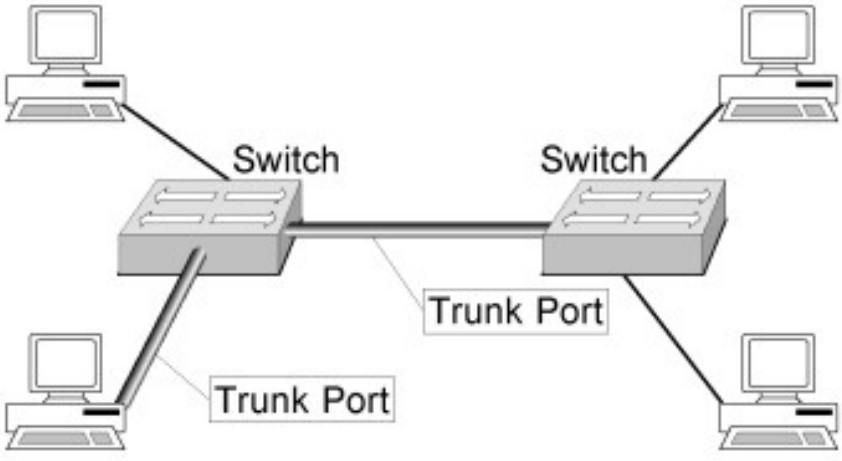
lõppseadet võrgu piires ühendada igas suvalises punktis, ilma et kaotaks kuuluvust talle määratud VLANi.

Trunking

Võimalust VLANi mitme kommutaatori peale laiendada tähistatakse terminiga trunking . Kommutaatoris reserveeritakse selleks üks füüsiline port kommutaatoritevahelise kommunikatsiooni jaoks ning kommutaatorite vaheline loogiline ühendus kannab nimetust trunk . Trunking realiseeritakse erinevate, osaliselt tootjatele kuuluvate trunking -protokollidega. Etherneti raam kapseldatakse kommutaatoritevahelise andmevahetuse käigus trunking -protokolli. Seeläbi suudab sihtkommutaator seostada infot vastava VLANiga. Standardina kasutatakse protokolli IEEE 802.1q ja näiteks tootjafirmale Cisco kuuluvaid protokolle ISL (Inter Switch Link) ja VTP (VLAN Trunking Protocol).

Ettevaatust sarnaste mõistetega

Mõnikord nimetatakse trunking -uks ka mitme kommutaatori füüsiliste ühenduste sidumist (koondamist), mille eesmärgiks on saavutada kõrgemaid läbilaskevõimeid. Käesolevat funktsiooni tähistatakse muuhulgas ka nimedega „ Channel Bonding “ või „ Channeling “. Kui dokumendis kasutatakse mõistet trunking, tuleb alati jälgida, millises tähenduses seda mõistet parasjagu kasutatakse. Antud juhul tähendab trunking võimalust VLANe mitme kommutaatori kaudu jaotada. Järgneval joonisel on kujutatud näide seadistusest kahe kommutaatoriga, mis on omavahel ühendatud Trunk -pordiga. Arvuti, mis on vasakpoolse kommutaatori puhul samuti ühendatud Trunk -pordiga, kujutab endast potentsiaalset turvariski, sest sellelt pääseb ligi andmetele kõikides VLANides, mis on konfigureeritud selle kommutaatori jaoks.

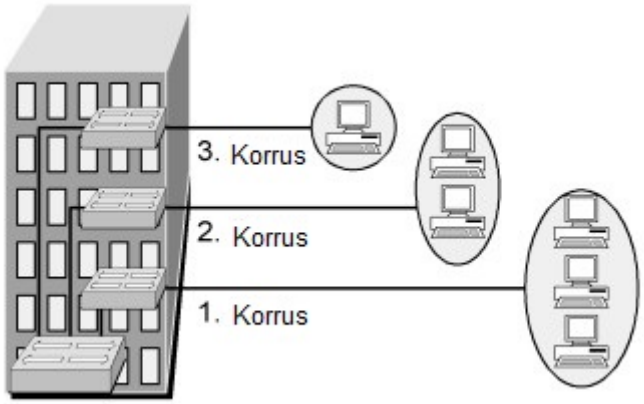


Joonis: Trunking

Switch – kommutaator; Trunk Port – magistraalport

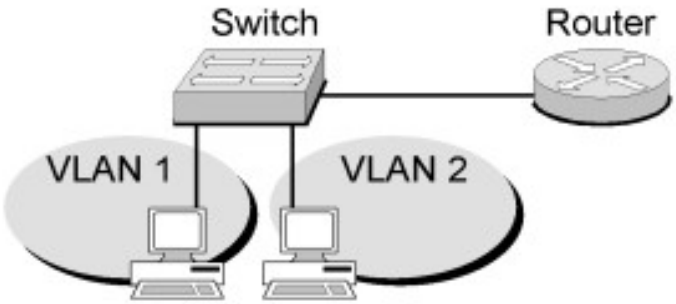
Kui VLAN toimib läbi mitme kommutaatori, suureneb andmevahetus nende komponentide vahel selle infohulga võrra, mida edastatakse Trunking -protokollide abil. Erinevate VLANide vaheline kommunikatsioon toimub OSI 3. kihi kaudu, mis tähendab, et pakettide marsruutimine toimub VLAN-ideüleselt. Marsruutimine võib toimuda mõnes marsruutimisfunktsioone toetavas kommutaatoris (vt lisaks mooduli B 3.302 Marsruuterid ja kommutaatorid sissejuhatuse lõiku 3. kihi

kommutaatorite kohta) või ühendatud marsruuteris, mis ühendab VLANe OSI 3. kihi tasandil. Järgnevad joonised on toodud näidetena (portidel põhineva) VLAN-i kohta, mis kulgeb ühe hoone piires läbi kolme erineva korruse ja konfiguratsiooni kohta, kus kommutaatori alla kuulub kaks erinevat VLAN-i.



Joonis: VLAN-i näide

Vastupidiselt mõningate tootjate väidetele tuleb arvestada asjaoluga, et VLANide väljatöötamisel ei ole eesmärgiks seatud turvanõuete täitmist võrkude lahutamisel. Kuna VLANidel on palju erinevaid punkte, mida saab rünnata, läheb kaitsevajadusega võrkude lahutamisel alati tarvis ka lisameetmeid. Järgneval joonisel kujutatud näite puhul võib eeldada, et VLAN 1 ja VLAN 2 ei ole teineteisest turvaliselt lahutatud, sest mõlemad VLANid on realiseeritud samal kommutaatoril.

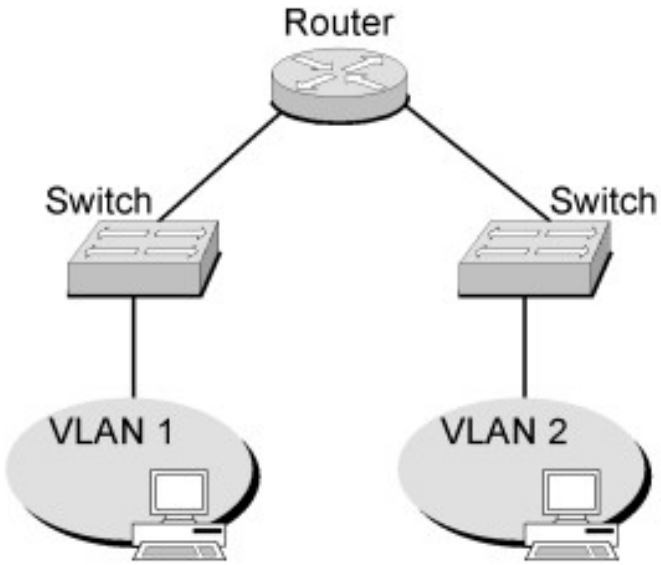


Joonis: kaks VLAN-i ühel kommutaatoril

Switch – kommutaator; Router – marsruuter; VLAN – virtuaalkohtvõrk

Kommutaatorile ei tohiks konfigureerida erineva turbevajadusega VLAN-e. Kui sellest ei ole olulistel põhjustel võimalik loobuda, tuleb piisava turbeastme tagamiseks kindlasti rakendada ka täiendavaid turvameetmeid. Mitte mingil juhul ei tohi sisevõrgu ja Interneti vahele jääva demilitariseeritud tsooni võrk olla konfigureeritud VLAN-ina samale kommutaatorile nagu sisevõrk. Järgnev joonis on näide kahe erineva turbevajadusega VLAN-i turvalisest lahutamisest, kus ühes kommutaatori kohta on konfigureeritud ainult üks VLAN. Võrkude ühendamise

tagab marsruuter, mis töötab paketifiltrina.



Joonis: VLANide turvaline lahutamine
Switch – kommutaator; Router – marsruuter; VLAN – virtuaalkohtvõrk
Kontrollküsimus:

- Kas on tarvis kasutada erineva turbevajadusega VLAN-e? Kui vastus on jah: kuidas toimub VLAN-ide lahutamine?

M 2.278z Marsruuterite ja kommutaatorite kasutamise tüüpstsenaariumid

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: IT-juht, administraator

Marsruuterite kasutusotstarbest sõltub suurel määral süsteemide konfiguratsioon. Lisaks määrab kasutusala ka täiendavad funktsioonid, mida marsruuter peab suutma täita.

Marsruuter sisevõrgus

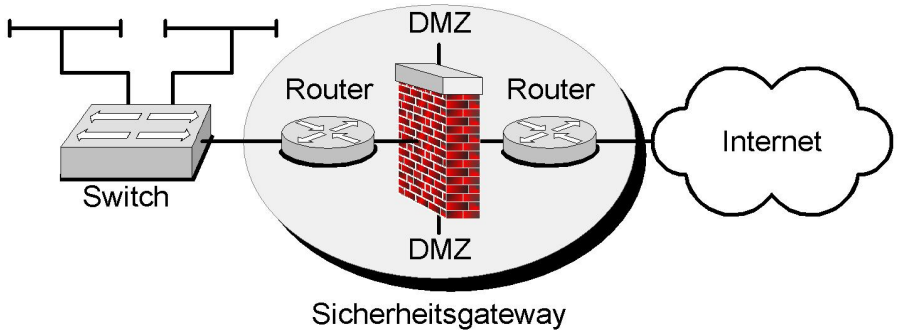
Marsruutereid kasutatakse paljudes süsteemides ainult LAN-to-LAN marsruuteritena, et ühendada alamvõrkusid ja takistada „kommuteeritud“ võrkude kõrvalmõjusid, nt nn leviedastustorme. Tänapäeval kasutatakse selles funktsioonis siiski üha sagedamini hoopis integreeritud marsruutimisfunktsiooniga kommutaatoreid (3. kihi või 4. kihi kommutaatoreid (vt M 2.277 Kommutaatori funktsionaalne kirjeldus). Antud kasutusstsenaariumi puhul sõltuvad marsruuterile seatavad turvanõuded olulisel määral marsruuteri kaudu ühendatud alamvõrkude turbevajadusest.

Marsruuter väliste võrkude ühendajana

Kui marsruuterit kasutatakse organisatsiooni võrgu ühendamiseks välisvõrkudega on tegu piirimarsruuteriga (border router). Sageli on piirimarsruuteritesse paigaldatud ka turvalüüs ja nad töötavad välise paketifiltrina (vt allpool). Võõrvõrkudega ühendatud marsruuterite puhul on seadme turvalisus ülimalt tähtis, sest see on avatud väljastpoolt tulevatele rünnetele.

Marsruuter paketifiltrina

Marsruutereid kasutatakse avalike võrkudega (nt Internetiga) ühendamisel sageli turvalüüside osana. Järgnevas näites koosneb turvalüüs sisemisest paketifiltrist, välisest paketifiltrist ja rakenduslüüsist. Turvalüüsides kasutatakse kesksete osadena rakenduslüüside asemel sageli ka Stateful-Inspection -süsteeme. Kehtestatud filtreerimisreeglid seadistatakse niihästi kesksel süsteemil kui ka marsruuteritel (sisemistel ja välistel). Marsruuteritel toimub reeglistiku rakendamine pääsuloendite (Access Control Lists) abil.



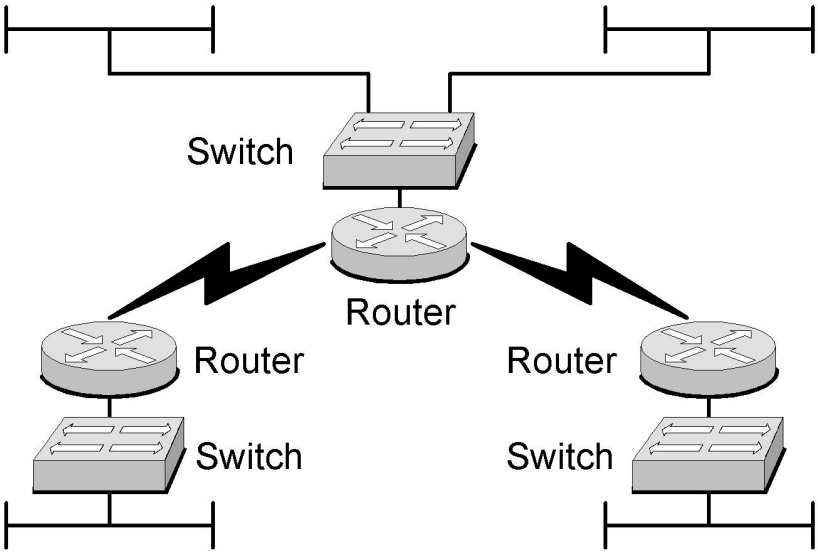
Switch – kommutaator; Router – marsruuter, DMZ – demilitariseeritud tsoon; Sicherheitsgateway - turvalüüs

Joonis 1: Marsruuter paketifiltrina

Pakettide filtreerimisfunktsioon on enamikes marsruuterites integreeritud operatsioonisüsteemi alla. Kuid leidub ka marsruutereid, mis pakuvad integreeritud Stateful-Inspection tulemüüri. Sides osalevate süsteemide haldamiseks (eriti filtreerimisreeglite rakendamiseks) on soovitatav kasutada ühte kokkuvõtvat kasutajaliidest. See aitab vältida konfigureerimisel tekkivaid vigu, mis võivad näiteks avada turvalüüsides turvaauke või häirida võrgu tööd. Antud kasutusotstarbel rakendatavale marsruuterile seatavad nõuded on kirjas M 2.73 Sobiva turvalüüsi (tulemüüri) põhistruktuuri väljavalimine . Lisaks tuleb konfigureerimisel arvestada miinimumnõuetega, mis on loetletud M 4.203 Marsruuterite ja kommutaatorite konfigureerimise kontroll-loend . Antud näites on kõige äärmisem paketifilter ühendatud avaliku võrguga ja kätkeb seetõttu endas ka kõige suuremat riski. Seetõttu peab selle marsruuteri konfiguratsioon olema eriti suurte piirangutega.

Ühendamine harudega

Marsruutereid saab kasutada harude ühendamiseks. Alljärgneval joonisel kasutatakse marsruutereid ühtse turbevajadusega ja ühtse administreerimisvastutusega kohtvõrkude (LAN-de) ühendamiseks. Nende kasutusvaldkondade puhul seadistatakse marsruuteritele tavaliselt kas liiga nõrgad filtreerimisreeglid või jäetakse see hoopis tegemata. Väikestes võrkudes võib kasutada staatilisi marsruutereid, kuid keskmistes või suurtes keskkondades kasutatakse marsruutimisprotokollidena Interior Gateway protokolle. Sides osalevad marsruuterid moodustavad seega osa suletud marsruutimisdomeenist. Ühendustehnoloogiatena võib kasutada ühendusi ATM, Frame Relay, ISDN, DSL või standard-püsiühendusi.



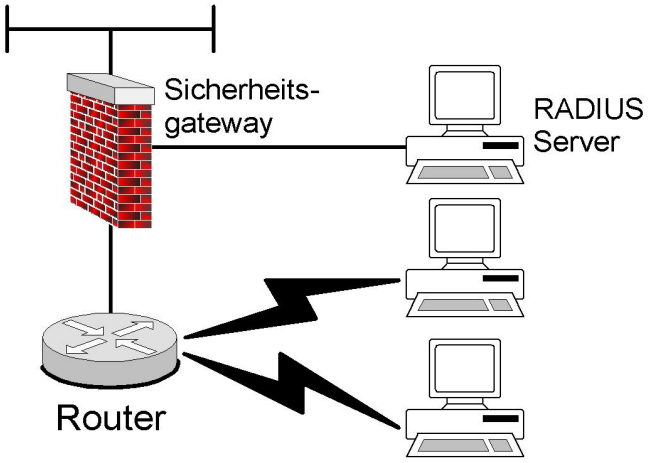
Switch – kommutaator; Router – marsruuter

Joonis 2: Ühendamine harudega

Kaugpöördus

Väikestes ja keskmistes võrkudes kasutatakse marsruutereid sageli ka kohtvõrkudesse (LAN) sissevalimiseks. Siiski ei tuleks sissevalimisvõimalusi integreerida LAN-i otse, vaid vähemalt läbi sissevalimis-marsruuteri, mis pakub

vastavaid turbevõimalus, et kaitsta LAN-i sissevalimise juurdepääsude kaudu toimuvate rünnete eest. Võimalik meetod, kuidas sissevalimist marsruuteri abil kaitsta on näha alloleval joonisel. Marsruuterit käitatakse turvalüüsi demilitariseeritud tsoonis. Lisaturvalisus saavutatakse RADIUS-serveriga autentimise abil. Marsruuter toimib sellisel juhul RADIUS-kliendina. Kaugkasutajad ei autendi end otse marsruuteris vaid RADIUS-serveris. Seeläbi saab RADIUS-serveris hallata tsentraalselt ka kasutajaid. Rakendades ühekordse parooli meetodit (One-Time-Password) koos riistvara-tokeniga või Smart Card -ga, saavutatakse tugev autentimine. RADIUS-severid toetavad tavaliselt OPT-põhiste protseduuride laiendamist kas plug-in -ide installeerimise või OTP-serveriga kommunikatsiooni abil. Tugeva autentimise sisseseadmise üheks täiendavaks võimaluseks on kaugpöörduslahenduse sidumine olemasoleva Public Key infrastruktuuriga (PKI). RADIUS-serveri konfiguratsioon peab sellisel juhul võimaldama juurdepääsu kataloogiteenusele. Seeläbi saavutatakse koos Smart Card -iga sertifikaadil põhinev tugev krüpteering. Lisameetmeid on kirjeldatud B 4.4 Virtuaalne privaatvõrk (VPN) ja B 4.5 IT-süsteemi kohtvõrguühendus ISDN kaudu .



Sicherheitsgateway – turvalüüs; Router – marsruuter

Joonis 3: Kaugpöördus

VPN

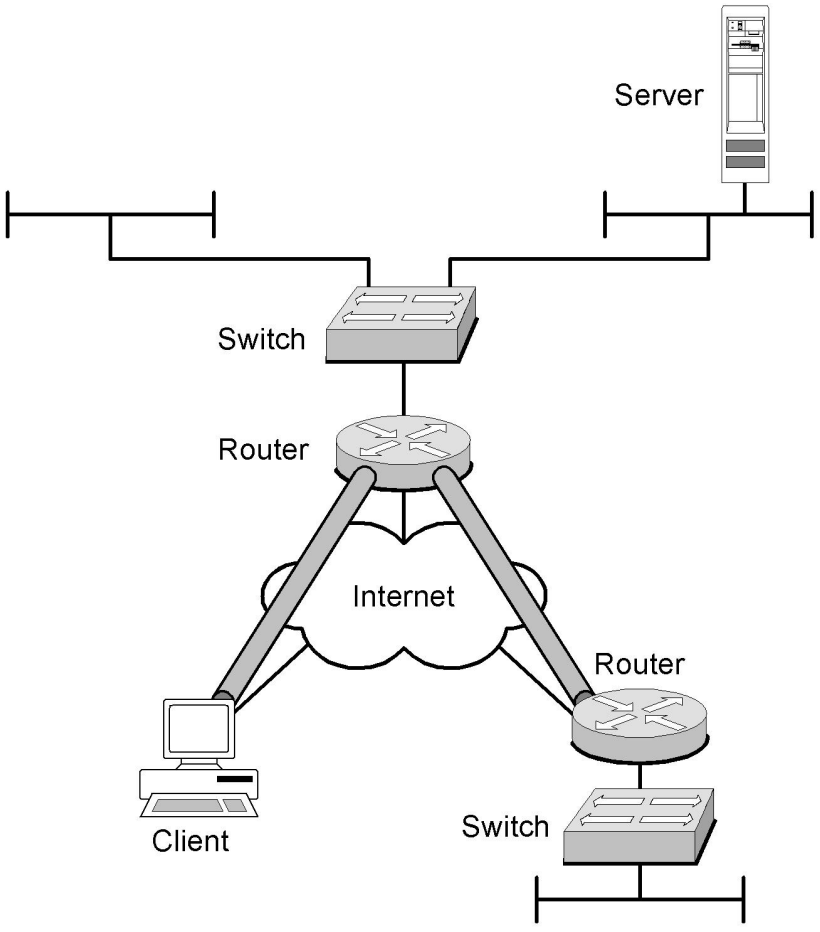
Üheks täiendavaks võimaluseks erinevate asukohtade turvaliseks ühendamiseks on virtuaalsete privaatvõrkude (VPN-de) kasutamine. VPN on turvatud tunnel, mis kulgeb läbi olemasolevate võrgu infrastruktuuride. Seetõttu on VPN-de kasutamisega võimalik edastada konfidentsiaalset infot turvaliselt ka ebaturvaliste võrkude (nt Interneti) kaudu. VPN-i piires kahe lõpp-punkti vahel toimuv andmevahetus krüpteeritakse. VPN-toega marsruuterid peavad toetama tugevat krüpteeringut (nt 3DES, AES). Paljudel saadaolevatel marsruuteritel on VPN-funktsioonide tugi. IPSec on standard, mis defineeritakse mitme RFC-e ja IEEE Internet-drafti kaudu. IPSec-i alusel saab seadistada VPNe ka erinevate tootjate seadmete vahel. IPSec tagab VPN-i lõpp-punktide vahel andmete usaldusväärsuse, tervikluse ja autentimise. IPSec põhineb OSI-lähtemudeli võrgukihil. See kasutab võtmete vahetamist Interneti kaudu (Internet Key Exchange (IKE)), et rakendada protokollide algoritmide kokkulepet vastavalt kohalikule konfiguratsioonile ning luua

krüpteerimis- ja autentimisvõtmeid. Üheks täiendavaks näiteks standardil põhineva VPN-tehnoloogia kohta on nn „SSL-VPN“, mille puhul toimub andmevahetus SSL/TLS-ga turvatud ühenduse kaudu. Lisaks IPSec-l ja SSL-l põhinevatele VPN-dele on olemas ka mitmeid teisi, nii tootjatele kuuluvaid kui ka avatud lähtekoodiga tehnoloogiad. Siinkohal tuleb arvestada, et need ei ole enamasti omavahel ühilduvad ning osad neist on saada ainult teatud süsteemiplatvormide jaoks. Juhul kui kasutatavaid komponente on võimalik kaasata olemasolevasse PKI-sse, tuleks seda kaaluda, sest seeläbi võib oluliselt kergendada VPN-de haldamist (eriti just võtmete haldamist) ja täiustada skaleeritavust.

Site-to-Site ja Client-to-Site VPN

Eristatakse Site-to-Site-VPN- i ja Client-to-Site-VPN- i. Site-to-Site-VPN on loodud võrkude ühendamiseks. VPN-i piiratakse seejuures mõlemal poolel vastavalt konfigureeritud, VPN-toega marsruuteritega. Sellised VPN-d on alternatiiviks kohalike võrkude ühendamisel kaugliikluse marsruutide kaudu. Client-to-Site-VPN- i puhul ehitatakse VPN üles kliendi ja VPN-toega marsruuteri vahele. Tihti tuleb selleks kliendile paigaldada vastava tootja VPN-klienditarkvara. Client-to-Site-VPN-i tuleks käsitleda täiendava alternatiivina kohtvõrkude kasutamiseks kaugpääsu kaudu.

Järgneval joonisel on kujutatud VPN-arhitektuur.

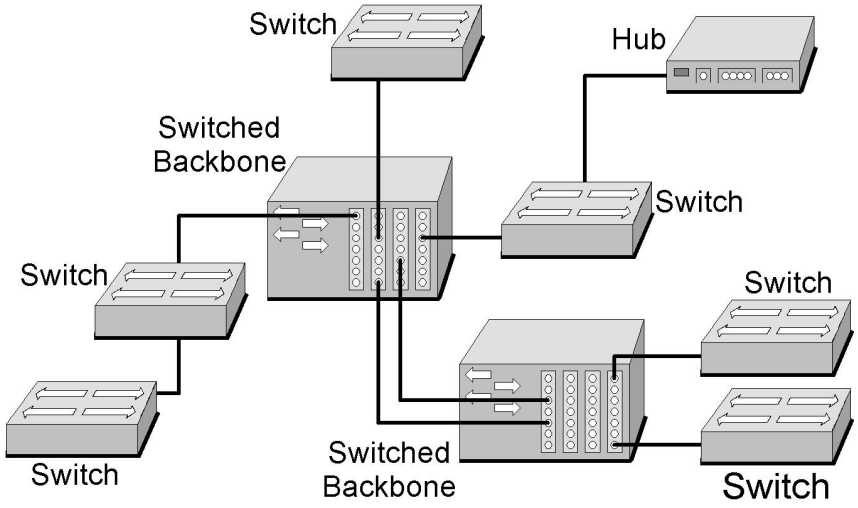


Server – server; Switch – kommutaator; Router – marsruuter; Client - klient

Joonis 4: VPN-arhitektuuri näide

Kommutaatorid

Kommutaatori kasutusotstarvet VLAN-de loomisel on kirjeldatud M 2.277 Kommutaatori funktsionaalne kirjeldus . Järgneval joonisel on kujutatud tüüpilist kommuteeritud võrku.



Switch – kommutaator; Hub – jaotur; Switched Backbone - kommuteeritud magistraal

Joonis 5: kommuteeritud võrk magistraal- ja juurdepääsukommutaatoritega

Joonisel tuleb vahet teha kahte tüüpi kommutaatorite vahel. Juurdepääsukommutaatorid, mille iseloomustavaks tunnuseks on suur arv ühendusi (porte), tagavad vahetu ühenduse lõppseadmetega. Juurdepääsukommutaatorid on omakorda ühendatud kesksete magistraalkommutaatoritega. Magistraalkommutaatorid moodustavad nn kommuteeritud magistraali (Switched Backbone). Kommuteeritud magistraal seob kokku ühendatud kommutaatorite ribalaiused, et tagada lõppseadmete vahel kõrge läbilaskevõimsus. Kommuteeritud magistraali iseloomustavaks tunnuseks on seega kõrge läbilaskevõime. Kommuteeritud magistraali läbilaskevõime sõltub erinevatest faktoritest, millega tuleb arvestada seadmete muretsemisel. Olulisemateks faktoriteks on maksimaalne aadressi-vahemälu dünaamiliselt tuvastatud MAC-aadresside säilitamiseks, magistraal-kommutaatori Backplane -i läbilaskevõime, samuti kommuteeritud magistraali liinikiirus. Tagamaks efektiivset ühenduste loomist erinevate kommutaatoritega ühendatud lõppseadmete vahel, peavad osalevad kommutaatorid joonisel kujutatud struktuurile sarnase struktuuri puhul omavahel vahetama dünaamiliselt tuvastatud kommuteerimistabeleid. Reeglina toimub see toojatest sõltuvate (firmade poolt loodud) protokollidega (nt Cisco Discovery Protocol – CDP). Suurtes kommuteeritud võrkudes on kommutaatorid tavaliselt kaskaadis. See saavutatakse nn Uplink -portidega.

Täiendavad kontrollküsimused:

- Kas vajaminevate võrgukomponentide kasutusotstarve on kindlaks tehtud?
- Millistel otstarvetel on tarvis kasutada marsruuterit?
- Milliseid funktsioone (VPN, Remote Access, paketi filtreerimine) peab marsruuter toetama?
- Kas marsruuteri kasutamisele seatavad nõuded on välja töötatud?

M 2.279 Marsruuterite ja kommutaatorite turvapoliitika koostamine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT-turvaosakond

Rakendamise eest vastutavad: IT-turvaosakond

Kuna marsruuterid ja kommutaatorid on võrgu kesksed elemendid, on nende turvaline ja nõuetekohane töö eriti oluline. Seda saab tagada ainult siis, kui seadmete käitamise nõuded on integreeritud olemasolevatesse turvatehnilistesse nõuetesse. Üldkehtivad turvatehnilised nõuded (eesmärgiks seatud turbeastme nõuded) tulenevad tervet organisatsiooni hõlmavatest turvasuunisest ning nende rakendamiseks ja täpsustamiseks tuleks antud kontekstis formuleerida eraldi spetsiaalse marsruuterite ja kommutaatorite turvasuunised. Sellega seoses tuleb kontrollida, kas lisaks kogu organisatsiooni hõlmavale turvapoliitikale on tarvis arvestada ka muude, hierarhias kõrgemalseisvate nõuetega nagu IT-turvapoliitika, paroolisuuniste või internetikasutuse nõuetega. Kõik marsruuterite ja kommutaatorite soetamisega ja käitamisega seotud isikud peavad tundma turvapoliitikat ning oma töödes sellest lähtuma. Nagu kõikide suuniste puhul, tuleb nende üldise auditi käigus regulaarselt kontrollida nende sisu ja rakendamist. Turvapoliitika peab esmalt täpsustama üldise vajaliku turbeastme ja sisaldama täpset infot marsruuterite ja kommutaatorite käitamise kohta. Järgnevalt on loetletud mõned punktid, millega tuleks arvestada:

- Üldine konfigureerimisstrateegia („liberaalne“ või „piirav“)
- Administraatorite ja auditeerijate töö reeglid:
- Milliste juurdepääsude kaudu tohivad administraatorid ja auditeerijad süsteemidele ligi pääseda (nt ainult kohapealsest konsoolist, eraldi administreerimisvõrgu kaudu või krüpteeritud ühenduste kaudu)?
- Millised toimingud tuleb dokumenteerida? Millisel kujul luuakse dokumentatsioon ja kuidas seda hooldatakse?
- Kas teatud muudatuste puhul on kohustuslik järgida nelja-silma-printsiipi?
- Millise skeemi järgi jagatakse administreerimisõiguseid?
- Nõuete profiilist tulenevad ettekirjutused seadmete soetamisel
- Installeerimise ja konfigureerimise nõuded
- Esmapaigaldamise protseduur
- Default -seadistuse kontrollimine võimalike turvariskide osas
- Füüsilise juurdepääsukontrolli reguleerimine
- Konsooli ja muude juurdepääsuliikide kasutamine ja konfigureerimine
- Kasutajate ja töörollide haldamise reeglid, volituste struktuurid (autentimise ja volitamise toimimine ja meetodid, volitused installeerimiseks, täiendite laadimiseks, konfiguratsiooni muutmiseks jne). Võimalusel tuleks administreerimiseks välja töötada töörollide jaotamise kontseptsioon.
- Reeglid VLAN-de ja VPN-de sisseseadmise ja kasutamise kohta (nt: ühe kommutaatori piires on keelatud erineva turbevajadusega VLANide kasutamine)
- Reeglid dokumentatsiooni koostamise ja haldamise kohta, dokumentatsiooni vorm: protseduurijuhised, kasutusjuhendid

- Kui üldised nõuded on välja töötatud: lubatud ja keelatud teenused, protokollid ja võrgud
- Turvalise käitamise nõuded
- Administreerimise kaitse (näiteks: juurdepääs ainult turvatud ühenduste kaudu)
- Krüpteerimise kasutamine (standardid, võtmete tugevus, kasutusvaldkonnad)
- Paroolikasutuse nõuded (paroolireeglid, paroolidega kaitstavad keskkonnad, paroolimuudatuste reeglid ja olukorrad, vajadusel paroolide deponeerimine)
- Töö ja hoolduse tööriistad, integreerimine olemasolevasse võrguhaldusesse
- Volitused ja protseduurid tarkvara uuendamisel ja konfiguratsiooni muutmisel
- Millised sündmused logitakse?
- Kuhu salvestatakse logifailid?
- Kuidas ja kui sageli toimub logide analüüsimine?
- Andmete varundamine ja taastamine (vt M 6.91 Marsruuterite ja kommutaatorite andmete varundus ja taaste)
- Sidumine üleorganisatsioonilise andmevarunduse kontseptsiooniga
- Tegutsemine rikete ja vigade korral, Incident Handling
- Reeglid töötõrgetele ja tehnilistele vigadele reageerimiseks (kohalik tugi, kaughooldus)
- Reeglid turvaintsidentide jaoks
- Ootamatuste ennetamine (vt M 6.92 Marsruuterite ja kommutaatorite hädaolukorraks valmisoleku plaan)
- Sidumine üleorganisatsioonilise ootamatuste ennetamise kontseptsiooniga
- Revisjon ja audit (vastutusalad, protseduurid, integreerimine kõikehõlmavasse revisjoni kontseptsiooni)

Turvapoliitika eest vastutab IT-turvaosakond, seega tuleb turvapoliitika muudatused ja kõrvalekalded kooskõlastada IT-turvaosakonnaga.Turvapoliitika koostamisel on soovitatav esmalt välja töötada maksimaalselt palju erinevaid nõudeid ja ettekirjutusi süsteemide turvalisuse tagamiseks. Seejärel saab neid viima neid vastavusse tegelike oludega. Ideaaljuhul saavutatakse niisuguse lähenemisega kõikide võimalike aspektidega arvestamine. Iga nõude puhul, mis teise tööetapi käigus jäetakse kõrvale või mida pehmendatakse, tuleb dokumenteerida sellise kõrvalejätmise põhjus.

Täiendavad kontrollküsimused:

- Kas marsruuterite ja kommutaatorite kasutamise kohta on koostatud vastav turvapoliitika?
- Millal toimus viimati turvapoliitika uuendamine?
- Kas turvapoliitikas on sõnastatud ka turbeaste?
- Kas turvapoliitika kirjeldab marsruuterite ja kommutaatorite sisseseadmise, käitamise ning tõrgete kõrvaldamise nõudeid?
- Kas turvapoliitikas on arvestatud komponentide erineva kasutusotstarbega?

M 2.280 Sobivate marsruuterite ja kommutaatorite ostmis- ja valimiskriteeriumid

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: administraator

Aktiivsed võrgukomponendid erinevad üksteisest oma jõudluse, pakutavate turvamehhanismide, kasutamismugavuse ja majanduslikkuse poolest. Soetamisel tehtud vead võivad olulisel määral mõjutada võrgu turvalisust, sest sobimatud seadmed ei pruugi võimaldada saavutada eesmärgiks seatud turbeastet. Enne marsruuterite ja kommutaatorite soetamist tuleb seega koostada nimekiri nõuetest, mille alusel saadaolevaid tooteid hinnata. Läbiviidud võrdlusele toetudes saab toote soetamisel olla kindel, et vastav toode suudab oma töös kõiki vajalikke nõudeid ka reaalselt täita.

Kesksed turvanõuded
IT-turvalisuse vaatepunktist seatakse aktiivsetele võrgukomponentidele nõudeks, et need peavad võimaldama administreerimist turvaliste protokollide kaudu ning et seadme kasutajate haldus peab võimaldama vajalikul määral rakendada tervet organisatsiooni hõlmavat töörollide jaotamise kontseptsiooni. Nõue, et paroole tohib seadmes salvestada ainult krüpteeritult, peaks tegelikult olema iseenesest mõistetav, kuid sellele vaatamata leidub jätkuvalt seadmeid, kus paroolid tuleb salvestada konfiguratsioonifailidesse tavateksti kujul. Uute seadmete soetamisel tuleks valikust välja jätta tooted, mis ei võimalda turvalist administreerimist ja mille puhul ei saa paroole salvestada krüpteeritult. IT-turvalisust võivad mõjutada ka aktiivsete võrgukomponentide funktsioonipõhised omadused. Tavaliselt on sellest mõjutatud üks peamisi näitajaid nagu käideldavus, näiteks kui seade ei saavuta ebapiisava mälu tõttu nõutud läbilaskevõimet. Lisaks ei tohi unustada ka tootjapoolset tuge, näiteks kui turvaaukude lappimiseks läheb kiirkorras tarvis vastavaid paiku.

Järgnevalt on loetletud marsruuterite ja kommutaatorite soetamise mõningad peamised nõuded. Seejärel kirjeldatakse veel ka mõningaid marsruuteritele ja kommutaatoritele esitatavaid erinõudeid.

Marsruuterite ja kommutaatorite üldkriteeriumid

1. Peamised funktsioonidele esitatavad nõuded

- Kas seade toetab kõiki vajaminevaid protokolle ja juhtmestike tüüpe?

2. Turvalisus

- Kas süsteem toetab turvalist administreerimist võimaldavaid protokolle? Kui marsruutereid ja kommutaatoreid ei administreerita eraldi administreerimisvõrgu kaudu, peab neid seadmeid saama konfigureerida turvaliste võrguprotokollide (nt SSH2) abil.

- Kas süsteem toetab paroolide krüpteeritud salvestamist? Seadmeid, mis salvestavad paroole mittekrüpteeritud kujul, ei tohiks enam soetada.

3. Hooldamine

- Kas tootja pakub regulaarselt täiendeid ja kiirelt kättesaadavaid turvapaiku? Eriti oluline on, et tootja reageeriks avastatud turvaaukudele võimalikult kiiresti.
- Kas toote osas on võimalik sõlmida hooldusleping uid? Sageli pääseb tootjapoolsetele täienditele ja tugiteenustele ligi ainult kehtiva hooldusleping u alusel.
- Kas hooldusleping utes on võimalik kindlaks määrata maksimaalne aeg, mis tohib kuluda probleemi kõrvaldamisele? Hooldusleping on kasulik ainult siis, kui garanteeritud reageerimis- ja tööprotsesside taastamisaegadega suudetakse täita seadmetele kehtestatud käideldavuse alaseid nõudeid.
- Kas tootja pakub ka tehnilist klienditeenindust (infoliini teenust), mis oleks võimeline probleemide korral kohe abi pakkuma? Käesolev punkt peaks kajastuma sõlmitud hooldusleping us. Lepingu sõlmimisel tuleb jälgida, mis keeles pakutakse tootjapoolset infoliini teenust.

4. Usaldusväärsus/rikkekindlus

- Kas tegu on usaldusväärse tootega? Töökindluse kohta peaks tootja suutma esitada kogemustele tuginevaid andmeid, nt Mean Time Between Failures (MTBF), Mean Time To Repair (MTTR).
- Kas tootja pakub kõrge käideldavusega lahendusi? Kui käideldavuse nõudeid ei suudeta katta hooldusleping utega, peab süsteem toetama kõrge käideldavusega lahendusi.

5. Kasutajasõbralikkus

- Kas toote installeerimine, konfigureerimine ja administreerimine on lihtne? Lisaks peaks olema võimalik läbida toodet puudutavaid koolitusi

6. Kulutused

- Kui suured on seadmete soetamiskulud?
- Kui suured on eeldatavad jooksvad kulud (hooldamine, käitamine, tugiteenus)? Nende kuludega tuleks arvestada juba planeerimisfaasis. Kontrollida tuleks hooldus- ja tugilepingute sisu (reageerimisaegu, infoliini olemasolu, personali kvalifikatsiooni jne).
- Kui suured on eeldatavad personaliga seotud jooksvad kulutused?
- Kas on tarvis soetada täiendavaid tarkvara- või riistvarakomponente (nt RADIUS-servereid, võrguhaldussüsteeme)? Sellele küsimusele tuleb vastata juba planeerimisfaasis. Kui näiteks võrguhaldussüsteem on juba kasutuses, tuleb kontrollida selle ühilduvust soetatavate seadmetega. Lisaks tuleb arvestada tööde mahuga, mis on vajalik seadmete integreerimiseks olemasolevasse infrastruktuuri.
- Kui kõrged on administraatorite koolituskulud?

7. Funktsionaalsus

- Kas süsteemi on võimalik turvaliselt integreerida olemasoleva võrguhalduse arhitektuuri hulka? Tuleks arvestada integreerimisele kuluva tööde mahuga. Tootja peaks edastama info toetavate NMS-protokollide kohta ja vajalikud MIB-tabelid.
- Kas süsteem toetab NTP-d? NTP on eriti oluline logimise jaoks, vt M 4.227 Lokaalse NTP -serveri kasutamine aja sünkroniseerimiseks .
- Kas süsteem toetab autentimisserverite kaasamist (nt RADIUS või TACACS+)? Kui autentimisserver on juba kasutuses, peab süsteem suutma seda ka kasutada.

8. Logimine

- Millised logimisvõimalused on olemas? Logimiseks pakutud võimalused peavad vastama vähemalt turvapoliitikas sõnastatud nõuetele.
- Kas logiandmete detailsust on võimalik konfigureerida?
- Kas logisse salvestatakse kõik olulised andmed?
- Kas süsteem toetab tsentraliseeritud logimist (nt syslog)? Marsruuterid ja kommutaatorid peavad toetama tsentraliseeritud logimist, et võimaldada logiandmeid eesmärgipäraselt hinnata.
- Kas logimine toimub selliselt, et andmekaitsest tulenevad nõuded on täidetud?
- Kas teavitusfunktsioonide tugi on olemas? Kiire ja tsentraliseeritud teavitamine marsruuteritele ja kommutaatoritele suunatud rünnete kohta peab olema tagatud seadmete teavitusfunktsioonidega. Selleks võib kasutada näiteks võrguhaldussüsteemi.

9. Infrastruktuur

- Mõõdud ja sobivus kaitsekappidega. Soetamisel tuleb arvestada ka marsruuterite ja kommutaatorite ruumivajadusega. Kas seadet on võimalik paigaldada ettenähtud kaitsekappidesse (seadmete kuju, kaal, kinnituselemendid)?
- Toide ja heitsoojus. Tootja peab edastama andmed voolutarbimise ja kasutuskeskkonna temperatuurinõuete kohta. Kas toite ja UPS-i olemasolev jõudlus on piisav? Kas olemasolev jahutusvõimsus on seadme heitsoojuse ärajuhtimiseks piisav?

Kommutaatorite erikriteeriumid

1. Jõudlus ja skaleeritavus

- Kas süsteem suudab täita jõudlusele seatud nõudeid? Tootja peab edastama info andmete läbilaskevõime kohta, eriti tuleb jälgida kommutaatori Backplane -i maksimaalset läbilaset. Täiendavad faktorid, mis võivad jõudlust mõjutada, on aadressivahemälu ja salvesti suurus.
- Kui suur on saadaolevate portide arv? Juurdepääsukommutaatoril peab olema piisav arv porte lõppseadmetega ühendamiseks. Sageli saab võrrelda erinevate kommutaatorite soetamiskulusid, lähtudes kuludest ühe pordi kohta.

- Kas süsteem on „ stackable “ või (nt täiendavate sissepistetavate kaartidega) moodulite kaupa laiendatav? Vajadus lisafunktsioonide kasutamise või suurema porditiheduse järele ei tohiks luua olukordi, kus seade tuleb enneaegselt välja vahetada.

2. Funktsionaalsus

- Kas kommutaator toetab 3. kihi kommuteerimist (marsruutimist)? Kohtvõrkudes võib see funktsioon olla kasulik jõudlusele (andmete läbilaskevõimele).
- Kas kommutaator toetab VLAN-e? VLAN-de rakendamisel peab tootja edastama andmed kasutatud standardi kohta.
- Kas kommutaator toetab Cut Through ja/või Store and Forward meetodit?

Marsruuterite erikriteeriumid
1. Jõudlus ja skaleeritavus

- Kas süsteem suudab täita jõudlusele seatud nõudeid? Tootjalt peab olema võimalik saada infot andmete läbilaskevõime kohta. Kui marsruuterit kasutatakse VPN-lõpp-punktina, kuuluvad tähtsate kriteeriumite hulka ka toetatavad krüpteerimisprotsessid ning jõudlus andmete krüpteerimisel ja dekrüpteerimisel.
- Kas seadet on võimalik moodulite kaupa laiendada? Arvestada tuleb standardina saadaolevate liideste arvuga, eriti aga toetatud liideste maksimaalse arvuga.

2. Funktsionaalsus

- Kas marsruuter toetab VPN-funktsioone? VPN-funktsioonidega marsruuter peab toetama IPSec-standardit ja tugevaid krüpteerimisalgoritme (3DES, AES).
- Kas marsruuter toetab ACL-de kasutamist? Arvestada tuleb soetatava marsruuteri filtreerimisfunktsioonidega (vt M 5.111 Marsruuterite pääsuloendite konfigureerimine).
- Milliseid marsruutimisprotokolle seade toetab? Marsruuter peab toetama turvalisi marsruutimisprotokolle (vt M 5.112 Marsruutimisprotokollide turvaaspektide arvestamine).

Kontrollküsimused:

- Kas marsruuterite ja kommutaatorite soetamisnõuded on defineeritud?
- Kas seejuures arvestati ka seadmete erineva kasutusotstarbega?
- Kas nõuded on kirjalikult fikseeritud?

M 2.281 Marsruuterite ja kommutaatorite süsteemikonfiguratsiooni dokumenteerimine

Algatamise eest vastutavad: IT-turvaosakond

Rakendamise eest vastutavad: administraator

Marsruuterite ja kommutaatorite konfigureerimiseks kasutatakse tavaliselt konfiguratsioonifaile, mis on salvestatud seadmesse. Turvalise töö tagamiseks on marsruuterid ja kommutaatorid varustatud terve rea erinevate konfigureerimisvõimalustega. Esmapaigaldamisel/tarnimisolekus on need seadistused standardväärtustega (default).

Aluskonfiguratsiooni dokumenteerimine

Seadme kasutussevõtmise konfiguratsioon tuleb dokumenteerida selliselt, et administraator või tema asendaja suudaks alati dokumentatsiooni abil tuvastada, millise konfiguratsiooniga on tegu. Konfiguratsioonifaili tuleb lisada kommentaar ja seda eriti neil juhtudel, kui konfiguratsioon erineb tavaväärtusest, selgitamaks vastava konfiguratsiooni valikupõhjuseid.

Muudatuste dokumenteerimine

Eranditult kõik konfiguratsiooni muutmised peavad olema administraatori jaoks mõistetavad. Soovitatav on dokumenteerida vähemalt järgnevad punktid:

- Mida muudeti?
- Miks muudeti (põhjus)?
- Millal muudeti (kellaaeg, kuupäev)?
- Kes muutis?

Muudatuste dokumenteerimiseks võib kasutada ka kommentaaride lisamist konfiguratsioonifailile. Siiski on tavaliselt mõistlik salvestada failis iga valiku kohta ainult viimane muudatus.

Turvalisust mõjutavate muudatuste täielik logi

Lisaks eelnevale tuleb vähemalt kõik turvalisust mõjutavad konfiguratsiooni muudatused salvestada ka logisse, et nende alusel oleks alati arusaadav, kuidas oli seade teatud hetkel konfigureeritud. Seda logi ei tohi hoida seadmes endas. Dokumenteerimise ja logimise kergendamiseks võib kasutada auditeerimist ja versioonikontrolli võimaldavat süsteemi, näiteks CVS-i. Sellise süsteemi täiendavaks eeliseks on võimalus varasem konfiguratsioon hädaolukorras kergesti taastada. Tsentraliseeritud administreerimiseks kasutatavates võrguhaldussüsteemides on dokumenteerimis- ja logimisfunktsioonid reeglina integreeritud. Dokumendi kujundus võiks olla selline, et see oleks arusaadav ka spetsialistile, kes ei ole tuttav vastava süsteemikeskkonna konkreetsete oludega.

Hädaolukorraks ettevalmistuse tagamiseks tuleks konfiguratsioonifailid salvestada ka vastava otstarbega serverisse. Konfiguratsiooniandmete tsentraliseeritud halduseks kasutatakse sageli TFTP-servereid. TFTP-servereid tohib käitada ainult turvatud administreerimisvõrgus, sest TFTP teenuses on terve rida kitsaskohti (vt G 2.87 Ebaturvalised protokollid avalikes võrkudes). Alternatiivne võimalus on edastamine SCP kaudu (vt M 5.64 Secure Shell (SSH)).

Täiendavad kontrollküsimused:

- Kas konfiguratsioonifaile hallatakse tsentraalselt?
- Kas konfiguratsioonifailid dokumenteeritakse lähtuvalt ülanimetatud punktidest?

- Kas kasutatakse versiooni kontrollsüsteemi?

M 2.282 Marsruuterite ja kommutaatorite seire

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator

Aktiivsete võrgukomponentide nõuetekohase töö ja kõikide konfiguratsiooniparameetrite õigsuse tagamiseks tuleb sisse seada regulaarne, võimalikult automaatne kontrolliprotsess. Selle juurde kuuluvad näiteks regulaarsed funktsioonikontrollid, muudatuste kehtestamine ja nende rakendamise kontrollimine, samuti logifailide ja teadete seire. Et töö ajal tekkivat suurt andmekogust tõhusalt töödelda, tuleb tavaliselt kasutada sobivaid tööriistu, et seire saaks toimuda võimalikult automatiseeritult. See võib toimuda näiteks võrguhaldussüsteemiga (NMS) sidumise läbi.

Seire kontrollnimekiri

Seireks võib kasutada M 4.203 Marsruuterite ja kommutaatorite konfigureerimise kontroll-loend esitletud kontrollnimekirja. Seire aluseks tuleks võtta marsruuterite ja kommutaatorite jaoks loodud turvapoliitika (vt M 2.279 Marsruuterite ja kommutaatorite turvapoliitika koostamine). Lisaks tuleks seireprotsessi raames arvestada järgnevate punktidega:

Mida testitakse/kontrollitakse?

- Seadmete üldist töövalmidust kontrollib administraator tavaolukorras regulaarselt töö käigus.
- Konfiguratsioonifailide terviklust tuleb kontrollida regulaarsete ajavahemike tagant. Marsruuterite ja kommutaatorite turvapoliitika peab kehtestama regulaarsed kontrollid koos töötajate vastutusalade määramisega.
- Administraator peab regulaarselt kontrollima andmevarunduse seisu (tsentraalselt salvestatud konfiguratsiooniandmeid).
- Administraator peab süsteemi dokumentatsiooni pidevalt uuendama. Tehtud uuendusi saab kontrollida auditi raames. Siinkohal tuleb arvestada ka moodulitega M 2.31 Volitatud kasutajate ja õiguste profiilide dokumenteerimine ja M 2.64 Logifailide kontroll .

Kuidas testitakse?

- Regulaarse seire saavutamiseks võib komponendid siduda võrguhaldussüsteemiga. Turvaeeskirjade rikkumised, tõrked ja vead on NMSi teavitusfunktsioonidega aegsasti avastatavad.
- Auditite raames kontrollitakse komponente tavaliselt pisteliselt. Auditid lähtuvad esmajoones marsruuterite ja kommutaatorite turvapoliitikast. Sellise kontrolli oluliseks osaks on süsteemi dokumentatsiooni värskuse, andmevarunduse seisu, paroolivahetuse, jms kontrollimine. Mooduli M 4.203 Marsruuterite ja kommutaatorite konfigureerimise kontroll-loend kontrollnimekirja rakendades saab kontrollida suuremat osa turvalisust puudutavatest seadistustest.
- Marsruuterite ja kommutaatorite turvaseadistuste kontrollimiseks on saada mitmeid tasuta turvatööriistu (nt Nessus). Sellised tööriistad võivad olla paigaldatud võrgus asuvasse arvutisse. Võimalusel tuleks kasutada kõige uuemat versiooni. Vajalikuks operatsioonisüsteemiks on sageli Unix või Linux. Vastava süsteemi kaudu on administraatoril võimalik marsruutereid ja kommutaatoreid skanneerida, et kontrollida nende seadmete erinevaid seadis-

tusi. Tasulised tööriistad võivad pakkuda üsna mugavaid võimalusi kontrollide hindamiseks ja toimunud skanneeringute ajaloo jälgimiseks.
- Marsruuterite ja kommutaatorite regulaarset kontrolliteenust pakuvad ka mitmed turvaettevõtted. Regulaarsete aruannete ja analüüside alusel antakse käitajale ülevaade komponentide seisukorrast.

Millal testitakse?

- Administraator kontrollib NMS-süsteemi abil seadmete töökindlust tavaliselt töö käigus ning enamasti toimub see automaatselt. Administraator peab süsteemi dokumentatsiooni pidevalt uuendama.
- Administraator peab regulaarselt (iga nädal) kontrollima andmevarunduse seisu, konfiguratsiooniandmete terviklust ja täiendavaid konfiguratsioonifaile.
- Pärast installeerimist peab administraator regulaarselt (iga kuu) süsteemi turvatööriistade abil skanneerima. Asetleidnud sündmused tuleb kontrollida ja arhiveerida.
- Turvapoliitika järgimist tuleb regulaarselt (nt kord aastas turvalisuse ja etalonturbe auditi raames) kontrollida.

Kes testib?

- Administraator peab regulaarselt kontrollima (komponentide funktsiooni, andmevarunduse seisu, konfiguratsiooniandmete terviklust, skanneeringuid jne).
- Turbeauditi ja etalonturbe auditi raames ei tohi turvapoliitika ja turvameetmete järgimist kontrollida mitte administraator, vaid sõltuvalt juurutatud turvahaldusprotsessist peab seda kontrollima kas audiitor, IT-turvalisuse eest vastutav töötaja või revident.

Milline info on kontrolli aluseks?

- Marsruuterite ja kommutaatorite turvapoliitika
- Marsruuterite ja kommutaatorite logifailid
- Süsteemi dokumentatsioon (vt M 2.281 Marsruuterite ja kommutaatorite süsteemikonfiguratsiooni dokumenteerimine)
- IT-turvakontseptsioon
- IT-etalonturbe kataloogid
- Läbiviidud skanneerimiste tulemused

Konfiguratsiooni kontrollimine

Marsruuterite ja kommutaatorite sisseseadmisel tuleb kontrollida kõiki tavaseadistusi ja vajadusel neid modifitseerida. Selle käigus toimub näiteks ebavajalike teenuste desaktiveerimine ja eelseadistuste kohandamine vastavalt käitamisega ja turvalisusega seotud vajadustele. Selleks vajalike tööetappide selgitused leiate M 4.201 Marsruuterite ja kommutaatorite turvaline lokaalne aluskonfiguratsioon ja M 4.202 Marsruuterite ja kommutaatorite turvaline võrgu-aluskonfiguratsioon . Default -seadistustega ümberkäimisele esitatavate nõuete rakendamist tuleb kontrollida regulaarsete auditite raames. Seeläbi saab tuvastada juhuslikke või tahtlikke muudatusi ja kontrollida tootja kõige uuemate soovituste elluviimist. See võib

toimuda iga seadmetüübi või iga operatsioonisüsteemi versiooni jaoks loodava paigaldusjuhendi alusel ning kontrollida tuleks igat konkreetset seadet. Siinkohal tuleb siiski arvestada asjaoluga, et osade tootjate operatsioonisüsteemi käsklused ei kuva kõiki default -seadistusi. Sel põhjusel tasub täieliku analüüsi saamiseks kasutada eraldi tarkvaratööriistu. Kõikide seadmete põhjalikuks testimiseks saab kasutada tarkvaratooteid, mis võimaldavad konfigureeritavate parameetritega automatiseeritud testimist.

Mirror Port

Andmevahetuse analüüsiks saab marsruuteri või kommutaatori ühe pordi seadistada peegelpordiks (Mirror Port). Antud seadistuse puhul replitseeritakse suvalise pordi kogu andmevahetus peegelpordis ning seda saab analüüsida vastava programmiga. Erinevalt muudest analüüsimeetoditest ei katkesta ega sega antud meetod andmevahetust. Nimetatud mehhanism võimaldab kasutada kahte analüüsimeetodit: Ühe defineeritud pordi kogu andmevahetuse peegeldamine või MAC-aadressi andmevahetuse peegeldamine. Teisel juhul peegeldatakse peegelpordis kogu defineeritud lähte- ja/või siht-MAC-aadressi andmemaht, mis läbib seadet. Peegelport ei tohi kuuluda produktiivsesse VLANi ega täispuu gruppi (STG - Spanning Tree Group). Standardina peab „Port Mirroring “ olema välja lülitatud. Port Mirroring konfiguratsiooni juurdepääs peab olema kaitstud. Pärast peegelpordi kasutamist tuleb see desaktiveerida. Tavakasutuse käigus tuleb regulaarselt kontrollida, kas pordipeegeldamise funktsioon on desaktiveeritud.

Täiendavad kontrollküsimused:

- Kas marsruuterite ja kommutaatorite regulaarne kontroll on turvapoliitikasse sisse töötatud?
- Milline on kontrollimisele kehtestud intervall?
- Millal kontrolliti viimati marsruutereid ja kommutaatoreid ja kes kontrollis?
- Kas kontroll dokumenteeriti?
- Kas kontrolli tulemusel algatati vastavad tegevused ja määrati vastutusalad?

M 2.283 Marsruuterite ja kommutaatorite tarkvara hooldus

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator

Igasugune tarkvara kasutamine kätkeb endas vajadust operatsioonisüsteemi ja konfiguratsiooni regulaarselt kontrollida ja hooldada. Kontrollida tuleb ka marsruutereid ja kommutaatoreid, et võimaldada nt laiendada funktsioone, kõrvaldada tarkvaravigu ning tõsta jõudlust ja turvalisust. Siinkohal tuleb arvestada, et praktikas võib marsruuterite ja kommutaatorite hooldamine sageli tähendada terve operatsioonisüsteemi tarkvara väljavahetamist. Täiendite või turvapaikade paigaldamine võib sageli osutuda võimatuks. Nagu kõikide konfiguratsioonimuudatuste puhul, tuleb ka siin olla ülimalt hoolikas, kuna oskamatu töö võib mõjutada seadmete funktsiooni ja turvalisust. Muudatuse hoolika planeerimise juurde kuulub eriti just ka varustrateegia (Fallback-Strategy).

Uue tarkvara paigaldamine

Täiendite paigaldamise ettevalmistamisel tuleb pöörata tähelepanu järgnevale:

- Tööde teostuseks tuleb valida sobiv aeg. Vajaminevat töömahtu ei tasu alahinnata ja igaks juhuks tuleb sellesse planeerida piisav seisakuaeg.
- Tootja poolt uuele tarkvara versioonile lisatud infotekstid (Release Notes) tuleb hoolikalt läbi lugeda.
- Kõiki tuntud funktsioone ei pruugi uutes tarkvaraversioonides enam olla, samuti võib esineda nende töös vigu. Mõnikord muutuvad ka default -seadistused.
- Programmi ning eriti operatsioonisüsteemi kõigi funktsioonide töö tagamiseks tuleb uusi versioone enne kasutuselevõtmist hoolikalt testida.
- Uued programmid või operatsioonisüsteemid ei pruugi olla sama tõhusad nagu vanad, nt lisandunud funktsioonide tõttu või vajadusest suurema salvesti järele. See võib olla probleemiks, kui marsruuterit või kommutaatorit käitati juba enne tarkvara uuendamist töökoormuse piiril.

Mitmed tootjad pakuvad täiendamise planeerimiseks konfiguratsioonitööriistu. Need võimaldavad lähtuvalt kasutatavast seadmest planeerida konfiguratsiooni ja valida vajalikke riistvarakomponente, samuti liideseid ja salvesteid. Täiendite juurutamiseks tuleb läbida järgnevad etapid:

- Täiendite soetamine usaldusväärsest allikast. Üldjuhul tuleks täiendeid hankida ainult tootjatelt. Kui tootja pakub täiendite jaoks kontrollsummasid või allkirjastab täiendite paketid digitaalselt, tuleb kontrollsummasid või allkirju kontrollida (vt M 2.273 Turvalisust mõjutavate paikade ja värskenduste kiire paigaldamine ja M 4.177 Tarkvarapakettide tervikluse ja autentsuse tagamine).
- Täiendite tervikluse ja töö kontrollimine
- Seadme lahutamine produktiivvõrgust või kõikide liideste desaktiveerimine

- Võimalusel tuleb olemasolevast konfiguratsioonist ja operatsioonisüsteemist teha varukoopia
- Täiendite paigaldamine
- Testimine
- Seadme reaktiveerimine võrgus

Konfiguratsiooni muutmine

Konfiguratsiooni saab muuta niihästi vahetult seadme süsteemikonsoolis (online) kui ka eraldi haldusarvutis vastava konfiguratsiooniprogrammi või tekstiredaktori (offline) abil. Mõlemal meetodil on omad eelised ja puudused, kuid üldjuhul tuleks siiski eelistada offline -konfigureerimist. Online -konfigureerimine ei pruugi olla eriti mugav, samuti ei saa kasutada abitööriistu, nt ei ole alati võimalik lisada kommentaare. Seevastu toimub jällegi süntaksi operatiivne kontrollimine. Kui konfiguratsioonifailid luuakse offline -režiimis, saab tavaliselt kasutada mugavaid tööriistu ja lisada kommentaare. Antud protseduuri puuduseks on asjaolu, et sageli tuleb konfiguratsioonifailidesse sisestada paroole loetava teksti kujul. Kuna konfiguratsioonifailides sisalduvad paroolid on loetavad ja seda ka siis, kui need kantakse seadmetesse üle võrgu kaudu, välja arvatud juhul, kui kasutatakse krüpteeritud ühendust, tuleb need muuta kohe pärast konfiguratsioonifaili paigaldamist. Teiseks võimaluseks on määrata paroolid online ja lugeda seejärel konfiguratsiooniandmeid koos krüpteeritud paroolidega. Tagamaks buutimisel kõige värskema konfiguratsioonifaili lugemist salvestist, tuleb muudetud konfiguratsioon pärast seadmesse laadimist salvestada. Mõningate seadmete puhul saab tsentraliseeritud administreerimise jaoks vajalikke konfiguratsioonifaile hoida ka eraldi serverites ja sealt laadida. See võib toimuda nii käsitsi kui ka automaatselt, näiteks buutimisel. Niimoodi saab muudatusi jagada seadmetele automaatselt. Buutimise käigus ei ole laadimine siiski soovitatav ja seda kasutatakse harva, kuna võimalik on laiaulatuslik kahjustumine, vigade teke ja liiga suur võrgukoormus. Konfiguratsioonifailide varundamine ja haldamine peaks seevastu toimuma vastava tsentraalse serveri kaudu. Igal juhul peab administreerimisarvuti, millel Offline -konfigureerimist teostatakse või millel konfiguratsiooniandmeid hoitakse, olema kaitstud volitamata juurdepääsude eest.

Täiendavad kontrollküsimused:

- Kas kasutatavate operatsioonisüsteemide turvaaugud on teada?
- Kas kasutatakse vanu versioone?
- Millal viimati uuendati?
- Kuidas kogutakse infot kasutatavate süsteemide turvaaukude kohta?
- Kas enne konfiguratsiooni muutmist toimub andmete varundamine?

M 2.284 Marsruuterite ja kommutaatorite turvaline tööst kõrvaldamine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: administraator

Aktiivsetele võrgukomponentidele salvestatud konfiguratsiooni- või logifailid sisaldavad palju infot võrgu, infrastruktuuri, organisatsiooni ja isegi selles töötavate inimeste kohta. Kui seade antakse edasi organisatsioonivälistele (nt tootjale või teenindusele seadme väljavahetamiseks või siis ostjale), on võimalik seda infot ära kasutada. Näiteks saab konfiguratsiooniandmetest välja uurida järgnevat infot:

- kasutatud protokollid (eriti marsruutimisprotokollid), IP-aadressid ja alamvõrgud
- VLAN-konfiguratsioon
- pääsuloendid (ACL-d)
- paroolid ja SNMP Community Strings
- administraatori nimi ja kontaktandmed (bänner)

Kuna loetletud andmete puhul on tegemist tundliku infoga, tuleb jälgida, et enne rikkis või vananenud seadmete kasutuselt eemaldamist või väljavahetamist nendes asuvad failid kas kustutataks või muudetaks loetamatuks. Protseduurid sõltuvad suuresti seadme tootjast. Marsruuterite ja kommutaatorite turvapoliitikas tuleb antud otstarbeks määrata kindlad vastutusalad. Paljud seadmed toetavad funktsiooni „ Factory-Resets “. Käsuga või mõnele lülitile vajutamisega taastatakse komponendile tootjatehases määratud default seaded. Siinkohal tuleb siiski arvestada, et Reset ei pruugi ilmtingimata taastada kõikide seadistuste esialgset seisundit. Seega on hädavajalik seadmed üle kontrollida. Mõningatel seadmetel saab konfiguratsioonifaile jälle vastavate käskudega kas täielikult kustutada või asendada teiste failidega. Kui kasutatud seadmetel pole ühtegi mainitud funktsiooni, tuleb konfiguratsioon kas individuaalselt ära muuta või salvesti füüsiliselt hävitada.

Mõningatel seadmetel saab salvestatud logifaile kustutada või üle kirjutada „Factory-Reset“ abil. Seda esineb aga siiski harva. Sageli saab logifaili kustutada ka mõne spetsiaalse käsuga. Enne seadme kasutuselt eemaldamist tuleb seega jälgida, et sinna ei jääks alles ühtki logifaili. Kui kasutatud seadmetel pole ühtegi eelnevalt loetletud funktsiooni, tuleb salvesti vajadusel füüsiliselt hävitada. Sageli on marsruuteritele paigaldatud kirjad IP-aadresside, Host-nimedega või muu tehnilise infoga. Ka need kirjad tuleb enne seadme kõrvaldamist eemaldada.

Täiendavad kontrollküsimused:

- Kas marsruuterite ja kommutaatorite turvapoliitikas on arvestatud turvalise utiliseerimisega?
- Kas konfiguratsioonifailid ja logifailid muudetakse enne utiliseerimist loetamatuks või kustutatakse turvaliselt?

- Kas enne utiliseerimist eemaldatakse seadmetelt pealekirjutatud info?

M 2.292 z/ OS-süsteemide seire

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator

Võimalike vigade ja turvaprobleemide kiire tuvastamine eeldab z/OS-süsteemide töö jooksvat jälgimist. Seire rakendamiseks saab kasutada operatsioonisüsteemi erinevaid andmeallikaid. Vastavaid andmeid saab analüüsida nii käsitsi, Operating funktsiooni kasutades kui ka automaatselt, programmide abil.

Z/OS-süsteemide seire rakendamisel tuleks arvestada järgmiste soovitustega:

- MCS-konsool - MCS-konsool (Multiple Console Support) kuvab tähtsamaid süsteemiteateid (vigu, turvameetmete rikkumisi jms), mille peale on kasutajal võimalik kohe reageerida. Selleks, et teadetetulvast kõige olulisemat välja filtreerida, tuleb ilmtingimata kasutada MPF-funktsiooni (Message Processing Facility). Siinkohal oleks soovitav tähtsamad teated edasi suunata spetsiaalsesse konsooli, samal ajal kui operatsioonisüsteemi kommunikatsioon toimib edasi teistes konsoolides. Kriitiliste teadete esiletõstmiseks tuleks kaaluda erinevate värvilahenduste kasutamist.
- SMF-analüüs - Peaaegu kõik operatsioonisüsteemi tegevused logitakse SMF-i abil (System Management Facility). Turvaintsidentide korral tuleb vastavad laused kindlasti läbi analüüsida. Varasemate sündmuste analüüsimiseks peab SMF-andmete jaoks olema loodud ka vastav arhiveerimisprotseduur. Kuna SMF-andmeid kasutatakse ka z/OS-operatsioonisüsteemi arve koostamise ja jõudluse analüüsides, tuleks kaaluda vastava aruandlussüsteemi loomist.
- SYSLOG-analüüs - Operatsioonisüsteem kirjutab kõik olulised sündmused ka nn süsteemilogisse SYSLOG (System Log), mida on võimalik SDSF-i abil (System Display and Search Facility) kas JES2-süsteemis või Flasher -eid kasutades JES3 süsteemis (JES - Job Entry Subsystem) käsitsi analüüsida. Tuleks kaaluda, kas analüüsimise otstarbel on tarvis luua ja kasutusele võtta programme, mis otsiksid SYSLOG-st kriitilise sisuga teateid ja koostaksid vastavad raportid.

Automatiseerimine

Tuleks kaaluda, kas on tarvis rakendada automaatselt töötavaid programme, mis tuvastaksid vastava eelseadistusega SYSLOG-teateid ja käivitaksid süsteemis vastavad vastureaktsioonid. Vastav tootevalik on lai, kasutada on võimalik ka MPF-i koos Exit -programmeerimisega.

Rakenduste logid

Paljud rakendused kirjutavad ka oma logisid, näiteks teeb seda ka USS-alamsüsteem (Unix System Services). Neid logisid tuleb samuti analüüsida, kas esineb võimalikke turvaintsidente ning olulisemad teated tuleb süsteemihaldajatele teatavaks teha.

Tsentraliseeritud kontroll

Suurte installeeritud süsteemide puhul, mis on eri asukohtade vahel ära jaotatud, peaks olema loodud tsentraalne koht (Focal Point), kuhu edastatakse kõik oluline käitamisega seotud info. Kaaluda võiks ka programmide kasutamist, mis võimaldavad ülevaatlikku jälgimist, võibolla isegi graafilisel kujul.

Täiendavad kontrollküsimused:

- Kas on olemas tsentraalne koht (Focal Point), kuhu edastatakse erinevate süsteemide informatsioon?
- Kas SMF-lauseid analüüsitakse turvaintsidentide tuvastamise eesmärgil?
- Kas olulisemate teadete filtreerimiseks ja paremini esiletoomiseks kasutatakse teadetefiltreid?

M 2.298z Interneti domeeninimede haldus

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: IT-juht

Interneti domeeninimed (Domains) tuleb registreerida registraatoris (Registrar). Registraator saab määrata nimesid mitmes ülemdomeenides (nt „klassikalistes“ domeenides nagu .com , .org , .gov ja erinevates riigidomeenides nagu .de Saksamaa, .at Austria ja .ch Šveits). Domeenid registreeritakse teatud ajavahemikuks. Tähtaja möödumisel tuleb registreerimist tasu eest pikendada. Kui registreerimise pikendamine ununeb, võivad tagajärjed olla ebameeldivad (vt G 2.100 Interneti domeeninimede taotlemise või haldamise vead). Seetõttu tuleb tagada kõikide organisatsiooni poolt kasutatavate domeenide regulaarne ja õigeaegne registreerimise ja pikendamine. Selleks tuleks igas organisatsioonis määrata osakond, mis koordineerib domeeninimede haldamist erinevate registraatorite juures. Lisaks domeeninimede haldamisele ja registreerimise õigeaegsele pikendamisele tuleb Interneti domeeninimede haldamisel arvestada ka veel järgnevate punktidega:

- DNS nimeserver - Peamine nimeserver erinevates alamvõrkudes. Domeeninimede registreerimisel tuleb määrata vähemalt kaks DNS-nimeserverit (Primary Nameserver- it), mille ülesandeks on arvutinimede sidumine IP-aadressidega. Nimeserveri käitajaks on sageli internetiteenuse pakkuja, kuid käitajaks võib olla ka organisatsioon ise. Nimeserveri määramisel tuleks jälgida vähemalt seda, et Primary Nameserver -id asuksid erinevates Class-C võrkudes. Kui see pole nii, võivad võrgu- ja internetiühendust tagavale marsruuterile suunatud Denial of Service ründed halvata kogu domeeni, kuna sel juhul ei suudeta enam ühtki selle domeeni nime teisendada. Kui nimeteisenduse käideldavusele on esitatud kõrgendatud nõuded, peaksid Primary Nameserver -id ideaaljuhul asuma erinevates võrkudes ja olema seotud erinevate teenusepakkujatega.
- Domeeninimed - Firma- ja tootenimedega domeenid. Internetiajastu alguses piisas organisatsioonile üldjuhul ühest ainsast omanimelisest internetidomeenist. WWW ülemaailmse populaarsuse kasvuga levis ka praktika registreerida lisaks firmanime kandvale domeenile veel ka tuntud tootenimedega domeenid.
- Domeenide kahmamise ennetamine - Vältimaks teie firma tooteid või teenuseid kajastavate nimedega domeenide registreerimist kolmandate isikute poolt, kes võivad neil aadressidel hakata levitama pornograafilist või muul moel problemaatilist sisu, mida külastajad võivad hakata seostama teie organisatsiooniga, tuleks võimalusel lisaks enda firmanimele ja tuntud tootenimede õigele kirjaviisile registreerida ka nende erinevad variatsioonid, näiteks liitsõnade puhul sidekriipsudega ja ilma. Nimed tuleks registreerida erinevate „oluliste“ ülemdomeenide all (nt .de , .com , .org , . info). Lisaks tasuks kontrollida, kas poleks mõistlik registreerida ka toodete või firmanimede teatud valestikirjutatud variante (näiteks teatud „näpuvigasid“). Registreerimisest tulenev lisavaev on tühine võrreldes vaevaga, mis võib näiteks kaasneda teatud domeeni väljanõudmisel kohtu kaudu. Selliste „igaks juhuks“ registreeritud domeenide jaoks tuleks luua vähemalt teatud mini-

maalne veebileht, mis nimetab õige pakkumisega seotud domeeninime ja juhib külastaja edasi õigele lehele. Vajadusel võib nende domeenide veebiserveriks olla ka organisatsiooni peamine veebiserver, kasutades vastavat nimeteisendust.

- Registraatorid ja registreerimisvahemikud - Paljudel üladomeenidel (nt .com ja .org) on olemas eraldi registraatorid. Registraatorit saab alati vahetada, kuid tavaliselt kaasnevad sellega ka kulud.
- Säilitage ülevaade kehtivusaegade, hindade ja kontaktide kohta - Registreerimise õigeaegse pikendamise tagamiseks tuleb kindlasti kõikide registreeritud domeenide puhul säilitada ülevaade nende registreerimise kehtivusaegade, pikenduse hinna ja registreerimiskoha pangaandmete kohta.
- Lepingu koostamine Interneti teenusepakkujatega - Kui organisatsioon ei registreeri ega halda oma domeene ise, vaid laseb seda teha Interneti teenusepakkujal, tuleb lepingu koostamisel jälgida, et kontroll domeenide üle kuuluks kindlasti organisatsioonile endale. See võib muutuda oluliseks näiteks registraatorite vahetamisel või nimevaidluste lahendamisel. Olukordade jaoks, kus teenusepakkuja teeb domeeninimede haldamise osas vigu, tuleb koostada vastavad regulatsioonid, sest niisugused olukorrad võivad põhjustada tõsiseid materiaalseid kahjusid. Kui nimeservereid ei käitata organisatsioonis endas, vaid hoitakse teenusepakkuja juures, tuleb teeninduslepetes sõnastada ka nimeserveri käideldavusele seatavad nõuded ja maksimaalne aeg, mis võib kuluda organisatsiooni DNSis tehtavate muudatuste sisseviimiseks.

Täiendavad kontrollküsimused:

- Millised domeeninimed on registreeritud?
- Kas domeenide registreerimise kehtivusaegade, hindade ja kontaktide kohta on olemas ülevaade?
- Kus käitatakse organisatsiooni nimeservereid?

M 2.299 Turvalüüsi (tulemüüri) turvapoliitika koostamine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT-turvaosakond

Rakendamise eest vastutavad: IT-turvaosakond

Kuna turvalüüsidel on täita kandev roll võrgu turvalisuse tagamisel, on eriti oluline tagada nende turvaline ja nõuetekohane käitamine. Seda saab tagada ainult siis, kui seadmete käitamise nõuded on integreeritud olemasolevatesse turvatehnilistesse nõuetesse. Üldkehtivad turvatehnilised nõuded (eesmärgiks seatud turbeastme nõuded) tulenevad tervet organisatsiooni hõlmavatest turvasuunisest ning nende täpsustamiseks ja rakendamiseks tuleks antud kontekstis formuleerida eraldi spetsiaalsed turvalüüside turvasuunised. Sellega seoses tuleb kontrollida, kas lisaks tervet organisatsiooni hõlmavale turvapoliitikale on tarvis arvestada ka muude, hierarhias kõrgemalseisvate nõuetega nagu nt IT-turvapoliitika, paroolisuuniste või internetikasutuse nõuetega. Kõik turvalüüsidega soetamisega ja käitamisega seotud isikud peavad tundma turvapoliitikat ning oma töös sellest lähtuma. Nagu kõikide suuniste puhul, tuleb nende sisu ja rakendamist regulaarselt üldise auditi käigus kontrollida. Turvapoliitika peab esmalt täpsustama üldise vajaliku turbeastme ja sisaldama täpset infot turvalüüside käitamise kohta. Järgnevalt on loetletud mõned punktid, millega tuleks arvestada:

- Konfiguratsiooni üldstrateegia: kuna võrgu turvalisuse tagamisel on keskne roll just turvalüüsil, peab turvalüüs (muuhulgas ka selle üksikud komponendid) olema konfigureeritud võimalikult turvaliselt.
- Milliste juurdepääsude kaudu tohivad administraatorid ja auditeerijad süsteemidele ligi pääseda (nt ainult kohapealsest konsoolist, eraldi administreerimisvõrgu kaudu või krüpteeritud ühenduste kaudu)?
- Millised toimingud tuleb dokumenteerida? Millisel kujul luuakse dokumentatsioon ja kuidas seda hooldatakse?
- Kas teatud muudatuste puhul on kohustuslik järgida nelja silma printsiipi? Eriti soovitav on seda rakendada turvalüüsi turvalisust puudutavate seadete muutmise puhul.
- Millise skeemi järgi jagatakse administreerimisõigusi?
- Nõuete profiilist tulenevad ettekirjutused seadmete soetamisel
- Turvalüüsi üksikkomponentide installeerimise ja konfigureerimise nõuded
- Esmapaigaldus.
- Default -seadistuse kontrollimine võimalike turvariskide osas.
- Füüsilise juurdepääsukontrolli reguleerimine.
- Konsooli ja muude juurdepääsuliikide kasutamine ja konfigureerimine.
- Kasutajate ja töörollide haldamise reeglid, volituste struktuurid (autentimise ja volitamise toimimine ja meetodid, volitused installeerimiseks, täiendite laadimiseks, konfiguratsiooni muutmiseks jne). Võimalusel tuleks administreerimiseks välja töötada töörollide jaotamise kontseptsioon.
- Reeglid dokumentatsiooni koostamise ja haldamise kohta, dokumentatsiooni vorm: protseduurijuhised, kasutusjuhendid.
- Turvalise käitamise nõuded

- Administreerimise kaitse (näiteks juurdepääs ainult turvatud ühenduste kaudu).
- Krüpteerimise kasutamine (standardid, võtmete tugevus, kasutusvaldkonnad).
- Paroolikasutuse nõuded (paroolireeglid, paroolidega kaitstavad keskkonnad, paroolimuudatuste reeglid ja olukorrad, vajadusel paroolide deponeerimine).
- Käitamise ja hoolduse tööriistad, integreerimine olemasolevasse võrguhaldusesse.
- Volitused ja protseduurid tarkvara uuendamisel ja konfiguratsiooni muutmisel.
- Logimine
- Millised sündmused logitakse?
- Kuhu salvestatakse logifailid?
- Kuidas ja kui sageli toimub logide analüüsimine?
- Andmevarundus ja Recovery
- Sidumine üleorganisatsioonilise andmevarunduse kontseptsiooniga.
- Tegutsemine rikete ja vigade korral, Incident Handling
- Reeglid töötõrgetele ja tehnilistele vigadele reageerimiseks (kohalik tugi, kaughooldus).
- Reeglid turvaintsidentide jaoks.
- Valmisolek hädaolukorraks
- Sidumine üleorganisatsioonilise ootamatuste ennetamise kontseptsiooniga.
- Revisjon ja audit (vastutusalad, protseduurid, integreerimine kõikehõlmavasse revisjoni kontseptsiooni)

Turvapoliitika eest vastutab IT-turvaosakond, seega tuleb kõik turvapoliitika muudatused ja kõrvalekalded kooskõlastada IT-turvaosakonnaga. Turvapoliitika koostamisel on süsteemide turvalisuse tagamiseks soovitav esmalt välja töötada maksimaalselt palju erinevaid nõudeid ja ettekirjutusi. Seejärel saab hakata neid vastavusse viima tegelike oludega. Ideaaljuhul aitab niisugune lähenemine arvestada kõigi võimalike aspektidega. Iga väljatöötatud nõude puhul, mis teise tööetapi käigus kõrvale jäetakse või pehmendatakse, tuleb dokumenteerida selle kõrvalejätmise põhjus.

Täiendavad kontrollküsimused:

- Kas turvalüüside kasutamise kohta on koostatud vastav turvapoliitika?
- Millal turvapoliitikat viimati uuendati?
- Kas turvapoliitikas on sõnastatud ka turbeaste?
- Kas turvapoliitika kirjeldab turvalüüside sisseseadmise, käitamise ning tõrgete kõrvaldamise nõudeid?
- Kas turvapoliitikas on arvestatud komponentide erineva kasutusotstarbega?

M 2.300 Turvalüüsi turvaline kõrvaldamine või selle komponentide asendamine

Algatamise eest vastutavad: IT-juht, IT-turbespetsialist

Rakendamise eest vastutavad: administraator

Enne turvalüüsi komponentide tööst eemaldamist või väljavahetamist tuleb seadmetest kustutada kogu informatsioon, mis võib kajastada turvalisust. Eriti kehtib see juhtudel, kui komponendid satuvad pärast kasutusest kõrvaldamist kolmandate osapoolte kätte (nt müüakse edasi), juhtudel, kus seade vahetatakse garantiikorras välja või toimetatakse kas tootjafirma või teenusepakkuja parandustöökotta ning isegi neil juhtudel, kui seadmeid kasutatakse mujal organisatsiooni siseselt edasi või kui need saadetakse utiliseerimisele. Sõltuvalt komponentide kasutusalast võivad need endas sisaldada nt järgmist infot:

- Konfiguratsioonifailid, mille abil on võimalik välja lugeda infot organisatsiooni võrgustruktuuri kohta (nt IP-aadressid, marsruutimistabelid, SNMP-Community Strings, Access-Control-Lists jms).
- Paroolifailid.
- Logifailid, mis võivad sisaldada turbega seotud infot või isikuandmeid.
- Kasutajaandmed, nt Web-Cache - või E-Mail-Spool -kataloogide andmed.
- Ohtlikud failid (pahavara) „karantiini-kaustadest“.
- Sertifikaadid ja võtmed (nt SSL-prokside SSL-sertifikaadid või SSH pääsuks vajalikud võtmed).

Andmed tuleb kustutada ja tulemust kontrollida

Kuna loetletud andmete puhul on tegemist tundliku infoga, tuleb jälgida, et enne rikkis või vananenud seadmete kasutuselt eemaldamist või väljavahetamist neis asuvad failid kas kustutataks või muudetaks loetamatuks. Pärast andmete kustutamist tuleb kontrollida, kas vastav toiming õnnestus. Vajalikud protseduurid sõltuvad suuresti seadme liigist ja kasutusalast. Antud otstarbeks tuleb turvalüüsi turvapoliitikas sõnastada kindlad vastutusalad. Vastavad failid võivad sõltuvalt seadmest ja selle kasutusalast asuda mitmes erinevas kataloogis, nt ALGde puhul salvestatakse erinevad konfiguratsioonifailid tihti hoopis teise kohta kui Cache -failid ning Spool - või Quarantine -kataloogid. Seetõttu tuleks enne kasutuselt kõrvaldamist välja selgitada kõik turvalisusega seotud failide asukohad.

Kõvaketta kustutamine

„Tavaliste“ arvutite puhul, mida kasutatakse turvalüüsi funktsioonides, tuleks kõvakettad mõne sobiva rakenduse abil kustutada selliselt, et kõvakettal olnud andmeid ei oleks võimalik enam taastada. Selle tagamiseks võib kasutada nt arvuti käivitamist mõne välise buutimisvahendi abil ning kõvaketta juhuslike andmetega üle kirjutada. Siinkohal on soovitatav ülekirjutamist mitu korda korrata. Eraldiseisvate seadmete puhul sõltub protseduur suuresti sellest, kas seade sisaldab kõvaketast ning kas seadmesse on paigaldatud püsimälu või mitte. Paljud seadmed on varustatud funktsiooniga „ Factory-Reset “, mille abil on võimalik kõik konfiguratsiooni puudutavad seadistused taastada väärtustele, mis on seadmel tehasest väljudes. Pärast tehaseseadete taastamisfunktsiooni kasutamist tuleb siiski

üle kontrollida, kas andmed on tõepoolest kustutatud ehk tarneseisundisse tagasi muudetud või on teatud andmed või failid siiski alles jäänud.

Salvesti kasutuskõlbmatuks muutmine

Seadmete puhul, kuhu on salvestatud eriti tundlikku turvalist puudutavat infot, mille puhul ei ole piisavalt kindel, kas andmed said turvaliselt kustutatud, tuleb mälukiibid või kõvakettad muuta vajadusel füüsiliselt kasutuskõlbmatuks.

Arvestamine varukoopiate andmekandjatega

Lisaks seadmesse salvestatud andmetele tuleb kontrollida, et tundlikku informatsiooni ei leiduks ka varukoopiate andmekandjates. Kui pärast seadme kasutuselt kõrvaldamist ei ole tarvis varukoopiate andmekandjaid alles hoida, (säilitamisnõuded võivad tuleneda arhiveerimisvajadusest või seadustest), tuleks kustutada ka varukoopiate andmekandjad.

Tähistused tuleb eemaldada

Sageli on turvalüüside komponentidele paigaldatud tähistused, mis sisaldavad IP-aadresse, Host-nimesid või muud tehnilist infot. Ka need tähistused tuleb enne seadme kõrvaldamist eemaldada.

Täiendavad kontrollküsimused:

- Kas turvalüüside turvapoliitikas on arvestatud turvalise utiliseerimisega?
- Kas konfiguratsioonifailid ja logifailid muudetakse enne utiliseerimist loetamatuks või kustutatakse turvaliselt?
- Kas enne utiliseerimist eemaldatakse seadmetelt pealekirjutatud info?

M 2.301z Turvalüüsiteenuse väljasttellimine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: IT-juht, IT-turvaosakond

Turvalüüside ülesehitamine ja käitamine nõuab küllaltki märkimisväärset finants- ja personaliressurssi. Kohtvõrkude ühendamisel ebausaldusväärsete võrkudega (eriti Internetiga) ei ole turvalüüsidest võimalik mitte mingil juhul loobuda. Seetõttu kaalutakse sageli võimalust jätta turvalüüsi käitamine mõne välise teenusepakkuja hooleks. Siinkohal on mõeldavad erinevad variandid:

- Käitamine kohapeal, administreerijad väljastpoolt organisatsiooni. Turvalüüsi käitatakse ja administreeritakse organisatsiooni enda ruumides. Tööde teostamiseks palgatakse väljastpoolt organisatsiooni vastav turvalüüsi administraator. Antud variandi puhul ei teki tihti isegi mitte kulude kokkuhoidu. Sarnaselt kõigi teiste variantidega on puuduseks asjaolu, et organisatsioonivälistel töötajatel ei ole organisatsioonist piisavat ülevaadet, mille tõttu on väga raske läbi viia tõhusat kontrolli.
- Remote Management. Turvalüüsi käitatakse organisatsiooni enda ruumides, kuid administreerimine toimub kaugpöörduse abil. Antud variandi puhul tuleb vältimatu abinõuna rakendada tugevat autentimist ja ühenduste krüpteerimist. Teenusepakkujatel tohib olla juurdepääs ainult turvalüüsile, mitte LA-Nis olevatele muudele andmetele ega kataloogidele. Võimalike väärkasutuste ennetamiseks tuleks siinkohal rakendada täiendavaid organisatsioonilisi abinõusid vastavalt B 4.4 Virtuaalne privaatvõrk (VPN) kirjeldatule. Nende alla kuuluvad näiteks:
- Juurdepääsu blokeerimine teatud ajaks ebaõnnestunud sisenemiskatsete korral
- Kaughoolduse juurdepääsu blokeerimine tavakasutuse ajaks ning hoolduseks vajaliku pääsu konkreetne lubamine täpselt määratletud ajavahemikuks.
- Organisatsioonivälise administraatorite õiguste piiramine selliselt, et turvasuuniseid ei oleks võimalik nõrgemaks seadistada.
- Sund- logout ühenduse katkemisel. Kaughooldust teostava koha ja PC-Gateway vahelise ühenduse katkemisel tuleb juurdepääs süsteemile sundlogout i abil lõpetada.
- Hosting. Antud lahenduse korral seatakse turvalüüs üles teenusepakkuja ruumidesse ja selle hooldamine toimub samuti teenusepakkuja juures. Antud variandi puhul peab organisatsioonisisese kohtvõrgu ja turvalüüsi vahel olema püsiv turvatud ühendus. Siinkohal on tarvis tagada nii ühenduse kui ka turvalüüsi-süsteemi kõrge käideldavus, kuna nende väljalangemisel puuduvad võimalused ühenduste loomiseks väljastpoolt.

Üldjuhul tuleks rakendada ka täiendavaid komponente, mille ülesanneteks on turvatud ja välise võrgu vahelise side võimaldamine. Siia alla kuuluvad näiteks infoserverid, mis peavad tagama info kättesaadavuse sisemistele ja välimistele kasutajatele, meiliserverid ning DNS-serverid. Reeglina paigaldatakse need turvalüüsi mõnda demilitariseeritud tsooni (vt M 2.77 Serverite integreerimine tulemüüri). Antud variandi puhul tuleb neid seega käitada mõne organisatsioonivälise

teenusepakkuja juures. See omakorda võib vajaminevaid kulutusi olulisel määral suurendada. Nii Remote Management kui ka Hosting lahenduse kasutamisel peab organisatsiooni ja teenusepakkuja vahel olema sisse seatud varuliin, et põhiühenduse rikke korral oleks jätkuvalt tagatud turvalüüsi administreerimine ja interneti-ühenduse kasutamine. Varuliini puhul peab olema tagatud, et sellele ühendusele kehtiks vähemalt sama kõrge turbeaste nagu põhiühendusele.

Erinevaid teenusepakkujaid omavahel võrreldes tuleks välja selgitada:

- Kas teenusepakkujal on ette näidata piisavad teadmised tehnika ja turbe vallas ning kuidas teenusepakkuja end vastavate teemadega kursis hoiab?
- Kas ja kui pika aja jooksul käitatakse turvalüüsisüsteemi ilma järelvalveta?
- Kuidas toimub personalijuhtimine, kuna reeglina osutatakse teenuseid mitmele kliendile korraga?

Ka neil juhtudel, kui turvalüüsi eest hoolitsemine jäetakse mõne teenusepakkuja kanda, tuleb ikkagi koostada organisatsioonisisene tulemüüri turvapoliitika, mis peab olema kooskõlas organisatsioonis kehtestatud turbeesmärkidega (vt M 2.71 Turvalüüsi (tulemüüri) turvapoliitika). Turvalüüsi teenuse väljasttellimisel on oluline, et sõlmitavates teeniduslepetes oleks kirjalikult fikseeritud:

- Teenusepakkuja poolt garanteeritav reaktsiooniaeg rikete või rünnete korral.
- Teenusepakkuja poolt garanteeritav käideldavus (jõudlus, maksimaalne tõrkesagedus).
- Mida tohivad ja mida peavad kajastama logid.
- Teenusepakkuja kohustuslikud turvameetmed (vt B 3.301 Turvalüüs (tulemüür)).

Turvalisuse seisukohast kriitiliste komponentide nagu nt turvalüüside väljasttellimisel tuleb kindlasti kõigil juhtudel järgida B 1.11 Väljasttellimine (Outsourcing) . Ideaaljuhul peaks teenusepakkujal olema juurutatud täielik, nt IT-etalonturbel baseeruv infoturbe haldussüsteem. Turvalüüsi väljasttellimise puhul on soovitatav vähemalt kontrollida, kas teenusepakkuja turvahaldus vastab moodulis B 1.11 Väljasttellimine (Outsourcing) kirjeldatud nõuetele.

Täiendavad kontrollküsimused:

- Kas turvalüüsi väljasttellimise otsus on IT-turvaosakonnaga kooskõlastatud?
- Kas protsessi käigus järgiti moodulit B 1.11 Väljasttellimine (Outsourcing) ?

M 2.302z Turvalüüside kõrge käideldavuse tagamine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator

Kaitstava võrgu ja välise võrgu ainukese ühenduskoha peaks alati moodustama turvalüüs. Antud nõude puhul tekib muidugi potentsiaalne oht, et turvalüüsist võib ühelt poolt saada pudelikael ning teiselt poolt jällegi süsteemi lüli, mille avarii halvab kogu organisatsiooni võrguside. Eelnevast tulenevalt kehtestatakse turvalüüside käideldavusele tihti väga kõrged nõuded. Seetõttu peavad turvalüüsi tähtsamad komponendid olema koostatud liiasusega. Ennekõike puudutab see nõue turvalüüsi neid komponente, mida läbivad infopäringud ja infosaadetised. Nimetatud kategooriate alla kuuluvad reeglina paketifiltrid, Application-Level-Gateway -d ehk rakenduslüüsid ning sõltuvalt olukorrast ka VPN-komponendid. Muude komponentide (nt viiruseskannerite või Intrusion-Detection- süsteemide) olulisust kaitstava võrgu turvalisuse tagamisel tuleb hinnata iga konkreetse juhtumi korral eraldi.

Turvalüüsi komponentide käideldavuse tõstmiseks on olemas mitmeid erinevaid mooduseid:

- Cold-Standby: Cold-Standby ehk külmad varuseadmed tähendab, et lisaks töötavale süsteemile hoitakse valmis sarnast varusüsteemi, mis ei ole sisse lülitatud. Süsteemi avarii korral on võimalik käsitsi käivitada varusüsteem ja integreerida see turvalüüsi alla.

Cold-Standby varusüsteemi eelised	Cold-Standby varusüsteemi puudused
- Turvalüüsi uuesti paigaldamisega, täpsemalt turvalüüsi uuesti ülesehitamisega seotud vaev on suhteliselt väike. - Turvalüüs ei ole liiga keeruline ning seetõttu on väärkonfiguratsioonide oht väike.	- Lisaks töösolevale süsteemile tuleb varuna hoida ka teist süsteemi, mis tähendab, et ka teise süsteemi konfiguratsiooni ja täiendeid tuleb jooksvalt uuendada. - Cold-Standby -süsteem ei suuda iseseisvalt tuvastada võimalikke rikkeid, mistõttu tuleb see käivitada käsitsi. Vastutus töösolevat süsteemi pidevalt jälgida ja vajadusel ka sekkuda jääb administraatorite kanda. - Sõltuvalt kasutatavast tootest võib turvalüüsi üksikkomponendi käivitamine nõuda administraatori kohalolu, sest teatud süsteemid lülituvad töörežiimi ainult pärast klaviatuuri abil toimunud kasutajapoolset sekkumist. Komponentide sisselülitamine netist juhitava pistikupesa abil on sellisel juhul välistatud.

Tabel 1: Cold-Standby varusüsteemi eelised ja puudused

- Hot-Standby: Hot-Standby ehk kuumade varuseadmete lahenduse puhul hoitakse lisaks põhisüsteemile samuti käepärast varusüsteem (enamasti täpselt sama konfiguratsiooniga nagu töösolev süsteem). Varusüsteem töötab paralleelselt koos põhisüsteemiga ning üks komponent tegeleb teiste komponentide seirega. Töösoleva süsteemi rikke korral on varusüsteem võimeline vastavad funktsioonid vahetult üle võtma. See võib toimuda nii automaatselt kui ka kasutajapoolse sekkumise tagajärjel. Kuna ümberlülitamine võib endaga kaasa tuua täiendavaid komplikatsioone, aitab kasutaja sekkumist vajav süsteem välistada Hot-Standby -süsteemile ümberlülitamist olukordades, kus on tegemist ekstreemselt lühikeste avariiaegadega. Võimalikult lühikeste seisukuaegade tagamiseks on Hot-Standby -režiimi puhul tarvis turvalüüsi tähtsamaid komponente kontrollida võimalikult lühikeste intervallide tagant

Hot-Standby varusüsteemi eelised	Hot-Standby varusüsteemi puudused
- Administraatoril puudub igasugune vajadus konsooli abil protsessi sekkuda. - Kuna varukomponendid võtavad avariilise süsteemi funktsioonid automaatselt üle, ei teki seisakuaegu peaaegu üldse või tekivad ainult lühikesed seisakuajad.	- Võrreldes Cold-Standby varusüsteemiga muutub turvalüüs vägagi keeruliseks, sest kõik töösolevad komponendid tuleb varustada täiendavate seirekomponentidega, mis kontrollivad pidevalt, kas süsteem töötab korrektselt. - Turvalüüsi iga olulisema komponendi jaoks tuleb muretseda eraldi seirekomponent, mida tuleb ka hallata.

Tabel 2: Hot-Standby varusüsteemi eelised ja puudused

- Paralleelkasutus: Paralleelkasutuse puhul töötavad kasutusrežiimis pidevalt kaks või rohkem turvalüüsi üksteise kõrval. Paralleelkasutus ei soodusta mitte ainult koormuse paremat jaotumist ja jõudluse kasvu, vaid vähendab ka avariidega seotud probleeme. Sõltuvalt valitud koormusjaotuse meetodist võib ühe süsteemi rikke korral teine süsteem selle ülesanded üle võtta. Ülevõtmisest tekib küll lühiajaline jõudluse langus, kuid funktsioon ise säilib täies mahus. Siinkohal tuleb muidugi jälgida, et kõiki süsteeme hoitaks järjekindlalt võrdsel tasemel. Turvalüüside puhul tuleb võrdse taseme all eelkõige silmas pidada korrektset aja sünkroniseerimist ja kõikide peamiste reeglite järjepidevat rakendamist. Samuti peab olema tagatud, et sisenevaid ja väljuvaid päringuid töötleks alati üks ja sama komponent, sest vastasel korral võivad ühendused katkeda. Eriti puudutab see Application-Level-Gateway -sid ja Stateful-Inspection- funktsiooniga paketifiltreid.

Paralleelkasutuse puhul tuleb eristada kaht varianti:

- Staatiline paralleelkasutus - Antud variandi puhul ei teki muutusi turvalüüside komponentide konfiguratsioonis (eelkõige marsruutimisinfos). Staatilise paralleelkasutuse näitena võiks tuua lahenduse, kus turvalüüsi paralleelsed komponendid täidavad erinevaid ülesandeid, seega nt HTTP toimib ühe sideharu ja SMTP teise paralleelse sideharu abil. Selline konfiguratsioon tõstab küll terve süsteemi jõudlust, kuid tekitab probleeme üksikute komponentide avarii korral, sest komponendid on erineval moel konfigureeritud ning neid ei ole võimalik niisama lihtsalt paralleelsete komponentidega asendada. See on ka põhjus, miks niisugusest turvalüüside struktuurist ja konfiguratsioonist tuleks reeglina loobuda.
- Dünaamiline paralleelkasutus/ Loadbalancing - Antud töörežiimi puhul mugandatakse turvalüüsi komponentide konfiguratsiooni ja jõudlust vastavalt kasutusest tulenevatele nõuetele. Näitena võib siinkohal välja tuua Loadbalancing funktsiooni, mille puhul toimub andmevoogude marsruutimine vastavalt sides osalevate komponentide koormatuse astmele. Loadbalancing funktsiooni puhul tuleb ilmtingimata jälgida, et töösse kaasatud komponentide automaatselt läbiviidav konfiguratsiooni muutmine ei tooks endaga kaasa muutusi kogu turvalüüsi jaoks kehtestatud turbereeglistikus. Loadbalancing võib moodustada osa High-Availability -lahendusest (HA-lahendusest). HA-lahenduse puhul on turvalüüsi komponendid varustatud seiresüsteemiga, mis jälgib nende käideldavust ja suunab rikke korral funktsioonid edasi varusüsteemile, et vastavat riket kompenseerida. Antud näite kontekstis tõstab eelnevalt lühidalt kirjeldatud Loadbalancing funktsioon vaid süsteemi jõudlust ning selle olemasolu ei tähenda, et tegu on kõrge käideldavusega süsteemiga. Kõrge käideldavuse jaoks on täiendavalt tarvis tagada, et süsteemi avarii korral oleksid olemas asendussüsteemid, mis suudaksid avariiga automaatselt, ilma administraatori sekkumiseta toime tulla. Sama tähtis nagu HA-komponentide pidev seire on siinkohal ka veel automaatne Fail-Over.

HA-lahenduse eeliseid ja puudusi tuleks võrrelda Hot-Standby -süsteemi eeliste ja puudustega. Hot-Standby -süsteemiga võrreldes on täiendavaks eeliseks siiski asjaolu, et kõiki turvalüüsi komponente rakendataks ka reaalselt mille tagajärjel toimub koormuse jaotumine, mis aitab omakorda tagada turvalüüsi käideldavust.

HA-süsteemidele esitatavad nõuded:

- Ka neil juhtudel, kui Fail-Over on toimunud automaatselt, peab turvalüüs jätkuvalt vastama turbedirektiivi nõuetele („Fail safe“ või „Fail secure“).
- HA-teostus ei tohi takistada turvalüüsi, täpsemalt selle turvafunktsioonide tööd.
- HA-lahendus peaks endas hõlmama vähemalt paketifiltrit ja Application-Level-Gateway -d, sest komponentide avarii korral kommunikatsioon reeglina enam ei toimi. Sama kehtib ka VPN-komponentidele.
- Välise võrguga ühenduse saamiseks peab eksisteerima kaks teineteisest sõltumatut ühendusvõimalust, nt kaks Interneti juurdepääsu, kumbki erinevalt teenusepakkujalt.
- Sisemised ja välimised marsruuterid peavad olema liiasusega, kasutades nt protokolle nagu „Virtual Router Redundancy Protocol“ (VRRP) või seadmete tootjafirma loodud „Hot Standby Routing Protocol“ (HSRP).
- Funktsioonide seireks tuleb kasutada paljusid erinevaid parameetreid, mitte lähtuda ühest ainsast parameetrist (nt lihtne käideldavuse testimine („ping“)

ei ole juurdepääsu kontrolliks piisav). Kui „ ping “ funktsiooni abil kontrollides on selgunud, et juurdepääs komponendile on olemas, võib näiteks edasi kontrollida, kas konfigureeritud teenused töötavad nii, nagu on ette nähtud.

- Kasutuselevõtu raames või kasutuse käigus tehtud väärkonfiguratsioonid ei pruugi olla kohe äratuntavad, sest funktsioonid võetakse osaliselt paralleelselt installeeritud komponentide poolt üle. Näiteks ei pruugi sõltuvalt olukorrast kohe silma torgata, et ALG aktiivsisu filtreerimisfunktsioon on välja lülitatud ja korrektselt konfigureeritud süsteem töötleb siiski vastavaid päringuid. Seetõttu on HA-lahenduse puhul oluline, et regulaarselt kontrollitaks logifaile ja hoiatusi kajastavaid teateid.

Paketifiltrite puhul on HA-lahenduse loomine enamasti lihtne. Eriti lihtsaks kujuneb HA-lahendus neil juhtudel, kus kõrgkäideldavust on tarvis tagada ainult üheastmelises struktuuris, mis koosneb ühest paketifiltrist. Paljud turustatavad tooted pakuvad selleks lihtsat lahendust, mille keerukus seisneb peamiselt selles, et vastav HA-funktsioon tuleb haldusliidesest sisse lülitada.

Palju keerulisemaks muutub HA-lahenduse loomine mitmeastmeliste (nt paketifiltritest ja Application-Level-Gateway -dest koosnevate) turvalüüside korral. Selliste lahenduste puhul tuleb tagada, et kõik komponendid oleksid kõrgkäideldavad, mis on omakorda seotud märgatava lisakuluga. Reeglina tuleb niisuguste lahenduste puhul lisaks seirefunktsioonidele rakendada veel ka dünaamilisi marsruutimisprotokolle (nt „Open Shortest Path First“, OSPF), mis suudaksid võrguliiklust vajadusel sobival moel suunata.

Dünaamilised marsruutimisprotokollid pole turvalisuse seisukohast vaadates mitte just päris probleemivabad (vt G 5.51 Marsruutimisprotokollide väärkasutus ja M 5.112 Marsruutimisprotokollide turvaaspektide arvestamine). Kui HA-lahenduse loomiseks on tarvis rakendada dünaamilisi marsruutimisprotokolle, tuleks täiendava turvaanalüüsi raames kontrollida, kas nende abil on võimalik saavutada vajalikku turbeastet. Mitmeastmelise turvalüüsi P-A-P-ketis peab teatud komponent täitma seirefunktsiooni. Vastav komponent otsustab, kas PAP-haru on võimeline oma funktsiooni täitma või mitte. Seireülesandeks on kõige parem kasutada iseseisvat seirekomponenti, mis ei täida mitte ühtegi muud ülesannet peale vajaliku funktsiooni jälgimise. Juhul kui iseseisva seirekomponendi integreerimine ei ole võimalik, peaks vastavat ülesannet täitma Application-Level-Gateway. Muuhulgas on niisuguse valiku eeliseks asjaolu, et paljud turvalüüsi funktsioonid on juurutatud ALG alla, st seiretarkvara on suuteline neid kontrollima juba kohapeal. Teisalt on ALG tihti integreeritud turvalüüsi kesksesse kohta, pakkudes otsest juurdepääsu ka turvalüüsi teistele komponentidele. Probleeme võib tekitada tõsiasi, et ALGd püüavad tihti võõra tarkvara paigaldamist takistada, mille eesmärgiks on vältida süsteemi kahjustamist. Tegelikult polegi kasutatava seiretarkvara vigu alati võimalik välistada, nagu pole võimalik välistada ka seda, et tarkvara võib ALG poolt tagatavat turvet märgatavalt vähendada.

Täiendav turvaanalüüs

Kõrgkäideldavust pakkuvad lahendused lähtuvad alati spetsiaalsetest nõuetest ning täiesti mõeldav on kombineerida omavahel eelpool kirjeldatud variante. Nendel juhtudel, kus turvalüüsi käideldavusele esitatavad nõuded annavad alust oletada, et tarvis läheb kõrgkäideldavust tagavat lahendust, viiakse enamasti läbi täiendav turvaanalüüs.

Täiendavad kontrollküsimused:

- Kas on tarvis kasutada HA-lahendust? Kui jah, siis millist liiki?

- Kuidas tagatakse, et automaatne Fail-Over ei too endaga kaasa turbeastme langemist?

M 2.303 Nutitelefonide, tahvel- ja pihuarvutite kasutamise strateegia määratlemine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT-turvaosakond
Rakendamise eest vastutavad: IT-turvaosakond

Enne pihuarvutite kasutuselevõttu tuleks organisatsioonil kindlaks määrata pihuarvutite kasutamise üldine strateegia. Eriti oluline on leida vastused järgnevatele küsimustele:

- Millisel otstarbel hakatakse pihuarvuteid kasutama?
- Kas tööandja varustab töötajad pihuarvutitega?
- Kas organisatsioon lubab kasutada isiklikke pihuarvutiteid või toetab seda ka ametlikult?

Edasiste otsuste jaoks on esmatähtis välja selgitada, mis otstarbel hakatakse pihuarvuteid kasutama, sest antud asjaolu mõjutab olulisel määral seda, milliseid seadmeid on tarvis soetada. Samuti on tarvis sellega arvestada pihuarvuteid käsitlevate turvasuuniste ja -reeglite sõnastamisel.

Andmete liigitamine klassidesse

Iga kasutaja ja iga institutsioon peaks enda jaoks läbi mõtlema, milliseid andmeid tohiks pihuarvutitesse salvestada ning milline võib olla vastavate andmete kaitsevajadus. Ettevõtetes ja ametiasutustes tuleks see kindlaks määrata mitte ainult pihuarvutite lõikes, vaid kõikide andmete osas. Näiteks tekivad erinevates kasutusvaldkondades ja tööprotsesside käigus erinevat liiki andmed, millele kehtivad kas kõrgendatud turbeaste või spetsiaalsed piirangud, nt isikuandmed, finantsandmed, konfidentsiaalsed või autoriõigusega kaitstud andmed. Seetõttu peaks iga institutsioon oma kõikvõimalikud andmeliigid kategoriseerima, lähtudes andmetele kehtivast turbeastmest ja andmetega ümberkäimisele kehtestatud piirangutest (vt M 2.217 Teabe, rakenduste ja süsteemide hoolikas liigitamine ja käitlus). Võimaldamaks töötajatel andmete liigitusega mõistlikult ümber käia, on soovitatav liigituste kohta koostada ülevaatlikud tabelid koos näidetega, kus on selgitatud, millist liiki andmeid tohib erinevatele IT-süsteemidele või rakenduste alla salvestada, kus tohib erinevaid andmeid töödelda ning kellele on lubatud erinevaid andmeid edasi saata.

Isiklike pihuarvutite kasutamine

Kui töötajad ei ole tööandja poolt vastavate töövahenditega varustatud, võib juhtuda, et tööülesannete täitmiseks hakatakse kasutama ka isiklikke pihuarvuteid, kuna töötajad leiavad, et see on tööks vajalik. IT-turvaosakond või IT eest vastutavad töötajad peaksid siiski kõikidel juhtudel hoolitsema selle eest, et isiklike vahendite kasutamine ei leiaks aset kontrollimatult, vaid selgete reeglite alusel. Juhtudel, kus pihuarvuteid soovitakse kasutada ainult päevaplaanide ja aadresside haldamise või meiliside otstarbel, võib isiklike pihuarvutite kasutamist enamasti lubada, eeldusel, et puuduvad igasugused muud põhjused, mis räägiksid selle vastu.

Kõrge turbeastme korral tuleks isiklike pihuarvutite kasutamine võimalusel keelata

Neil otstarvetel, kus pihuarvutite kasutamisega tekib seadmetele kõrge kaitsevajadus, on isiklike pihuarvutite kasutuse lubamine väga küsitav. Põhjuseks on asjaolu, et isiklikus kasutuses olevate seadmete puhul ei toimu enamasti ei tsentraliseeritud konfigureerimist ega ka haldust ning seetõttu on nende seadmete puhul praktiliselt võimatu tagada vastuvõetavat turbeastet. Sellistel juhtudel on tungivalt soovitatav mitte lubada isiklike pihuarvutite kasutamist. Otsuse langetamisel tuleks arvestada tõsiasjaga, et isiklike pihuarvutite kasutuse lubamine võib mõjutada ka organisatsiooni tulevast IT-strateegiat. Langetades otsuse, et tööülesannete täitmiseks on isiklike pihuarvutite kasutamine keelatud, tuleb silmas pidada, et vastavaid keeldusid on tarvis ka kontrollida ning et keelu tagajärjed võiad olla ka hoopis ebaefektiivsed. Vastav otsus tuleks koos otsuseni viinud põhjendustega dokumenteerida ja sellest töötajatele sobilikul moel teada anda.

Näide:

Ettevõte ei varusta oma töötajaid pihuarvutitega, kuid nõustab töötajaid siiski isiklike pihuarvutite ostmisel ja nende ühendamisel töökohaarvutiga. Pärast seda, kui tööandja viis arvutid operatsioonisüsteemilt Windows 7 üle operatsioonisüsteemile Windows 8, selgus, et Windows 8 all ei olnud olemasolevate pihuarvutite jaoks sobivaid draivereid. Töötajate kaebustelaviini alla sattudes oli ettevõttel valida, kas varustada töötajad uute pihuarvutitega või minna tagasi Windows 7 baasil töötavate töökohaarvutite kasutamisele. Langetades otsuse, et tööülesannete täitmiseks on isiklike pihuarvutite kasutamine keelatud, tuleb silmas pidada, et vastavaid keeldusid tuleb ka kontrollida ning et keeldudest ei pruugita kinni pidada. Vastav otsus tuleks koos otsuseni viinud põhjendustega dokumenteerida ja töötajatele sobilikul moel teatavaks teha.

Kontrollküsimused:

- Kas pihuarvutite kasutamise kohta on olemas üldine strateegia?
- Kas pihuarvutite puhul on kindlaks määratud, milliseid andmeid tohib neisse salvestada?
- Isiklike pihuarvutite kasutamine: kas isiklike pihuarvutite kasutamine on asutuses selgelt reguleeritud?
- Kas asutuses hoolitsetakse selle eest, et isiklike pihuarvutite kasutamist jälgitakse ja kas rikkumisi karistatakse?

M 2.304 Nutitelefonide, tahvel- ja pihuarvutite turvapoliitika ja kasutamise reeglid

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: IT-juht, IT-turvaosakond

Pärast seda kui asutus on otsustanud pihuarvutid kasutusele võtta, tuleb nende kasutamine sisse töötada üldisesse turbestrateegiasse. Pihuarvutite väärkasutuse ärahoidmiseks on olemas palju erinevaid võimalusi. Selleks, et vastavaid võimalusi ka aktiivselt rakendataks, tuleks koostada asjakohased turvasuunised, kus oleks välja toodud kõik kohustuslikud turvamehhanismid. Iga asutus peaks ennast kurssi viima pihuarvutite kasutamisega seotud võimaluste ja ohtudega. Selle käigus tuleks lähtuda kahest turbeaspektist:

- Pihuarvutitesse salvestatud andmete turvalisuse tagamine
- Pihuarvutite kasutamise mõjud teiste asutusesiseste IT-süsteemide turvalisusele.

Lähtuvalt pihuarvutite turvasuunistest tuleks töötajatele koostada ka lühike ja ülevaatlik infoleht pihuarvutite turvalise kasutamise kohta.

Väärkasutuse ärahoidmine

Pihuarvuti kerge kaal ja väikesed mõõtmed, mis võimaldavad seda kergesti transportida ja teiste silme alt ära panna, ei ole eeliseks mitte ainult kasutajale vaid ka varastele. Seetõttu tuleks pihuarvuteid hoida alati turvalises kohas. Töölähteuste ajal ei tohi neid jätta järelvalveta. Eriti oluline on, et neid ei unustataks kuhugi sõidukitesse. Peaaegu kõiki pihuarvutite ja märkmike variante on võimalik kaitsta volitamata juurdepääsu eest kas PIN-koodide või paroolide abil. Kahjuks pole siiski kõik tootjate poolt pakutavad turvamehhanismid nii turvalised, nagu need võiksid olla. Seetõttu peaksid pihuarvutite kasutajad ennast nt Interneti abil informeerima, kui usaldusväärsed on tegelikult vastava seadme olemasolevad turvamehhanismid.

Senikaua kuni tõhusamaid turberakendusi pole veel installeeritud, tuleks igal juhul kasutada olemasolevaid turvamehhanisme (vt M 4.228 Pihuarvutite turvamehhanismide rakendamine). Kõik kasutajad peaksid teadma, kui tõhusad on nende poolt kasutatavad turvamehhanismid, ning eriti peaksid nad teadma nende võimaluste piire. Oluline on ka paroolide ja PIN-koodide hoolikas valik, st need peaksid olema piisavalt pikad, et neist ei oleks võimalik liiga kergelt jagu saada. Mitte mingil juhul ei tohi hoida pihuarvutit ja selle parooli ühes ja samas kohas.

Töötajate teavitamine võimalikest ohtudest

Kõiki pihuarvutite kasutajaid tuleks teavitada mitte ainult pihuarvutite eelistest, vaid ka nende kasutamisega seotud potentsiaalsetest ohtudest ja probleemidest, samuti nende puhul rakendatavate turvameetmete tõhususe piiridest. Kuna ka pihuarvutite operatsioonisüsteemide (nt Palm OS, Windows CE, Windows Mobile, Symbian OS) puhul tuleb ikka ja jälle ilmsiks uusi turvaauke, peaks IT-turvaosakond hoidma ennast kursis kõige uuemate teadaolevate ohtudega. Sõltuvalt vajadusest tuleb töötajaid informeerida võib-olla koguni regulaarselt tuvastatud kitsaskohtadest ja muuta neid ohtude suhtes tähelepanelikumaks.

Pihuarvutite kasutusreeglid

Üldreeglid

Pihuarvutis on andmed reeglina palju kehvemini kaitstud kui mõnes organisatsioonisiseses IT-süsteemis. Sõltumata sellest, kas töö juures kasutatakse isiklikke või tööandja soetatud pihuarvuteid, peab tööandja võtma töötaja käest kirjaliku kinnituse järgmiste kohustuste kohta:

- loetelu andmeliikidest, mille salvestamine pihuarvutisse on keelatud,
- kinnitus, et andmeid ei tohi sisestada ega lugeda suvalises kohas, kuna sõltuvalt olukorrast võib tekkida nende volitamata lugemise oht,
- kuidas, millal ja kes varundab pihuarvutite andmed,
- loetelu pihuarvutite kasutamiseks vajalikest tehnilistest tingimustest. Siia alla kuulub eelkõige rakendatavate turvamehhanismide kindlaksmääramine, turbe jaoks vajaliku riistvara ja tarkvara valik ning nende installeerimine, samuti ettekirjutused käsitletavate IT-süsteemide turvalise konfigureerimise kohta.

Pihuarvutit ei tohi kuhugi järelvalveta jätta. Kui pihuarvutit on tarvis jätta nt sõidukisse, tuleks seda teha selliselt, et seade ei jääks sõidukis väljast vaadatuna nähtavale kohale. Seade peaks olema pilkude eest varjatud või suletud pakiruumi. Pihuarvuti on vara, mis võib ligi meelitada potentsiaalseid taskuvargaid.

Kui pihuarvutit kasutatakse võõrastes bürooruumides, tuleb järgida vastava organisatsiooni kohapealseid turvareegleid. Võõrastes ruumides nagu nt hotellitubades ei tohiks pihuarvutit jätta nähtavale kohale. Tuleks aktiveerida kõik parooli kaitsemehhanismid. Seadme lukustamine kappi aitab ennetada juhuvargusi.

Isiklike pihuarvutite kasutamine

Ametiasutuse või ettevõtte töö raames tuleks pihuarvutite kasutamiseks kehtestada muuhulgas järgnevad reeglid:

- Pihuarvutite mõistlik rakendamine eeldab üldjuhul selle sünkroniseerimist töökohaarvutiga, nt kalendermärkmiku, aadressiraamatu, e-maili teenuse jms kasutamiseks. Seetõttu peab olema selge, kas töökohal lubatakse installeerida vajalikku riist- ja tarkvara ning kes peaks selle installeerima. Antud kohustus ei tohi jääda kasutajate endi kanda.
- Isiklike pihuarvutite kasutamise puhul peab olema selge, mil määral abistab kasutajaid probleemide puhul vastav kasutajatugi. Samuti tuleks juba eelfaasis välja selgitada, kuidas toimub isiklike pihuarvutite kaasamine asutuse IT-strateegiasse.

Tööandja pihuarvutite kasutamine

Tööandja pihuarvutite kasutamisel vajavad reguleerimist muuhulgas järgnevad punktid:

- Töötajad peavad teadma, kas nad tohivad pihuarvuteid sünkroniseerida ka isiklike arvutitega või mitte. Ühelt poolt kergendab see töökohtumiste aegade kooskõlastamist, teiselt poolt jällegi on oht, et pahavara võib edasi kanduda töökoha IT-süsteemidesse ja sisekasutuseks mõeldud dokumendid võivad sattuda isiklikesse arvutitesse.
- Kasutajatele tuleb õpetada, kuidas pihuarvutitega võimalikult hoolikalt ümber käia, et nad teaksid, kuidas ennetada pihuarvuti kadumist ja vargust

ning kuidas tagada oma käitumisega seadmete võimalikult pikk kasutusiga (nt aku eest hoolitsemine, seadme hoidmine väljaspool büroo- või eluruume, liiga kõrgete või liiga madalate temperatuuride taluvus).
- Reguleeritud peaks olema ka pihuarvutite haldamine, hooldamine ja edasiandmine.

Integreerimine teiste turvalahenduste alla

Pihuarvutite rakendamisel tuleks kaaluda mitte ainult seda, kas pihuarvuti kaitseks oleks mõttekas kasutada turvatarkvara, vaid ka seda, mil määral suudab pihuarvuti teha koostööd oma rakenduskeskkonna turvatarkvaraga. Kaks näidet:

- Kasutaja loeb ja kirjutab oma Desktop-PCga tihti meile, mis on krüpteeritud, st digitaalselt allkirjastatud. Kasutaja soovib teel olles meilidega tegelemiseks kasutada oma pihuarvutit. Krüpteeritud, st digitaalselt allkirjastatud meilidega ümberkäimisel võib aga pihuarvutites tekkida mitmetel põhjustel erinevaid probleeme. Näiteks eksisteerib seni veel väga vähe krüpteerimis- ja allkirjastamislahendusi, mis ühilduksid samahästi nii levinud Office baasil kui ka PDA baasil loodud meiliprogrammidega Selliste rakenduste puhul kasutatakse tihti vajalike krüptograafiliste võtmete salvestamiseks ka veel lisaks kiipkaarte või muid turvalube (token). Kiipkaardi lugemisseadet on võimalik lisada vaid vähestele pihuarvutitele. Pealegi töötavad paljud PKI-rakendused serveripõhiselt, st sertifikaatide kontrollimiseks või sidepartnerite avalike võtmete päringuks vajavad nad juurdepääsu mõnele serverile.
- Ettevõtetes salvestatakse eranditult kõik andmed, nii töökohtades kui ka serverites krüpteeritult. Kui kasutaja soovib organisatsioonisiseseid andmeid pihuarvutisse üle kanda, võidakse hiljem teel olles avastada, et pihuarvutisse on laetud pääsuõigusega kaitstud failid, mida ei ole võimalik pihuarvutis lugeda. Andmete konfidentsiaalsust silmas pidades on antud näide parem variant. Pihuarvutisse üle kantud andmeid pihuarvuti reeglina ei krüpteeri või krüpteerib väga nõrgalt, mistõttu on need nõrgemini kaitstud kui mõnes organisatsioonisiseses IT-süsteemis.

Seetõttu tuleb niisugused kasutusjuhud, st pihuarvutite rakenduste integreerimine ettevõtte ülejäänud turvatarkvara alla ilmtingimata pihuarvutite turvasuunistes kindlaks määrata, et pihuarvutite kasutus ei nõrgendaks kehtestatud turbeastet.

Vajadusel - Pihuarvutite kasutamiskeeld

Tuleks läbi mõelda, kas pihuarvutite kasutamist või koguni kaasavõtmist on tarvis ametiasutuse raames või teatud kindlates ruumides piirata. See võib olla mõttekas nt ruumides, kus tahetakse keelata jutuajamiste pealtkuulamist või ruumi fotografeerimist.

Kui teatud asutuse IT-turvapoliitika näiteks ei luba võõraid IT-seadmeid nagu nt pihuarvuteid endaga kaasa tuua, tuleb kõikide sissepääsude juures sellele ka selgelt viidata. Vastavate piirangute täitmist tuleb ka regulaarselt kontrollida. Külastajate jaoks tuleks sellistel juhtudel luua võimalus kaasa toodud mobiiltelefonid, pihuarvutid või sülearvutid turvaliselt hoiule anda. Näiteks võivad sissepääsude kõrvale olla paigaldatud suletavad laekad.

Kontrollküsimused:

- Kas pihuarvutite kasutamise kohta on olemas aktuaalne turvaeeskiri?
- Kuidas kontrollitakse pihuarvutite kasutamise turvaeeskirjade järgimist?

- Kas iga pihuarvuti kasutaja on saanud vastavast pihuarvuti eeskirjast koopia või infolehe selle kohta, millised on tähtsamad turvamehhanismid?
- Kas IT-turvameetmete koolituse raames käsitletakse ka pihuarvutite kasutamise turvaeeskirja?
- Kas pihuarvutite kasutajaid on teavitatud reeglitest, mida nad peavad kohustuslikus korras järgima?
- Kas pihuarvutite kasutajaid on teavitatud sellest, millised on seadmete sobivad hoiutingimused?

M 2.305 Sobivate nutitelefonide, tahvel- ja pihuarvutite valimine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator, varumisosakond, IT juht

Nutitelefonid, tahvel- ja pihuarvutid on saadaval väga erinevates variantides ja seadmeklassides. Erinevused ei seisne mitte ainult seadmete mõõtmetes ja jõudluses, vaid ka turvamehhanismides ja kasutusmugavuses. Lisaks seavad erinevad tooted ka erinevaid tingimusi kasutuskeskkonna teistele riist- ja tarkvarakomponentidele.

Pihuarvutite mudelite rohkus ja nendes kasutatavad erinevad operatsioonisüsteemid tekitavad ühilduvusprobleeme muu riist- ja tarkvaraga.

Pärast otsuse langetamist, et asutuses hakatakse kasutama nutitelefone, tahvel- või pihuarvuteid, tuleks esmalt analüüsida asutuse vajadusi. Vajaduste analüüsi eesmärk peaks olema selgitada esmalt välja kõik konkreetsetel juhtudel kõne alla tulevad kasutusvaldkonnad ning teisalt kasutusvaldkondadest tulenevad nõuded riist- ja tarkvarakomponentidele ning dokumenteerida analüüsi tulemused nõuete loeteluna.

Vastava nõuete loetelu alusel tuleks seejärel hinnata saadaolevate seadmete nõuetelevastavust ja valida välja sobivad seadmed. Kui asutus lubab töötajatel kasutada ka isiklikke nutitelefone, tahvel- või pihuarvuteid, tuleks lubada üksnes selliseid isiklikke seadmeid, mis vastavad asutuse nõuetele. Kogemused on näidanud, et erinevate kasutusvaldkondade jaoks on üpris mõttekas soetada erinevat tüüpi seadmed. Sellest hoolimata tuleks seadmetüüpide valikut siiski ka piirata, sest vastasel korral muutub kasutajatoe osutamine liiga keeruliseks.

Samuti tuleb tagada, et kaasaskantavates seadmetes kasutatav tarkvara oleks tsentraalselt ja efektiivselt hallatud (vt M 4.230 Pihuarvutite tsentraalne haldus). Ka vajaminev serveritaristu peaks olema selline, mille haldamine ei oleks üleliia töömahukas.

Järgnev nimekiri annab üldistatud ülevaate võimalike hindamiskriteeriumite kohta, kuid see ei pretendeeri mitte mingil juhul täiuslikkusele ning kindlasti on seda nimekirja võimalik täiendada.

Üldised kriteeriumid
Hooldus

- Kas toodet on lihtne hooldada?
- Kas tootja väljastab tarkvarale regulaarselt värskendusi?
- Kas toote kohta on võimalik sõlmida hooldusleping?

Usaldusväärsus ja rikkekindlus

- Kas tegu on usaldusväärse tootega?
- Kas toodet on võimalik rakendada pidevkasutuses?
- Kas tootesse on integreeritud backup-mehhanism?
- Kas andmevarundus toimib automaatselt?
- Kas toote mälu on võimalik turvaliselt kustutada?

Kasutajasõbralikkus

- Kas kasutajad on suutelised süsteeme efektiivselt, turvaliselt ja ilma vigadeta kasutama ka ilma mahukaid koolitusi läbimata?
- Kas sünkroniseerimistarkvara on võimalik konfigureerida selliselt, et süsteem ei koormaks kasutajaid liigsete tehniliste detailidega? Kas sellele vaatamata säilib alati siiski ka kõrge turbeaste?
- Kas seadme mõõtmed ja kaal on planeeritud kasutusvaldkonna jaoks sobivad? Kas aku tööiga on igapäevatööks piisava kestvusega?

Kulud

- Kui suurte kulutustega tuleb arvestada riist- ja tarkvara soetamisel?
- Kui suured on eeldatavad riistvara ja tarkvaraga seotud jooksvad kulud (hooldamine, kasutamine, tugiteenus)?
- Kui suured on eeldatavad personalikulud (administraatorid/kasutajatugi)?
- Kas on tarvis soetada täiendavaid tarkvara- või riistvarakomponente nagu nt dokkimisjaamad ja konverteerimistarkvara?

Funktsioon
Installeerimine ja kasutuselevõtt

- Kas toote installeerimine, konfigureerimine ja kasutamine on lihtne?
- Kas seadet ja kasutatavat sünkroniseerimistarkvara on võimalik konfigureerida selliselt, et tulemus vastaks ettenähtud turbenõuetele?
- Kas konfiguratsiooni olulisemaid parameetreid on võimalik kaitsta volitamata kasutajate tehtavate muudatuste eest?
- Kas toode ühildub enamlevinud riist- ja tarkvaraga (operatsioonisüsteemidega, draiveritega)?

Haldamine

- Kas tootega kaasasolev dokumentatsioon sisaldab detailset teavet kõikide tehniliste näitajate ja haldamisega seotud andmete kohta?
- Kas nutitelefone, tahvel- ja pihuarvuteid on võimalik hallata tsentraalselt juhitava haldustarkvaraga? Kas haldamisliides on koostatud nõnda, et süsteem viitab konfiguratsioonis esinevatele vigadele, konfiguratsiooni ebaturvalisusele või selle kõrvalekalletele või takistab nende rakendamist?

Logimine

- Kas tootel on olemas logimisfunktsioon?
- Kas logiandmete detailsust on võimalik konfigureerida?
- Kas logisse salvestatakse kõik olulised andmed?

Side ja andmeedastus

- Kas nutitelefon, tahvel- ja pihuarvuti toetab kõiki vajalikke andmeedastustehnoloogiaid nagunt WLAN, Bluetooth, GSM, UMTS, LTE või infrapuna)?

Turve
Side, autentimine ja juurdepääs

- Kas nutitelefonis, tahvel- ja pihuarvutis on olemas sobivad funktsioonid kasutajate identifitseerimiseks ja autentimiseks?
- Kas seadme abil on võimalik turvaliselt edastada ka teistsugustesse lõppseadmetesse salvestatud andmeid? Kas see kehtib kõikidele liidestele, nt ka traadita ühenduste jaoks?
- Kas tootes on võimalik kasutada turvamehhanisme (nt krüpteerimist ja viirusetõrjetarkvara)?
- Kas toote arhitektuur võimaldab ka hiljem uusi turvamehhanisme juurde installeerida?
- Kas mobiilne kasutaja saab juurdepääsu lõppseadmetele ainult pärast õnnestunud autentimist?

Vaatamata IT-halduse poolt langetatud tootevalikule tuleb alati arvestada sellega, et töötajad eelistavad kindlasti hoopis teistsuguseid nutitelefone, tahvel- ja pihuarvuteid ning püüavad neid oma igapäevatöös kasutama hakata, nõudes võib-olla koguni nende seadmete ametlikku heakskiitmist. Sellisteks juhtudeks

tuleks luua sobivad protseduurireeglid.

Nutitelefonide, tahvel- ja pihuarvutite osasid funktsioone on võimalik kasutada ainult koostöös väliste teenuseosutajatega. Kui väline teenuseosutaja ei suuda garanteerida andmete konfidentsiaalsuse ja tervikluse säilimist, ei tohi vastava teenuseosutaja andmesidelahendusi kasutada organisatsioonisiseseks kasutuseks mõeldud andmete transportimiseks. Läbi mobiilivõrgu toimub andmeedastus nt enamatel juhtudel küll vähemalt alguses krüpteeritult („õhuliides"), kuid seejärel saadetakse andmed tihti mobiilsideoperaatori võrgus krüpteerimata kujul edasi ja salvestatakse teenuseosutaja serverisse ilma krüpteerimata. Kahtluse korral tuleks selliste teenuste kasutamisest loobuda.

Kontrollküsimused

- Kas soetamist puudutav otsus on administraatorite ja tehnilise personaliga kooskõlastatud?
- Kas potentsiaalselt sobivate seadmete hindamisel on kasutatud vajaduste analüüsi tulemusi?
- Kas vajaduste analüüs on tehtud?

M 2.306 Kahjudest teatamine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: kasutajad

IT-süsteemide avariidest, defektidest või vargustest tuleb viivitamata organisatsioonile teada anda. Selleks peaks iga organisatsioon kehtestama selged teavitamisprotseduurid ja nimetama kontaktisikud. See kehtib ka mobiilsetele andmekandjatele. Defektidest tuleks teada anda ka väiksemate odava hinnaga andmekandjate puhul, et IT-haldusega tegeleval osakonnal oleks võimalik välja selgitada, kas defekt on pigem erand või puudutab tervet soetatud partiid. Suur usaldusväärsus ja pikk kasutusiga on eriti tähtsad andmevarunduse ja arhiveerimise otstarbel rakendatavate andmekandjate puhul. Varguste puhul jällegi on tarvis tegutseda võimalikult kiiresti, sest tegeleda tuleb mitte ainult uute seadmete soetamisega, vaid ka puudutatud andmete võimaliku väärkasutuse ärahoidmisega. Sülearvutites, pihuarvutites ja muudes sarnastes seadmetes, samuti mobiilsetes andmekandjates nagu nt USB-mälupulkades võib olla konfidentsiaalseid andmeid, mille kaotsiminekust tuleb viivitamata teatada.

Nende hulka kuuluvad näiteks:

- Pääsuandmed, nt paroolid: kõikide potentsiaalselt puudutatud IT-süsteemide pääsuandmed tuleb ära muuta nii kiiresti kui vähegi võimalik.
- Konfidentsiaalseks liigitatud informatsioon (nt patsientide toimikud): sobivate vastumeetmete rakendamiseks tuleb juhtunust teavitada kõiki puudutatud osapooli (nt eriarste, kliente, jne).

Sideühendusi võimaldavate kaasaskantavate seadmete kaotamisel tuleks kasutada nende seadmete blokeerimis-, kustutus- ja positsioneerimisfunktsioone. Suur osa Mobile-Device-Management-lahendusi võimaldab selliseid funktsioone kasutada. Selleks tuleb juba varakult kehtestada asjakohased reeglid ning võtta vastava olukorra saabudes koostöös seadme kasutajaga viivitamata vastumeetmeid (vt M 6.159 Nutitelefonide ning tahvel- ja pihuarvutite kaotuste ja varguste ennetamine).

Kadumaläinud seadmete või andmekandjate väljailmumine ei peaks põhjustama mitte ainult rõõmu, vaid andma ka ainest järelemõtlemiseks. Enne nende vahendite uuesti kasutuselevõtmist tuleks need võimalike manipulatsioonide suhtes üle kontrollida (nt kas kruvisid on avatud või pitser eemaldatud). Veendumaks, et seadmetes ei ole peidus manipuleeritud programme, tuleks vastavad seadmed uuesti installeerida, (vt M 4.28z Sülearvuti tarkvara reinstalleerimine kasutaja vahetumisel). Samasuguse ettevaatlikkusega nagu seadmeid tuleks käsitleda ka kadunud ja uuesti väljailmunud andmekandjaid, kuna need võivad sisaldada kahjurvara.

Kontrollküsimused:

- Kas töötajad on teadlikud sellest, kuidas ja kuhu tuleb teatada kahjudest?

M 2.307 Väljasttellimissuhte nõuetekohane lõpetamine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond

Rakendamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, spetsialist

Üldjuhul on selle meetme soovitusi võimalik rakendada vaid siis, kui lepingu lõpetamist puudutavad olulised valdkonnad on reguleeritud juba teenusepakkujaga sõlmitud lepingus. Lepingulise suhte lõppemisel peab aset leidma nõuetekohane puudutatud teenuste, nt IT käitamise ja nendega seotud vastutuse üleandmine kas tellijale või mõnele uuele teenusepakkujale.

Võtta tuleb meetmeid, mis tagaksid, et teenuse sisseostmiseks sõlmitud lepingu lõppemine ei mõjutaks organisatsiooni igapäevatööd:

- Teenuse üleminek uuele teenusepakkujale kujutab endast uut väljasttellimise (outsourcing) protseduuri. Siinkohal tuleb rakendada vajalikke meetmeid moodulist „Väljasttellimine".
- Seesttellimise (insourcing) puhul tuleb vajaminevaid meetmeid rakendada sarnaselt moodulis „Väljasttellimine" kirjeldatule. Seesttellimise strateegiale, IT turvakontseptsioonile, üleviimisele ja hädaolukorraks valmisolekule kehtivad samad nõuded nagu „klassikalisele" väljasttellimise protseduurile.

Arvestada tuleks järgnevate aspektidega:

- Riistvara ja tarkvara (liidesprogrammide, tarkvaratööriistade, pakktöötluse protsesside, makrode, litsentside varukoopiate) omandiõigused peavad olema selged.
- Teenusetarnijaga tuleb kokku leppida, kuidas toimitakse juhul, kui teenuse sisseostmine tahetakse lõpetada, kuid teenuseosutaja kasutatud tööriistu, protseduure, skripte ja pakkprogramme soovitakse edasi kasutada.
- IT-süsteemid, IT-rakendused ja tööprotsesside kulg peavad olema dokumenteeritud piisava täpsusega.
- Teenusepakkuja peab teenuse tellijale edastama või üle andma kõik vajalikud andmed.
- Kõik teenusepakkuja juures salvestatud andmed tuleb turvaliselt kustutada.
- Asutusesisene või asutuseväline personal, kes peab teenusepakkuja ülesanded üle võtma, peab saama vastavad juhised ja läbima vastavasisulise koolituse.
- Lepingus on soovitatav kindlaks määrata üleminekuperiood, mille jooksul on endine teenusepakkuja kohustatud küsimuste ja probleemide korral toeks olema.

Kontrollküsimused:

- Kas teenuseosutajaga sõlmitavad väljasttellimislepingud ja pilvteenuse lepingud sisaldavad kõiki teenuse nõuetekohase lõpetamise sätteid?
- Kas lepingulise suhte lõpetamisel välise teenuseosutaja ja pilvteenuse pakkujaga on tagatud, et sellel puudub negatiivne mõju asutuse igapäevatööle?

M 2.308z Väljakolimise kord

Algatamise eest vastutavad: sisekommunikatsiooni juht, ametiasutuse/ettevõtte juhtkond

Rakendamise eest vastutavad: sisekommunikatsiooni osakond, töötajad

Hoonest osaliselt või ka täielikult välja kolides tuleb tähelepanu pöörata järgmistele punktidele:

- Enne väljakolimisega alustamist tuleb kõikide IT-turvalisusega seotud esemete (riistvara, tarkvara, andmekandjate, paberdokumentide jms) kohta koostada inventari loetelud.
- Igat töötajat tuleb kirjalikult informeerida sellest, mille eest ta kolimise käigus vastutab. Sellega välditakse olukordi, kus töötajad hoolitsevad küll oma tööks vajalike vahendite ja asjade eest, kuid jätavad mõningad asjad lihtsalt laokile, oletades, et küllap vastutab nende eest keegi teine.
- Ebavajalikud vananenud seadmed, andmekandjad jms tuleb enne väljakolimist vastavalt M 2.13 Tundlike ressursside jäljetu hävitamine sobilikul moel utiliseerida. Mitte mingil juhul ei tohi vanu töövahendeid vanasse asukohta lihtsalt vedelema jätta, isegi mitte neil juhtudel, kui rendileandja, uus rentnik või ruumide ostja soovib neid edasi kasutada või lubab need ise utiliseerida.
- Pärast väljakolimisega seotud tööde lõpetamist tuleb KÕIK ruumid veelkord üle kontrollida, et veenduda, kas kõik turvalisuse seisukohast olulised töövahendid on ikka kaasa võetud. Peamised kohad, kuhu töövahendeid tihti maha unustatakse, on tööruumidest eemal asuvad panipaigad nagu keldrid või pööningud.

Kõik töös kasutatud vahendid tuleb järjekindlalt kokku koguda ja minema toimetada ning hiljem vajaduse korral turvalisel moel utiliseerida (vt M 2.177 Kolimise turve).

Täiendavad kontrollküsimused:

- Kas kolimise tarbeks koostatakse ja jagatakse töötajatele kätte inventari loetelud?
- Kas pärast väljakolimist kontrollitakse hoone veelkord üle, et välistada asjade mahaunustamist?

M 2.309 Mobiilse IT-kasutuse turvapoliitika ja eeskirjad

Algatamise eest vastutavad: IT-turvaosakond, IT-juht

Rakendamise eest vastutavad: IT-turvaosakond, IT-juht

Väljaspool institutsiooni kasutatavate IT-seadmete puhul tuleb arvestada palju rohkemate ohtudega kui nende IT-seadmete puhul, mis asuvad organisatsiooni kaitsvate seinte vahel. Sellele vaatamata on palju võimalusi, kuidas mobiilseid IT-seadmeid liikuva töö puhul kaitsta. Selleks, et vastavaid võimalusi ka aktiivselt rakendataks, tuleks koostada asjakohased turvasuunised, kus peaksid olema toodud kõik kohustuslikud turvamehhanismid. Lisaks tuleks kasutajatele koostada mobiilsete IT-süsteemide turvalise kasutamise kohta lühike ja ülevaatlik infoleht.

Töötajate teavitamine võimalikest ohtudest

Kogemused on näidanud, et mida väiksemaks ja kergmaks muutuvad IT-seadmed, seda hooletumalt käiakse nendega ümber. Seetõttu tuleks töötajate tähelepanu juhtida asjaolule, et mobiilsete IT-süsteemide ja sinna salvestatud andmete puhul on tegemist väärtusliku varaga. Kuna mobiilseid IT-seadmeid on väga palju erinevaid variante erinevates kombinatsioonides (alates mobiiltelefonist, pihuarvutist kuni WLAN-liidesega sülearvutini välja), tuleks töötajatele ohtude ja vastuabinõude selgitamisel lähtuda nende kasutatavatest konkreetsetest seadmetest ja nende spetsiifikast.

Ettevaatus info edastamisel

Töötajaid tuleks teavitada ka sellest, et nad ei tohi ringi liikudes rääkida konfidentsiaalsest infost suvaliste isikutega, samuti peavad nad hoolitsema, et kolmandatel isikutel ei oleks võimalik konfidentsiaalset infot näha ega pealt kuulata. Eriti oluline on sidepartneri täpse identiteedi väljaselgitamine neil juhtudel, kui detailset infot on plaanis edastada telefoni teel (vt G 3.45 Sidepartnerite puudulik autentimine).

Mobiilsete IT-süsteemide kasutusreeglid

Enne mobiilsete IT-süsteemide kasutamist tuleb paika panna erinevad reeglid:

- Kasutajad peavad teadma, millist liiki andmeid on liikuva töö puhul lubatud töödelda mobiilsete IT-seadmetega. Selleks on tarvis, et andmed oleksid liigitatud klassidesse, mis aitaksid kasutajatel võimalikult lihtsalt tuvastada neile kehtivaid piiranguid (vt M 2.217 Teabe, rakenduste ja süsteemide hoolikas liigitamine ja käitlus). Mobiilsetes IT-süsteemides ei tohi hoida ega töödelda ärisaladusi kajastavaid andmeid.
- Kõrge turbeastme alla kuuluvaid andmeid (nt hinnapakkumisi, tehnilisi andmeid, ettevõtte majandusandmeid) tuleks mobiilsetesse IT-seadmetesse salvestada alati vaid krüpteeritud kujul.
- Mobiilsete IT-süsteemide kasutamise puhul on tarvis otsustada, kas tööülesannetes ringi liikuvatel töötajatel lubatakse vastavate seadmetega oma institutsiooni siseandmetele ligi pääseda või mitte. Kui seda lubatakse, tuleb vastavat juurdepääsu ka piisavalt kaitsta (vt M 5.121 Turvaline side mobiilseadme ja töökoha vahel ja M 5.122 Sülearvuti turvaline ühendamine kohtvõrguga).

- Tööandja peab kindlaks määrama, kas vastavaid seadmeid lubatakse kasutada ka isiklikuks otstarbeks, nt erakirjade kirjutamiseks või mängude mängimiseks pärast tööaja lõppu.
- Kasutajatele tuleb õpetada, kuidas mobiilsete IT-süsteemidega võimalikult hoolikalt ümber käia, et nad teaksid, kuidas ennetada seadmete kadumist ja vargust ning kuidas tagada seadmete võimalikult pikk kasutusiga (nt aku eest hoolitsemine, seadme hoidmine väljaspool büroo- või eluruume, liiga kõrgete või liiga madalate temperatuuride taluvus).
- Reguleeritud peaks olema ka mobiilsete IT-süsteemide haldamine, hooldamine ja edasiandmine.
- Iga kord, kui seadme kasutaja vahetub, tuleb kõik vajalikud paroolid turvaliselt edasi anda (vt M 2.22 Paroolide deponeerimine).

Mobiilseid IT-süsteeme ei tohiks jätta ilma järelvalveta kuhugi laokile. Kui mobiilset IT-süsteemi on tarvis jätta sõidukisse, tuleks seda teha nii, et seade ei jääks sõidukis väljast vaadatuna nähtavale kohale. Seade peaks olema pilkude eest varjatud või suletud pakiruumi. Mobiilne IT-süsteem on vara, mis võib ligi meelitada potentsiaalseid taskuvargaid. Kui mobiilseid IT-süsteeme kasutatakse võõrastes bürooruumides, tuleb järgida vastava organisatsiooni kohapealseid turvareegleid. Võõrastes ruumides nagu nt hotellitubades ei tohiks mobiilseid IT-süsteeme jätta niisama laokile. Hiljemalt nüüd tuleks aktiveerida kõik parooli kaitsemehhanismid. Seadme lukustamine kappi aitab ennetada juhuvargusi.

Andmekandjate ja dokumentide utiliseerimine

Ka liikuva töö puhul tekib tihti materjali, mida on tarvis utiliseerida ainuüksi juba seetõttu, et pagas ei muutuks üleliia raskeks. Kui institutsioonide siseruumides on vanade või kasutuskõlbmatute andmekandjate ja dokumentide utiliseerimiseks välja kujunenud kindlad protseduurid (vt M 2.13 Tundlike ressursside jäljetu hävitamine), siis liikuva töö puhul pole neid kahjuks alati võimalik rakendada. Seetõttu tuleks enne oma aja ära teeninud andmekandjate ja dokumentide hävitamist täpselt järele mõelda, kas need võivad sisaldada ka tundlikku informatsiooni. Kui see on nii, tuleb vastavad andmekandjad ja dokumendid kahtluse korral siiski endaga kaasa võtta. Sama kehtib ka siis, kui andmekandjad on muutunud defektseks, kuna ka sellistest andmekandjatest on ekspertidel võimalik infot siiski veel kätte saada. Ka võõraste institutsioonide purustitesse tuleks suhtuda ettevaatlikkusega, kuna nende puhul ei pruugi alati selge olla, kes vastava utiliseerimise läbi viib, st kui turvaliselt see läbi viiakse.

Mobiilsete IT-süsteemide kasutuskeeld

Tööandja peaks läbi mõtlema, kas mobiilsete IT-süsteemide kasutamist või koguni kaasavõtmist on tarvis ametiasutuse või ettevõtte piirides või teatud kindlates ruumides piirata. Antud nõude rakendamine võib olla mõttekas nt nõupidamisruumides (vt M 5.80 Kaitse mobiiltelefonidega pealtkuulamise eest). Kui institutsiooni IT-turvapoliitika ei luba mobiilseid IT-süsteeme endaga kaasa tuua, tuleb kõikide sissepääsude juures sellele ka selgelt viidata. Vastavate piirangute täitmist tuleb ka regulaarselt kontrollida.

Täiendavad kontrollküsimused:

- Kas mobiilsete IT-süsteemide kasutamise kohta on olemas ajakohane turvaeeskiri?
- Kuidas kontrollitakse mobiilsete IT-süsteemide kasutamise turvaeeskirjade järgimist?

- Kas iga mobiilse IT-süsteemi kasutaja on saanud vastavast eeskirjast koopia või infolehe selle kohta, millised on tähtsamad turvamehhanismid?
- Kas IT-turvameetmete koolituse raames käsitletakse ka mobiilsete IT-süsteemide kasutamise turvaeeskirja?
- Kas mobiilsete IT-süsteemide kasutajaid on teavitatud reeglitest, mida nad on kohustatud järgima?
- Kas mobiilsete IT-süsteemide kasutajaid on teavitatud sellest, millised on seadmete sobivad hoiutingimused?

M 2.310z Sobivate sülearvutite valimine

Algatamise eest vastutavad: IT-turvaosakond, IT-juht

Rakendamise eest vastutavad: administraator, varumisosakond, IT juht

Sülearvutite puhul eksisteerib väga erinevaid variante ja seadmeklasse. Erinevused ei seisne mitte ainult seadmete mõõtmetes ja jõudlusnäitajates, vaid ka turvamehhanismides ja kasutajamugavuses. Lisaks seavad erinevad tooted ka erinevaid tingimusi kasutuskeskkonna riist- ja tarkvarakomponentidele. Sülearvutite mudelite rohkus ning erinevad operatsioonisüsteemid tekitavad sülearvutite ja PC tarkvara ja riistvara vahel ja ka nende liidestes hulgaliselt ühilduvusprobleeme. Pärast otsuse langetamist hakata organisatsioonis kasutama sülearvuteid, tuleks koostada nõuete loetelu, mille alusel oleks võimalik pakutavaid tooteid üksteisega kõrvutada. Lõplike toodete valik peaks tuginema eelnevalt läbi viidud toodete hindamisel. Kasutuskogemused on näidanud, et erinevate kasutusvaldkondade jaoks on üpris mõttekas kaaluda erinevate seadmetüüpide soetamist. Sellele vaatamata tuleks seadmetüüpide valikut siiski ka piirata, sest vastasel korral muutub kasutajatoe osutamine liiga keeruliseks. Alustuseks tuleks läbi viia vajaduste analüüs. Vajaduste analüüsi eesmärgiks peaks olema esmalt selgitada, millised on konkreetsel juhul kõne alla tulevad kasutusvaldkonnad ning teisalt, millised on kasutusvaldkondadest tulenevad nõuded riist- ja tarkvarakomponentidele.

Järgnev nimekiri annab üldistatud ülevaate võimalike hindamiskriteeriumite kohta, kuid see ei ole mitte mingil juhul täiuslik ning seda on kindlasti võimalik täiendada.

1 Üldkriteeriumid

1.1 Hooldamine

- Kas toodet on lihtne hooldada?
- Kas tootja väljastab tarkvarale regulaarselt täiendeid?
- Kas toote kohta on võimalik sõlmida hooldusleping?

1.2 Usaldusväärsus/rikkekindlus

- Kas tegu on usaldusväärse tootega?
- Kas toodet on võimalik rakendada pidevkasutuses?
- Kas tootesse on integreeritud Backup -mehhanism? Kas andmevarundust on võimalik läbi viia automatiseeritult?

1.3 Kasutajasõbralikkus

- Kas toote installeerimine, konfigureerimine ja kasutamine on lihtne?
- Kas sünkroniseerimistarkvara on võimalik konfigureerida selliselt, et süsteem ei koormaks kasutajaid liigsete tehniliste detailidega? Kas sellele vaatamata säilib siiski ka kõrge turbeaste?
- Kas seadme mõõtmed ja kaal on planeeritud kasutusvaldkonna jaoks sobivad? Kas aku tööiga on igapäevatööks piisava kestvusega?

1.4 Kulutused

- Kui suurte kulutustega tuleb arvestada riist- ja tarkvara soetamisel?
- Kui suured on eeldatavad riistvara ja tarkvaraga seotud jooksvad kulud (hooldamine, kasutamine, tugiteenus)?
- Kui suured on eeldatavad personaliga seotud jooksvad kulutused (administraatorid/kasutajatugi)?
- Kas on tarvis soetada täiendavaid tarkvara- või riistvarakomponente (nt dokkimisjaamu, konverteerimistarkvara)?

2. Funktsioon

2.1 Installeerimine ja kasutuselevõtt

- Kas seadet ja kasutatavat sünkroniseerimistarkvara on võimalik konfigureerida selliselt, et turbele seatud eesmärke on kindlasti võimalik saavutada?
- Kas olulisemaid konfiguratsiooni parameetreid on võimalik kasutaja tehtavate muudatuste eest kaitsta?
- Kas toode ühildub enamlevinud riist- ja tarkvaraga (operatsioonisüsteemidega, draiveritega)?

2.2 Haldamine

- Kas tootega kaasasolev dokumentatsioon sisaldab detailset infot kõikide tehniliste näitajate ja haldamisega seotud andmete kohta?
- Kas sülearvuteid on võimalik hallata tsentraalselt juhitava haldustarkvara abil? Kas haldamisliides on koostatud selliselt, et süsteem viitab vigadega, ebaturvalistele ning kõrvalekalletega konfiguratsioonidele või takistab nende rakendamist?

2.3 Logimine

- Kas tootel on olemas logi?
- Kas logiandmete detailsust on võimalik konfigureerida? Kas logisse salvestatakse kõik olulised andmed?
- Kas juurdepääs logiandmetele on juurdepääsu kaitsega kaitstud?
- Kas toode võimaldab logiandmeid salvestada lisaks kohapealsetele süsteemidele veel ka eemalolevatele arvutitele (tsentraalne protokoll)?

2.4 Side ja andmeedastus

- Kas sülearvuti toetab kõiki vajaminevaid andmeedastusviise (nt infrapuna, bluetooth või GSM)?

2.5 Turvalisus: side, autentimine ja juurdepääs

- Kas sülearvutil on olemas sobivad funktsioonid kasutajate identifitseerimiseks ja autentimiseks?
- Kas seadme abil on võimalik turvaliselt edastada ka teistsugustesse lõppseadmetesse salvestatud andmeid?
- Kas seadmega on võimalik kasutada täiendavaid turvamehhanisme (nt krüpteerimist või viirusetõrjetarkvara)?
- Kas toote arhitektuur võimaldab ka hiljem uusi turvamehhanisme juurde installeerida?

- Kas mobiilne kasutaja saab juurdepääsu kohapeal olevatele lõppseadmetele ainult õnnestunud autentimiskatse tagajärjel?
- Kas süsteemiarhitektuuri ülesehitus võimaldab uusi autentimismehhanisme ka hiljem juurde integreerida?

Pärast seda, kui kõik soetatavale tootele kehtestatud nõuded on kirja pandud, tuleb hakata saadaolevaid tooteid analüüsima, et välja selgitada, milline toode suudab neid nõudeid täita. On küllaltki ootuspärane, et kõik tooted ei ole võimelised kõiki nõudeid korraga või võrdselt hästi täitma. Seetõttu tuleks hinnata, kui suureks võib osutuda erinevate nõuete osatähtsus. Toetudes läbiviidud hindamisele (vastavalt nõuete kataloogile), võib langetada põhjendatud ostuotsuse.

Täiendavad kontrollküsimused:

- Kas vajaduste analüüs on tehtud?
- Kas väljaselgitatud vajaduste alusel on toimunud potentsiaalselt sobivate seadmete hindamine?
- Kas soetamist puudutav otsus on administraatoritega ja tehnilise personaliga kooskõlastatud?

M 2.311 Kaitsekappide planeerimine

Algatamise eest vastutavad: IT-juht, varumisosakonna juht, IT-turvaosakond

Rakendamise eest vastutavad: varumisosakond, tehnikaosakond

Kaitsekappide kasutamine võib olla mõttekas mitmel erineval põhjusel, muuhulgas nt puuduva serveriruumi asendamiseks või ka olemasoleva serveriruumi turvalisuse tõstmiseks. Kuna kaitsekappide hinnad pole just kõige soodsamad, tuleks enne soetamist luua vastav kontseptsioon, mis arvestaks kõikide kaitsekappide jaoks planeeritavate kasutusvaldkondadega. Muuhulgas tuleb selleks välja selgitada, milliste ohtude eest soovitakse erinevaid komponente kaitsekappide abil kaitsta, seega nt kas eesmärgiks on kaitsta seadmeid tulekahju või hoopis volitamata ligipääsu eest. Peale selle on ülimalt soovitatav võrrelda erinevate tootjate hinnapakkumisi. Kaitsekappide soetamisega ja ülalpidamisega tekkivaid kulusid tuleks võrrelda serveriruumi või andmekandjaarhiivi sisseseadmise ja ülalpidamisega seotud kuludega.

Vastava ruumi planeerimisel tuleb piisava füüsilise turvalisuse tagamiseks arvestada tuleohutuseeskirjadega kuni valve- ja tuletõrjesignalisatsiooni paigaldamiseni välja ning seda vajadusel ka vastava kaitsekapi sees. Planeerimisel tuleb näiteks arvestada ka sellega, et eelistada tuleks ruume, kus ei ole veetorusid, sest võimalikud lekked võivad endaga kaasa tuua suuri kahjustusi, mida kõik kaitsekapid ei suuda ära hoida. Kui kaitsekappi soovitakse kasutada serverikapina, tuleb vastavalt kaitsevajadusele kasutusele võtta täiendavad kaitsemeetmed nagu nt liigpingekaitse, toite avariilülitid, kliimaseade, UPS ning vajadusel ka tõrgete kaugindikatsioon.

Täiendavad kontrollküsimused:

- Kas enne kaitsekappide soetamist viiakse läbi sellekohaste vajaduste analüüs?

M 2.312 Infoturbealase koolitus- ja teavitusprogrammi kavandamine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, infoturbespetsialist, personalijuht

Rakendamise eest vastutavad: infoturbespetsialist, ülemused

Infoturbe juurutamine ja selle taseme hoidmine sõltub olulisel määral töötajatest. Kuna töötajad on need, kes kasutavad ja haldavad infoturbega seotud tehnilisi süsteeme, oleneb infoturvet puudutavate tahtlike ja hooletusvigade arv paljuski sellest, mil määral järgivad töötajad turbealaseid ettekirjutusi ja norme. Turvakontseptsiooni põhjal võetavad tehnilised ja töökorralduslikud meetmed võivad tööülesannete täitmist puudutada väga erineva nurga alt. Meetmed võivad nt ette näha kohustuslikku paroolivahetust, sisenemist teatud ruumidesse üksnes vastava loa alusel, kohustust kanda enda töötõendit riietuse küljes nähtaval kohal või osaleda regulaarselt turbealastel koolitustel.

Iga asutuse eesmärk peaks olema, et kõik töötajaid mõistaksid infoturbe kasulikkust ja hädavajalikkust nii tööülesannete täitmisel kui ka asutuse jaoks tervikuna, et töötajad aktsepteeriksid infoturvet ja aitaksid ka ise aktiivselt kaasa infoturbe tagamisele. Töötajad peavad järgima asutuses kehtestatud nõudeid ja aitama enda käitumisega kaasa nii infoturbe säilitamisele kui ka selle edasiarendamisele. Samuti peaksid töötajad suutma võimalikult ruttu tuvastada turbe seisukohalt kriitilisi olukordi ja nendele õigesti reageerima.

Loetletud eesmärkide saavutamiseks on tarvis, et asutuses oleks juurutatud töötajate pidev teavitusprotsess. Töötajate infoturbealase teadlikkuse suurendamisele peaksid järgnema täiendavad koolitused, mille käigus edastatakse kogu vajaminev teave ja oskused (vt M 2.557 Infoturbealase koolitusprogrammi kontseptsioon). Kuna teavitus- ja koolitusprogrammide teemad on üksteisega tihedalt seotud, tuleks nendele asutuse kõikidel tasanditel piisavalt tähelepanu pöörata. Selleks, et töötajad mõistaksid teavitusmeetmete olulisusust ja et meetmete planeerimise, võtmise ja järjepidevuse tagamiseks oleks olemas vajalikud ressursid, peab juhtkond koolitusmeetmeid piisavalt toetama (vt M 3.96 Juhatuse tugi teavitusele ja koolitusele).

Alljärgnevalt kirjeldatakse mõningaid teemasid, mida võiks teavitusprogrammides käsitleda.

Teavitusmeetmete eesmärgi sõnastamine

Infoturvet käsitleva teavitustöö eesmärk on suurendada töötajate teadmisi infoturbest, et töötajate käitumine vastaks asutuses kehtestatud turbenõuetele. Teavitustöö tegemiseks tuleks esmalt sõnastada üldine eesmärk ja täpsustada seda hiljem erinevate sihtrühmade jaoks. Sõnastamine aitab meetmete väljatöötamisel arvestada konkreetsete vajadustega ja loob aluse, mille põhjal saab hiljem kontrollida meetmete edukust. Eesmärgi sõnastamisel võiks keskenduda sellele, miks on infoturve asutuse ja selle töötajate jaoks oluline.

Eesmärgi sõnastuse näide:

- Töötajad mõistavad infoturbe olulisust nii asutuse kui ka enda töökoha kontekstis. Nad on kursis asjakohaste turvaohtudega ning suudavad hinnata turvaintsidentide ja kehtivate reeglite vastu eksimise tagajärgi. Töötajad aktsepteerivad infoturbe meetmeid ja on valmis neid nii järgima kui ka nende tagamisele ja edasiarendamisele aktiivselt kaasa aitama.

Sihtrühmade analüüs

Sihtrühmade analüüsiga jaotatakse töötajad infoturbe vaatevinklist erinevatesse sihtrühmadesse, nagu nt administraatorid, personaliosakonna töötajad, asutusevälised töötajad jt. Samuti tuleks sihtrühmade analüüsimisel arvestada töötajate võimalike tööalaste muudatustega asutuse struktuuris, nt töötaja asumine mõnda teise osakonda, ametikohustuste muutumine, tööasukoha muutumine jmt. Sihtrühmade analüüsimine võimaldab kohandada infoturbealaseid teavitusmeetmeid erineva taustaga töötajate spetsiaalsete vajadustega (vt M 3.93 Teavitus- ja koolitusprogrammide sihtrühmade analüüs).

Teavitusmeetmete eesmärkide täpsustamine sihtrühmadele

Teavitusmeetmete väljatöötamisel tuleb lähtuda sihtrühma vajadustest. Eesmärk võib olla nt turvaintsidentide tagajärgede selgitamine töötajatele võimalikult praktiliste näidete varal. Samuti on osutunud väga tõhusaks töötajate eraelust võetud valdkondade kaasamine infoturbe teavitusprotsessidesse, nt kuidas ennetada viimasel puhkusel tehtud digifotode kaotsiminekut või kuidas toimida nutitelefoni kaotamise korral.

Teavitusmeetmete teemade määratlemine

Teavituskampaaniad võiksid käsitleda teemasid, mis põhjendavad infoturbe olulisust nii asutusele kui ka selle töötajatele. Siia kuuluvad nt teavitamine päevakohastest ohtudest või õige käitumise treenimine reaalsete turvaintsidentide näitel. Siinkohal tuleks jälgida, et võimalikult paljud teemad oleksid tihedalt seotud nii asutuse kui ka teavitusmeetmete sihtrühmadega. Täiendava materjalina võib kasutada häid teemakohaseid artikleid, samuti võib tuua näiteid teiste sarnaste asutuste kohta.

Materjalide ja metoodika valimine

Materjalide ja metoodika valimisel tuleks lähtuda asutuses juurdunud töökultuurist. Eesmärk on töötajate infoturbealase teadlikkuse suurendamine võimalikult meeldejäävalt ja pikaks ajaks, hoides seejuures kulud kontrolli all. Muu hulgas tähendab see töötajate teadmiste, suhtumise ja oskuste treenimist selles suunas, et nad suudaksid nõrki kohti ja turvaintsidente avastada võimalikult vara ning oleksid võimelised neid olukordi analüüsima ja nendele õigesti reageerima. Selle eesmärgi saavutamiseks tuleb kantseliitlikult sõnastatud juhiste, ülitäpselt sõnastatud ettekirjutuste ja sihtrühmale arusaamatu oskussõnavara asemel kasutada lihtsat ja arusaadavat suhtluskeelt (vt ka M 3.47z IT-turbealased tegevus- ja rollimängud).

Teavitusmeetmete võtmine

Teavitamine ja koolitamine on omavahel tihedalt seotud, mis toetuvad üksteisele ja ka täiendavad teineteist. Infoturbealane teavitustöö peaks motiveerima töötajaid tegutsema (vt M 2.198 Personali teavitamine infoturbe küsimustest). Teavitamisele peavad järgnema koolitusmeetmed, mille eesmärk on õigete käitumismustrite süvendamine (vt M 2.557 Infoturbealase koolitusprogrammi kontseptsioon). Praktikas tähendab see aga koolitajatele rasket ülesannet, kuidas panna töötajaid üleüldse infoturbest huvituma ja kuidas õpetada adekvaatset infoturbealast käitumist. Ilma toetavate meetmeteta hakkab teadmiste tase kohe pärast koolituste toimumist järsult langema. Seetõttu tuleb koolitusmaterjali omandamist toetada, nt

pideva kordamisega (vt M 3.95z Õppematerjali kinnistamine).

Teavitustöö edukuse mõõtmine

Teavitustööle seatud eesmärkide saavutamist ja teavitustöö kvaliteeti tuleb mõõta ja analüüsida. Selleks tuleb teavituskampaaniates osalejate teadmisi hinnata sobivate tunnusnäitajate või kriteeriumite alusel juba enne meetmete võtmist, samuti nende ajal ja pärast meetmete võtmist. Nõnda on võimalik tuvastada, kas teavituskampaania on olnud edukas ja mis suunas areneb töötajate infoturbealane teadlikkus. Lisateavet leiate meetmest M 3.94 Õpitulemuste edukuse mõõtmine ja hindamine .

Teavituskampaania sisu ajakohastamine

Asutuse infoturve on valdkond, mis on pidevas muutumises ja arenemises. Kuna IT-süsteemid, protsessid, tööülesanded ja konkurentsiolukord muutuvad pidevalt, muutuvad koos nendega ka potentsiaalsed ohud, riskid ja nende ennetamiseks vajalikud turbemeetmed. Kindlasti tuleb pöörata tähelepanu ka senise infoturbealase teavitustöö tulemustele, eriti mis puudutab meetmete vältimatut ümbertöötamist juhtudel, kus õpitulemuste mõõtmine ja hindamine näitab, et materjali omandamine töötajate hulgas pole piisav. Neid muudatusi tuleb hoolikalt analüüsida. Teavitusmeetmete sisu tuleb pidevalt ajakohastada.

Kontrollküsimused:

- Kas asutusel on olemas erinevatele sihtrühmadele suunatud infoturbealased teavitusprogrammid?
- Kas teavitusprogrammi kontrollitakse ja täiendatakse pidevalt?

M 2.313 Turvaline sisselogimine internetiteenustesse

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: kasutajad

Paljude Interneti baasil toimivate teenuste kasutamiseks peavad kasutajad ennast eelnevalt sisse logima. Reeglina tuleb selleks sisestada vähemalt kasutajatunnus ja parool, kuid tihti küsitakse sisselogimisel ka rohkem infot nagu nt eesja perekonnanime, tööandjat, meiliaadressi jne. Iga kasutaja peaks täpselt järele mõtlema, milliseid andmeid temalt parasjagu soovitakse, kuna tagajärjeks võivad olla nt soovimatud reklaamikampaaniad. Nende vältimiseks tuleks edastada võimalikult vähe detailset informatsiooni. Peale selle tuleks täpselt läbi lugeda andmekaitset puudutavad viited. Kasutajad peaksid enne igat isikuandmete sisestamist hoolikalt järele mõtlema, kui palju andmeid soovivad nad endast vastavale teenusepakkujale tegelikult edastada ja millise edasise kasutamisega on nad nõustuvad. Kui teenuse kasutamise eelduseks on töötava meiliaadressi olemasolu, saab selleks kasutada nt suvalisi, võibolla tasuta internetiteenuse vahendusel loodavaid meiliaadresse. Kui teatud internetiteenuseid vajatakse regulaarselt tööülesannete täitmiseks, tuleks töötajatele koostada sellekohased kasutussuunised, mis juhendavad, kuidas täita sisselogimise käigus nõutavaid sisestusvälju.

Internetiteenuste kasutamiseks valitud paroolid peaksid olema hoolikalt valitud ja järgima vastavaid ettekirjutusi (vt M 2.11 Paroolide kasutamise reeglid). Ennekõike on oluline, et niisugused paroolid ei kattuks olulisi andmeid kaitsvate paroolidega, nt bürooarvuti paroolidega. Kui sisselogimine eeldab isikuandmete kasutamist, peaks see võimalusel toimuma ainult SSLiga turvatult (vt M 5.66 TLS-i/SSL-i kasutamine). Juhtudel, kus teatud teenuse kasutamine eeldab tundliku info sisestamist ebaturvalise ühenduse vahendusel, tuleks hoolikalt kaaluda, kas niisugust teenust on üleüldse tarvis kasutada. Paljude internetiteenuste puhul on paroolide kasutamine varustatud *recovery* -funktsiooniga, mis pakub abi juhtudeks, kui parool on ununenud. Tihti tuleb selleks vastata mõnele küsimusele. Teenusepakkuja salvestab küsimuse vastuse ning parooli unustamisel esitatakse kasutajale vastav küsimus. Tihti on esitatavad küsimused juba teenusepakkuja poolt kindlaks määratud, küsitakse nt ema või kodulooma nime, lemmikvärvi või sünnikohta. Kahjuks pakuvad vaid vähesed teenusepakkujad võimalust küsimusi ise koostada.

Teadmiseks: paljude *Social Engineering* või *Phishing* rünnete puhul pole küsitud mitte lihtsalt parooli, vaid on jäetud mulje, nagu küsitaks täiesti põhjendatult kodulooma nime või lemmikvärvi. Seetõttu on *recovery* -funktsiooni puhul mõttekas mitte anda ausaid vastuseid, vaid selliseid, millest ükski ründaja ei suudaks mingeid järeldusi teha, kuid mille te ise suudate meelde jätta.

Täiendavad kontrollküsimused:

- Kas internetiteenuste kasutamiseks valitakse teistsugused paroolid kui büroo töökeskkonna kasutamiseks?

M 2.314z Kõrgkäideldava serveriarhitektuuri kasutamine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: IT-turvaosakond, administraator

Tööprotsesside, rakenduste ja teenuste käideldavus sõltub tihti suurel määral ühe tsentraalse serveri töökorrast. Mida rohkem rakendusi vastava serveri all töötab, seda suurem peab olema serveri tõrkekindlus. Serveris on reeglina palju erinevaid potentsiaalseid ohuallikaid (Single Points of Failure) ehk komponente, mille rike võib endaga kaasa tuua terviksüsteemi avarii: CPUd, kõvakettad, toitesüsteem, ventilaatorid, Backplane -d jne. Terviksüsteemi funktsioonide taastamine võib niisugustel juhtudel nõuda väga palju aega. Lisaks varuosade piisava varu hoidmisele võib käideldavuse tõstmiseks kaaluda järgmisi võimalusi:

- Cold-Standby
- Hot-Standby (manuaalne ümberlülitus)
- Cluster (manuaalne ümberlülitus) - Load balanced Cluster ja Failover Cluster

Kõik loetletud tehnikad pakuvad erineva tugevusega käideldavust ning reeglina on need seotud ka erinevate kuludega.

Cold-Standby

Cold-Standby ehk külmad varuseadmed tähendab, et lisaks töötavale süsteemile hoitakse valmis sarnast varusüsteemi, mis ei ole sisse lülitatud. Süsteemi avarii korral on võimalik käsitsi käivitada varusüsteem ja see võrgu alla integreerida. Kui võtta aluseks üksikute asenduskomponentide piisava varu hoidmine, on siinkohal tegemist kõige lihtsama liiasust pakkuva süsteemilahendusega, millel on nii omad eelised kui ka puudused.

Cold-Standby varusüsteemi eelised	Cold-Standby varusüsteemi puudused

- Cold-Standby lahenduste rakendamisel ei suurene terviksüsteemi keerukus. - Cold-Standby süsteemi kulusid arvestades peab silmas pidama vaid lisariistvaraga seotud kulutusi, mistõttu on see kõikidest võimalikest variantidest kõige soodsam. - Süsteemide uuesti ülesehitamine ja muutmine on võimalik ilma käideldavuse langemiseta. Igapäevakasutuseks vajalikud funktsioonid lülitatakse selleks lihtsalt Cold-Standby süsteemile ümber.	- Lisaks olemasolevale süsteemile tuleb valmis hoida teine samasugune süsteem. - Ka varusüsteemi konfiguratsiooni ja täiendeid tuleb jooksvalt uuendada. - Kuna varusüsteem tuleb sisse lülitada käsitsi, peavad administraatorid pidevalt jälgima põhisüsteemi, et avarii puhul sekkuda. - Kui rakendusandmed ei asu välises salvestussüsteemis, mis tähendab, et juurdepääs on võimalik otse läbi varusüsteemi, tuleb need migreerida Cold-Standby süsteemi alla.

Tabel: Cold-Standby varusüsteemi eelised ja puudused

Antud lahendus sobib sellisteks kasutusjuhtudeks, kus lühikesed või piiratud seisakuajad, kuni administraator vajalikul moel sekkub, ei too endaga kaasa kriitilisi olukordi. Näited:

- Väikeste võrkude (intraneti) server
- Vähekülastatavad internetiserverid

Hot-Standby (manuaalne ümberlülitus)

Hot-Standby lahenduse puhul hoitakse lisaks põhisüsteemile samuti varusüsteemi, kuid see on sisse lülitatud ja töötab paralleelselt koos põhisüsteemiga. Põhisüsteemi funktsioone jälgitakse ning avarii korral lülitub kasutusse paralleelsüsteem. Vahetumine võib toimuda nii automaatselt kui ka käsitsi. Automaatse ümberlülituse tarbeks peab süsteem olema varustatud täiendavate funktsioonidega nagu nt automaatse rikketuvastusega. Vastavaid lahendusi käsitletakse lähemalt alalõigus Cluster. Võimalikult lühikeste seisakuaegade tagamiseks tuleb varusüsteemi seisundit pidevat kontrollida

Hot-Standby varusüsteemi eelised	Hot-Standby varusüsteemi puudused

- Seisakuajad on võrreldes Cold-Standby lahendustega palju lühemad. - Sarnaselt Cold-Standby süsteemile on antud lahendus võrreldes järgnevalt vaadeldavate kõrgkäideldavust tagavate lahendusega suhteliselt soodne. - Varusüsteemi hoitakse töös ning seda on võimalik kasutada ka andmete paljundamiseks. - Süsteemide uuesti ülesehitamine ja muutmine on võimalik ilma käideldavuse langemiseta. Igapäevakasutuseks vajalikud funktsioonid lülitatakse selleks lihtsalt Hot-Standby süsteemile ümber.	- Kas selle lahenduse puhul on olemasolevast riistvarast kasutuses alati vaid pool. - Varusüsteemi tuleb jooksvalt uuendada. - Hot-Standby süsteemi käsitsi ümberlülituse valimine eeldab, et süsteemi eest vastutav töötaja peab seda pidevalt jälgima.

Tabel: Hot-Standby varusüsteemi eelised ja puudused

Hot-Standby süsteemi sobib kasutada niisuguste lahenduste puhul, kus lühikesed seisakuajad ei too endaga kaasa kriitilisi olukordi. Muuhulgas tuleb läbi mõelda ka Hot-Standby serveri süsteemiseire ja ümberlülitusega seotud probleemistik. Võimalikud kasutusvaldkonnad on näiteks:

- Tihti muutuva sisuga veebiserverid
- Väikeste võrkude serverid (Application-serverid, meiliserverid)
- Andmebaasiserverid ja failiserverid (nt lisaserverid peamise serveri pidevaks toetamiseks, mis lülitatakse vajadusel ümber peaserveri funktsioonidesse.

Cluster (manuaalne ümberlülitus)

Cluster moodustub arvutite grupist, mis sisaldab kahte või enamat paralleelselt töötavat arvutit, eesmärgiga suurendada rakenduse või teenuse käideldavust või jõudlust. Rakendusi ja teenuseid on võimalik aktiivselt teostada nii ühel arvutil kui ka mitme arvuti vahel jagatult (jõudluse tõstmine). Sõltuvalt funktsioonist eristatakse:

- Load balanced Cluster
- Failover Cluster

Lahendused

Load balanced Cluster

Load balanced Cluster lahenduse puhul jagatakse rakenduse või teenuse etapid sõltuvalt serverite koormusele serverite vahel ära. Kui rakendus või teenus seda võimaldab, saab lisaks koormuse jaotamisele (Load Balancing) ja seeläbi kasvavale jõudlusele niimoodi vähendada avariidega seotud probleeme. Koormuse jaotamise funktsiooni üheks eelduseks on, et vastavate rakenduste ja teenuste puhul ei tohi tarvis minna kirjutusõigusega juurdepääse. Süsteemi liiasust saab niisugustel juhtudel luua seeläbi, et sarnase võimusega süsteemid asetatakse Load-Balancing protsessi abil „teineteise kõrvale“, hoolitsedes selle eest, et ühe serveri väljalangemisel oleksid teised serverid võimelised selle funktsioone üle võtma.

Load balanced Cluster süsteemi eelised	Load balanced Cluster süsteemi puudused
- Antud lahendus pakub võimalust tõsta nii käideldavust kui ka jõudlust. - Kõik olemasolevad ressursid on pidevalt rakenduses. - Lahendus on suuresti skaleeritav. - Terviksüsteemi keerukus on madalam kui Failover Cluster süsteemi puhul.	- Antud lahendust ei saa rakendada kõikide rakendusliikide puhul. Load Balancing lahenduse kasutamiseks ei sobi eelkõige sellised rakendused, mis kasutavad peale puhta kirjutusjuurdepääsu ka muid juurdepääsu liike ja vajavad kõikide serverite samaaegset juurdepääsu samadele salvestusressurssidele.

Tabel: Load balanced Cluster süsteemi eelised ja puudused

Load balanced Cluster on optimaalne lahendus neis kasutusvaldkondades, kus lisaks käideldavusele omab suurt tähtsust ka süsteemi jõudlus ning kus rakendused võimaldavad oma funktsioone laiali jaotada. Sellised kasutusvaldkonnad on näiteks veebiserverid, eranditult vaid kirjutusjuurdepääsudega Front-end rakendused (nt Web-Server-Farmes) Failover Cluster.

Failover Cluster lahendusega on tegu siis, kui teatud Cluster -süsteemi ühe osa avarii korral võtab mõni teine Cluster i osa avariilise rakenduse või teenuse funktsioonid üle automaatselt (Takeover). Teenuste automaatset ülevõtmist funktsioonilt võrdse komponendi poolt juhul, kui süsteemi teatud komponendis tekib avarii, nimetatakse Failover . Failover -funktsioonide puhul rakendatakse enamasti eraldiseisvat „ heartbeat “ (südamelöök) ühendust, mis tagab Cluster

-serverite vahelise kommunikatsiooni. Võimaldamaks avarii korral otsest juurdepääsu, peab Cluster -serveritel olema lisaks klient-võrguga ühendusele ka eraldiseisev ühendus haldusvõrguga. Automaatne Failover funktsioon eeldab kõikide tarkvara- ja riistvarakomponentide sobilikku seiret. Seetõttu on oluline kindlaks teha, et Failover mehhanismi funktsioon ei põhineks valedel oletustel. Failover-Cluster -süsteemi rakendamisel tuleb arvestada järgnevate punktidega:

- Juurdepääs ühisele salvestile: Lisaks serveri oma kõvaketastele, mis sisaldavad operatsioonisüsteemi ja käitamiseks vajalikke andmeid, on Cluster lahenduse puhul mõttekas salvestada rakendusandmed ühisesse salvestisse. Juurdepääs neile kõvaketastele võimaldatakse ainult sellele Cluster i osale, mis parasjagu töötab. Lisaks ühistele kõvaketastele on võimalik kasutada ka tiražeeritud kõvakettaid. See on mõttekas neil juhtudel, kui Failover peab toimima kuskilt eemalolevast asukohast. Lokaalse Failover lahenduse puhul tuleks kaaluda, kas tiražeerimisega kaasnev süsteemi keerukus ja sellega seotud sõltuvus ei kujuta endast mitte lisaohtu vajaminevale käideldavusele.

- Rakenduse ülekandmisvõimalused: Ühe rakenduse installeerimine paralleelselt kahele või rohkemale serverile korraga eeldab enamasti täiendavate litsentside olemasolu. Lisaks sellele on tarvis kontrollida, kas vastav rakendus üldse võimaldab rakendada Failover -funktsioone.

- NSPoF (No Single Points of Failure): Kui Cluster -lahenduse Failover -funktsiooni toimimist on võimalik mõne üksiku komponendi avariiga takistada, loob see vastuolu Cluster -arhitektuuri tegeliku eesmärgiga. Vältimaks Single Points of Failure võimalikkust, tuleb analüüsida terviksüsteemi ja üksikkomponentide (võrgukomponentide, süsteemimälu, põhimälu, võrgukaartide, kommutaatorite, jaoturite jms) avarii tekkevõimalusi.

- Operatsioonisüsteem ja Cluster -serverite konfiguratsioonid: Kõigil Cluster -serveritel peaks olema ühesugused operatsioonisüsteemi versioonid, täiendid, teegid ja rakenduste versioonid. Võimalikult ühesugune riistvara- ja tarkvarakonfiguratsioon aitab Failover funktsiooni töölelülitumisel tagada süsteemi võimalikult sarnase edasitoimimise. Lisaks väheneb identsete süsteemide puhul ka terviksüsteemi keerukus (kasutatakse ühesugust Failover -tarkvara, ühesuguseid võrguliideseid, ühine salvestisüsteem ühildub kõikide süsteemidega, ühtmoodi haldamine ja hooldamine).

- Eraldiseisvad ja liiasusega ühendused serverite vahel: Cluster -serverite vaheline side peaks toimima sõltumata võrgu koormusest võimalikult takistusteta, et Failover -protsess saaks toimuda võimalikult ruttu. Kuna käideldavusele esitatavad nõuded on kõrged, on ka liiasus siinkohal vajalik.

- Toimivate tarkvaratoodete kasutamine Failover protsessi juhtimiseks: Otsus, kas Failover peaks aset leidma või mitte, on väga keeruline. Uued endaarendatud tarkvaratööriistad võivad sisaldada vigu, millega võib kaasneda terviksüsteemi käideldavuse langus.

- Kõikvõimalike Failover aspektide hoolikas testimine: Põhjalik testimine on muuhulgas väga vajalik ka selleks, et välistada igasuguste ootamatute veaallikate (Single Points of Failure) teke. Eriti hoolikalt tuleb kõikvõimalike vigade suhtes testida serverite seiresüsteemi ja Failover -juhtimissüsteemi.

Failover Clusters süsteemi eelised	Failover Clusters süsteemi puudused
- Tänu automaatselt toimivale Takeover funktsioonile on võimalik märkimisväärselt tõsta süsteemi käideldavust. - Käsitsi sekkumine ei ole vajalik.	- Lahendus on väga keeruline. - Failover Cluster lahendusi ei saa hästi skaleerida. - Pidevas kasutuses on ainult üks osa ressurssidest. - Täiendav riistvara ja tarkvara viib suurte kulutusteni.

Tabel: Failover Cluster süsteemi eelised ja puudused

Nagu eelnevast eeliseid ja puudusi kõrvutavast tabelist näha, on Failover Cluster süsteemi mõttekas rakendada vaid siis, kui ühele või enamale rakendusele kehtivad väga kõrged käideldavusnõuded. Lisaks suurtele kuludele tuleb arvestada, et vastutavatel töötajatel peavad olema väga head erialateadmised nii kasutatavatest operatsioonisüsteemidest ja rakendustest kui ka Failover -funktsioonidest. Lisaks on Failover lahendusi mõttekas serverite puhul rakendada vaid siis, kui ka kõik ülejäänud sõltuvad komponendid nagu nt võrguühendused või klientide käideldavus on varustatud vastava liiasusega. Erinevateks kasutusvaldkondadeks, kus kõrge käideldavuse puhul rakendatakse reeglina Failover Cluster lahendusi on näiteks:

- andmebaasi rakendused
- File Storage
- dünaamilise sisuga rakendused
- meiliserverid

Kui igapäevatöö, rakendused või teenused esitavad käideldavusele kõrgeid nõudeid, tuleks kindlasti mõelda, mille abil vastavaid nõudeid realiseerida. IT ja IT-turbe eest vastutavad töötajad peaksid niisuguste serverite jaoks välja töötama kontseptsioonid ja valima nende jaoks sobiliku arhitektuuri.

Täiendavad kontrollküsimused:

- Millised liiasused on loodud kõrgete käideldavusnõuetega serveritele?
- Kas teenuste või rakenduste käsitsi ümberlülitamise puhul on tagatud, et käideldavus säilib?

- Kuidas tagatakse, et Failover funktsioon lülitub tööle ainult siis, kui see on hädavajalik?

M 2.315 Serveri kasutuselevõtu planeerimine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: IT-juht, administraator

Serverite turvalise käitamise üheks põhjapanevaks eelduseks on piisavas mahus läbi viidud planeerimistöö. Serveri kasutuselevõtu planeerimine võib toimuda mitmes etapis vastavalt *Top-Down* -visandi printsiibile: terviksüsteemi kontseptsiooni visandi alusel määratakse kindlaks spetsiifiliste osakontseptsioonide koostamiseks vajalik konkreetne planeerimistöö. Planeerimine ei hõlma endas aga mitte ainult neid valdkondi, mida seostatakse turbega selle klassikalises tähenduses, vaid ka täiesti tavapäraseid igapäevatöös kajastuvaid aspekte, mis samuti mõjutavad turvalisust.

Üldkontseptsioon

Üldkontseptsioonis tuleks leida vastused näiteks järgnevatele tüüpilistele küsimustele:

- Milliseid ülesandeid peaks planeeritav süsteem suutma täita? Millised teenuseid peaks server võimaldama kasutada? Kas süsteemi käideldavusele seatakse mingisuguseid erinõudeid või on erisoove seoses salvestatud või töödeldavate andmete konfidentsiaalsuse või tervikluse tagamisega? Loetletud eeldused töötatakse välja üldise planeerimistöö raames ning nende sisu lähtub üldistest eemärkidest. Mida täpsemalt on teada raamtingimused ning mida täpsemini on sõnastatud eeldused, seda lihtsamaks muutuvad kõik edasised planeerimisetapid.
- Kas süsteemis tuleks rakendada teatud kindlat liiki riistvarakomponente? Antud tingimus võib olla oluline näiteks operatsioonisüsteemi valikul.
- Milliseid üldtingimustest tulenevaid nõudeid tuleb arvestada riistvara puhul (CPU, töömälu, kõvaketaste mahu, võrgu koormustaluvuse puhul).
- Kas serveri rakenduskeskkonna puhul on tegemist homogeense või heterogeense arvutivõrguga?
- Kas uut süsteemi on tarvis vananenud või olemasoleva süsteemi asendamiseks? Kas uus süsteem peaks suutma vana süsteemi andmebaase või riistvarakomponente üle võtta?
- Kas arvutitele peaks olema võimalik installeerida ka täiendavaid operatsioonisüsteeme *Multiboot* funktsiooni abil?

Osakontseptsioonid

Serveri kasutuselevõtu planeerimisel tuleks arvestada järgmiste osakontseptsioonidega:

- Autentimine ja kasutajate haldamine: Millist tüüpi kasutajate haldamist ja kasutajate autentimist soovitakse süsteemis kasutada? Kas kasutajaid soovitakse hallata ainult lokaalselt või tahetakse kasutada tsentraliseeritud haldamissüsteemi? Kas süsteem peaks suutma rakendada ka tsentraliseeritud võrgupõhist autentimisteenust või vajatakse ainult lokaalset autentimisteenust? Täiendavat infot autentimismehhanismide kohta leiate M 4.133 Sobivate autentimismehhanismide valimine .

- Kasutaja- ja rühmakontseptsioon: Võttes aluseks üleorganisatsioonilised kasutajaid, nende õigusi ja töörollide jaotumist käsitlevad kontseptsioonid, tuleb süsteemi jaoks koostada vastavad reeglid (vt M 2.30 Kasutajate ja kasutajarühmade määramise protseduurid ja M 2.31 Volitatud kasutajate ja õiguste profiilide dokumenteerimine).
- Haldamine: Kuidas peaks toimuma süsteemi haldamine? Kas kõik seadistused tehakse lokaalselt või integreeritakse vastav server tsentraliseeritud haldamist ja konfigureerimist juhtiva süsteemi alla?

Programmide, süsteemi- ja kasutajaandmete lahushoidmine

- Partitsiooni- ja failisüsteemi *Layout*: Planeerimisfaasis tuleks koostada esimesed hinnangud selle kohta, kui palju oleks süsteemile tarvis kettaruumi. Haldamise ja hooldamise lihtsustamiseks on soovitatav, nii palju kui see on võimalik, eraldada üksteisest operatsioonisüsteem (süsteemi programmid ja konfiguratsioon), rakendusprogrammid ja rakenduste andmed (nt andmebaasiserverid ja andmed) ning vajadusel ka kasutajaandmed. Erinevad operatsioonisüsteemid pakuvad selleks erinevaid lahendusi (partitsioonideks jagamine Windowsi all, failisüsteemi Unixi all). Tihti võib olla mõttekas salvestada teatud liiki andmed isegi eraldi kõvaketta eraldi kettasüsteemile. Niiviisi on võimalik nt reinstalleerimise või süsteemi uuendamise järel hakata teiste partitsioonide andmeid kohe kasutama, ilma et neid oleks tarvis ümber kopeerida.

Kõrge turbeastme korral tuleks võimalusel lubada ainult krüpteeritud failisüsteeme

Serverites, kuhu tahetakse salvestada andmeid, mille puhul kehtivad konfidentsiaalsusest tingitud kõrged turbenõuded, soovitatakse ilmtingimata rakendada krüpteeritud failisüsteeme. Siinkohal pole ilmtingimata vajalik, et kõik failisüsteemid oleks varustatud krüpteeringuga. Sageli piisab ka sellest, kui krüpteeritult töötab vaid see konkreetne failisüsteemi osa, kuhu andmeid reaalselt salvestatakse. Selle tagamiseks tuleb tegeleda vastava partitsiooni- ja failisüsteemi *Layouti* planeerimisega. Üksikfailide ja -kataloogide jaoks sobilike krüpteerimisprotseduuride valikul tuleks piirata kasutajate võimalusi, st kasutajad ei tohiks olla võimalust valida, kas salvestada andmed krüpteeritult või krüpteerimata. Planeerimisfaasis tuleks dokumenteerida partitsioonideks jaotamise kava ja partistsioonide ettenähtud suurused.

Võrguteenused ja võrguühendus

Serveri võrguühenduse planeerimisel tuleb lähtuda serverile salvestatavate või seal töödeldavate andmete konfidentsiaalsusele, terviklusele ja käideldavusele esitatavatest nõuetest. Üldjuhul soovitatakse mitte ühendada serverit samasse IP-allvõrku koos klientidega, kes vastavat serverit kasutama hakkavad. Neil juhtudel, kui server on klientidest lahutatud vähemalt marsruuteri abil, tekivad palju paremad võimalused juurdepääsude juhtimiseks ja võimalikele probleemidele viitavate võrguliikluse anomaaliate tuvastamiseks.

Kõrge turbevajaduse puhul eraldi osavõrk ja paketifilter

Server, kuhu salvestatakse või kus töödeldakse andmeid, millele kehtivad seoses andmete konfidentsiaalsuse või tervikluse tagamisega kõrged turbenõuded,

peaks olema paigutatud eraldi IP-alamvõrku ning olema ülejäänud võrgust eraldatud vähemalt ühe paketifiltriga. Väga kõrge kaitsevajaduse korral tuleks kasutusele võtta *Application Level Gateway*. Tavalise kaitsevajaduse korral võib serveri, mida kasutavad ainult sisevõrgu kliendid, erandkorras paigutada ka samasse alamvõrku koos klientidega. Siiski soovitatakse ka niisugustel kasutusjuhtudel enne võrgustruktuuri muutusi paigutada server siiski eraldiseisvasse alamvõrku.

Sõltuvussuhetega arvestamine

Sõltuvalt arvuti puhul kindlaksmääratud kasutusvaldkonnast võib vajadusel tarvis minna juurdepääse erinevatele teenustele (nt veebi-, faili-, andmebaasi-, prindi-, DNS või meiliserveri teenustele). Hilisemate probleemide, nt liiga väikese edastusvõimuse või vaheleühendatud turvalüüsidest põhjustatud raskuste ennetamiseks tuleb loetletud vajadustega arvestada juba planeerimisfaasis.

Haldamiseks jms vajalikud lisateenused

Lisaks vajaminevale teenusele, milleks server kasutusele võetakse, läheb tihti tarvis ka veel lisateenuseid, mille abil saab serverit efektiivselt kasutada ja hallata. Näiteks võrgu baasil toimiva halduse jaoks läheb tarvis turvalist juurdepääsu (näiteks SSH, vt M 5.64 Secure Shell (SSH)), või on veebilehele üleslaetavaid andmeid tarvis võrgu kaudu üle kanda veebiserverisse. Kui niisugustest vajadustest tekkiv võrguside liigub läbi ebaturvaliste võrkude, tuleb rakendada sobivaid turvalisi protokolle. Lisaks sellele tuleb tagada, et teenuseid saaksid kasutada ainult volitatud kasutajad ja arvutid. Selleks võib kasutada paroolide jagamist, rakendada paketifiltrit, (vt M 4.238 Lokaalse paketifiltri rakendamine või B 3.301 Turvalüüs (tulemüür)) või ka teisi sobilikke mehhanisme. Mitte ühegi teenuse kasutamist ei tohiks võimaldada ebaturvalise võrgu nagu nt Interneti vahendusel, välja arvatud juhtudel, kus see on konkreetselt niimoodi ette nähtud.

Võrguteenuste ja võrguühenduste kohta tuleb luua ülevaade

Planeerimisfaasis tuleks luua ülevaade ettenähtud ja vajalike võrguteenuste ning nendega seoses vajaminevate võrguühenduste kohta. Enamikel juhtudel tuleb juba planeerimisfaasis mõelda ka sellele, kui palju tohib süsteem sõltuda võrguühenduse funktsioneerimisest.

- Tunnel või VPN: Juhtudel, kus juba planeerimisfaasis võib oletada, et süsteemile on tarvis ligi pääseda läbi ebaturvaliste võrkude, tuleks juba võimalikult varakult hakata otsima selleks sobivaid lahendusi. Juurdepääsu võib lahendada nt VPNi abil.
- Seire: Süsteemi käideldavuse ning süsteemi ja selle poolt pakutavate teenuste koormuse jälgimiseks võiks kasutada sobivat seiresüsteemi. Selleks tuleb ühele täiendavale serverile installeerida *Monitoring-Daemon*, kellele teatud lokaalne *Agent* edastab vastavad seireandmed. Lisaks on võimalik jälgida ka väliste süsteemide poolt pakutavate võrguteenuste kasutamisega seotud tegevusi. Probleemide korral võib nt automaatselt laekuda teade mõnele administraatorile.
- Logimine: Kasutatud teenused ja süsteemi poolt edastatud teated peaksid kajastuma logis, kuna vastav info on väga oluline veadiagnostikaks, rikete kõrvaldamiseks, samuti võimalikke rünnete tuvastamiseks ja rünnetega seotud asjaolude väljaselgitamiseks. Planeerimisfaasis tuleks otsustada, millist infot peaksid logid kajastama ja kui kaua tuleb vastavaid logiandmeid säilitada. Lisaks sellele tuleb otsustada, kas logianded tuleks salvestada lokaalselt või tsentraalsesse logiserversisse, mis asub võrgus.

Logifailide kontrollimiseks tuleb määrata tähtajad

Logiandmete kontrollimisele oleks mõistlik mõelda juba planeerimisfaasis, st tuleks kindlaks määrata, kuidas ja milliste ajavahemike tagant vastavaid andmeid tuleb läbi töötada.

Kõrge käideldavus

Kui süsteemi või selle poolt pakutavate teenuste käideldavusele seatakse kõrgeid nõudeid, tuleks juba planeerimisfaasis mõelda, kuidas vastavaid nõudeid kõigi paremini täita (vt M 6.43 Liiasusega Windowsi serverid).

Kõik planeerimisfaasis vastuvõetud otsused tuleb dokumenteerida selliselt, et vastavate otsuste langetamise põhjused oleksid arusaadavad ka tulevikus. Siinjuures on oluline arvestada, et vastavat infot peaksid suutma kasutada ka kõik teised, mitte ainult selle kirjapanija. Seetõttu on oluline jälgida, et vastav info oleks piisavalt struktureeritud ja arusaadav.

Täiendavad kontrollküsimused:

- Milline dokumentatsioon eksisteerib serveri kasutuselevõtu planeerimise kohta?

M 2.316 Serveri turvapoliitika kehtestamine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: IT-juht, IT-turvaosakond, administraator

Kõikidele serveritele kehtivate turvanõuete aluseks on üleorganisatsiooniline turvapoliitika. Üldises turvapoliitikas kajastuvaid nõudeid tuleb antud konteksti jaoks täpsustada ja koostada eraldi serverit või serverirühma kajastav turvapoliitika. Sellega seoses tuleb kontrollida, kas lisaks tervet organisatsiooni hõlmavale turvapoliitikale on tarvis arvestada ka muude, hierarhias kõrgemalseisvate nõuetega nagu nt IT-turvapoliitika, paroolisuuniste või internetikasutuse nõuetega. Kõik serveri soetamisega ja käitamisega seotud isikud peavad tundma turvapoliitikat ning oma töös sellest lähtuma. Nagu kõikide suuniste puhul, tuleb nende sisu ja rakendamist regulaarselt üldise auditi käigus kontrollida. Turvapoliitika peab täpsustama üldeesmärgiks seatud turbeastme ja sisaldama põhjapanevat infot serverite käitamise kohta. Ülevaatlikkuse parandamiseks võib olla mõttekas koostada erinevate kasutusvaldkondade jaoks spetsiaalsed turvapoliitikad.

Üldstrateegia: kas liberaalne või piirav?

Esimese asjana tuleks otsustada, kas konfigureerimise ja halduse üldstrateegia lähtub printsiibist „liberaalne“ või „piirav“, kuna kõik edasised otsused sõltuvad suurel määral sellest valikust. Serverite puhul, mis salvestavad ja töötlevad andmeid ainult tavalises turbeastmes, võib valida suhteliselt liberaalse üldstrateegia, mis lihtsustab paljudel juhtudel nende konfigureerimist ja haldamist. Siiski on ka niisugustel kasutusjuhtudel siiski soovitatav, et strateegia oleks „ainult nii liberaalne kui parasjagu vajalik“. Serverite puhul, mis salvestavad või töötlevad kõrge turbeastmega andmeid, soovitatakse enamasti valida piirav üldstrateegia. Eriti kõrges turbeastmes töötavate serverite puhul tuleks kolmest peamisest aspektist vähemalt ühe jaoks valida piirangutest lähtuv konfigureerimis- ja haldusstrateegia. Järgnevalt on loetletud mõned punktid, millega tuleks arvestada:

Füüsilise juurdepääsukontrolli reguleerimine: Server tuleks üldjuhul üles seada või paigaldada ainult suletavasse serveriruumi või serverikappi. Lisaks on tarvis kindlaks määrata, kellel on õigus vastavasse ruumi siseneda, st kellel on serveritele juurdepääs.

Administraatorite ja auditeerijate töö reeglid:

- Millise skeemi järgi jagatakse administreerimisõiguseid? Millised on erinevatele administraatoritele jagatavad õigused ning kuidas toimub nende õiguste saamine?
- Milliste juurdepääsude kaudu tohivad administraatorid ja auditeerijad süsteemidele ligi pääseda (nt ainult kohapealsest konsoolist, eraldi administreerimisvõrgu kaudu või krüpteeritud ühenduste kaudu)?
- Millised toimingud tuleb dokumenteerida? Millisel kujul luuakse dokumentatsioon ja kuidas seda hooldatakse?
- Kas teatud muudatuste puhul on kohustuslik järgida nelja silma põhimõtet?

Installeerimise ja aluskonfiguratsiooni nõuded

- Milliseid andmeallikaid kasutatakse installeerimiseks?
- Kas kasutajate haldamine ja autentimine peaks toimuma kohapeal või on tarvis rakendada tsentraliseeritud autentimisteenust?

- Kasutajate ja töörollide haldamise reeglid, volituste struktuurid (autentimise ja volitamise toimimine ja meetodid, volitused installeerimiseks, täiendite laadimiseks, konfiguratsiooni muutmiseks jne). Võimalusel tuleks administreerimiseks välja töötada töörollide jaotamise kontseptsioon.

Installeeritavatele tarkvarapakettidele esitatavad nõuded

- Juhul kui planeerimisfaasis võeti vastu otsus, et teatud failisüsteemi osad tuleb varustada krüpteeringuga, on siinkohal soovitatav kindlaks määrata, kuidas see lahendus realiseeritakse:
- Milliseid failisüsteemi osi on tarvis krüpteerida?
- Millist mehhanismi tuleks kasutada krüpteeritud failisüsteemi integreerimiseks?
- Milliseid krüpteerimisalgoritme ja kui pikki võtmeid tuleks kasutada?
- Millist liiki andmeid hakatakse salvestama krüpteeritud failisüsteemidesse?
- Kuidas toimub krüpteeritud failisüsteemide kaasamine varundamise alla?

Krüpteeritud failisüsteemid vajavad kõrgendatud tähelepanu

Krüpteeritud failisüsteemide rakendamisel on selle jaoks soovitatav luua eraldi kontseptsioon ja dokumenteerida hoolikalt kõik konfiguratsiooni puudutavad detailid, kuna vastasel korral võivad probleemide esinemisel (nt võtme või võtme parooli kadumisel, ebakorrektse konfiguratsiooni jms korral) failisüsteemis olnud andmed täielikult kaduma minna:

Reeglid dokumentatsiooni koostamise ja haldamise kohta

Turvalise käitamise nõuded

- Millistel kasutajatel on lubatud ennast lokaalselt süsteemi sisse logida?
- Millistele kasutajatele antakse võrgu kaudu toimiv juurdepääs? Milliseid protokolle tohib kasutada?
- Millistele ressurssidele tohivad kasutajad ligi pääseda?
- Paroolikasutuse nõuded (paroolireeglid, paroolimuudatuste reeglid ja olukorrad, vajadusel paroolide deponeerimine).
- Kelle on õigus süsteem välja lülitada?

Võrguside ja võrguteenused

- Kas on tarvis kasutada lokaalseid paketifiltreid?
- Millised võrguteenuseid peaks server võimaldama?
- Millised autentimisprotseduurid tuleks valida pakutavate teenuste kasutamiseks?
- Millistele välistele võrgupõhistele teenustele tohib arvutist ligi pääseda?
- Kas on tarvis integreerida osadeks jaotatud failisüsteemi?

Ettevaatust osadeks jaotatud failisüsteemide kasutamisel

Osadeks jaotatud failisüsteemi, mille puhul kasutajaandmed edastatakse krüpteerimata, tuleks kasutada ainult sisevõrkudes. Kui osadeks jaotatud failisüsteemi on tarvis kasutada läbi ebaturvalise võrgu, tuleb selleks rakendada sobivaid kaitsemeetmeid (krüptograafiliselt kaitstud VPN, tunneldamine).

Logimine

- Millised sündmused logitakse?
- Kuhu salvestatakse logifailid? Kas logifailid tuleb salvestada lokaalselt või tuleks kasutada tsentraliseeritud serverlahendust, kuhu kõik võrgus olevad süsteemid oma logiandmed edasi saadavad?
- Kuidas ja kui sageli toimub logide analüüsimine?
- Kellel on juurdepääs logifailidele?
- Kas on tagatud, et isikuandmeid sisaldav info ei satuks volitamata isikute kätte?
- Kui pikaks ajaks tuleks säilitada logifailid?

Eelnevalt loetletud punktide abil saab koostada kontrollnimekirja, millest võib olla palju abi auditite ja revisjonide puhul. Turvapoliitika eest vastutab IT-turvaosakond, seega tuleb kõik turvapoliitika muudatused ja kõrvalekalded kooskõlastada IT-turvaosakonnaga. Turvapoliitika koostamisel on süsteemide turvalisuse tagamiseks soovitatav esmalt välja töötada maksimaalselt palju erinevaid nõudeid ja ettekirjutusi. Seejärel saab neid hakata viima vastavusse tegelike oludega. Ideaaljuhul aitab niisugune lähenemine arvestada kõikide võimalike aspektidega. Iga väljatöötatud nõude puhul, mis teise tööetapi käigus kõrvale jäetakse või pehmendatakse, tuleb dokumenteerida selle kõrvalejätmise põhjus.

Täiendavad kontrollküsimused:

- Kas serverite kasutamise kohta on koostatud vastav turvapoliitika?
- Millisel kujul on koostatud turvapoliitika dokumentatsioon?
- Millal toimus viimati turvapoliitika uuendamine?
- Kas turvapoliitikas on sõnastatud ka turbeaste?

M 2.317 Serveri soetamise kriteeriumid

Algatamise eest vastutavad: IT-juht, IT-turbespetsialist

Rakendamise eest vastutavad: varustaja

Serveri soetamisel on tarvis tähelepanu pöörata nii riistvarale kui ka tarkvarale, millest server üles ehitatakse. Serveri soetamisel tehtud vead võivad olulisel määral mõjutada võrgu turvalist käitamist, sest sobimatu riist- ja tarkvara ei pruugi saavutada üldist, eesmärgiks seatud turbeastet. Enne serveri soetamist tuleb seetõttu koostada nõuete nimekiri, mille alusel oleks võimalik pakutavaid tooteid üksteisega kõrvutada. Läbiviidud võrdlusele toetudes saab toote soetamisel olla kindel, et vastav server suudab kõiki vajalikke nõudeid ka reaalselt oma töös täita. IT-turvalisust võivad mõjutada ka serverite erinevate funktsioonide omadused. Tavaliselt on sellest mõjutatud üks peamisi näitajaid nagu käideldavus, näiteks kui server ei saavuta ebapiisava mälumahu tõttu kas nõutud reaktsiooniaega või läbilaskevõimet. Lisaks ei tohi unustada ka tootjapoolset tuge, näiteks kui turvaaukude lappimiseks läheb kiirkorras tarvis vastavaid paiku.

Kesksed turvanõuded

IT-turbest lähtuvalt on serveritele esitatavad peamised nõuded järgnevad:

- rakendatav riistvara ja tarkvara peab olema selline, mis võimaldaks saavutada serveri käideldavusele ja andmete terviklusele seatud nõudeid,
- serveri haldamisel peab olema võimalik rakendada turvalisi protokolle,
- kasutajate haldamiseks peab olema võimalik rakendada üleorganisatsioonilist töörollide jaotamise kontseptsiooni ning
- eriti tundlikke andmeid peab saama vajadusel krüpteerida.

Järgnevalt on loetletud erinevad nõuded, mida võiks serverite soetamisel silmas pidada.

1. Peamised funktsioonidele esitatavad nõuded

- Kas seade toetab kõiki vajaminevaid riistvaraliideseid?
- Kas tarkvara toetab kõiki vajaminevaid protokolle ja failiformaate?

2. Turvalisus

- Kas süsteem toetab turvalist administreerimist võimaldavaid protokolle? Kui servereid ei hallata eraldiseisva haldamisvõrgu kaudu, tuleb haldamiseks kasutada piisavalt turvalisi võrguprotokolle.

3. Hooldamine

- Kas tootja pakub tarkvara jaoks regulaarselt täiendeid ja kiirelt kättesaadavaid turvapaiku? Eriti oluline on, et tooja reageeriks avastatud turvaaukudele võimalikult kiiresti.
- Kas toote osas on võimalik sõlmida hooldusleping? Sageli pääseb tootjapoolsetele täienditele ja tugiteenustele ligi ainult kehtiva hooldusleping alusel.
- Kas hooldusleping on võimalik kindlaks määrata maksimaalne aeg, mis tohib kuluda probleemi kõrvaldamisele? Hooldusleping on kasulik ainult siis, kui garanteeritud reageerimis- ja tööprotsesside taastamisaegadega suudetakse täita seadmetele kehtestatud käideldavusnõudeid.

- Kas tootja pakub ka tehnilist klienditeenindust (infoliini teenust), mis oleks võimeline probleemide korral kohe abi pakkuma? Käesolev punkt peaks kajastuma sõlmitud hoolduslepingus. Lepingu sõlmimisel tuleb jälgida, mis keeles pakutakse tootjapoolset infoliini teenust.

4. Usaldusväärsus/rikkekindlus

- Kas riistvara- ja tarkvara kohta on võimalik hankida usaldusväärset infot, mis käsitleks nende usaldusväärsust ja tõrkekindlust?
- Kas tootja pakub vajadusel ka kõrge käideldavusega lahendusi? Neil juhtudel, kui käideldavusele seatud nõudmisi ei ole võimalik tagada hooldelepingute sõlmimisega, tuleks valida selline süsteem, mis toetaks kõrgkäideldavust tagavaid lahendusi.

5. Kasutajasõbralikkus

- Kas toote installeerimine, konfigureerimine, haldamine ja kasutamine on lihtne? Lisaks peaks olema võimalik läbida toodet käsitlevaid koolitusi.

6. Kulutused

- Kui suurte kulutustega tuleb arvestada riist- ja tarkvara soetamisel?
- Kui suured on eeldatavad jooksvad kulud (hooldamine, käitamine, tugiteenus)? Nende kuludega tuleb arvestada juba planeerimisfaasis. Kontrollida tuleks hooldus- ja tugilepingute sisu (reageerimisaegu, infoliini olemasolu, personali kvalifikatsiooni jne).
- Kui suured on eeldatavad personaliga seotud jooksvad kulutused?
- Kas on tarvis soetada täiendavaid tarkvara- või riistvarakomponente? Sellele küsimusele tuleb vastata juba planeerimisfaasis. Kui näiteks võrguhaldussüsteem on juba kasutuses, tuleb kontrollida selle ühilduvust soetatavate seadmetega. Lisaks tuleb arvestada tööde mahuga, mis on vajalik lahenduse integreerimiseks olemasolevasse infrastruktuuri.
- Kui suured on administraatorite koolituskulud?
- Milliste kulutustega tuleb arvestada juhtudel, kui mälumahuga seotud nõudmiste suurenemise tõttu on tarvis üle minna uuele riistvara versioonile? Sellistel juhtudel võivad kulud olla palju suuremad kui ainult uue riistvara maksumus, sest paljude tarkvaratootjate litsentsihinnad sõltuvad suuresti kas protsessorite arvust või nende taktsagedusest, mistõttu tuleb lisaks uue riistvaraversiooni soetamisele arvestada ka uute programmilitsentside soetamiskuludega.

7. Logimine

- Milliseid lahendusi saab kasutada logimiseks? Logimiseks pakutavad lahendused peavad vastama vähemalt turvapoliitikas sõnastatud nõuetele. Eriti olulised on alltoodud punktid.
- Kas logiandmete detailsust on võimalik konfigureerida?
- Kas logisse salvestatakse kõik olulised andmed?
- Kas süsteem toetab tsentraliseeritud logimist (nt syslog)?
- Kas logimine toimub kooskõlas andmekaitsest tulenevate nõuetega?

- Kas teavitusfunktsioonide tugi on olemas?

8. Infrastruktuur

- Mõõtmed ja sobivus kaitsekappidega. Soetamisel tuleb arvestada ka serverite ruumivajadusega. Kas seadet on võimalik paigaldada ettenähtud kaitsekappidesse (seadmete kuju, kaal, kinnituselemendid)?
- Toide ja heitsoojus. Tootja peab edastama andmed voolutarbimise ja kasutuskeskkonna temperatuurinõuete kohta. Kas toite ja UPSi olemasolev jõudlus on piisav? Kas olemasolev jahutusvõimsus on seadme heitsoojuse ärajuhtimiseks piisav?

Kõik nõuded ja nende põhjal langetatud valikuotsused tuleb dokumenteerida selliselt, et vastavate otsuste langetamise põhjused oleksid arusaadavad ka tulevikus.

Täiendavad kontrollküsimused:

- Kas kõik serveritele esitatavad nõuded on dokumenteeritud?

M 2.318 Serveri turvaline installeerimine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator

Pärast serveri kasutuselevõtu planeerimisfaasi (vt M 2.315 Serveri kasutuselevõtu planeerimine) läbimist ja vastava turvapoliitika (vt M 2.316 Serveri turvapoliitika kehtestamine) koostamist võib hakata süsteemi installeerima.

Installeerimise kontseptsioon

Enne installeerimistöödega alustamist on soovitatav koostada lühike installeerimiskontseptsioon, milles kajastuvad planeerimisfaasis väljatöötatud funktsionaalsed nõuded ja turvapoliitika ettekirjutused. Üldjuhul on parem, kui installeerimine viiakse läbi kahes osas: esmalt installeeritakse ja konfigureeritakse alussüsteem ning seejärel seatakse sisse kõik ülejäänud vajalikud teenused ja rakendused. Enamlevinud operatsioonisüsteemide tootjate paigaldusprogrammid võimaldavad sellist lähenemist üldiselt võrdselt hästi rakendada.

Etalon-süsteem

Kirjeldatud tööetappe ei tule ilmtingimata läbi viia iga serveri puhul eraldi. Selline lähenemine võib olla isegi kahjulik, sest sarnase tööprotsessi pidev kordamine võib suurendada vigade tekkevõimalusi. Seetõttu soovitatakse kirjeldatud etapid esmalt võimalikult hoolikalt läbi teha mõnel etalonsüsteemil ja vajalikud konfiguratsioonid võimalikult täpselt kirja panna, et tekiks vastava operatsioonisüsteemi jaoks oludega kohandatud installeerimiskontseptsioon. Siinkohal tuleb arvestada, et eelpool kirjeldatud viisil loodud installeerimiskontseptsioone tuleb kontrollida ja uuendada ka selliste operatsioonisüsteemi muudatuste puhul, millega ei kaasne otseselt üleminekut uuele versioonile (nt *Service-Packs, Update-Releases*).

Installeerimine

Käesolev meede sisaldab ainult soovitusi installeerimise esimeste sammude läbiviimiseks ning ei kirjelda lõplikke konfiguratsioone, mis oleksid seotud konkreetse kasutusvaldkonnaga. Konfigureerimisel läbitavad etapid sõltuvad väga suurel määral konkreetsest süsteemist ja kasutusvaldkonnast ning seetõttu käsitletakse vastavaid soovitusi eraldi meetmetes.

Dokumentatsioon

Dokumenteerida tuleks vähemalt installeerimise ja hilisema konfigureerimise olulisemad etapid, et vastavad läbiviidud tööd oleksid arusaadavad ka tulevikus. Näiteks võib koostada installeerimise kontrollnimekirja, kus on võimalik teha läbiviidud tööetappide kohta kastikeste sisse linnukesi ja tehtud seadustused üles märkida. Vastav dokumentatsioon on suureks abiks vigade analüüsil või hilisemal reinstalleerimisel. Siinkohal tuleb arvestada, et lisaks dokumentatsiooni koostajale peaks vastavat dokumentatsiooni suutma kasutada ka administraatorid, kes võivad olla antud valdkonnaga ainult osaliselt seotud. Seetõttu on oluline, et dokumentatsioon oleks hästi struktureeritud ja arusaadav.

Offline installeerimine

Installeerimine ja aluskonfiguratsiooni loomine peaks võimalusel toimuma kas ainult *offline* režiimis või siis vähemalt turvalises võrgus (installeerimis- või haldusvõrgus). Seda on oluline järgida, kuna installeerimise käigus ei jagata reeglina veel ühtki parooli ning kaitsemehhanismid on välja lülitatud, kuid sõltuvalt olukorrast võib olla juba võimalik süsteemile juurde pääseda. Juhul kui installeerimine peaks osaliselt toimuma võrgu kaudu (nt erinevate pakettide järelpaigaldus), tuleks võimalusel selleks kasutada haldusvõrgus asuvat installeerimisserverit.

Turvaliste andmeallikate kasutamine

Asjaolu, et paigaldatav versioon peaks pärinema usaldusväärsest allikast, on eriti oluline operatsioonisüsteemi installeerimisel. Eriti oluline on see siis, kui nt *CD-Images* laetakse alla Internetist. Sellistel juhtudel tuleks ilmtingimata kontrollida, kas paketid on varustatud digitaalallkirjadega, mida oleks võimalik kasutada pakettide tervikluse ja autentsuse kontrollimiseks (vt M 4.177 Tarkvarapakettide tervikluse ja autentsuse tagamine). Pakette ja *CD-Images* , millel puuduvad digitaalsed allkirjad ning mis pole isegi varustatud kontrollsummaga, tuleks võimalusel vältida.

Partitsioonide loomine ja failisüsteemi *layout*

Kõvaketaste partitsioonide loomisel tuleb lähtuda planeerimisfaasis (vt M 2.315 Serveri kasutuselevõtu planeerimine) koostatud kontseptsioonist. Krüpteeritud failisüsteemi kasutamisvajaduse puhul tuleb arvestada, et vastav süsteem tuleb juurutada enne seda, kui andmed süsteemi ümber kopeeritakse, sest tagantjärele pole failisüsteemi krüpteerimine tihti enam võimalik. Ka *Raid* -süsteemid ja - *Levelid* peavad olema esmalt lõpuni konfigureeritud ning alles seejärel saab asuda vajalike failisüsteemide juurutamise kallale.

Riistvara ja *Bootloader* -i sisseseadmine

Installeerimistööde esimese etapi jaoks on üldjuhul tarvis konfigureerida ainult see riistvara osa, mis on vajalik süsteemi buutimiseks (nt RAID-ajamite, krüpteeritud failisüsteemide vms käivitamiseks) ja installeerimistöödega jätkamiseks (sõltuvalt vajadusest nt võrgukaardid). Ülejäänud riistvara osad võib sisse seada installeerimistööde teise etapi käigus. Alusinstallatsiooni viimaseks tööks on enamasti *Bootloader* -i installeerimine ja konfigureerimine, mis peab tagama, et süsteemi käivitamisel käivituks operatsioonisüsteem. Üldjuhul on *Bootloader* varustatud menüüga, mis lubab valida erinevate installeeritud operatsioonisüsteemide või nende konfiguratsioonide vahel. *Bootloader* -i konfigureerimisel tuleb olla väga hoolikas, kuna selle töö korrektsest teostamisest oleneb, kas süsteem üldse käivitub või mitte. Tehtud konfiguratsioon tuleks kirja panna. Mõningad süsteemid pakuvad vastava installeerimistöö käigus võimalust luua buutimisdiskett, millega on võimalik süsteemi avarii korral käivitada. Süsteemide puhul, mis ei ole füüsiliselt volitamata juurdepääsu eest kaitstud, tuleks *Bootloader* võimalusel varustada sobiva parooliga.

Logifunktsiooni võimlikult kiire sisselülitamine

Juhul kui see pole toimunud juba automaatselt, tuleks hiljemalt nüüd, st alusinstallatsiooni lõpetamisel sisse lülitada logi, mis kajastab süsteemis asetleidvaid sündmusi. Logiandmetest võib olla suur abi probleemide lahendamisel ning need võivad anda väärtuslikku infot täiendavate installeerimistööde ja konfiguratsioonide jaoks.

Värskendamine

Pakettide värskendamine

Juhtudel, kus süsteemi installeerimiseks kasutatakse CDd, DVDd või mõnda muud „ *offline* “ andmekandjat, tuleks pärast alusinstalleeringu lõpetamist kontrollida, kas tootja või edasimüüja pole vahepeal väljastanud antud toote mõnda uuemat versiooni või turvapaika(vt M 2.35 Teabe hankimine turvaaukude kohta ja M 2.273 Turvalisust mõjutavate paikade ja värskenduste kiire paigaldamine).

Vajamineva serveriprogrammi installeerimine

Pärast seda, kui operatsioonisüsteem on installeeritud, aluskonfiguratsioon tehtud ning värskendamine lõpule viidud, võib hakata paigaldama ja konfigureerima

vajaminevaid serveriprogramme. Vastavate tööde puhul soovitatakse lähtuda samasugusest protseduurist nagu operatsioonisüsteemi paigaldamisel.

Täiendavad kontrollküsimused:

- Kas installeerimiseks on koostatud vastav kontseptsioon?
- Kas süsteemis rakendatakse Bootloader -it? Kui jah, siis millist?
- Kas paketid värskendati pärast installeerimist?

M 2.319 Serveri üleviimine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator

Kui tekib vajadus teatud serveri funktsioonid mõne teise serveri poolt üle võtta, tuleb planeerida vastava serveri üleviimine. Eriti oluline on hoolikalt läbiviidud planeerimistöö nendes kasutusvaldkondades, kus serverile ja selle teenustele esitatakse käideldavuse osas kõrgeid nõudeid. Enamikel juhtudel on soovitatav teostada „funktsioonide üleviimine“ asendussüsteemile väljaspool tavapärast tööaega. Kui see pole võimalik, tuleb võtta tarvitusele meetmed, mis tagaksid, et üleviimise käigus ei tekiks andmekadu ning et seisakuajad jääksid talutavatesse piiridesse. Olulisemate serverite üleviimiseks tuleb seetõttu eelnevalt koostada vastav üleviimiskontseptsioon. Selle käigus tuleks ennekõike arvestada järgmiste punktidega:

- Andmete üleviimine ja konfiguratsioon. Pärast andmete üleviimist uuele süsteemile tuleb kontrollida, kas andmed kanti üle täies mahus ning kas vastav toiming viidi läbi korrektselt. Juhtudel, kus uues süsteemis soovitakse kasutusele võtta uus serveritarkvara, tuleb eelnevalt kontrollida, kas uus versioon suudab vanade andmehulkadega korrektselt ümber käia. Siia alla ei kuulu mitte ainult võimalus vanemas versioonis loodud andmeid korrektselt lugeda, vaid ennekõike ka võimalus neid andmeid muuta või uusi andmehulki lisada. Nimetatud valdkondades esineb sageli probleeme, mistõttu soovitatakse siinkohal läbi viia põhjalik testimine. Lisaks on oluline, et uus süsteem suudaks vana teenuse konfiguratsiooni korrektselt üle võtta või võimaldaks seda „sarnaste funktsioonide abil järgi ehitada“.
- Teenuse ühilduvus. Tuleb tagada, et teenus töötaks asendussüsteemis selliselt, et see ühilduks ka vana teenusega. Eriti oluline on see siis, kui uuele süsteemile üleviimise raames tahetakse kasutusele võtta ka uus serveriprogrammi versioon, millele peavad juurde pääsema ka vana versiooni kliendid. Isegi sellistel juhtudel, kus tootjal on ette näidata aruanded klientidest, kelle puhul on vastavad üleviimised juba edukalt läbi viidud või kui tootja kinnitab, et „tootel ei esine probleeme tagasiühilduvusega“, „toode tagab täieliku tagasiühilduvuse varasemate versioonidega“ vms, on siiski tungivalt soovitatav enne toote kasutuselevõttu läbi viia vastavad testid.
- Krüptograafilised võtmed Kasutusvaldkondades, kus serveri andmed või failisüsteemid on varustatud krüpteeringuga, muutub väga oluliseks vastavate võtmete turvaline edastamine: võtmed on salvestatud tihti hoopis teise kohta kui kasutajaandmed. Näiteks juhtudel, kus vastavaid andmeid kopeeritakse süsteemis rakendatavate programmide abil kas otse plokikaupa või kui vana süsteemi kõvakettad paigutatakse uude süsteemi ümber, tuleb tagada, et nendega koos edastatakse ka vajalikud võtmed, kuna vastasel korral muutub juurdepääs krüpteeritud andmetele võimatuks.
- Nimede ja aadresside muutmine. Kui serverile pääseb ligi ainult kas IP-aadressi või DNS-nimede alusel, on selle üleviimine suhteliselt probleemivaba, kuna sellistel juhtudel saab asendussüsteem vana süsteemi IP-aadressi lihtsalt üle võtta. Probleeme tekitavad enamasti need juhtumid, kus uuele

süsteemile tuleb anda küll sama DNS-nimi, kuid IP-aadressi ei ole võimalik üle võtta. Selleks, et aadressi muudatus kõikidele klientidele „pärale jõuaks“, kulub teatud hulk aega. Üleviimise planeerimisel tuleb arvestada vastavate viivitustega. Juhtudel, kus juurdepääs süsteemile on lahendatud teismoodi (nt kui aadress võetakse mõne teise kataloogiteenuse tõttu kasutuselt maha), tuleb arvestada, et ka sellisel moel sisseviidud muudatuse rakendumiseks peab mööduma teatud hulk aega, enne kui see täielikult tööle rakendub. Kõige suuremad probleemid tekivad siis, kui kliendid kasutavad serverit mõne rakenduse abil, mille puhul salvestatakse serveri IP-aadress või serveri nimi mõnda kohapeal asuvasse konfiguratsioonifaili või -andmebaasi. Juhul kui suur arve kliente on tarvis ümber konfigureerida käsitsi, võib see võtta väga palju aega, mistõttu tuleb sellised tööd ette planeerida.

- Püsiühendused. Juhul kui eksisteerib kliente, kes on kas pikka aega kestva või koguni püsiühenduse vahendusel ühenduses teenusega, mis on tarvis uuele arvutile üle viia (selliseid juhtumeid esineb nt mõningate andmebaaside puhul), tuleb sellega üleviimise planeerimisel arvestada. Vajadusel tuleb võimalike klientide nimetatud ühendused lõpetada käsitsi. Ka sellised tööd tuleb ette planeerida. Serveri üleviimistööde jaoks on soovitatav üleviimiskontseptsiooni väljatöötamisel koostada ka asjakohane kontrollnimekiri, mida oleks võimalik üleviimise käigus samm-sammult läbi töötada. Üleviimise planeerimise ja kontrollnimekirja koostamise käigus tuleb jälgida, et iga läbiviidav samm sõltuks ainult sellele eelnenud sammudest.

Juhul kui teenuse käideldavusele seatakse kõrgeid nõudeid, tuleks võimalike probleemide tuvastamiseks ja kõrvaldamiseks enne tegelikku üleviimist tervet vajaminevat protseduuri testimiskeskkonnas testida, luues selleks võimalikult originaalilähedased tingimused.

Täiendavad kontrollküsimused:

- Kas üleviimise jaoks on koostatud vastav kontseptsioon?

M 2.320 Serveri nõuetekohane kasutuselt kõrvaldamine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: administraator

Serveri kasutuselt kõrvaldamine ei tohi aset leida ilma vastava ettevalmistuseta. Vastavast ettevõtmisest tuleb informeerida kasutajaid ning erinevate meetmete abil tuleb tagada

- kõikide oluliste andmete säilimine,
- kõikide vastavast serverist sõltunud süsteemide ja teenuste funktsiooni säilimine ja
- kogu konfidentsiaalse info eemaldamine kasutuselt kõrvaldatava serveri andmekandjatelt.

Selleks on ülimalt oluline, et oleks olemas ülevaade, milliseid andmeid serveri eri kohtadesse salvestatakse ja millisel moel neile andmetele ligi pääseb. Eespool nimetatud informatsiooni alusel tuleks läbi viia serveri kasutusest kõrvaldamise planeerimine.

Selle käigus tuleks arvestada järgmiste punktidega:

- Andmete varundamine. Enne serveri kasutusest kõrvaldamist tuleb serverile salvestatud vajaminevad andmed varundada, st arhiveerida kas mõnele välisele andmekandjale (nt magnetlintidele, CD- või DVD-ROMidele) või kanda üle mõnele varusüsteemile. Pärast andmete varundamist tuleb kontrollida, kas kõik andmed on korrektselt varundatud. Nende valdkondade kohta leiate täiendavat infot moodulitest B 1.4 Andmevarunduspoliitika ja B 1.12 Arhiveerimine .
- Varusüsteem. Juhul kui serveri pakutud teenuseid on tarvis edasi kasutada, tuleb õigel ajal muretseda vastav varusüsteem. Asjakohase planeerimistöö, soetamise ja kasutuselevõtmise tarvis peavad olema kasutada sobivad ressursid, vt M 2.319 Serveri üleviimine .
- Kasutajate informeerimine. Juhul kui süsteem lülitatakse välja ja asendussüsteemi ei paigaldata, tuleb kasutajaid sellest õigel ajal informeerida, et nad saaksid vajaduse korral oma andmed ise varundada.
- Süsteemi kajastavate viidete eemaldamine. Süsteemi kasutuselt kõrvaldamise käigus tuleb lisaks muule kustutada ka süsteemiviited. Siia alla kuulub nt DNS-sissekande ja teiste kataloogiteenuste sissekannete kustutamine ning olenevalt kasutusvaldkonnast ka muude viidete kustutamine. Näiteks veebiserveri kasutuselt kõrvaldamisel tuleks oma veebilehtedelt kustutada kõik viited kõrvaldatud veebiserverile.

Andmete turvaline kustutamine

- Väljalülitamisele kuuluva süsteemi andmete kustutamine. Tarvis on tagada, et kõvaketastele ei jääks tundlikku informatsiooni. Kõvaketaste uuesti formaatimine ei ole selle jaoks piisav, kõvakettad tuleb vähemalt üks kord täie-

likult üle kirjutada. Siinkohal tuleb arvestada, et ketaste loogiline kustutamine installeeritud operatsioonisüsteemide kustutamisfunktsioonidega ega ka ketaste uuesti formaatimine ei kõrvalda kõvakestastel olnud andmeid jäädavalt. Sobiva tarkvaraga on äsjaloetletud meetoditel kustutatud andmeid tihti võimalik isegi suurema vaevata taastada. Täiendavaid teemakohaseid juhiseid leiate meetmetest M 2.13 Tundlike ressursside jäljetu hävitamine ja M 2.167 Andmete kustutamiseks või hävitamiseks sobivate lahenduste valik .

- Andmevarunduseks kasutatud andmekandjate kustutamine. Pärast süsteemi kasutuselt kõrvaldamist tuleb vajaduse korral kustutada või kasutuskõlbmatuks muuta ka süsteemi varundamiseks kasutatud andmekandjad, seda muidugi eeldusel, et vastavaid andmeid ei lähe enam tarvis.
- Täiendava info eemaldamine. Serverisüsteemid sisaldavad tihti ka täiendavaid andmeid (nt konfiguratsiooniandmeid), mis on kas salvestatud püsimällu või on kirjutatud seadmele selle tähistamiseks (nt arvuti nimi, IP-aadress ja igasugune muu tehniline info). Kui võimalik, tuleks vastav info enne seadme edasiandmist eemaldada, kuna potentsiaalne ründaja võib ka niisugusest infost saada vihjeid rünnete toimepanekuks. Eespool toodud soovituste alusel on soovitatav koostada kontrollnimekiri, mis tuleks kasutuselt kõrvaldamise protsessi käigus samm-sammult läbi töötada. Selle abil saab vältida ka üksikute vajalike etappide unustamist.

Kontrollküsimused:

- Kuidas toimub süsteemi kasutuselt kõrvaldamine?

M 2.321 Klient-server-võrgu kasutuselevõtu planeerimine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: IT-juht, administraator

Klientide turvalise käitamise üheks põhjapanevaks eelduseks on piisavas mahus läbiviidud planeerimistöö. Kasutuselevõtu planeerimine võib toimuda mitmes etapis vastavalt *Top-Down* -visandi printsiibile: terviksüsteemi kontseptsiooni visandi alusel määratakse kindlaks spetsiifiliste osakontseptsioonide koostamiseks vajalik konkreetne planeerimistöö. Planeerimine ei hõlma endas aga mitte ainult neid valdkondi, mida seostatakse turbega selle klassikalises tähenduses, vaid ka täiesti tavapäraseid igapäevatöös kajastuvaid aspekte, mis avaldavad samuti mõju turvalisusele.

Üldkontseptsioon

Üldkontseptsioonis tuleks leida vastused näiteks järgnevatele tüüpilistele küsimustele:

- Milliseid ülesandeid peaksid kliendid suutma täita? Milliseid teenuseid peavad kliendid suutma kasutada? Kas süsteemide käideldavusele esitatakse mingisuguseid erinõudeid, või on erisoove seoses salvestatud või töödeldavate andmete konfidentsiaalsuse või tervikluse tagamisega?
- Kas süsteemis tuleks rakendada teatud kindlat liiki riistvarakomponente? Antud tingimus võib olla oluline näiteks operatsioonisüsteemi valikul.
- Milliseid üldistest tingimustest tulenevaid nõudmisi tuleb arvestada riistvara valiku puhul (CPU, töömälu, kõvaketaste mahu, võrgu koormustaluvuse puhul).
- Kas klientide jaoks planeeritud rakenduskeskkonna puhul on tegemist homogeense või heterogeense arvutivõrguga?
- Kas kliente rakendatakse olemasolevate süsteemide varulahendusena? Kas vana süsteemi andmebaase või riistvarakomponente on tarvis üle võtta?
- Kas arvutitele peaks olema võimalik installeerida ka täiendavaid operatsioonisüsteeme *Multiboot* funktsiooni abil?

Soovitatav on luua üks või mitu geneerilist nõudmiste profiili (nt „üldine büroo PC“, „arendustegevuse arvuti“ või „administreerimis-klient“, mida saaks konkreetsete planeerimistööde käigus aluseks võtta.

Osakontseptsioonid

Planeerimisel tuleks arvestada järgmiste osakontseptsioonidega:

- Autentimine ja kasutajate haldamine: Millist tüüpi kasutajate haldamist ja kasutajate autentimist soovitakse kasutada? Kas kasutajaid soovitakse hallata ainult lokaalselt või tahetakse kasutada tsentraliseeritud haldamissüsteemi? Kas süsteem peaks suutma rakendada ka tsentraliseeritud võrgupõhist autentimisteenust või vajatakse ainult lokaalset autentimisteenust? Täiendavat infot autentimismehhanismide kohta leiate M 4.133 Sobivate autentimismehhanismide valimine ja M 4.250 Keskse võrgupõhise autentimisteenuse valimine .
- Kasutaja- ja rühmakontseptsioon: Võttes aluseks üleorganisatsioonilised kasutajaid, nende õigusi ja töörollide jaotumist käsitlevad kontseptsioonid,

tuleb klientide jaoks koostada vastavad reeglid (vt M 2.30 Kasutajate ja kasutajarühmade määramise protseduurid ja M 2.31 Volitatud kasutajate ja õiguste profiilide dokumenteerimine).

- Haldamine: Kuidas peaks toimuma süsteemide haldamine? Kas kõik seadistused tehakse lokaalselt või integreeritakse kliendid tsentraliseeritud haldamist ja konfigureerimist juhtiva süsteemi alla?

Programmide, süsteemi- ja kasutajaandmete lahushoidmine

- Partitsiooni- ja failisüsteemi *Layout*: Planeerimisfaasis tuleks koostada esimesed hinnangud, kui palju oleks süsteemile tarvis kettaruumi. Haldamise ja hooldamise lihtsustamiseks on soovitatav, nii palju kui see on võimalik, eraldada üksteisest operatsioonisüsteem (süsteemi programmid ja konfiguratsioon), rakendusprogrammid ja rakenduste andmed (nt andmebaasiserverid ja andmed) ning vajadusel ka kasutajaandmed. Erinevad operatsioonisüsteemid pakuvad selleks erinevaid lahendusi (partitsioonideks jagamine Windowsi all, failisüsteemid Unixi all). Tihti võib olla mõttekas salvestada teatud liiki andmed isegi eraldi kõvakettale ja eraldi kettasüsteemile. Sel viisil on võimalik nt reinstalleerimise või süsteemi uuendamise järel hakata teiste partitsioonide andmeid kohe kasutama, ilma et neid oleks tarvis ümber kopeerida.

Kõrge turbeastme korral tuleks võimalusel lubada ainult krüpteeritud failisüsteeme

Eraldi töökohtades, kuhu tahetakse salvestada andmeid, mille puhul kehtivad konfidentsiaalsusest tingitud kõrged turbenõuded, soovitatakse ilmtingimata rakendada krüpteeritud failisüsteeme. Siinkohal pole ilmtingimata vajalik, et kõik failisüsteemid oleks varustatud krüpteeringuga. Sageli piisab ka sellest, kui krüpteeritult töötab vaid see konkreetne failisüsteemi osa, kuhu andmeid reaalselt salvestatakse. Selle tagamiseks tuleb tegeleda vastava partitsiooni- ja failisüsteemi *Layout* -i planeerimisega. Juhul kui eraldi töökohtadesse salvestatavate andmete konfidentsiaalsusnõuded on kõrged, tuleb süsteemid vajadusel varustada krüpteerimisprogrammiga, mis krüpteeriks kogu kõvaketta ning viiks läbi kasutaja autentimise (nt kiipkaardi abil) juba enne operatsioonisüsteemi käivitamist (Pre-Boot-Authentication).

- Võrguteenused ja võrguühendus: Klientide võrguühenduse planeerimisel tuleb lähtuda turbenõuetest, mis on kehtestatud andmetele, millele kliendid peavad ligi pääsema. Sõltuvalt arvutitele kehtestatud rakendusvaldkonnast, läheb vajadusel tarvis ka täiendavaid juurdepääse muudele võrgus pakutavatele teenustele. Hilisemate probleemide, nt liiga väikse edastusvõime või vaheleühendatud turvalüüsidest põhjustatud raskuste ennetamiseks tuleb loetletud vajadustega arvestada juba planeerimisfaasis.
- Seire: Juhtudel, kus klientide käideldavusele on kehtestatud erinõuded, võib rakendada seiresüsteeme (Monitoring Systems). Selleks tuleb ühele serverile installeerida Monitoring-Daemon , kellele teatud lokaalne Agent edastab vastavad seireandmed, nt andmed süsteemi koormatuse või järelejäänud

vaba kettaruumi kohta. Probleemide korral võib süsteem nt automaatselt edastada asjakohase hoiatava teate.

- Logimine: Logifunktsiooni kasutamine on oluline ka klientide puhul, kuna vastav info on väga oluline veadiagnostikaks, rikete kõrvaldamiseks, samuti võimalike rünnete tuvastamiseks ja rünnetega seotud asjaolude väljaselgitamiseks. Planeerimisfaasis tuleks otsustada, millist infot peaksid logid kajastama ja kui kaua tuleb vastavaid logiandmeid säilitada. Lisaks sellele tuleb otsustada, kas logianded tuleks salvestada lokaalselt süsteemidesse või tsentraalsesse logiserverisse, mis asub võrgus.

Logifailide kontrollimiseks tuleb määrata tähtajad

Logiandmete kontrollimise protseduurid ja kontrollimise tähtajad oleks mõistlik kindlaks määrata juba planeerimisfaasis. Kui klientide käideldavusele seatakse kõrgeid nõudeid, tuleks juba planeerimisfaasis mõelda, kuidas vastavaid nõudeid kõigi paremini täita.

Kõik planeerimisfaasis vastuvõetud otsused tuleb dokumenteerida selliselt, et vastavate otsuste langetamise põhjused oleksid arusaadavad ka tulevikus. Siinjuures on oluline arvestada, et vastavat infot peaksid suutma kasutada ka kõik teised, mitte ainult selle kirjapanija. Seetõttu on oluline jälgida, et vastav info oleks piisavalt struktureeritud ja arusaadav.

Täiendavad kontrollküsimused:

- Kas klientide rakendamisvõimalustega tegeldi juba enne nende soetamist ja installeerimist?
- Milline dokumentatsioon eksisteerib klientide kasutamise planeerimise kohta?

M 2.322 Klient-server-võrgu turvapoliitika kehtestamine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: IT-juht, IT-turvaosakond, administraator

Kõikidele klientidele kehtivate turvanõuete aluseks on üleorganisatsiooniline turvapoliitika. Üldises turvapoliitikas kajastuvaid nõudeid tuleb antud konteksti jaoks täpsustada ja koostada erinevaid kliendirühmi käsitlevad turvapoliitikad. Sellega seoses tuleb kontrollida, kas lisaks tervet organisatsiooni hõlmavale turvapoliitikale on tarvis arvestada ka muude, hierarhias kõrgemalseisvate nõuetega nagu nt IT-turvapoliitika, paroolisuuniste või internetikasutuse nõuetega. Kõik kasutajad ja muud isikud, kes on seotud klientide soetamisega ja käitamisega, peavad tundma turvapoliitikat ning sellest oma töödes lähtuma. Nagu kõikide suuniste puhul, tuleb nende sisu ja rakendamist regulaarselt üldise auditi käigus kontrollida. Turvapoliitika peab täpsustama üldise, eesmärgiks seatud turbeastme nõudeid ja sisaldama põhjapanevat infot klientide käitamise kohta. Ülevaatlikkuse parandamiseks võib olla mõttekas koostada erinevate kasutusvaldkondade jaoks spetsiaalsed turvapoliitikad.

Üldstrateegia: kas liberaalne või piirav?

Esimese asjana tuleks otsustada, kas konfigureerimise ja halduse üldstrateegia lähtub printsiibist „liberaalne“ või „piirav“, kuna kõik edasised otsused sõltuvad suurel määral sellest valikust. Klientide puhul, mis salvestavad ja töötlevad andmeid ainult tavalises turbeastmes, võib valida suhteliselt liberaalse üldstrateegia, mis lihtsustab paljudel juhtudel nende konfigureerimist ja haldamist. Siiski on ka niisugustel kasutusjuhtudel siiski soovitatav, et strateegia oleks „ainult nii liberaalne kui parasjagu vajalik“. Klientide puhul, mis töötavad kõrges turbeastmes, soovitatakse enamasti valida piirav strateegia. Eriti kõrges turbeastmes töötavate klientide puhul tuleks kolmest peamisest aspektist vähemalt ühe jaoks valida piirangutest lähtuv konfigureerimis- ja haldusstrateegia. Järgnevalt on loetletud mõned punktid, millega tuleks arvestada:

Klientide kasutajate tööks kehtestatavad reeglid

- Kas on ette nähtud, et süsteemi kasutab ainult üks kasutaja või kasutavad seda vaheldumisi erinevad kasutajad?
- Kas kasutajatel on lubatud teatud konfiguratsiooniseadeid ise muuta (nt ekraani taustapilti, ekraani pimenduspilti vms) või tulevad kõik seadistusi puudutavad ettekirjutused ühest kindlast tsentraalsest allikast?
- Kas kasutajate juurdepääsu teatud süsteemi osadele on tarvis piirata? Loetletud nõuded mõjutavad reeglina nii süsteemi kasutusõiguste jagamist kui ka selle installeerimist ja aluskonfiguratsiooni loomist.
- Milliseid andmeid tohivad kasutajad lokaalselt klientidele salvestada? Üldiselt tuleks kõik äritegevusega seotud andmed salvestada tsentraalselt serverisse, kus neid regulaarselt varundatakse. Vastasel juhul tuleb hoolitseda selle eest, kliendi andmevarunduskontseptsioonis võetaks arvesse et kõiki lokaalselt klientidele salvestatud kasutaja andmeid.
- Kas kasutajad on kohustatud arvutid tööpäeva lõppedes välja lülitama või peavad arvutid töötama ööpäevaringselt? Klient-arvutite väljalülitamise kasuks pärast tööpäeva lõppu räägivad argumendid nagu nt tuleohutus ja elektri kokkuhoid. Sellele lisaks pole enamik klient-arvutites rakendatavad kõva-

kettad loodud pidevaks kasutamiseks. Arvutite pidev tööshoidmine võib siiski olla ka vajalik, nt kui andmete automaatne varundamine peab toimuma öötundidel, või kui arvuteid kasutatakse ka muude rakenduste tarbeks.

Administraatorite ja auditeerijate töö reeglid

- Millise skeemi järgi jagatakse administreerimisõigusi? Millised on erinevatele administraatoritele jagatavad õigused ning kuidas toimub nende õiguste saamine?
- Milliseid süsteemi juurdepääsukanaleid tohivad kasutada administraatorid ja auditeerijad?
- Millised toimingud ja sündmused tuleb dokumenteerida? Millisel kujul luuakse dokumentatsioon ja kuidas seda hooldatakse?
- Kas teatud muudatuste puhul on kohustuslik järgida nelja silma põhimõtet?

Installeerimise ja aluskonfiguratsiooni nõuded

- Milliseid andmeallikaid kasutatakse installeerimiseks?
- Kas kasutajate haldamine ja autentimine peaks toimuma kohapeal või on tarvis rakendada tsentraliseeritud autentimisteenust?
- Kasutajate ja töörollide haldamise reeglid, volituste struktuurid (autentimise ja volitamise toimimine ja meetodid, volitused installeerimiseks, täiendite laadimiseks, konfiguratsiooni muutmiseks jne). Võimalusel tuleks administreerimiseks välja töötada töörollide jaotamise kontseptsioon.
- Installeeritavatele tarkvarapakettidele esitatavad nõuded
- Juhul kui planeerimisfaasis võeti vastu otsus, et klientide teatud failisüsteemi osad tuleb varustada krüpteeringuga, on siinkohal soovitatav kindlaks määrata, kuidas see lahendus realiseeritakse.
- Krüpteeritud failisüsteemide rakendamisel on selle jaoks soovitatav luua eraldi kontseptsioon ja dokumenteerida hoolikalt kõik konfiguratsiooni puudutavad detailid, sest probleemide esinemisel (nt võtme või võtme parooli kadumisel, ebakorrektse konfiguratsiooni jms korral) võivad failisüsteemis olnud andmed minna täielikult kaduma.
- Eeskirjad dokumentatsiooni koostamise ja haldamise kohta Installeeritavatele tarkvarapakettidele esitatavad nõuded.
- Juhul kui planeerimisfaasis võeti vastu otsus, et klientide teatud failisüsteemi osad tuleb varustada krüpteeringuga, on siinkohal soovitatav kindlaks määrata, kuidas see lahendus realiseeritakse.
- Krüpteeritud failisüsteemide rakendamisel on selle jaoks soovitatav luua eraldi kontseptsioon ja dokumenteerida hoolikalt kõik konfiguratsiooni puudutavad detailid, kuna probleemide esinemisel (nt võtme või võtme parooli kadumisel, ebakorrektse konfiguratsiooni jms korral) võivad failisüsteemis olnud andmed täielikult kaduma minna.

Reeglid dokumentatsiooni koostamise ja haldamise kohta

Turvalise käitamise nõuded

- Millistel kasutajatel on lubatud ennast süsteemi sisse logida?

- Kuidas saavad kasutajad end IT-süsteemi suhtes autentida? Üldiselt tuleks loobuda automaatsest logimisest, mille korral logitakse kasutaja sisse ilma aktiivse autentimiseta kliendi sisselülitamisel.
- Kas süsteemi tuleks integreerida osadeks jaotatud failisüsteem?
- Kas kliendi turvapoliitikat kohandatakse regulaarselt tegelikele nõudmistele?
- Kas kasutajatele antakse juurdepääs ühele või mitmele LAN-ile või Internetile? Milliseid protokolle tohib kasutada? Organisatsiooni sees kasutatavate töökohaarvutite klientide puhul pole reeglina üldse hädavajalik ning sageli pole see isegi soovitatav, et tavakasutajatel oleks võrgu kaudu juurdepääs ka veel mõnele teisele töökohaarvutile.
- Millistele ressurssidele tohivad kasutajad ligi pääseda?
- Paroolikasutuse jaoks tuleb kehtestada nõuded (paroolireeglid, paroolimuudatuste reeglid ja olukorrad, vajadusel paroolide deponeerimine).
- Kelle on õigus süsteem välja lülitada?
- Kas süsteem tuleks varustada Boot -lukuga, mis takistaks väliste andmekandjate nagu nt diskettide, CD-ROM-ide või USB-mälupulkade käivitamist? Tavakasutuse jaoks on soovitatav rakendada sellist lukku, mille eemaldamise õigus on ainult administraatoril, rikete otsimiseks ja kõrvaldamiseks juhtudel, kus arvutit on vaja käivitada avariiotstarbeks loodud buutimisvahendiga (vt M 6.24 Rikkejärgse buutimismeedia olemasolu).

Võrguside ja võrguteenused

- Kas on tarvis kasutada lokaalseid paketifiltreid?
- Millistele välistele võrgupõhistele teenustele tohib arvutist ligi pääseda?
- Kas on tarvis integreerida osadeks jaotatud failisüsteemi? Osadeks jaotatud failisüsteemi, mille puhul kasutajaandmed edastatakse ilma krüpteerimata, tuleks kasutada ainult sisevõrkudes. Kui osadeks jaotatud failisüsteemi on tarvis kasutada läbi ebaturvalise võrgu, tuleb selleks rakendada sobivad kaitsemeetmed (krüptograafiliselt kaitstud VPN, tunneldamine).

Logimine

- Milliseid andmeid logitakse?
- Kuidas ja milliste ajaintervallide tagant toimub logide analüüsimine?
- Kes tegeleb logide analüüsimisega?

Eelnevalt loetletud punktide abil saab koostada kontrollnimekirja, millest võib olla palju abi auditite ja revisjonide puhul. Turvapoliitika eest vastutab ITturvaosakond. Kõik turvapoliitika muudatused ja kõrvalekalded tuleb kooskõlastada IT-turvaosakonnaga. Turvapoliitika koostamisel on süsteemide turvalisuse tagamiseks soovitatav esmalt välja töötada maksimaalselt palju erinevaid nõudeid ja ettekirjutusi. Seejärel saab neid hakata viima vastavusse reaalsete oludega.

Ideaaljuhul aitab niisugune lähenemine arvestada kõikide võimalike aspektidega. Iga väljatöötatud nõude puhul, mis teise tööetapi käigus kõrvale jäetakse või pehmendatakse, tuleb dokumenteerida selle kõrvalejätmise põhjus. Kasutajaid puudutavate reeglite väljatöötamisel tuleks siiski silmas pidada, et igasuguste reeglite kehtestamise mõttekus sõltub sellest, kas neid on võimalik igapäevatöös

reaalselt kasutada, ja sellest, kui hästi on võimalik neid juurutada ja kontrollida nende järgimist. Näiteks teatud kataloogide juurdepääsude piirangud ei täida sugugi oma eesmärki, kui sellekohased piirangud on sõnastatud küll turvapoliitikas, kuid kasutajatele jagatakse jätkuvalt juurdepääsuõigusi, mis ei kaitse neid reaalselt vastavate juurdepääsuvõimaluste eest. Turvapoliitika väljatöötamise raames kehtestatud juurdepääsude piirangud tuleks seetõttu alati realiseerida arvutite installeerimiseks ja konfigureerimiseks mõeldud ettekirjutustega.

Liiga suured piirangud võivad olla negatiivse mõjuga

Kliente käsitleva turvapoliitika sõnastamisel on oluline saavutada tasakaal turvalisuse (funktsioonide piiramise ning piiratud kasutajaõiguste andmise) ja kasutajasõbralikkuse vahel. Juhul kui kasutajad külvatakse üle piiravate reeglitega, mis ei ole neile piisavalt läbipaistvad, või mida halvemal juhul tajutakse isegi ahistamisena, võib soovitud eesmärgi asemel tekkida olukord, kus töötajad hakkavad üles näitama ülisuurt loomingulisust, kuidas nimetatud piirangutest mööda minna. Antud aspekt on peamine põhjus, miks klientide jaoks loodavad suunised peavad olema teistsugused kui nt serverite või aktiivsete võrgukomponentide suunised. Viimaste puhul on info reeglina suunatud vaid suurte tehniliste teadmistega kasutajatele ja administraatoritele, kellele on piiranguid palju lihtsam selgitada.

Kontrollküsimused:

- Kas klientide kasutamise kohta on koostatud vastav turvapoliitika?
- Millisel kujul on koostatud turvapoliitika dokumentatsioon?
- Millal toimus viimati turvapoliitika uuendamine?
- Kas turvapoliitikas on sõnastatud ka turbeaste?

M 2.323 Kliendi korrakohane kasutuselt kõrvaldamine

Algatamise eest vastutavad: IT-juht, IT turvaosakond
Rakendamise eest vastutavad: administraator

Kliendi kasutuselt kõrvaldamisel tuleb enneköike tagada

- võimalike klientsüsteemi salvestatud oluliste andmete säilimine;
- kogu konfidentsiaalse info eemaldamine arvuti andmekandjatelt.

Selleks on ülimalt oluline, et oleks olemas ülevaade, milliseid andmeid süsteemi eri kohtadesse salvestatakse.

- Andmete varundamine. Enne arvuti kasutusest kõrvaldamist tuleb lokaalselt salvestatud vajaminevad andmed varundada, st arhiveerida kas mõnele välisele andmekandjale (nt magnetlintidele, CD- või DVD-ROMidele) või kanda üle mõnele varusüsteemile. Pärast andmete varundamist tuleb kontrollida, kas kõik andmed on korrektselt varundatud. Lokaalselt salvestatud andmete varundamiseks võib kõnealuses kontekstis olla mõistlik anda kasutajate käsutusse eraldiseisvad ajamid, nt kas CD- või DVD-kirjutajad (vt B 1.4 Andmevarunduspoliitika ja B 1.12 Arhiveerimine).
- Süsteemi kustutamine kataloogiteenuste ja andmebaaside kasutajanimekirjadest. Võrgupõhiste teenuste kasutusõigused, st otseselt klient-arvutiga (mitte kasutajaga) seotud õigused tuleb kustutada. Puudutatud õiguste näidetena võib siinkohal välja tuua turvalüüsi proksiserverite sissekanded ja IP-aadresside baasil jagatavad võrguteenuste kasutajaõigused. Juhul kui klient on registreeritud võrgupõhiste kataloogiteenuste või andmebaaside kasutajana (nt Windowsi domeeni, Active Directory, NIS-i vms all), tuleb vastavad sissekanded kas kustutada või vähemalt nendega seotud kontod desaktiveerida.
- Süsteemis olevate andmete kustutamine. Tuleb tagada, et kõvaketastele ei jääks tundlikku informatsiooni. Kõvaketaste uuesti formaatimine ei ole selle jaoks piisav, kõvakettad tuleb vähemalt üks kord täielikult üle kirjutada. Siinkohal tuleb arvestada, et ei ketaste loogiline kustutamine installeeritud operatsioonisüsteemide kustutamisfunktsioonidega ega ka ketaste uuesti formaatimine ei kõrvalda kõvaketastel olnud andmeid jäädavalt. Sobiva tarkvaraga on äsjaloetletud meetodite abil kustutatud andmeid võimalik tihti isegi suurema vaevata taastada (vt M 2.13 Tundlike ressursside jäljetu hävitamine ja M 2.167 Andmete kustutamiseks või hävitamiseks sobivate lahenduste valik .
- Andmevarunduseks kasutatud andmekandjate kustutamine. Pärast süsteemi kasutuselt kõrvaldamist tuleb vajaduse korral kustutada ka süsteemi varundamiseks kasutatud andmekandjad, seda muidugi eeldusel, et vastavaid andmeid ei lähe enam tarvis.
- Täiendava info eemaldamine. Juhul kui arvutitesse on salvestatud potentsiaalselt tundlikke andmeid (nt teatud konfiguratsiooniandmeid) ka teistesse kohtadesse peale kõvaketta (nt püsimällu), tuleb need enne seadme edasiandmist sealt eemaldada.

Eespool toodud soovituste alusel on soovitatav koostada kontrollnimekiri, mis tuleks kasutuselt kõrvaldamise protsessi käigus samm-sammult läbi töötada. Selle abil saab ka vältida üksikute vajalike etappide unustamist.

Kontrollküsimused:

- Kuidas toimub süsteemi kasutuselt kõrvaldamine?

M 2.324 Windows 7 kasutuselevõtu planeerimine

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: IT-juht, IT-turvaosakond, administraator

Windows 7 süsteemide reguleeritud ja turvaline juurutamine eeldab ulatuslikku planeerimist. Planeerimisfaasis luuakse hädavajalikud eeldused Windows 7 süsteemide turvaliseks käitamiseks. Konkreetsed planeerimistööde etapid sõltuvad suuresti Windows 7 süsteemide jaoks ettenähtud kasutusvaldkondadest. Kasutuselevõtu protseduuri üksikud etapid tuleb planeerida võimalikult detailselt. Selleks on tarvis arvestada mitte ainult erinevate valdkondade, vaid ka organisatsiooni sees väljakujunenud protsesside ja toimingutega. Kõik valdkonnad ja protsessid tuleb defineerida, kirja panna ning muuta kõigile seotud osapooltele ligipääsetavaks.

Windows 7 juurutamise üheks üldiseks eelduseks on asjaolu, et töödeks tuleb varuda piisavalt aega. Suuremate ettevõtete ja ametiasutuste puhul tuleb siinjuures arvestada, et planeerimisetapi pikkuseks oleks küllaltki reaalne arvestada pool aastat. Lisaks võib kogemustele tuginedes väita, et ajakava tuleb tööde käigus kindlasti mitmeid kordi ümber hinnata. Windows 7 kasutuselevõtu planeerimisel tuleks arvestada järgmiste turvalisust puudutavate aspektidega:

Uus paigaldus või üleviimine / Upgrade

Windows 7 juurutamiseks võib kasutada mitmeid erinevaid protseduure. Juurutamine võib toimuda Windows -infrastruktuuri paralleelse ülesehitamisega (uued kliendid juurutatakse paralleelselt olemasolevate klientidega). Samuti võib juurutamiseks kasutada olemasolevate klient-arvutite üleviimist või Update -i. Siinkohal ei ole võimalik anda üldkehtivaid soovitusi, kuna juurutamine sõltub suuresti kohapealsetest konkreetsetest oludest. Vajalik protseduur tuleb välja töötada vastavalt kõnealuse ettevõtte või ametiasutuse vajadustele. Esmajärjekorras on tarvis otsustada, kas Windows 7 juurutamiseks installeeritakse klient-arvutid täielikult uuesti või toimub hoopis üleviimine. Praktikas tuleb tihti ette, et täiemahulise reinstalleerimise asemel otsustatakse pigem olemasolevate klient-süsteemide üleviimise kasuks. Mahukas planeerimistöö pole vajalik mitte ainult uue paigalduse, vaid ka vanematelt Windows versioonidel uuematele versioonidele üleminekul (st domeenikontrollerid, nt versioonile Windows Server 2008). Siinjuures tuleb tähelepanu pöörata täiendavatele migratsiooniaspektidele serveril (nt M 4.424z Vanemate tarkvarade turvaline kasutamine alates Windows 7-st). Üleviimise üksikud etapid tuleb planeerida võimalikult detailselt, kuna puuduliku planeerimistöö tagajärjel võivad teostuse käigus kergesti tekkida turvaaugud.

Windows 7 on saadaval erinevate redaktsioonidena (editions), on erinevalt vanematest versioonidest nüüd paralleelselt võimalik kasutada ka erinevaid migreerimisvõimalusi. Institutsioon peab enda jaoks kindlaks määrama, millist Windows 7 redaktsiooni kasutatakse (vt M 2.440 Windows Vista ja Windows 7 sobiva versiooni valimine). Iga uusinstallimise või kohandamise (upgrade) korral tuleb arvestada ka Windows 7 klientide aktiveerimisnõuetega (vt M 4.336 Hulgilitsentslepinguga Windows süsteemide aktiveerimine alates Windows Vistast või Windows Server 2008-st ja M 4.343z Hulgilitsentsilepinguga Windowsi süsteemide reaktiveerimine alates Windows Vistast või Windows Server 2008-st). Kui lisaks klientidele soovitakse üle viia ka vanemate Windowsi versioonide domeenid, tuleb täiendavalt arvestada ka vajalike üleviimise aspektidega serveri poolel.

Üleviimise puhul tuleb arvestada, et sõltuvalt olukorrast on tarvis jagada täiendavaid juurdepääsuõigusi (nt spetsiaalsele üleviimisega tegelevale meeskonna-

le ning võimalike ühilduvusega seoses üleskerkivate probleemide tõttu tuleb nõrgendada turvaseadeid. Pärast üleviimisprotseduuri lõppemist tuleb nimetatud seaded viia tagasi võimalikult kõrgele turbeastmele. Täiendavad, üleviimisprotseduuri jaoks vajalikud õigused tuleb pärast üleviimise lõppemist tühistada. Üldjuhul kehtib nõue, et üleviimise lõppemisel tuleb saavutada sama kõrge turbeaste nagu täiesti uue paigalduse korral. Üleviimisprotsessi lõppedes on soovitatav võrrelda omavahel kõikide turvaseadete, nt õiguste ja kasutajarühmadesse kuulumise kohta püstitatud eesmärke ja saavutatud hetkeolukorda. Kindlaks tuleb määrata üleviimise ajaline kestus ning sellest plaanist täpselt kinni pidada. Üleviimine kui protseduur ei tohi muutuda „tavaolukorraks“. Lisaks kõigele muule mõjutab see olulisel määral turvalisust, sest üleviimise käigus toimub reeglina turvaseadete nõrgendamine.

Tarkvara ühilduvuse kontrollimine üleminekul Windows 7-le

Tuleb kindlaks määrata, mis tarkvara hakatakse kasutama Windows 7-ga töötavates klientides. Juba olemasoleva tarkvara puhul tuleb kontrollida, kas see hakkab või Windows 7 keskkonnas tööle (vt M 2.441 Uue tarkvara ühilduvuse kontroll koostööks Windows Vista ja Windows 7-ga). Sama kehtib ka uue tarkvara kohta, mille soetamist alles planeeritakse ning mida soovitakse kasutada pärast migreerimist Windows 7-ks. Kui institutsioonil on olemas asjakohased riistvaralahendused, võib kaaluda ka virtualiseerimist. Selleks tuleb Windows 7-ga töötavasse klienti installida ka virtualiseerimistarkvara.

Virtualiseerimistarkvaraga luuakse virtuaalne riistvara, millesse saab installida teistsuguse operatsioonisüsteemi koos vajamineva rakendustarkvaraga. Windows 7 redaktsioonidesse Enterprise ja Ultimate Edition on Microsoft paigaldanud juba ka asjakohase virtualiseerimistarkvara VirtualPC. Virtualiseerimistarkvara kasutamisel tuleb hoolitseda ka virtuaalse operatsioonisüsteem piisava turbe eest.

Kasutuse planeerimine segakeskkonnades

Windows 7 klientide rakendamisel segakasutuskeskkondades võib muutuda hädavajalikuks turvaseadete nõrgendamine (nt pole võimalik tagada võrguside läbivat digitaalset allkirjastamist). Antud asjaolu tuleb planeerimisel arvestada. Eriti tuleb hoolt kanda selle eest, et pärast seda, kui saavutatakse homogeenne keskkond, (st kasutuskeskkond, mis koosneb eranditult Windows 7 klientidest ja serveritest), viidaks turvaseadistused tagasi kõige kõrgemale võimalikule turbeastmele.

Active Directory planeerimine

Kasutajate kontseptsiooni planeerimisel tuleb Windows 7 puhul kindlaks määrata, kuidas hakatakse kasutajakontosid haldama (User Account Control – UAC) (vt M 4.340 Windows kasutajakonto haldamise (UAC) kasutamine alates Windows Vistast). Kasutada tuleks selliseid seadistusi, mis ei muuda standardkasutajate privileege varasemast suuremaks. Active Directory puhul tuleb näiteks välja töötada vastavad rühma- ja OU-struktuurid (Organizational Unit – organisatsiooni allüksus). See on vajalik, kuna sobivad OU-struktuurid aitavad ettevõtete puhul kaasa Windows 7 süsteemide töö lihtsustamisele, muutes protsessid läbipaistvamaks ja seeläbi ka turvalisemaks. Lisaks tuleb planeerida ka Active Directory kasutajarühmade grupeerimissuuniste struktuur. Grupeerimissuunistel põhinevate mehhanismide nagu nt õiguste pärimise blokeerimise või nn Security Filtering kasutamise üle tuleb otsustada juba planeerimisfaasis. Siinjuures tuleb arvestada

kasutajarühmadele mõeldud grupeerimissuuniste väljatöötamise järjekorraga (M 2.326 Windows Vista ja Windows 7 grupeerimissuuniste planeerimine). Täiendavat infot üldiste, Active Directory planeerimist puudutavate juhiste kohta leiate M 2.229 Active Directory planeerimine . GPOAccelerator-tööriista abil peab domeeniadministraator looma klientsüsteemis rühmasuuniste vajalikud konfiguratsioonid. Seejärel tuleb need ümber paigutada domeenikontrollerile. Alternatiivselt võib selleks kasutada ka Remote Server Administration Tool'i (RSAT), sest integreeritud on programm rühmapoliitikate haldamiseks, millega saab konfigureerida rühmapoliitikaid ja ühendada tööjaamast Active Directory objektiga. Security Compliance Manager pakub ka võimalust luua Windowsi süsteemide jaoks turvamalle ja importida neid rühmapoliitikatena domeenikontrollerile. Erinevate Windowsi versioonide vastavad turvamallid on koos abivahenditega IT etalonkaitse kataloogi jaoks saadaval BSI veebilehel.

Secure Boot

Windows 8-ga ühilduv tarkvara tuleb Microsofti suuniste järgi tarnida koos aktiveeritud Secure Boot'iga. See BIOS-järeltulija UEFI funktsioon peab tagama, et keelatakse buutiva operatsioonisüsteemi manipuleerimine, nt kahjurvaraga. Secure Boot väldib ka Live-operatsioonisüsteemide käivitamist mobiilsete andmekandjatega. Secure Boot'i kasutamine on igal juhul soovitatav.

Turvakontseptsioon / turvapoliitika

Usaldava platvormi mooduli (ingl Trusted Platform Module, TPM) korral on tegemist krüptokiibiga, mis pakub mh turvafunktsioone (juhuslike arvude loomine, räsifunktsioonid), platvormi oleku turvalist mõõtmist ja turvalist salvestit rakenduste võtmematerjali (nt kõvaketta krüpteerimine) ning operatsioonisüsteemi jaoks. Mõnede arvutite korral tuleb see TPM-kiip sisse lülitada seadistamise kaudu BIOS-is. Standardi kohaselt võtab Windows alates versioonist Windows 8 ülemvõimu olemasoleva, mittekäivitatud TPM-i üle operatsioonisüsteemi käivitamise ajal. TPMi kasutamine Windows 8-s on sellega seotud kontrolli kaotamise tõttu vaieldav. Nii võiks operatsioonisüsteemi funktsioonide kasutamisega kahjurvaraprogrammid TPM-is kaitsta võtit kolmandate isikute (k.a administraatorid, audiitorid või kriminalistid) juurdepääsu eest ja krüpteerida sellega nt kasutajaandmeid, mis välistab kolmandate tootjate tarkvara juurdepääsu andmetele. Seetõttu tuleb TPM-i kasutust asutuses eelnevalt kaaluda ja teha sellekohased otsused.

Kasutajate kontseptsioon

Kasutajate kontseptsiooni väljatöötamisel tuleb kindlaks määrata, kuidas käiakse ümber lokaalsete ja tervet domeeni puudutavate kasutajakontodega. Serveritesse salvestatavate kasutajaprofiilide rakendamine mõjutab eelkõige Backup - strateegiat ning EFS-i (Windows Encrypting File System) kasutamist. Alates Windows 8 juurutamisest on olemas võimalus, et kasutajad logivad süsteemi sisse ka Windows Live ID-ga või ühendavad kasutajakonto Live-ID-ga. See peab võimaldama kasutajatel kasutada pilvteenuseid, nagu nt OneDrive (varem SkyDrive), või sünkroonida süsteemide vahel automaatselt andmeid, nagu seadistusi äppide või lemmikute jaoks. Siinjuures on ka võimalus, et tundlikud või isikuandmed väljuvad teadlikult või tahtmatult ettevõttest ning tekib kontrolli kaotuse oht andmete üle. Et Windowsi süsteemi sisselogimisel Live-ID abil on olemas võimalus, et konfidentsiaalsed andmed sünkroonitakse seadmetega, mis ei ole asutuse kontrolli all, tuleks sisselogimine Live-ID-ga keelata rühmapoliitikaga: kasutajad ei tohi li-

sada Microsofti kontosid või nendega sisse logida menüüs Arvuti konfiguratsioon | Windowsi seadistused | Turvaseadistused | Kohalikud poliitikad | Turvavalikud | Kontod: Microsofti kontode blokeerimine. Igal juhul tuleb siinjuures tähelepanu pöörata sellele, et poliitikat tuleb rakendada enne kui kasutaja Live-ID-ga sisse logib. Kui Live-ID-ga on profiil juba loodud, on sellega ka hiljem võimalik sisse logida, kui poliitika on juba jõus.

Kui tahetakse kasutada Microsofti pilvteenuseid, on Windows 8 keskkonnas võimalik ühendada domeenikonto Live-ID-ga, mille kaudu toimub edaspidi domeeni sisselogimine ja võimalik on ka Windows Store'i kasutamine. Sünkroniseerimisseadistuste konfigureerimine toimub rühmapoliitika kaudu, mis reguleerib, milliseid pilve funktsioone kasutada ja millised andmeid saab selle kaudu sünkroniseerida. Neid sünkroniseerimisseadistusi saab konfigureerida menüüs Arvuti konfiguratsioon | Administratiivsed mallid | Windowsi komponendid | Seadistuste sünkroniseerimine.

Kui pilve salvestiteenuse OneDrive kasutamine ei ole vajalik, tuleks pilve salvestifunktsioonid täielikult inaktiveerida, et failid ei väljuks märkamatult ettevõttest. OneDrive'i inaktiveerimine on võimalik seadistuse „SkyDrive'i kasutamise keelamine failide salvestamiseks" poliitikas Arvuti konfiguratsioon | Administratiivsed mallid | Windowsi komponendid | SkyDrive. Pilve salvesti teenuste kasutamiseks rühmatöö funktsiooniga ettevõtte kontekstis pakub Microsoft OneDrive Pro ettevõtetele võrgusalvestit. Dokumentide raamatukogu haldavad asutuse administraatorid.

Kasutajakontseptsiooni kavandamisel tuleb reguleerida kasutajakonto kontrollimist (User Account Control, UAC) (vt M 4.340 Windows kasutajakonto haldamise (UAC) kasutamine alates Windows Vistast). Seadistused soovitatakse valida nii, et standardkasutajate jaoks ei oleks võimalik privileegide suurendamine.

Halduskontseptsioon

Halduskontseptsioon tuleb koostada eeltööde käigus enne Windows 7 kasutuselevõtmist. Eriti oluline on määratleda, kuidas peaks toimuma klientide kaughaldus ning kuidas tuleks lokaalsete halduskontodega ümber käia. Vastav kontseptsioon peaks käsitlema muuhulgas ka personaliküsimusi ja organisatoorse töö vastutusalasid. Halduskontseptsiooni tuleb juurutada töötajate vastutusalade lahutamine (Segregation of Duties). Selle printsiibi rakendamist on tarvis planeerida nii organisatoorsest kui ka tehnilisest vaatevinklist. Juhul kui Windows 7 süsteeme rakendatakse Active Directory keskkonnas, tuleb kindlaks määrata haldusega seotud vastutus ja volituste piirid, samuti Active Directory klient- ja kasutajaobjektidele antavate haldamisõiguste suunised.

Windows 8 juurutamisega juurutati ka äppide kontseptsioon, mis on täiendus klassikalistele töölauarakendustele. Äpid on rakendused, mida kasutajad võivad alla laadida Microsoftile kuuluvast veebipoest (Windows Store). Äppide eelis on nende lihtne installeerimine. Windows Store'i kasutamiseks tuleb sisse logida kas Windowsi konto (Live-ID) või sisselogimiskontoga, mis on Live-ID-ga ühendatud. Üldiselt on ettevõtete puhul soovitatav eemaldada süsteemist standardsed äpid, mida ei vajata, ja lubada installeerida üksnes veebipoest saadavaid äppe. Samuti on võimalik kasutada ettevõtte oma App-Store'i, et äppe levitada. Peale selle pakub Windows mehhanismi Sideloading, mille abil saab äppe ilma App-Store'ita otse sihtarvutitele installeerida. Sideloading'i kasutamise eeldus on Windows 8

Enterprise litsentsi olemasolu ja sihtsüsteemi ühendus domeeniga.

Windowsi veebipoe kasutamist tuleb konfigureerida asutuse turvasuunistest ja andmekaitsenõuetest lähtudes. Windows Store'i juurdepääsu seadistusi saab konfigureerida rühmapoliitika kaudu menüüs Arvuti konfiguratsioon | Windowsi seadistused | Administratiivsed mallid | Store. Windows 8 keskkonnas on võimalik ka kontrollida, kas äppidel tohib olla juurdepääs kasutaja asukohale, nimele ja profiilipildile.

Logimise/ auditeerimise kontseptsioon

Windows 7 süsteemi turvalisuse tagamiseks on tarvis jälgida, kas kehtestatud turvasuunistest (vt M 2.325 Windows Vista ja Windows 7 turvapoliitika kavandamine) peetakse kinni või mitte. Kogutavate andmete puhul on väga oluline välja töötada nende regulaarse läbitöötamise organisatsioonilised ja tehnilised küljed. Erinevad turbeaspektid, mida on tarvis jälgida logimisfunktsiooni korraldamisel, on kogutud meetmesse M 4.344 Windows Vista, Windows 7 ja Windows Server 2008 süsteemi seire. **Andmete talletamine, varundus ja krüpteerimine**

Kindlaks tuleb määrata koht, kuhu salvestatakse kasutajate andmed (vt M 2.138 Struktureeritud andmetalletus). Üldjuhul on soovitatav hoiduda andmete salvestamisest klientsüsteemidesse. Selleks peab serveris olema sobiv salvestamistaristu. Strateegia tuleb valida iga juhtumi puhul eraldi, lähtudes konkreetsetest asjaoludest. Mõningate kasutusvaldkondade, nt kaasaskantavate IT-süsteemide puhul on andmete talletamine klientsüsteemis siiski vajalik. Selleks tuleb planeerida kliendi andmetalletus ja selle (krüptograafiline) kaitse (vt M 4.29z Kaasaskantavatele IT-süsteemidele mõeldud krüpteerimistoote kasutamine). Vajalikud tehnilised meetmed, mis peavad tagama lokaalse andmetalletuse turvalisuse (nt kõvaketta krüpteerimine, EFS või offline -failide krüpteerimine), tuleb planeerida kindlasti juba enne lokaalse andmetalletuse kasutuselevõttu. Andmete talletamiseks klientsüsteemis ja andmete krüpteerimiseks on Windows 7-s olemas BitLocker, mis tagab buutimispartitsiooni offline -krüpteerimiskaitse. Offline-krüpteerimiskaitse tähendab seda, et krüpteerimisega saavutatav kaitse toimib vaid sel ajal, kui süsteem on välja lülitatud. Windows 7 puhul suudab BitLocker krüpteerida juba ka teisi partitsioone.

BitLocker koos TPM-iga (Trusted Platform Module) tagab buutimisprotsessi käigus ka süsteemi tervikluse. BitLockeri kasutuselevõttu tuleks kaaluda eriti kaasaskantavate IT-süsteemide puhul. Kui BitLockerit soovitakse kasutusele võtta, tuleb kindlaks määrata ka see, millist autentimismeetodit hakatakse kasutajate autentimiseks rakendama (valida saab nelja variandi vahel). Lisateavet BitLockeri kohta leiate M 4.337z BitLockeri Drive Encryption kasutamine . Tagamaks kasutajate ja projektidega seotud spetsiifiliste andmete, samuti programmide ja operatsioonisüsteemi andmete selge eraldamine, tuleb planeerida sobiv kataloogistruktuur. Näiteks võib kasutada kaht põhikataloogi – \ Projektid ja \ Kasutajad –, kuhu luuakse omakorda alamkataloogid salvestatavate projektide ja kasutajate failide tarbeks. Windows 7 juurutamisel tuleb välja töötada ka sobiv andmevarundusstrateegia. Sobiv strateegia tuleb välja töötada kõikidele IT-süsteemidele ja andmeliikidele.

Konkreetsed lahendused olenevad suurel määral klientsüsteemidesse salvestatud andmeliikidest. Neil juhtudel, kus klientsüsteemides andmeid ei talletata ja kasutatakse vaid tüüptarkvara ning kasutajate profiilid on salvestatud serveritesse,

võib olenevalt olukorrast andmete varundamisest klientsüsteemides ka loobuda. Seevastu neil juhtudel, kus andmed salvestatakse Windows 7-ga töötavatesse arvutitesse, tuleb andmevarunduse planeerimisel kindlasti ka nende andmetega arvestada (vt M 6.32 Regulaarne andmevarundus ja M 6.33 Andmevarunduskontseptsiooni loomine). Andmevarunduskontseptsiooni koostamisel tuleb kindlaks määrata EFS-i või BitLockeri rakendamine. Kui otsustatakse EFS-i kasuks, tuleb üldjuhul järgida meedet M 6.56 Andmevarundus krüptoprotseduuride kasutamisel . Eriti oluline on andmevarunduskontseptsiooniga reguleerida, kuidas tuleks taasteprotseduuride käigus võtmematerjaliga ümber käia (vt M 4.147z EFS-i turvaline kasutamine Windows 'i keskkonnas).

Windowsi versioonide kasutuselevõtmisel tuleb välja töötada ka sobiv andmevarunduse strateegia. Protseduur tuleb iga IT-süsteemi ja andmeliigi jaoks eraldi kindlaks määrata. Rakendus sõltub suurel määral klientsüsteemidesse salvestatud andmeliikidest. Juhul kui klient-süsteeme ei rakendata andmete salvestamiseks, vaid ainult tüüptarkvara kasutamiseks ning kasutajate profiilid on salvestatud serveritesse, võib mõningatel juhtudel klient-süsteemi baasil toimivast andmevarundusest isegi loobuda. Seevastu juhtudel, kus salvestatakse Windowsi klientide andmeid, tuleb andmevarunduse kavandamisel arvestada ka nende andmetega. Täiendavat teemakohast teavet leiate meetmetest M 6.32 Regulaarne andmevarundus ja M 6.33 Andmevarunduskontseptsiooni loomine .

Backup-stratreegia kavandamisel tuleb arvesse võtta EFS-i või muud kliendipoolset kõvaketta krüpteeringut. EFS-i rakendamisel tuleb üldjuhul järgida meedet M 6.56 Andmevarundus krüptoprotseduuride kasutamisel. Eriti oluline on Backupkontseptsiooniga reguleerida, kuidas tuleks ümber käia võtmematerjaliga taasteprotseduuride käigus (vt ka M 4.147z EFS-i turvaline kasutamine Windows 'i keskkonnas).

Windows toetab tänapäeval peaaegu igas arvutis olemas olevat krüptokiipi TPM (Trusted Platform Module), et salvestada selles turvaliselt võtmed ja sertifikaadid. Ühelt poolt suurendab see krüptograafiliste rakenduste turvalisust, aga teiselt poolt piirab ka kasutajate ja administraatorite juurdepääsu, sest neile on ette nähtud üksnes piiratud juurdepääs TPM-sisudele. Seetõttu tuleb TPM-i kasutamisel rakendada täiendavaid meetmeid krüptograafiliste saladuste kaotamise vastu tõrkevigade tõttu.

Roll-out

Planeerimisfaasis tuleb välja töötada kõik installeerimise käigus läbitavad etapid ehk roll-out -tööetapid. Muuhulgas tuleb täpselt kindlaks määrata töötajate vastutus seoses erinevate roll-out -tööetappidega. Lisaks tuleb koostada ka roll-out-avariikontseptsioon. Vastav avariikontseptsioon peab tagama, et üleviimiskatse ebaõnnestumisel oleks võimalik töötav süsteem kiiresti taastada. Kavandamisetapis tuleb välja töötada kõik installeerimise käigus läbitavad etapid ehk roll-outtööetapid. Muu hulgas tuleb täpselt kindlaks määrata töötajate vastutus seoses erinevate roll-out-tööetappidega. Lisaks tuleb koostada ka roll-out-hädaolukorra kontseptsioon. Vastav hädaolukorra kontseptsioon peab tagama, et üleviimiskatse ebaõnnestumisel oleks võimalik töötav süsteem kiiresti taastada. Kui lisaks kliendi operatsioonisüsteemidele migreeritakse ka server, tuleks kõigepealt teostada serveri üleminek. Seejärel tuleb migreeritud klientidele üle võtta uuesti loodud või muudetud rühmapoliitikad, Active Directory seaded või volituste kontseptsioonid.

Täiendavad kontseptsioonid

Lisaks eelpool loetletud kontseptsioonidele võib sõltuvalt kasutusvaldkonnast tarvis minna ka veel täiendavaid kontseptsioone, milleks võib olla nt nimekontseptsioon (arvutite, kasutajarühmade ja kasutajate nimeandmise põhimõtted), tarkvara jagamise kontseptsioon või rakenduste üleviimise kontseptsioon. Windows 7 süsteemide turvalisust mõjutab nendest kõige enam rakenduste üleviimise kontseptsioon (nt registreerimise pääsuõiguste nõrgendamise tõttu) ning seepärast tuleb selle planeerimisel olla väga hoolikas. Kõik täiendavalt vajalikud kontseptsioonid tuleb samuti välja töötada planeerimistööde käigus. Reeglina on ettevõttes või ametiasutuses vastavad kontseptsioonid juba olemas ning on tarvis ainult kontrollida, kas neid on võimalik rakendada ka Windows 7 keskkonnas. Planeerimistööde käigus tuleks luua muuhulgas ka ülevaade, milliseid kasutajaid ja administraatoreid on tarvis koolitada ning panna paika ka vastavate koolituste toimumisajad. Eriti põhjalikult tuleb haldamise ja turvalisuse osas koolitada administraatoreid. Tuleks kasutusele võtta alles pärast piisavat koolitust.

Lisaks eespool loetletud kontseptsioonidele võib olenevalt kasutusvaldkonnast tarvis minna veel täiendavaid kontseptsioone, milleks võib olla nt nimekontseptsioon (arvutite, kasutajarühmade ja kasutajate nimeandmise põhimõtted), tarkvarajagamise kontseptsioon või rakenduste üleviimise kontseptsioon. Windowssüsteemi turvalisust mõjutab nendest kõige enam rakenduste üleviimise kontseptsioon (nt registreerimise pääsuõiguste nõrgendamise tõttu) ning seepärast tuleb selle kavandamisel olla väga hoolikas.

Kõiki täiendavaid kontseptsioone tuleb arvesse võtta ka kavandamisetapis. Reeglina on ettevõttes või ametiasutuses vastavad kontseptsioonid juba olemas ning on tarvis ainult kontrollida, kas need sobivad ka rakendatud Windowsi operatsioonisüsteemiga. Muu hulgas tuleks ka kavandada, milliseid kasutajaid ja administraatoreid on tarvis koolitada ning millal see peaks toimuma. Eriti põhjalikult tuleb Windowsi versioonide haldamise ja turvalisusega seoses koolitada administraatoreid. Windowsi süsteemid tuleks kasutusele võtta alles pärast piisavat koolitust.

Kontrollküsimused:

- Kas kõik konkreetse kasutuse jaoks vajalikud kontseptsioonid on koostatud?
- Kas on olemas poliitikad Windowsi süsteemide uue installatsiooni või ülemineku/uuenduse jaoks ja kas need on kõikidele osalistele kättesaadavad?
- Kas ülemineku tõttu laiendatud pääsuõigused ja domeenide nõrgendatud turvaseadistused viiakse pärast ülemineku lõpetamist tagasi kõige kõrgemale võimalikule turvalisuse astmele?
- Kas toimub Windows-kliendi rühmapoliitikate konfigureerimine vastavate tööriistadega, nagu nt RSAT?
- Kas Windows-kliendi operatsioonisüsteemide jaoks on olemas kasutaja- ja halduskontseptsioon?
- Kas on olemas eeskirjad, et kontrollida kindlaksmääratud turvapoliitikatest kinnipidamist?
- Kas Windowsi versioonide jaoks on olemas kontseptsioon andmete salvestamiseks, varundamiseks ja kasutajaandmete krüpteerimiseks?
- Kas on olemas nõuded äppide installeerimiseks Windows-Store'ist ja nende kasutamiseks? Kas nõudeid võetakse vastavalt arvesse ka kavandamisel?
- Kas pilvteenuste, nt OneDrive'i kasutamine on klient-süsteemi turvapoliitikas reguleeritud, ja kas sellega arvestatakse juurutamise kavandamisel?

- Kas on tehtud põhjendatud otsus TPM-i kasutamiseks, ning kas on olemas adekvaatsed kontseptsioonid seal salvestatud krüptograafiliste andmete kaotamise puhuks?

M 2.325 Windows 7 turvapoliitika kavandamine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: IT-juht, administraator

Windows 7 kasutuselevõtu üheks olulisemaks organisatoorseks ülesandeks on asjakohase turvapoliitika kavandamine ja sõnastamine. Antud turvapoliitika peab kindlaks määrama kõik Windows 7 kasutamisele kehtestatavad turvasuunised. Windows 7 turvapoliitikaga defineeritud nõuded rakendatakse ellu vastavate turvaseadistustega operatsioonisüsteemi tasandil ja/või organisatoorsete meetmete abil. Neil juhtudel, kus tehniliste meetmete rakendamisest üksi ei piisa, tuleb kahte valdkonda omavahel kombineerida, st tehnilist teostust tuleb toetada organisatoorsete meetmetega. Võimalusel tuleks organisatoorsetele meetmetele alati eelistada tehnilisi lahendusi.

Loodav Windows 7 turvapoliitika peab lähtuma vastavas ettevõttes või ametiasutuses seni kehtinud turvapoliitikast ning ei tohi minna sellega vastuollu. Reeglina toimub Windows 7 turvapoliitika koostamisel olemasolevate suuniste mugandamine või asjakohane täiendamine. Selliste tööde käigus tuleb pöörata kõrgendatud tähelepanu Windows 7 omastele tehnoloogiatele (nt Remote Desktop -ile). Windows 7 infrastruktuuri planeerimisel peab arvestama, et enamasti tuleb lähtuda küll üldkehtivast turvapoliitikast, kuid planeerimine ise mõjutab Feedback -protsessi kaudu omakorda ka turvapoliitikat. Windows 7 turvapoliitika koostamisel on oluline ka jälgida, et tööde käigus arvestataks kõikide kehtivate seadustest tulenevate ettekirjutustega. Windows 7 turvapoliitika tuleb dokumenteerida ja vajalikus mahus klient-server-võrgu kasutajatele teada anda. Seda peaksid tundma ja rakendama kõik administraatorid. Järgnev teemade loetelu annab üldise ülevaate valdkondadest, mida tuleks käsitleda vastava turvapoliitika väljatöötamisel. Sõltuvalt ettevõtte või ametiasutuse konkreetsetest kasutusvaldkondadest, tuleb loomulikult arvestada veel ka täiendavate aspektidega.

Füüsiline turvalisus

Windows 7 turvapoliitika väljatöötamisel tuleb käsitelda füüsilist turvalisust, kuna Windows 7 puhul on tegu klientoperatsioonisüsteemiga, mida rakendatakse ka kaasaskantavates arvutites. Seetõttu tuleb siinkohal rakendada füüsilist turvalisust kajastavaid üldisi soovitusi moodulitest B 3.201 Klient ja B 3.202 Autonoomne IT-süsteem .

Vastutusalad

Turvapoliitika peab määratlema töötajate vastutusalad seoses Windows 7 süsteemide käitamisega. Iga administraatori puhul tuleb kindlaks määrata tema konkreetne vastutusala. Erinevad vastutusalad võivad olla näiteks:

- turvaparameetrite muutmine (kohapeal),
- turvaparameetrite muutmine Active Directory -s
- süsteemide haldamine Active Directory -s
- logiandmete kontrollimine
- pääsuõiguste ja süsteemiõiguste andmine
- konfiguratsioonimuudatuste kinnitamine ja läbiviimine ning tarkvara installeerimine
- paroolide deponeerimine ja vahetamine ning
- andmevarunduse ja andmete taastamise läbiviimine.

Ka lõppkasutajatel on klient-server-võrgus teatud vastutus, juhul kui neile on soovitakse anda õigusi teatud administratiivsete operatsioonide teostamiseks. Tavaliselt piirduvad need vastutusalad siiski juurdepääsuõiguste määramisega oma failidele, juhul kui need on konkreetselt määratud ja neile ei kehti hierarhias kõrgemal asuva kataloogi eelseadistused. Süsteemide haldamisega peaksid tegelema piisava koolituse saanud võrguadministraatorid ning hädaolukorraks valmisoleku planeerimise raames tuleb tagada sobivate asendajate olemasolu.

Kasutajakontod

Enne kasutajakontode sisseseadmist on tarvis otsustada, kas vastavad kontod luuakse kohapeal või Active Directory -s. Haldamise lihtsustamise eesmärgil soovitatakse kontod üldjuhul luua Active Directory -s. Lisaks kontode loomisele tuleb kindlaks määrata ka kontodele kehtestatavad piirangud. Eriti puudutab see paroolide kasutamist ja süsteemi reageerimist sisselogimiskatsetele.

Windows 8-ga viidi täiendavalt sisse sisselogimine Microsofti kontoga (Windows-Live ID), mis võimaldab kasutajatel sisse logida igasse Windows 8 arvutisse. Live ID-ga võimaldatakse ka pilvteenuste kasutamist ning äppide ja rakenduste sünkroniseerimist mitmete arvutite vahel. Kontrollimatu andmekaotuse suurenenud riski tõttu ei tohiks ettevõtte keskkonnas kasutada sisselogimist Live-ID-ga ega ka Live-ID ühendamist Active Directory kontoga.

Volituste kontseptsioon

Windows 7 turvapoliitika peab sisaldama muu hulgas ka õiguste kontseptsiooni. Õiguste kontseptsioon sätestab ennekõike nii tavaliste kui ka haldamisega tegelevate kasutajate õigused. Probleeme tekitab siinkohal tõsiasi, et Windows 7 ei ole nii võimalusterohke. Seetõttu on tarvis planeerida ja rakendada vastav rühmakontseptsioon (kohapealne või domeenis). Selleks tuleb luua vastavad kasutajarühmad, mis järgiksid organisatsiooni hierarhiat ja olemasolevate töörollide jaotumist. Õiguste kontseptsiooni ellurakendamine toimub sobilike õiguste andmisega eri kasutajarühmadele ning vajadusel ka asjakohaste suuniste (nt Software Restriction Policies) koostamise abil. See eeldab, et töötajate vastutusalad ja tööprotsessid tuleb läbi töötada ja koostada vastav kontseptsioon.

Volituste kontseptsioonis peaksid kajastuma järgmised valdkonnad:

- Süsteemiõigused ja kasutajaõigused (nt õigus arvutisse sisse logida kohapeal või kaugpöörduse abil, õigus süsteemi välja lülitada).
- Ühiskasutusse antud võrgu juurdepääsuõigused (eriti neil juhtudel, kus kasutatakse Peer-to-Peer funktsiooni).
- Failide juurdepääsuõigused (rakendus- ja süsteemifailidele).
- Juurdepääsuõigused Registry sissekannetele.

Kasutajaõigusi tuleb hoolikalt planeerida, sest neil on eesõigus kõikide teist liiki õiguste, eriti faili- ja kataloogiõiguste ees. Kasutajaõigused kehtivad Windows 7-ga töötava süsteemi kohta tervikuna. Kasutajaõiguste andmiseks rakendatakse grupipoliitikaid, mis koostatakse Active Directory baasil toimiva domeeni kasutajate puhul otse Active Directorys ning ülejäänud süsteemide puhul lokaalselt (vt M 2.326 Windows Vista ja Windows 7 grupeerimissuuniste planeerimine). Õiguste andmisel tuleb jälgida, et õigused seotaks eelistatult kasutajagrupi, mitte üksikute kasutajatega. Kasutajate kontseptsiooni planeerimisel tuleb Windows 7 puhul kindlaks määrata, kuidas hakatakse kasutajakontosid haldama (User Account

Control – UAC) (vt M 4.340 Windows kasutajakonto haldamise (UAC) kasutamine alates Windows Vistast).

Side turvalisus

Windows 7 turvapoliitika peab käsitlema ka andmeside jaoks vajaliku turvalisuse tagamist. Turvapoliitika koostamisel on esmalt soovitatav sõnastada andmeedastuse peamised nõuded (planeeritav eesmärk) ning seejärel töötada välja erinõuded, mis tulenevad kohapealsetest konkreetsetest oludest.

Nõuete ja nende juurde kuuluvate erandite väljatöötamisel on kõige olulisemateks teemadeks autentsus, konfidentsiaalsus, terviklus ja käideldavus. Turvapoliitikas sõnastatud nõuete tehniline teostus võib sõltuvalt rakendatavatest mehhanismidest ja kohapealsetest oludest suurel määral erineda. Kahe võimaliku teostuse kirjelduse leiate meetmetest M 5.90 IPSec'i protokolli kasutamine Windowsi keskkonnas ja M 5.123 Võrgusuhtluse kaitse Windowsis . Nõuete rakendamisel tuleb analüüsida, kas Windowsi enda tulemüür on teiste tootjate eraldi tulemüüridega võrreldes funktsioonidelt võrdne. Windowsi enda tulemüür suudab täita tavapäraseid turbenõudeid enamasti alles alates versioonist Windows 7. Kui institutsioonil on juba olemas tsentraalselt hallatav turbetarkvara, on selle tulemüürifunktsioonid sageli palju paremini turbetarkvaraga integreeritud kui Windowsi erinevate versioonide omad. Eriti just segakasutuskeskkondade puhul on eelnevat arvesse võttes soovitatav sõnastada eraldi igat tüüpi süsteemide turbeastmed ning arvestada sealjuures tehnilise koostöövõime, soetamiskulude ja tsentraalse juhtimise võimalusega.

Alates Windows 7-st saab sisseehitatud sensorite, nt GPS-sensorite andmeid ka kokku koguda. Neid andmeid kasutavad rakendused ja teenused, eelkõige internetipõhised teenused. Sensoriandmetele pääseb enamasti juurde kõikide installitud rakenduste kaudu ning ka teenuse- ja kasutajakontodega. Seetõttu tuleks see funktsioon tavajuhul desaktiveerida, sest muidu on tegemist IT-süsteemi kasutajate andmealase enesemääramisõiguse rikkumisega. Kui sensoreid on tarvis tööle lülitada, tuleks esmalt täpselt paika panna, mis otstarbel ja kuidas tohib neid kasutada. Kindlaks tuleb määrata, millisel tarkvaral ning millistel teenuse- ja kasutajakontodel tohib olla juurdepääs sensoriandmetele. Samuti tuleb teavitada töötajaid sellest, mis liiki andmeid sel moel kogutakse ja kuidas neid edasi kasutatakse.

Kõigepealt tuleb kontrollida, kas kasutajatelt on vaja võtta eraldi nõusolek. Täiendava turbemeetmena tuleks süsteem krüpteerida ja varustada juurdepääsukaitsega, sest muidu on oht, et kolmandad isikud võivad sensoriandmeid ekstraheerida ning kasutada neid inimestega manipuleerimiseks (social engineering).

Logimine

Windows 7-l on võimalusi turvalisust puudutavate sündmuste logimiseks (nt edukate ja/või ebaõnnestunud sisselogimiskatsete registreerimiseks). Siiski tuleks arvestada, et kõikide võimalike logifunktsioonide täielik rakendamine võib suurel määral koormata süsteemi ja kulutada palju kettaruumi. Logifunktsiooni seadistuste määramisel tuleb arvestada süsteemiseire üldkontseptsiooniga.

Rakendused ja äpid

Koos Windows 8-ga viidi alternatiivselt klassikalise töölaua programmi kasutamisele täiendavalt ellu uus äppide kontseptsioon. Äppe saab salvestada Microsofti enda Windows Store'i kaudu Internetist. Windows Store pakub kasutajatele võimalust äppe otsida ja neid süsteemi installeerida. Et äpid vajavad konkreetsete

funktsioonide jaoks juurdepääsu erinevatele ressurssidele, nt kalendrile, aadressiraamatule või GPS-i andurile, ning võivad seeläbi ligi pääseda ka võimalikele kriitilistele andmetele, tuleb turvapoliitika planeerimisel kavandada ja reguleerida ka Windows Store'ist äppide installeerimist ja kasutamist. Turvatoodete, nt viirusetõrje valimisel tuleks tähelepanu pöörata ka sellele, et rakendatav toode oleks võimeline tuvastama ka kahjulikke või modifitseeritud äppe, sest kunagi ei saa täielikult välistada, et vaatamata kvaliteedikontrollile ja Windows 8 äppide nõuetele võivad kahjulikud failid sattuda ka Windows Store'i. Kuidas toimub ettevõtte kontekstis äppide lubamine või nende kaitsmine, tuleb reguleerida vastavas äppide suunises. Täiendavaid suuniseid võib leida abivahendist Äppide kasutamine Windows 8 keskkonnas.

Protokollimine

Kõik Windowsi versioonid pakuvad palju võimalusi turvalisust puudutavate sündmuste protokollimiseks (nt edukate ja/või ebaõnnestunud katsete registreerimiseks). Siiski tuleks arvestada, et kõikide võimalike logifunktsioonide täielik rakendamine võib suurel määral süsteemi koormata ja kulutada palju mäluruumi. Protokolliseadistuste määratlemisel tuleb arvesse võtta süsteemiseire üldkontseptsiooni (vt M 4.344 Windows Vista, Windows 7 ja Windows Server 2008 süsteemi seire).

Kasutusvaldkondade spetsiifikaga seotud aspektid

Sõltuvalt kasutusvaldkonnast tuleb planeerimistööde käigus arvesse võtta ka täiendavaid spetsiifilisi nõudeid. Näiteks täiendavad turbeaspektid võivad eriti kergesti tekkida Peer-to-Peer teenuste kasutamisega seoses ning turvasuunised peavad neid valdkondi kajastama (vt M 5.152 Info ja ressursside vahetamine võrdõigusteenuste (p2p) kaudu). Võimalusel tuleks Peer-to-Peer funktsioonide kasutamisest loobuda, sest need võivad mõjutada klient-server-võrgu ohutust. Windows 7 süsteemi mobiilse rakenduse erinevad aspektid on koondatud meetmesse M 2.442 Windows Vista ja Windows 7 kasutamine kaasaskantavates arvutites . Üheks täiendavaks näiteks kasutusotstarbe spetsiifikast tulenevate turvaaspektide kohta on EFSi kasutamine (vt M 4.147z EFS-i turvaline kasutamine Windows 'i keskkonnas). Analoogselt tuleb arvesse võtta BitLocker'i kõvaketta krüpteerimise kasutust (vt M 4.337z BitLockeri Drive Encryption kasutamine).

Microsoft Baseline Security Analyzer (MBSA)

Microsoft Baseline Security Analyzer (MBSA) on tasuta tööriist, mis uurib Windowsi installatsioonis tüüpilisi turvalisusega seotud probleeme. MBSA kasutamine võib turvalisema Windowsi konfiguratsiooni loomist toetada sellega, et seda käitatakse vastavatel süsteemidel kohe alguses ja vajaduse korral regulaarselt.

Kontrollküsimused:

- Kas Windows 7 turvapoliitika käsitleb kõiki olulisi valdkondi?
- Kas Windows 7 turvapoliitika rakendamisel arvestati Feedback - protsessiga?
- Kas Windows 7 loodud turvapoliitika on dokumenteeritud ning kas see on edastatud kasutajatele ja administraatoritele?
- Kas kõik kasutajad on läbinud Windows 7 turvapoliitika rakendamiseks vajaliku ettevalmistuse?

- Kas Windowsi klientide turvapoliitika lähtub ettevõtte või asutuse kehtivatest turvapoliitikatest?
- Kas klientvõrgu kõiki kasutajaid on piisaval määral teavitatud Windowsi mobiilse kasutuse turvapoliitikast?
- Kas vastutused Windows-klientide kasutamiseks on reguleeritud turvapoliitikas?
- Kas turvapoliitika sisaldab õiguste kontseptsiooni, milles reguleeritakse nii tavaliste kasutajate kui ka administraatorite õigusi?
- Kas klientidel alates Windows 8-st võetakse arvesse Windows Store'i äppide kasutamist?
- Kas User Account Control'i (UAC) kasutamine on reguleeritud õiguste kontseptsioonis?
- Kas turvapoliitikas on reguleeritud ka turvalisusega seotud nõuded andmete edastamise korral?
- Kas turvapoliitika planeerimise aluseks on Windows-klientide erinevad kasutusstsenaariumid?

M 2.326 Windows 7 grupeerimissuuniste planeerimine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: IT-turvaosakond, administraator

Grupipoliitikad on loodud selleks, et konfiguratsiooni seadete kogumikku, mille hulka kuuluvad eriti just ka turvaseadistused, oleks võimalik rakendada teatud objektide rühmale korraga. Grupipoliitika niinimetatud objekt (ingl Group Policy Object, GPO) hõlmab etteantud konfiguratsiooniparameetrite kogumikku. Igale parameetrile saab määrata konkreetse väärtuse, mis võib sõltuvalt olukorrast pärineda ka ainult ühest piiratud väärtusskaalast. Üldjuhul saab väärtuse valikutes määrata seadistuseks ka defineerimata, mille puhul kehtivad vastava parameetri jaoks automaatselt standardseadistused.

Kliendi grupipoliitikaid tuleks planeerida ja kasutusele võtta standardsete protsessidena, nagu järgnevalt kirjeldatud:

1. Klientrakenduste nõuete ja turbeseadistuste väljaselgitamine ning klientkonfiguratsiooni defineerimine
2. Otsuse langetamine selle kohta, milliseid seadistusi tuleb hallata tsentraalselt
3. Katseinstallatsioon
4. Grupipoliitikatega hallatavate seadistuste (ja kontrollnimekirjade) dokumenteerimine, klientide ettevalmistuskontseptsiooni kohandamine
5. Sündmusi mõnda haldusserverisse ümber suunata ja seal jälgida (nt System Centeri serverisse) või
6. klientides programmiga GPLogView.exe (eraldi Microsofti käest saadaval) analüüsida.

Seadistuste eksportimine:

- a. Klientidesse tööriistadega gpedit.msc, rsop.msc või gpresult;
- b. või määrata domeenikontrolleriga GPO-sündmustele sündmustelogi filtrid ja regulaarselt kontrollida, kas GPO-objekt(id) on veavabad ja töötavad.

Grupipoliitikad kujutavad endast peamist mehhanismi, mille abil on võimalik ellu rakendada M 4.244 Windowsi klientoperatsioonisüsteemide turvaline süsteemikonfiguratsioon soovitatud turvaseadistusi. Neid on võimalik rakendada parameetrite defineerimisel konkreetsete arvutite või kasutajate jaoks kohapeal (lokaalsete GPOde jaoks) ning Active Directory baasil toimivas keskkonnas lisaks ka asukoha ja domeeni tasandil ehk organisatsiooni erinevate allüksuste tasandil.

Grupipoliitika objekti piires on parameetrid kokku kogutud kas puulaadse struktuuri alusel või failisüsteemi stiilis teemade kaupa. Siinkohal tekib kõige kõrgemal tasandil üldine kaksikjaotus, st jaotumine arvuti ja kasutaja seadistusteks. Seeläbi on võimalik piiranguid defineerida nii arvuti- kui ka kasutajapõhiselt. Grupipoliitika osas, mis käsitleb kasutajaid, defineeritud seaded määravad muuhulgas kindlaks ka rakenduste eripärasid puudutavad piirangud. Täiendavate administratiivsete mallide importimisega on võimalik grupipoliitikate abil tsentraliseeritud moel konfigureerida ka veel teisi, nt Microsoft Office rakendusi. Üldjuhul soovitatakse

kasutada grupipoliitikaid, mis lähtuksid kas kasutajate eripäradest või rakenduste eripäradest. Grupipoliitika alla kuuluvaid kasutajaid ja arvuteid on võimalik üksikult desaktiveerida selliselt, et grupipoliitika rakendamisel jäetakse vastav desaktiveeritud osa selle mõju alt välja. Mõningates kasutusvaldkondades tõuseb selle tagajärjel kiirus. Grupipoliitika mõne mittevajaliku osa desaktiveerimise üle otsustamisel tuleb üldjuhul lähtuda hetkeolukorrast. Grupipoliitikate kehtestamisel tuleb arvestada erinevustega, mis tekivad lokaalsete grupipoliitikate ja Active Directory grupipoliitikate kehtestamise puhul. Lokaalsete grupipoliitikate defineerimisel ei saa rakendada kõiki neid seadistusi, mida on võimalik rakendada Active Directory baasil toimivate GPOde puhul. Näiteks puuduvad lokaalses grupipoliitikas Kerberose ja süsteemiteenuse poliitikad. Üksikud poliitikad nagu nt Paroolide salvestamine kõigile domeenikasutajatele reversiivse krüpteeringuga toimivad ainult siis, kui neid kasutatakse domeenis. Üksikparameetrite seadete määramisel tuleb seetõttu alati arvestada ka konkreetsete poliitikate mõjuvaldkondadega. Windows 7 puhul lihtsustab kasutajakontode halduse funktsioon (User Account Control – UAC) lokaalsete administraatorivolituste kasutamist tavakasutajatel.

Väljastatud administraatoriõigused on küll alati seotud kindla ülesandega ja nende kehtivusaeg on piiratud, kuid sellest hoolimata saavad kasutajad nende abil muuta ka süsteemi turbeseadistusi. Seetõttu tuleks turbeseadistusi konfigureerida üksnes Active Directory grupipoliitikatega. Nii ei saa neid enam lokaalselt muuta.

Lokaalsete grupipoliitikate planeerimine

Grupipoliitikate kehtestamisel tuleb arvestada lokaalsete grupipoliitikate ja Active Directory grupipoliitikate erinevustega. Lokaalsete grupipoliitikate defineerimisel ei saa rakendada kõiki neid seadistusi, mida on võimalik rakendada Active Directory baasil toimivate GPO-de puhul. Näiteks puuduvad lokaalses grupipoliitikas Kerberose ja süsteemiteenuse poliitikad. Mõned poliitikad, nt Store passwords using reversible encryption for all users in the domain, töötavad ainult domeenikeskkonnas. Seetõttu tuleb parameetriseadistuste kindlaksmääramisel alati arvestada ka konkreetsete poliitikate mõjuvaldkondadega.

Grupipoliitikate läbitöötamise järjekord on järgmine:

1. Lokaalsed grupipoliitikad
2. Asukoha GPO-d
3. Domeeni GPO-d
4. Organisatsiooniüksuste GPO-d

Windows 7 puhul on läbitöötamise järjekord sama, kuid valida saab kolme tasandi vahel, mis võimaldavad lokaalseid grupipoliitikaid, täpsemalt kokkukoondatud grupipoliitikaobjekte (Multiple Local Group Policy Objects – MLGPO) läbi töötada järgmises järjekorras:

1. Lokaalsete arvutite poliitikad;

2. Administraatorite ja mitteadministraatorite poliitikad (ainult kasutajapoliitikad);
3. Kasutajaspetsiifilised lokaalsed grupipoliitikad (ainult kasutajapoliitikad).

Siinkohal tuleb arvestada, et administraatorite ja mitteadministraatorite poliitikad ning kasutajaspetsiifilised lokaalsed grupipoliitikad sisaldavad üksnes kasutajapoliitikaid. Arvutipoliitikaid saab lokaalselt konfigureerida üksnes lokaalse arvutipoliitikaga.

Grupipoliitika valdkonnad

Arvuteid käsitlevas grupipoliitika osas eksisteerivad järgnevad valdkonnad: tarkvaraseaded, Windowsi seaded|skriptid, Windowsi seaded|turvaseaded, administratiivsed mallid. Tarkvaraseaded on olulised eelkõige siis, kui kasutatakse domeeni.

Nende abiga on võimalik grupipoliitika vahendusel tarkvara installeerida, värskendada ja deinstalleerida. Skriptipoliitikate abil on võimalik täpsustada skripte, mis käivitatakse süsteemi sisse- ja väljalülitamisel. Turvaseadete poliitikad jagunevad veel omakorda järgnevate valdkondade vahel: kontopoliitikad (paroolipoliitikad, konto sulgemispoliitikad, Kerberose poliitika), lokaalsed poliitikad (seirepoliitikad, kasutajaõiguste andmine, turvavalikud), sündmuste logi, piiratud grupid, süsteemiteenused, registreerimine, failisüsteem, avalike võtmete poliitikad, tarkvara piiramise poliitikad, IP-turvapoliitikad.

Turvaseadistusi käsitlevate poliitikate kehtestamisel tuleb pöörata tähelepanu järgnevale:

- Kontopoliitikad rakenduvad Active Directory keskkonnas vaid domeeni tasandil.
- Piiratud gruppide poliitikate rakendamine ei suuda takistada modifikatsioone seoses grupi liikmelisusega. Poliitika järgneva rakendumiskorra ajal vastavad volitamata modifikatsioonid lihtsalt tühistatakse.

Administratiivseid malle kasutatakse Windowsi koostisosade, süsteemi, võrgu ja muude rakenduste konfigureerimiseks.

Rakenduste eripäradest lähtuvad poliitikad

Rakenduste eripärasid käsitlevate poliitikate kasutusvaldkondadeks on Arvuti konfiguratsioon|Administratiivsed mallid ja Kasutajate konfigureerimine|Administratiivsed mallid. Lisaks Windowsi komponentide nagu nt NetMeetingu, Internet Explorer-i, Windows Explorer-i, ja Windows Messenger-i konfigureerimisele on nende abil võimalik konfigureerida ka teisi rakendusi, mis on varustatud oma administratiivsete mallidega nagu nt Microsoft Office. Sellised täiendavad administratiivsed mallid tuleb administraatoritel lisada konkreetselt eraldi vastavasse grupipoliitikasse. Enamikes ametiasutustes ja ettevõtetes on soovitatav võimalikult palju kasutada rakenduste eripäradega arvestavat konfigureerimist, mis toimiks tsentraliseeritult, kuna turvaseadistuste tsentraliseeritud ettekirjutamine aitab kõrvaldada paljusid turvariske. Valikud, milliseid komponente ja/või rakendusi tuleks vastavate GPOde abil tsentraalselt konfigureerida, sõltuvad suurel määral kohapealsetest oludest. Ka siinkohal tuleks üldjuhul lähtuda põhimõttest, et ebavajalikud rakendused ja komponendid (nt Windows Messenger)

tuleb desaktiveerida. Vajaminevad rakendused ja komponendid tuleb konfigureerida võimalikult laiaulatuslike piirangutega. Näiteks kui tekib vajadus kasutada Microsoft NetMeeting-ut, kuid Desktop Sharing funktsiooni ei soovita kasutada, tuleb see vastavate poliitikate defineerimisega desaktiveerida. Kuna Windows 7 pakub administratiivsete mallide puhul palju enam konfigureerimisvõimalusi kui sellele eelnenud versioonid, muudab see planeerimise varasemast mahukamaks.

Windows 7 puhul väärivad eraldi mainimist järgmised rakendusi juhtivate poliitikate turbeuuendused:

- Internet Exploreri laiendatud GPO-konfigureerimisvõimalused. Laiendustest puudutatud valdkonnad on Phishing Filter, kaitserežiimi (Protected Mode) tsentraalne aktiveerimine ja ActiveXi juhtelementide käsitlemine. Rakendusepõhiseid poliitikaid saab konfigureerida asukohas Computer Configuration | Administrative Templates | Windows Components | Internet Explorer ning asukohas User Configuration | Administrative Templates | Windows Components | Internet Explorer. | _ BitLockeri ajamikrüpteeringu jaoks mõeldud GPOkonfigureerimisvõimalused. Neid rakendusepõhiseid poliitikaid saab konfigureerida asukohas Computer Configuration | Administrative Templates | Windows Components | BitLocker Drive Encryption. TPM-iga seotud poliitikaid saab konfigureerida asukohas Computer Configuration | Administrative Templates | System | Trusted Platform Module Services.
- Windows Defenderile mõeldud GPO-konfigureerimisvõimalused. Kuna Windows Defender on välja töötatud peamiselt erakasutajaid silmas pidades, on sellega saavutatav turbeaste madal, mistõttu ei ole seda soovitatav kasutada töökeskkondades ainukese kahjurvara tuvastava ja käitleva lahendusena. Kolmandate tootjate turbelahenduse või kahjurvara eest kaitsva lahenduse paralleelset käitamist Windows Defenderiga tuleb esmalt töökeskkonda jäljendavas keskkonnas katsetada. Võimalikke probleeme saab vajaduse korral vältida Windows Defenderi desaktiveerimisega, kasutades rakendusepõhist poliitikat asukohas Computer Configuration | Administrative Templates | Windows Components | Windows Defender.

Kasutajate eripäradest lähtuvad poliitikad

Windows 7 võimaldab sõnastada kasutajate eripärasid arvestavaid grupipoliitikaid, mida saab rakendada kasutajapõhiselt. Spetsiaalselt Active Directory keskkonnas võib see endaga kaasa tuua turbealaseid eeliseid, nt seetõttu, et piiranguid saab sõnastada lähtuvalt kasutajatüübist, mille abil saab teineteisest eristada nt tavakasutajaid ja administraatoreid. Iga eripära on võimalik ellu rakendada sobiva OU-struktuuri ja asjakohaste grupipoliitikate defineerimise abil.

Grupipoliitikaid kasutades on võimalik piirata ka Windows 7 kasutaja töökeskkonnas saadaolevaid funktsioone. Valdkondadest, mida võiks konfigureerida sobilike parameetrite seadete defineerimise abil, on eriti soovitavad MMC, startmenüü, Taskbar , Desktop , nähtavad süsteemijuhtimiskomponendid ning lubatud Windows-rakendused.

Tavakasutaja töökeskkonna piiramiseks tuleks võimalusel rakendada järgmisi piiranguid:

- Kuvada tohiks ainult selliseid süsteemijuhtimiskomponente, mida on lubatud kasutada,
- Enamike MMC Snap-In -ide kasutuse tõkestamine (juhul kui kasutatakse sertifikaate, tuleks Certificate Snap-In kasutust siiski lubada,
- Taskplanneri kasutuse piiramine,
- Active Desktop -i desaktiveerimine või selle kasutuse piiramine,
- Start -menüü ja Taskbar -i piirangud,
- Irdmäluseadmete kasutamise ja paigaldamise piirangud Windows 7-s,
- Alates Windows 8-st on olemas võimalus logida süsteemi sisse Microsofti kontoga, et laadida Windows Store'ist alla äppe või kasutada Microsofti pilvteenuseid (nt Skydrive). Ettevõtte keskkonnas tuleks turvalisuse kaalutlustel kasutada selle asemel tsentraalselt hallatavaid domeenikontosid.

Poliitikate Käivitada ainult lubatud Windows-rakendusi ja Mitte käivitada loetletud Windows-rakendusi määratlemisel tuleb arvestada, et sellised piirangud kehtivad ainult siis, kui vastavaid rakendusi käivitatakse Windows Explorer-iga. Piirangud ei kehti, kui „keelatud“ rakendus käivitatakse Taskmanager -ist, käsuviibalt (command prompt) või mõne teise programmi seest. Selle ärahoidmiseks saab sõltuvalt vajadustest kasutada teistsuguseid vahendeid, nt kehtestada tarkvarakasutust piirava poliitika (ingl Software Restriction Policy). Lisaks tuleks kasutada ka rakenduste eripäradest lähtuvaid poliitikaid, mis lubavad kehtestada rakendustele ja süsteemikomponentidele vastavaid piiranguid kasutajapõhiselt.

Kasutamine väljaspool Active Directory keskkondi

Neil juhtudel, kus Windows 7-t kasutatakse autonoomsetes arvutites, pole võimalik rakendada globaalsete grupipoliitikate abil toimivat tsentraliseeritud konfigureerimist. Sellisel juhul tuleb lokaalsetes grupipoliitikates kehtestatud turvaseadistuste parameetrid konfigureerida iga arvuti puhul eraldi. Selle protsessi aluseks tuleb võtta planeerimise etapis väljatöötatud mehhanism, mis käsitleb lokaalsete grupipoliitikate hooldamist mitme arvuti puhul.

Kasutamine Active Directory baasil toimivates keskkondades

Windows 7 süsteemide kasutamisel Active-Directory baasil toimivates keskkondades (Windows 2008 domeenides) on samuti võimalik rakendada lokaalseid grupipoliitikaid iga arvuti puhul eraldi. Erandiks on asjaolu, et tsentraliseeritud halduse eeliseid on siiski võimalik kasutada. Seetõttu on Active Directory baasil loodud grupipoliitika ehk turvaseadistuste ellurakendamise puhul üldjuhul alati soovitatav võtta aluseks kas organisatsiooni asukoht, domeen või selle allüksused. Võimalusel tuleks loobuda lokaalsete grupipoliitikate rakendamisest üksikutes arvutites, kuna neid ole võimalik hästi tsentraliseeritult hallata. Kui teatud põhjustel on siiski tarvis paralleelselt kasutada lokaalseid ja Active Directory baasil toimivaid grupipoliitikaid, tuleb kõikide grupipoliitikate parameetrite seadistused viia omavahel kooskõlla. Active Directory baasil toimivate grupipoliitikate rakendamisel on tarvis planeerida nende kasutamine domeenis (Windows 2008).

Täiendavat infot Active Directory baasil toimivate grupipoliitikate kohta leiate M 2.231 Windowsi grupipoliitika planeerimine . **Üldjuhul tuleb enne Active Direc-**

tory baasil toimivate grupipoliitikate rakendamist läbi töötada järgnevad aspektid:

- Active Directory OU- ja grupistruktuur
- GPOde hierarhia Active Directory -s ja GPO üldkontseptsioon
- Grupipoliitikate pärimine
- GPO kattuvuse blokeerimine ja kohustamine
- Prioriteetide kehtestamine ehk mitme GPO korraga töötlemise järjekorra kindlaksmääramine
- Kehtivate seadete arvutamine grupipoliitika iga parameetri jaoks ja GPO-de töötlemisjärjekord
- Grupipoliitikate läbitöötamise juhtimine
- Grupipoliitikate linkimine
- GPOde kaitsmine

Sama moodi hallatakse ka Windows 7 tööd reguleerivaid poliitikaid:

Windows 7-s on grupipoliitikaobjektide koostamiseks ja haldamiseks mõeldud standardsed snap-in 'id Group Policy Management ja Group Policy Object Editor läbinud uuenduskuuri. Windows 7 tööd reguleerivaid poliitikaid saab koostada vaid Windows 7-s olemasolevate tööriistade uute versioonidega. Windows 7 poliitikate haldamiseks Active Directory keskkonnas tuleks eranditult kasutada Windows 7 domeeni liiget. Arvutite eripärasid kajastavad grupipoliitikad rakenduvad tööle buutimisprotsessi raames, kasutaja eripärasid kajastavad grupipoliitikad alles kasutaja sisselogimisel. Kasutajate eripäradega arvestaval grupipoliitikal on siinjuures eesõigus ning sõltuvalt olukorrast võib see arvuti eripäradega arvestava grupipoliitika seaded isegi üle kirjutada. Active Directory baasil toimivatele grupipoliitikate jaoks saab kasutada niinimetatud Loopback-töötlemisrežiimi. Viimane kindlustab selle, et kasutajate eripäradega arvestav grupipoliitika ei saaks tühistada arvutipoliitikat. Vastav töötlemisrežiim tuleks eelkõige sisse lülitada siis, kui seaded on konkreetselt seotud arvutiga ning ei tohiks sõltuda kasutajatest. Loopback -töötluse puhul eristatakse kahte varianti: Asendamine ja Kokkuliitmine. Asendamisrežiimis rakendatakse arvutite eripärasid kajastavaid grupipoliitikaid ilma kasutaja eripärasid kajastavaid seadeid käsitlemata. Kokkuliitmisrežiimis liidetakse kasutajate GPO seaded arvutite GPO seadetega. Otsus, kas grupipoliitika tuleks tööle rakendada Loopback -režiimis ning milline variant selleks valida, sõltub alati konkreetsest kasutusalast ja olemasoleva keskkonna poolt etteantavatest tingimustest. Sõltuvalt kasutusalast võib selle režiimi valimine pakkuda teatud turbealaseid eeliseid, kuid sellele vaatamata pole võimalik siinkohal jagada üldkehtivaid soovitusi. Tulevaste probleemide vältimiseks on juba grupipoliitikate väljatöötamise käigus tarvis teada, millisest operatsioonisüsteemi versioonist alates hakatakse rakendama grupipoliitikas kavandatavaid seadeid. Erinevused GPO parameetrite seadistustes võivad olla tingitud erinevate Service Pack -ide kasutamisest. Grupipoliitikate eranditega rakendamist võimaldavateks mehhanismideks on Turvafiltrid (ingl Security Filtering) ja WMI filtrid.

Security Filtering mehhanism aitab määratleda turvagruppe, kus kehtib vastav turvapoliitika.

Standardseadistuses on grupipoliitika rakendusvaldkonnaks Autenditud kasutajad. WMI filtrid lähtuvad grupipoliitikas rakendamisel arvuti eripäradest (nt operat-

sioonisüsteemist, Service Pack -i versioonist, kõvaketta ruumist). Mõlemad mehhanismid võimaldavad Active Directory -s paindlikult juhtida grupipoliitika rakendamist nii kasutaja- kui ka arvutiobjektil. Nende kasutamine eeldab siiski täpset paneerimistööd ja põhjalikku testimist.

Turvamallid

Grupipoliitikate parameetreid saab seadistada mitte ainult otse vastava MMC Snap-In -iga, vaid ka vajamineva turvamalli importimisega. Turvamalle rakendatakse turvaseadete konfigureerimiseks. Need salvestatakse teksti kujul poliitikafailidesse (INF-failidena) ning neid saab töödelda MMC Snap-In -iga Turvamallid , samuti tavaliste tekstiredaktoritega. Paljud valmis kujul turvamallid on vabalt saadaval nii Microsofti kui ka teiste tootjate allikatest. Üldjuhul võiks siinkohal soovitada järgmist lähenemist:

- Esmalt tuleks välja valida mõni olemasolev turvamall (nt Microsoftilt). Turvamalli valikul tuleks otsus langetada mõne kõrgema turbeastmega malli nagu nt hisecws kasuks, kuna turbe seisukohast tuleks eelistada olukordi, kus vajadusel tuleb „turvalist“ seadistust nõrgendada, mitte vastupidi.
- Mall tuleb viia kooskõlla kohapealsete oludega ning selleks vajaminevad muudatused tuleb põhjendada ja dokumenteerida.
- Koostatud mall imporditakse vastavasse grupipoliitikasse. Tagamaks, et turvamalli importimisel grupipoliitikasse kõik seaded ka tõepoolest üle kirjutatakse, soovitatakse kasutada valikut Andmebaasi puhastus enne importimist. Turvamallide üheks täiendavaks rakendusvaldkonnaks on veel kehtivate seadistuste turvaanalüüs. Hetkel arvutis kehtivaid seadeid on võimalik võrrelda INF-faili seadetega. Analüüsi saab läbi viia kas MMC Snap-In -iga Turvakonfiguratsioon ja -analüüs või käsuviibalt käsuga secedit. Turvamalliga secsetup.inf, mis asub kataloogis %SystemRoot%\repair.

Isiklike administratiivsete mallide defineerimine

Turvapoliitikate turvaseaded kajastuvad mitte ainult Windows-seaded valdkonnas, vaid ka administratiivsete mallide valdkonnas. Administratiivsed mallid koosnevad üksikutest parameetritest, mis konfigureerivad sinna juurdekuuluvate Registry -võtmete seadistusi. Vastavad ADM-failid määravad üksikud parameetrid, mida on võimalik konfigureerida administratiivsete mallide raames. Windows 7 puhul asendatakse ADM failid ADMX template failidega, mis kasutavad uut süntaksit, mis põhineb XML registri poliitikal. ADMX failide eelis ADM failide ees on see, et nad on keeleliselt neutraalsed ja koos keelekohaste ADMLfailidega võib mõnda keeleversiooni kasutada. Administratiivseid malle on võimalik ka ise defineerida. Seda on soovitatav kasutada eelkõige siis, kui ettevõttes või ametiasutuses on sageli tarvis muuta otseseid Registry -seadeid. Administratiivse malli defineerimisega on Registry -seadeid võimalik mugavalt grupipoliitika mehhanismi abil laiali jagada. Muuhulgas on seeläbi võimalik tagada Registry -seadeid reaalne ellurakendamine kõikides arvutites.

Kehtestatud grupipoliitikate testimine

Testid peavad ühelt poolt tagama, et vajalikes funktsioonides ei esineks piiranguid ning et kõik turvalisust puudutavad seaded toimiksid korrektselt.

Grupipoliitikate haldamine Microsoft PowerShelliga

Alates Windows 7-st on loodud võimalus hallata grupipoliitikaid ka PowerShelli käsureaga. Sisselogimise ja süsteemi käivitamise ajal saab käivitada PowerShelli skripte. PowerShelli käitusfaasisüsteemi kaitsmisel tuleb arvestada meetmega M 4.421 Windows PowerShelli turve .

Kontrollküsimused:

- Kas turvaseaded jagatakse sobival moel erinevatele GPOdele?
- Kas kõikide arvutite puhul suudetakse tagada õigete GPOde rakendamine?
- Kas GPOde koostamisel ja hooldamisel arvestatakse ka organisatoorsete aspektidega?
- Kas rühmasuunistes konfigureeriti kõik turvalisusega seotud seadistused?
- Kas kõik mittevajalikud rakendused ja komponendid on rühmasuuniste abil või tarkvara kasutamise kaudu rakenduse kontrolliks inaktiveeritud?
- Kas kasutajatele on sisse seatud Windows-klientide vajadustele vastav töökeskkond?
- Kas rühmasuuniseid testitakse enne nende tootmiskeskkonnas rakendamist?
- Kas süsteemide kaitseks kaasati tootja konfiguratsioonisoovitusi?
- Kas kasutatakse tööriistu, mis võimaldavad turvaseadistuste tsentraalset ja ühtset konfigureerimist?

M 2.327 Kaugpääsu turve Windows 7-s

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator

Remote Desktop põhineb terminaliteenuste tehnoloogial (RDP-protokollil) ning võimaldab süsteemi sisse logida läbi võrgu. Remote Assistance lisab Remote Desktopile võimaluse pääseda olemasoleva seansi raames ligi ekraanil olevatele ressurssidele ning võtta vajadusel üle ka arvuti juhtimine.

Windows 7 puhul on need kaugjuhtimismehhanismid samuti toetatud.

Remote Desktop mehhanismi kasutatakse peamiselt Windows 7 all töötavate arvutite võrgu kaudu hooldamiseks. Remote Assistance mehhanismi kasutamine on mõeldav nt ettevõtetes ja ametiasutustes sellistel juhtudel, kus kasutajaid on tarvis abistada kas organisatsiooni sees või ka väljaspool organisatsiooni toimiva IT-tugikeskuse kaudu. Remote Desktop mehhanismi rakendamisel tuleb arvestada, et sihtkoha arvutisse saab olla korraga sisselogitud ainult üks kasutaja. Remote Desktop -i ei tuleks selles kontekstis mõista kui terminaliteenuste asendajat. Remote Desktop ja Remote Assistance mehhanisme saab sisse ja välja lülitada vastavate grupipoliitikate objektide abil:
(Computer configuration | Administrative templates | Windows components | Terminal services, User configuration | Administrative templates | Windows components | Terminal services ning Computer configuration | Administrative templates | System | Remote Assistance) või kohapeal Control Panel (System | Remote).

Nende kahe tehnoloogia kasutamisel tuleb arvestada järgnevaga.

Windows 7 ja 8 keskkonnas tuleb kõigepealt järgmiste rühmasuunise objektide abil aktiveerida kaugpöördus: Arvuti konfiguratsioon | Administratiivsed mallid | Süsteem | Kaugpöördus. Kaugtöölaua konfiguratsioon aktiveeritakse alates Windows 7-st järgmiste rühmasuunise objektide abil: Arvuti konfiguratsioon | Administratiivsed mallid | Windows-komponendid | Kaugtöölaua teenused.

Alates Windows 7-st on lokaalse seadistuse tee süsteemijuhtimise kaudu järgmine: Süsteem ja turvalisus | Süsteem | Kaugseadistused.

- Kasutada tuleb tugevat krüpteeringut (128-bitist, seadetes valida kõrgeim aste). Windows 7 puhul leiab need seadistused asukohast Computer Configuration | Administrative Templates | Windows Components | Remote Desktop Services | Remote Desktop Session Host | Security . Seadistuses Set client connection encryption level tuleb samuti valida kõrgeim aste.
- Automaatsest paroolisisestusest tuleks loobuda. Windows 7 puhul tuleb aktiveerida seadistus asukohas Computer Configuration | Administrative Templates | Windows Components | Remote Desktop Services | Remote Desktop Session Host | Security.
- Vahemälu, printeri, failide salvestuskoha ja smartcard 'i ühenduste ümbersuunamist tuleks võimaluse korral vältida.

Windows 7 puhul leiab need asukohast Computer Configuration | Administrative Templates | Windows Components | Remote Desktop Services | Remote Desktop Session Host | Device and Resource Redirection ja Temporary Folders.

- Täiendavat kaitset kaugtöölaua kasutamise korral pakub võrguautentimise funktsioon (Kasutaja autentimine autentimisega võrgutasandil on kaugühenduste korral kohustuslik), mida saab kasutada alates Windows Server 2008-st. Selle funktsiooniga autendivad kaugtöölauakliendid kõigepealt enne tegeliku kaugtöölauaühenduse loomist ühendust luua sooviva kasutaja võrgu kaudu. Volitamata isikud, kellel ei ole domeenikontot, ei saa seega kaugtöölauaühendust käivitada. Selle funktsiooni kasutamise korral tuleb tagada, et ettevõttes kasutataks kaugtöölauakliente, mis toetavad võrguautentimist. Windows Server 2012 ja Windows 8 keskkonnas on autentimine võrgutasandil standardi kohaselt nõutud.

Remote Desktop -juurdepääsu volitatud kasutajate ringi piiramiseks tuleb kasutajaõigused määrata kas vastavate poliitikatega Allow logon through Terminal Services, Deny logon through Terminal Services (Lubada terminaliteenuste kaudu sisselogimine, Keelata terminaliteenuste kaudu sisselogimine) või täpsustada vastavad kasutajad Control Panel -i abil. Standardseadistuses on kaugpöörduse kasutamine lubatud administraatorite kasutajarühmale ja kasutajarühmale Remote Desktop Users , mis on pärast installeerimist veel tühi. Remote Assistance seansi loomiseks on võimalik rakendada kahte järgmist võimalust:

- Seanss luuakse standardsel moel ainult kasutaja poolt esitatud konkreetsel palvel eesmärgiga kaugpöörduse kaudu abi saamiseks.
- Sobiva konfiguratsiooni korral on ka abistajal endal võimalik kasutajale aktiivselt abi pakkuda.

Hetkel sisselogitud kasutaja peab seansi loomise otseselt heaks kiitma. Ühenduse loomise kitsaskohaks on siinkohal kasutaja, kuna tema puhul ei toimu autentimist. Sellest tulenevalt on tarvis Remote Assistance abistamismehhanisme käsitleda piisava ettevaatlikkusega. Kaugpöördusel toimiva abi võimaldamisel on tarvis luua vastavad poliitikad, mis peaksid suutma tagada järgmist:

- Seanss tuleks luua ainult konkreetse kutse alusel. Vajadusel pakkuda kaugpöördusel toimivat abiteenust, ühenduse loomise õigused tohivad olla ainult teatud kindlatel kasutajarühmadel (nt tugiteenust pakkuvatel töötajatel). Definitsiooni loomisel peaks siinkohal järgmina vormingut \ või \.<domeeninimi>\<kasutajanimi> <domeeninimi>\<rühmanimi> <kasutajanimi>@<domeen>.<TopLeveldomeen>.
- Olemasolevate kasutajate või gruppide vahel valida ei ole võimalik.
- Kutse maksimaalne kehtivusaeg tuleb seadistada vastavalt sellele, mis on konkreetse ettevõtte või ametiasutuse puhul vastuvõetav.
- Juhul kui kaugpöörduse baasil toimiva abiteenuse kutse salvestatakse mõnda faili, tuleks selleks väljastada parool, et vähendada kutsete volitamata kasutusega seotud ohte.
- Juhtimise liik (Allow helpers to only view the computer või Allow helpers to remotely control the computer (Abistajatel on lubatud arvutiga vaid tutvuda või Abistajatel on lubatud arvutit kaugpääsu abil juhtida) tuleks kehtestada võimalikult suurte piirangutega (Abistajatel on lubatud arvutiga vaid tutvuda).

Remote Desktop ja/või Remote Assistance mehhanismide kasutamisel tuleb arvestada nende mõjuga konfiguratsioonile ja tulemüüri haldamisele. Üldjuhul soovitatakse keelata Remote Desktop ja Remote Assistance ühenduste rakendamine

väljaspool koduvõrku. Kokkuvõtlikult võib seega öelda, et kaugpöördusel toimivate mehhanismide kasutamine tuleks väga hoolikalt läbi kaaluda. Mehhanismide eeliseid ja puudusi omavahel võrreldes tuleks eriti pöörata tähelepanu võimalikele erinevustele seoses kasutajate autentimisega. Juhul kui ettevõttes või ametiasutuses ei lähe Remote Desktop ja Remote Assistance mehhanisme tarvis, tuleks need ilmtingimata desaktiveerida.

Alusseaded GPOdele

Järgnevalt toodud seadistused kehtivad ainult mõlema mehhanismi kasutamise korral. Juhul kui üht kahest mehhanismist ei kasutata või kui kumbagi mehhanismi ei kasutata, tuleks vastav seadistus kindlasti desaktiveerida. Selleks tuleb muuta allpool loetletud poliitikate seadistusi. Järgnev grupipoliitikate seadistusi kajatav tabel on koostatud arvutite jaoks, mida on tarvis konfigureerida Remote Desktop ja Remote Assistance mehhanismide kasutamiseks.

Poliitika	Seisund	Seadistus
Computer configuration | Windows settings | Administrative templates | Encryption and security | Set client connection encryption level	aktiveeritud	kõrgeim aste
Computer configuration | Windows settings | Administrative templates | Terminal services | Encryption and security | Always prompt client for password	aktiveeritud	
Computer configuration | Windows settings | Administrative templates | Terminal services | Client/server data redirection | *	aktiveeritud/ desaktiveeritud	
Computer configuration | Administrative templates | System | Remote Assistance | Offer Remote Assistance	desaktiveeritud	
Computer configuration | Administrative templates | System | Remote Assistance | Solicited Remote Assistance	aktiveeritud	Abistajad tohivad arvutit kaugpääsuga juhtida Maksimaalne kehtivusaeg: 8 tundi

Tabel: Grupipoliitikate seadistuste tabel arvutitele

Järgnev grupipoliitikate seadistusi kajatav tabel on koostatud arvutite jaoks (Windows 7), mida on tarvis konfigureerida Remote Desktop ja Remote Assistance mehhanismide kasutamiseks.

Poliitika	Seisund	Seadistus
Windows Vista: Computer configuration | Administrative templates| Windows settings | Terminal services |Terminal server |Security | Always prompt client for password Windows 7: Computer configuration | Administrative templates| Windows settings | Remote desktop services | Remote Desktop Session Host |Security | Always prompt for password	aktiveeritud	
Windows Vista: Computer configuration | Administrative templates| Windows settings | Terminal services |Terminal server |Security | Set client connection encryption level Windows 7: Computer configuration | Administrative templates| Windows settings | Remote desktop services | Remote Desktop Session Host |Security| Set client connection encryption level	aktiveeritud	kõrgeim aste

Windows Vista ja Windows 7: Computer configuration | Administrative templates | Administrative templates | System | Remote Assistance | Solicited Remote Assistance|	desaktiveeritud	
Windows Vista ja Windows 7: Computer configuration | Administrative templates | System | Remote Assistance | Solicited Remote Assistance	aktiveeritud	Abistajad tohivad arvutit kaugpääsuga juhtida Maksimaalne kehtivusaeg: 5 minutit

Tabel: Grupipoliitikate seadistuste tabel kasutajatele

Järgnev grupipoliitikate seadistusi kajatav tabel on koostatud kasutajate jaoks, mida on tarvis konfigureerida Remote Desktop ja Remote Assistance mehhanismide kasutamiseks.

Poliitika	Seisund	Seadistus
User configuration | Windows settings | Administrative templates | Terminal services | Set rules for remote control of Terminal Services user sessions	aktiveeri-tud	Täielik juurdepääs kasutaja loaga
User configuration | Windows settings | Administrative templates | Terminal services| Client | Do not allow storing of passwords	aktiveeri-tud	

Tabel: Grupipoliitikate seadistuste tabel kasutajatele

Järgnev grupipoliitikate seadistusi kajatav tabel on koostatud kasutajate jaoks, mida on tarvis konfigureerida Remote Desktop ja Remote Assistance mehhanismide kasutamiseks.

Poliitika	Seisund	Seadistus

Windows Vista: User configuration | Administrative templates | Windows settings|Terminal services | Remote Desktop Connection Client | Do not allow storing of passwords Windows 7: User configuration| Administrative templates | Windows settings | Terminal services | Remote Desktop Connection Client | Do not allow storing of passwords	aktiveeri-tud	
Windows Vista: User configuration | Administrative templates | Windows settings|Terminal services | Terminal Server | Assistance | Rules for Terminal Services for remote control | | Windows 7: User configuration | Administrative templates | Windows settings|Remote desktop services | Remote Desktop Session Host |Assistance | Rules for Terminal Services for remote control | |	aktiveeri-tud	Täielik juurdepääs kasutaja loaga

Tabel: Grupipoliitikate seadistuste tabel kasutajatele

Kontrollküsimused:

- Kas kaugpöördusel toimivad juhtimismehhanismid on täielikult desaktiveeritud, kui nende kasutamist ei ole ette nähtud?
- Kas töötajad on saanud koolituse Remote Assistance mehhanismi turvalise kasutamise osas?
- Kas rühmasuunised on konfigureeritud turvaliselt ja vajadustest lähtudes?

- Kas kaugpöördus võib toimuda üksnes pärast konkreetset kutset EasyConnect'i või kutsefaili kaudu?
- Kas kutse maksimaalne kestus on seadistatud oletatavale suurusele?
- Kas kutse salvestamisel failis antakse failile parool?
- Kas kaugpöörduse kavandamisel võetakse arvesse mõjusid tulemüüri konfigureerimisele?
- Kas kaugpöördusel toimivad juhtimismehhanismid on täielikult inaktiveeritud, kui nende kasutamist ei ole ette nähtud?

M 2.328 Windows XP kasutuselevõtt mobiilsel arvutil

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator, kasutaja

Windows XP rakendamisel mobiilsetes arvutites tuleb, nagu ka kõikide teiste mobiilsete PCde puhul, järgida moodulit B 3.203 Sülearvuti .

Andmete krüpteerimine

Mobiilsed arvutid viibivad tihti kasutuskeskkondades, mille turvalisus on palju madalam kui kaitsvas bürookeskkonnas. Seetõttu tuleks mobiilsete arvutites olevad kaitsmist vajavad andmed varustada krüpteeringuga (vt M 4.29 Kaasaskantavatele IT-süsteemidele mõeldud krüpteerimistoote kasutamine). Lisaks kolmandate tootjate poolt pakutavatele lahendustele võib krüpteerimiseks kasutada ka Windows XP enda mehhanisme:

- krüpteeringuga failisüsteemi EFS (*Encrypting File System*),
- *offline* -failide krüpteeringut.

Täiendavat infot EFSi turvalise kasutamise kohta leiate M 4.147 EFS-i turvaline kasutamine Windows 'i keskkonnas .

Offline -failide kontseptsioon juurutati esmakordselt operatsioonisüsteemiga Windows 2000. *Offline* -failide puhul on tegemist põhimõtteliselt võrgupõhisesse ühiskasutusse antud dokumentide koopiatega. Need failid salvestatakse kohapealses arvutis vastavasse andmebaasi, mistõttu on võimalik dokumentidele juurde pääseda ka siis, kui võrgu kaudu toimiv ühiskasutuse luba ei ole parasjagu saadaval. *Offline* -failide krüpteerimisvõimalus juurutati alates operatsioonisüsteemist Windows XP. Kogu *offline* -failide salvesti, mis sisaldab kõikide kasutajate faile, krüpteeritakse spetsiifilise arvutivõtmega. Krüpteering on kasutajate jaoks läbipaistev ning seda saavad sisse ja välja lülitada ainult administraatorid. Aktiveerimine toimub Windows Exploreri kaustaseadistuses *Tools* | *Folder Options* | *Offline Files* | *Encrypt offline files to secure data* või grupipoliitikaga *Computer Configuration* | *Administrative Templates* | *Network* | *Offline Files* | *Encrypt the offline file cahe* . *Offline* -failide krüpteerimine on soovitav aktiveerida eriti neil juhtudel, kus sünkroniseeritavad originaaldokumendid on krüpteeritud ning kohapeal hoitavaid *offline* -koopiaid võib hoida krüpteeritud kujul. Mobiilsetes arvutites hoitavate andmete kaitseks rakendatava strateegia (Windows XP EFS, *offline* -failide krüpteerimine või krüpteerimine mõne muu toote abil) valik sõltub iga konkreetse juhtumi asjaoludest ja vajadustest.

Lokaalne tulemüür

Vastupidiselt statsionaarsele, organisatsioonisisesele *Desktop* -lahendusele on mobiilseid kliente võimalik Internetti ühendada ka otse. Sellistel juhtudel tuleb igasuguste eranditeta kasutada lokaalselt installeeritud tulemüüri. Windows XP-ga juurutati uus funktsioon - *Internet Connection Firewall* (ICF), mis nimetati alates Service Pack 2-st ümber Windows-Firewall-iks. Windows-Firewall on seisundiga seotud paketifilter, mis analüüsib igat TCP/IP ja UDP paketti ning töötleb neid vastavalt konfiguratsioonile. Alates Windows XP Service Pack 2-st sisaldab ICF/Windows-Firewall muuhulgas järgnevaid täiendusi:

- Standardseadistuses aktiveeritud kõikide liideste jaoks
- Kaitse toimib juba *boot* -protsessi käigus
- Tsentraliseeritud konfigureerimine GPO-de abil
- Lähtekoha-aadresside piirangud pordile
- Käsuviiba (*command prompt*) tugi
- *Lock-Down* režiim
- Erandite nimekirjad rakenduste jaoks
- Mitme *Policy Profile* rakendamise võimalus
- RPC tugi
- Tootja aluskonfiguratsiooni taastamisvõimalus
- Järelvalveta installeerimise toetamine.

Windows-Firewall filtreerib eranditult vaid sissetulevaid ühendusi. Väljuvatele pakettidele seevastu ei kehtestata mingisuguseid piiranguid. See tähendab, et Windows-Firewall ei võimalda näiteks piirata olemasolevate internetiserverite juurdepääsuvõimalusi. Seega ei ole programmide puhul võimalik ei kehtestada ega ka kontrollida nende juurdepääsusid Internetile. Seetõttu ei suuda Windows-Firewall pakkuda kaitset Trooja hobuste vastu, mis on juba arvutisse sisse tunginud. ICFi rakendamine (enne Service Pack 2-e) on ettevõtte või ametiasutuse kontekstis väga raskendatud, kuna sellel puuduvad tsentraliseeritult toimivad konfigureerimisvõimalused. Grupipoliitikaga *Computer Configuration | Administrative Templates | Network | Network Connections | Prohibit use of Internet Connection Firewall on your DNS domain network* on võimalik ICF vaid täielikult desaktiveerida. ICFi konfigureerimine toimub iga võrguliidese puhul eraldi Windows XP süsteemis kohapeal. Alates Service Pack 2 juurutamisest on administraatoritel võimalik Windows-Firewall-i ka tsentraliseeritult hallata, rakendades grupipoliitikaid *Computer Configuration | Administrative Templates | Network |Network Connections | Windows-Firewall* . Windows-Firewall-i konfigureerimisel on võimalik luua erinevaid profiile, mis lubab Windows-Firewall-i mitmesuguste keskkondade (nt organisatsioonisisese võrgu või mobiilse kasutuse jaoks) erinevalt konfigureerida. Organisatsiooni sisevõrgu puhul võib siinkohal kaalude piirangute kehtestamist sissetulevale andmesidele (nt piirata arvutite kaugpöördusel toimivaid ligipääse). Mobiilse kasutuse puhul seevastu ei tohiks Windows-Firewall-ile lubada mitte mingisuguseid erandeid ning kogu sissetulev andmeside tuleks blokeerida. Juhul kui kliendi haardeulatusse jääb mõni *Domain Controller* , rakendatakse domeeni profiili, kuid muudel juhtudel aktiveeritakse mobiilne profiil. Pärast Service Pack 2 installeerimist aktiveeritakse Windows-Firewall standardseadistusena kõikide võrguliideste jaoks. Sõltuvalt konkreetse ettevõtte või ametiasutuse kohapealsetest oludest võivad sellega kaasneda ka probleemid (vt M 2.329 Windows XP SP2 kasutuselevõtt).

Nii ICF kui ka Windows-Firewall võimaldavad kasutada logimisfunktsiooni. Pärast tulemüüri aktiveerimist on see standardseadistuse järgi desaktiveeritud ning see tuleb eraldi tööle lülitada. Logifunktsiooni on siinjuures võimalik eraldi rakendada nii vastuvõetavate kui ka kõrvalejäetud pakettide jaoks, mis lubab logifunktsiooni seadistada vastavalt vajadustele. Logimine leiab aset W3C poolt standar-

diseeritud formaadis *Extended Log File Format* . Kui logifail saavutab maksimaalse suuruse, luuakse failist koopia ja selle nimetusele lisatakse täiend *old* . Logifaili korduval maksimumsuuruse saavutamisel kirjutatakse varundatud logiandmed üle ja need lähevad kaotsi. Sel põhjusel tuleks logifailide puhul arvestada, et need oleksid piisavalt suured. Kuna logiandmed salvestatakse kohapeal, tuleb luua mehhanism, mis tegeleks vastavate andmete kokkukogumisega. Windows XP ise ühtki sellist mehhanismi ei paku. Juhul kui Windows XP all töötavaid arvuteid on tarvis kaitsta kohtvõrgust või Internetist (mobiilse kasutuse raames) tulevate rünnete vastu, on reeglina soovitatav kasutada mõne kolmanda tootja poolt pakutavat *Personal Firewall* -i, kuna vastavatel toodetel on reeglina palju rohkem funktsioone (nt võimaldavad need filtreerida väljuvaid ühendusi ja piirata Interneti juurdepääsuks volitatud programmide loetelu). Juhul kui *Personal Firewall* lahendust pole installeeritud ega aktiveeritud, tuleks mobiilse IT-süsteemi puhul sisse seada vähemalt Windows-Firewall (või ICF enne SP2 kasutuselevõttu). Täiendavat infot antud teema kohta leiate M 5.91 Interneti-PC personaalse tulemüüri installeerimine .

Täiendav kontrollküsimus:

- Milliseid mehhanisme rakendatakse Windows XP süsteemide kaitsmisel rünnete vastu?

M 2.329 Windows XP SP2 kasutuselevõtt

Algatamise eest vastutavad: IT-turvaosakond, administraator

Rakendamise eest vastutavad: administraator

Microsofti Windows XP Service Pack 2 on saadaval alates augustist 2004. 12. aprillil 2005 lõppes ajavahemik, mil SP2 installeerimist oli võimalik spetsiaalse Microsofti tööriista abil takistada ka siis, kui Interneti baasil toimiv *Windows-Update* -teenuse on aktiveeritud. SP2 installeerimist saavad jätkuvalt takistada ainult sellised organisatsioonid, mis kasutavad oma *Update* -serverit. Lisaks olemasolevate mehhanismide kõrvaldatud vigadele ja parandustele sisaldab Service Pack 2 ka mõningaid turbealaseid muudatusi ja täiendusi. Siinkohal võib näiteks välja tuua:

- Kokku rohkem kui 600 uut turvapoliitikat (Windows-Firewall, Security Center, Internet Explorer jne).
- Windows-Firewall täiendused (varem Internet Connection Firewall, ICF), ennekõike tsentraliseeritud haldamise võimaluse lisamine.
- Internet Exploreri täiendused: *Add-on Management* , *Pop-up Blocker* , *Zone Elevation Blocking* , järjepidev MIME-töötlus, ActiveX-juhtelementide käsitlemine piirangutega.
- Võimalus integreerida kolmandate tootjate viirusetõrjetarkvara nn turvekeskusesse (*Security Center* -isse), mis on loodud Windowsi turvaseadistuse tsentraalseks haldamiseks ja seireks.
- Salvesti kaitse *Buffer Overflow* vastu: Süsteemi tuum ja teegid tõlgiti spetsiaalsete kompilaator-lippudega, mis peaks suutma pakkuda kaitset puhvri ületäitumise (*Buffer Overflow*) vastu. Vastavat „ *No Execute* “ *Flag* -i (NX-i) kasutavad mõningad uuemad protsessorid.
- Allalaaditud failide ja manuste märgistamine NTFS-ajamitel (*Attachment Execution Service*).
- *Raw-Socket* -ite kasutuse ja IP-pakettide manipuleerimise märgatav vähenemine, *Denial-of-Service* abinõude integreerimine TCP/IP pinu alla.
- USB-kirjutuskaitse juurutamine, st vastava konfiguratsiooni abil on võimalik USB-mäluseadmetele nagu mälupulkadele või ketastele ligi pääseda ainult lugemisõigusega (sellega takistatakse volitamata andmeeksport USB-vahenditest).

Uute sätete konfiguratsioonid ning eriti grupipoliitikad tuleb kindlaks määrata juba enne SP2 installeerimist. Grupipoliitika muutmine võib põhjustada Windows XP klientidega toimivates ettevõtetes ja ametiasutustes väga laiaulatuslikke muudatusi, mistõttu peavad administraatorid olema nende läbiviimisel väga hoolikad.

Probleemide ennetamine

Tänu laiautuslikele muudatustele esineb eriti just suurtes ettevõtetes ja ametiasutustes oht, et Service Packs 2 installeerimise tagajärjel võivad tekkida probleemid. Eriti kriitiliseks võib olukord kujuneda neil juhtudel, kui rakendused muutuvad kasutuskõlbmatuks või kui tekivad probleemid tulemüüri ja viirusetõrje programmidega. Selliste probleemide vältimiseks on tarvis SP2 juurutamine hoolikalt ette planeerida ning põhjalikult läbi testida. Enne juurutamist tuleks

eelkõige kontrollida rakendustarkvara funktsioneerimisvõimet. Service Pack 2 installeerimise tagajärjel võivad tekkida järgnevad probleemid:

- Probleemid GPOde haldamisel vanade tööriistadega, kuna uued administratiivsed mallid koosnevad liiga pikkadest märgijadadest.
- MMC *Snap-In Group Policy Result Set* ei tööta enam *Remote* päringute korral, kuna pärast installeerimist on standardseadistuses aktiveeritud tulemüür.
- Probleemid DCOM-rakendustega, kuna juurutati uus DCOM-autentimismudel (nt *Group Policy Result Set* tegumite delegeerimisel mitte-administraatoritest kasutajatele).
- Probleemi rakendustega standardseadistuses aktiveeritud tulemüüri tõttu.
- Probleemid rakendustega TCP/IP-pinu muudatuste tõttu (*Raw-Sockets* kasutamise piirangute tõttu).
- Skripti ja ActiveX-veateated, pildikuvamise probleemid salvestatud veebilehtede avamisel rakendustes (muuhulgas võivad puudutatud olla ka Microsoft Office tooted).
- Täiendava tarkvara automaatne installeerimine (nt Windows Movie Maker). Sõltuvalt olukorrast tuleb see vajadusel eemaldada.

Loetletud probleemide jaoks on nii Internetis kui ka erialastes ajakirjades pakutud terve rida lahendusi, millega administraatorid peaksid ennast enne SP 2 installeerimist kurssi viima.

Täiendavad kontrollküsimused:

- Kas kontrolliti rakenduste ühilduvust?
- Kas uute seadistuste konfiguratsioonid on kindlaks määratud?

M 2.330 Windows 7 turvapoliitika ja selle elluviimise regulaarne kontroll

Algatamise eest vastutavad: IT-juht, IT-turvaosakond, administraator

Rakendamise eest vastutavad: IT-turvaosakond, administraator

Kehtiva Windows 7 turvapoliitika võimalike rikkumiste tuvastamiseks on tarvis regulaarselt läbi viia kontrolle. Vastavad kontrollid peaksid leidma kindla koha organisatoorsetes protsessides. Kontrollide tulemused tuleb dokumenteerida, et oleks võimalik avastada ka korduvaid rikkumisi.

Siinkohal tuleb arvestada järgmiste aspektidega:

- Olemasolevate turvapoliitikate puhul tuleb kontrollida nende sisu ja ajakohasust. Aja möödudes avastatakse Windows 7 kohta loomulikult igasuguseid uusi turbeaspekte, mida tuleks turvapoliitikate kontrollimisel sobival määral arvestada. Vajadusel tuleb turvapoliitikad ümber töötada ja määrata sellele uued rakendamispõhimõtted.
- Windows 7 turvapoliitikate rakendamine peab toimuma võimalikult hoolikalt. Hetkel toimivate seadistuste ja nende võimalike kõrvalekallete väljaselgitamiseks võrreldes turvapoliitikates defineeritud parameetrite väärtustega võib rakendada automatiseeritult tarkvaratööriistu nagu nt secedit (vt M 4.243z Windowsi klientoperatsioonisüsteemide haldustööriistad).
- Kontrollida tuleb failisüsteemi, Registry ja Network Share pääsuõiguste sisu. Kasutajatel tohivad olla ainult vajalikud õigused.
- Samuti tuleb kontrollida kasutajaõigusi (süsteemiõigusi).
- Tähelepanu tuleb pöörata muudatustele, mis on tekkinud seoses uue tarkvara installeerimise ja vana tarkvara (Windowsi komponentide või rakendustarkvara) eemaldamisega. Neil asjaoludel asetleidnud turvaseadistuste (grupipoliitika objektide, pääsuõiguste jne) muutused tuleb sobival moel realiseerida, kusjuures kriitiliste muudatuste puhul tuleb enne ellurakendamist läbi viia turvaanalüüs.

Lisaks tuleb kontrolli käigus arvestada M 2.10 Riistvara ja tarkvara inventuur , et tuvastada ja välja lülitada tarkvara, millele ei ole antud kasutusluba.

Kontrollküsimused:

- Kas Windows 7 turvapoliitika ja selle elluviimise regulaarseks kontrollimiseks on organisatsiooni sees loodud sobiv organisatoorne protsess?
- Kas kehtiva turvapoliitika rikkumiste tuvastamiseks ja kõrvaldamiseks on koostatud vastavad abinõud?

M 2.331 Nõupidamis-, ürituse- ja koolitusruumide kavandamine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, organisatsiooni juht

Rakendamise eest vastutavad: organisatsiooni juht, töötajad

Nõupidamis-, ürituse- ja koolitusruumide võimalikest kasutusotstarvetest ei sõltu mitte ainult ruumide sisustuse valik, vaid ka vajaminevate turvameetmete kehtestamine. Seetõttu tuleks alustuseks kirja panna kõikide ruumide planeeritavad kasutusvaldkonnad, et seejärel saaks ruumide jaoks välja valida erinevatele nõuetele vastava sisustuse ja kehtestada nii organisatsioonilised kui ka tehnilised kasutusreeglid. Nõupidamis-, ürituste- ja koolitusruumide asukoht tuleks võimalusel valida selline, et võõrad ei peaks asjatult läbi maja kõndima, st vastavate ruumide asukohale peaksid jääma võimalikult lähedale sissekäik, sanitaarruumid ja söökla.

Nõupidamis-, ürituse- ja koolitusruumideni viiv tee ei tohiks võimalusel kulgeda turvalisuse poolest oluliste alade ligidal ning kindlasti mitte läbi selliste alade. Nõupidamis-, ürituse- ja koolitusruumide asukoht ja sisseseade peaksid olema valitud sellised, et need segaks võimalikult vähe igapäevaseid tööprotsesse. Nõupidamis-, ürituste- ja koolitusruumideni, sanitaarruumideni ja sööklani viivad teed peaksid olema tähistatud selliselt, et neist oleks võimalik lihtsalt aru saada. Sellega välditakse ruume otsivate inimeste äraeksimist. Samuti võtab konkreetne märgistus igasugused argumendid nende suust, kes ette planeeritult „kogemata“ kuhugi ära eksivad. Ruumide jaoks tuleks sisse seada broneerimissüsteem, mille abil oleks võimalik ka tagantjärele näha, kes vastavaid ruume kasutas. Vastav süsteem aitab kergesti tuvastada ka kõrvalepõiklemise võimalusi.

Täiendavad kontrollküsimused:

- Kas on olemas dokumentatsioon, mis sätestab erinevate ruumide ettenähtud kasutusvaldkonnad?
- Kas nõupidamis-, ürituste- ja koolitusruumide asukoht ja sisseseade on valitud selliselt, et need segaksid võimalikult vähe igapäevaseid tööprotsesse?

M 2.332 Nõupidamis-, ürituste- ja koolitusruumide sisustamine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT-turvaosakond, organisatsiooni juht

Rakendamise eest vastutavad: tehnika juht, organisatsiooni juht

Nõupidamis-, ürituste- ja koolitusruumid tuleb sisustada vastavalt kehtestatud kasutusvaldkonnale kas alaliselt või ajutiselt (kasutusotstarbe vaheldumise korral) selliselt, et neid oleks võimalik kasutada vastavalt muutuvatele vajadustele. Koolitusruumide õppekohad tuleb sisustada selliselt, et IT-seadmete arv ja paigutus jätaksid inimestele piisavalt ruumi, et nad üksteist ei segaks, samuti tuleb arvestada, et inimestele jääks õppekohas piisavalt ruumi, et oleks võimalik probleemivabalt dokumentidega, kirjaplokkide jms ümber käia. Nõupidamis-, ürituste- ja koolitusruumid peavad olema sisustatud otstarbekohaselt. Siia alla kuuluvad näiteks erinevad abivahendid nagu projektorid ja tahvlid. Sisseseade valikul tuleb muuhulgas arvestada järgmiste aspektidega:

- Toitepistikute asukohad peaksid olema seal, kus projektorit, sülearvuteid või muid vahendeid reaalselt kasutatakse. Pistikupesi peaks olema ruumis ka piisaval arvul, et kõik saaksid oma kaasaskantavaid töövahendeid nagu nt sülearvuteid ka reaalselt kasutada. Antud aspekt toetab ka IT-turvet, kuna pistikupesade puudusel tekivad kontrollimatud omavahelised kaabliühendused ja tähelepanematus, mille tulemusel võivad tekkida igasugused kahjustused.
- Nõupidamis-, ürituste- ja koolitusruumide voolutoide tuleb sisse seada selliselt, et see oleks viimases alajaotuses teistest ruumidest lahutatud. Sellega tagatakse, et vastavate ruumide võimalik voolukõikumine ei mõjuta teisi ruume. Optimaalne oleks luua oma alajaotus „Nõupidamis-, ürituste- ja koolitusruumid“. Seeläbi pole enam olukorras, kus mõni kaitse on ennast välja lülitanud, tarvis vastavat alajaotust eraldi kuhugi kaugele maja peale otsima minna.
- Ruumid peaksid olema varustatud vähemalt ühe püsivõrgu telefoniühendusega, et inimesed oleksid kättesaadavad ka vastavates ruumides asetleidvate ürituste ajal. Eriti oluline on see neil juhtudel, kui ürituste vältel soovitakse mobiiltelefonide kasutamine kas ära keelata või kui ruumides on kehtestatud koguni mobiiltelefoni kaasavõtmise keeld. Siseühenduste jaoks tuleks telefoniliin püsivalt sisse lülitada. Välisvõrgust sisse tulevate ja välisvõrku minevate kõnede väärkasutuse tõkestamiseks tohivad vajadusel telefoni sisse lülitada ainult volitatud isikud.
- Tuleks kaaluda, kas ruumidesse seatakse sisse ka võrgupistikud interneti-ühenduse või sisevõrkude kasutamiseks. Kuna sisevõrkudele võivad sellise kasutusvõimalusega kaasneda mitmed ohud, tuleb vastavaid võrgupääse piisaval moel kaitsta (vt M 2.204 Ebaturvalise võrkupääsu tõkestamine). Kui Interneti juurdepääs on vajalik, tuleks kaaluda, kas seda oleks võimalik lahendada eraldi, st mitte läbi intraneti.
- Kui nõupidamis-, ürituste- ja koolitusruumides seatakse sisse WLAN, tuleb tarvitusele võtta täiendavad turbemeetmed.

Täiendav kontrollküsimus:

- Kas nõupidamis-, ürituste- ja koolitusruumid on sisustatud selliselt, et väljastpoolt tulevate isikutega vestluste jaoks on võimalik tagada optimaalne ja turvaline keskkond?

M 2.333 Nõupidamis-, ürituste- ja koolitusruumide turvaline kasutamine

Algatamise eest vastutavad: IT-turvaosakond, organisatsiooni juht

Rakendamise eest vastutavad: organisatsiooni juht, kasutajad

Igas organisatsioonis peaks olema niisuguste ruumide kasutamiseks kehtestatud kindlad reeglid. Reeglid peaksid muuhulgas sisaldama kasutajatele suunatud üldisi käitumisreegleid, samuti nii statsionaarselt paigaldatud kui ka kaasavõetud seadmete kasutusreegleid. Muuhulgas tuleks arvestada järgmiste aspektidega:

- Nõupidamistest ja koolitustest osavõtjaid, kes tulevad väljastpoolt organisatsiooni, ei tohiks väljaspool koosoleku- ja koolitusruume jätta järelvalveta (vt M 2.16 Välispersonali ja külastajate valve ja saatmine).
- Tarvis on kehtestada reeglid, millistel tingimustel lubatakse välispersonalil kasutada kaasatoodud IT-süsteeme nagu nt mobiiltelefone ja sülearvuteid.
- Olemasolevaid püsivõrgu telefoniühendusi tuleb kaitsta võimaliku väärkasutuse eest. Selleks võib nt väliste numbrite valimisel nõuda parooli sisestamist.
- Ruumis peaksid olema kas ülesriputatud või laialijaotatud telefoninumbrid, kuhu kasutajad saavad pöörduda probleemide korral, nt IT-tugiteenuse või võtmehalduse telefoninumbrid. Kontaktisikud peavad olema kättesaadavad kogu tavapärase bürootööaja vältel.
- Kui ruumi on püsivalt paigaldatud projektor ja ka täiendavaid seadmeid, tuleb tarvitusele võtta vajalikud abinõud, mis kaitseksid vastavaid seadmeid võimaliku varguse eest. Seadmetele võib paigaldada nt teraskaablitest valmistatud vargalukud. Mõistlik oleks kasutada ka suletavaid kappe.

Korrashoid

- Pärast iga ürituse lõppemist tuleks ruumidest eemaldada kõik materjalid, mis võivad endas sisaldada tundlikku informatsiooni. Seetõttu tuleks pärast ürituse lõppu endaga kaasa võtta ka kasutatud pabertahvli paberid ning kohapeale jäävad tahvlid enda järel ära kustutada. Siinkohal ei tohiks ära unustada ka paberikorvi rännanud ebaõnnestunud kavandeid.
- Paljudes nõupidamis-, ürituste- ja koolitusruumides leidub statsionaarselt paigaldatud IT-süsteeme nagu nt koolitusarvuteid. Nende puhul tuleks arvestada järgnevate aspektidega:
- Nõupidamis- ja koolitusruumides kasutatavate IT-süsteemide konfigureerimine ja haldamine peab toimuma vastavalt vajadustele (vt M 4.225 Logiserveri kasutamine turvalüüsis). Tuleb määrata administraatorid, kes vastutavad otseselt koolitusarvutite haldamise eest. Lisaks tuleb ametisse nimetada kontaktisikud, kes tegelevad sageli esinevate probleemidega. Vastavad isikud peavad suutma ka kiiresti abiteenust osutada.
- Koolitusarvutitega ruumidesse tuleb keelata kaasa tuua kõikvõimalike esemeid, mis võiksid mõjutada negatiivselt vastavate IT-süsteemide tööd, st igasugused joogid ja söögid peavad jääma ukse taha. See omakorda tähendab, et kohvipausid peavad aset leidma väljaspool koolitusarvutitega ruumi.

- Täpselt peavad olema reguleeritud nõupidamis- ja koolitusruumides asuvate LAN-liideste ja kodukeskjaama liideste kasutusõigused.
- Samuti ei tohiks unustada evakuatsiooniteede korrektset tähistamist ning õiget käitumist tulekahjude korral (vt M 1.6 Tuletõrje-eeskirjade täitmine).
- Ruumide kasutamisel ilmnenud probleemide, nt pabertahvli paberi lõppemisel või seadme defekti korral tuleb teavitada vastutavaid töötajaid, et vastavad puudused saaksid kõrvaldatud võimalikult kiiresti.

Nõupidamis-, ürituste- ja koolitusruumide lukustamine

Nõupidamis-, ürituste- ja koolitusruumide lukustamise puhul on reeglina võimalik valida kahe lukustusmeetodi vahel, mis on tihti omavahel vastuolus. Juhul kui ruumi hoitakse pidevalt lukus, on ruumis asuv IT küll väga hästi kaitstud terve rea erinevate ohtude eest, kuid samas välistab see võimaluse kasutada ruumi spontaanselt. Pidevalt avatud nõupidamis-, ürituste- ja koolitusruume saab seevastu küll igal ajal kasutada, kuid ITle tähendab see jällegi kõrgenenud riski. Ruumi lukustamise eeliseks on muuhulgas tõsiasi, et see suurendab tõenäosust hoida nõupidamis-, ürituste- ja koolitusruumide sisseseade soovitud seisukorras. IT-turbe seisukohast tuleks nõupidamis-, ürituse- ja koolitusruumid väljaspool nende kasutusaega lukustada. Samal ajal tuleb loomulikult kindlustada, et ruumide kasutusvajadusel oleksid need kiiresti ja vastavalt vajadustele kasutusvalmis. Nõupidamis-, ürituste- ja koolitusruumide võtmeid peaks saama ühest kindlast kesksest kohast, nt registraatori käest või vastavast osakonnast.

Sülearvuti ja dokumentide hoiustamine

Reeglina puudub nõupidamis-, ürituste- ja koolitusruumides võimalus dokumente, IT-süsteeme jms eraldi luku taha panna. Seetõttu peaks olema võimalik neid ruume vähemalt selleks ajaks, kui üritusest osavõtjad ajutiselt ruumist lahkuvad, kas lukustada või organiseerida ruumi järelvalve mõne oma töötaja poolt.

M 2.334z Sobiva hoone valimine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, sisekommunikatsiooni juht
Rakendamise eest vastutavad: sisekommunikatsiooni osakond

Lisaks hoone asukoha planeerimisele (vt M 1.16 Hoone sobiv asukoht), mis tegeleb hoone ümbruse hindamisega, tuleb hoone sobivust hinnata ka seestpoolt. Üldjuhul tuleb muidugi juba hoonet valides kontrollida, kas kõiki hilisemaks kasutuseks vajalikke meetmeid on selles võimalik rakendada või mitte. Mõningate meetmete ellurakendamiseks vajalikke eeldusi on võimalik luua ka tagantjärele, kuid see on seotud väga suurte kuludega ning võib ka ebaõnnestuda. Käesolev meede peaks aitama kergendada olemasolevate hoonete vahel valiku tegemist, püüdes ennetada võimalikult paljusid tüüpilisi hiljem esilekerkivaid probleeme. Samas võib seda kasutada ka uue hoone planeerimisel. Sõltuvalt sellest, kas hoonet soovitakse osta või rentida, langeb erinevatele aspektidele ka erinev osatähtsus.

IT-turbe seisukohast vaadatuna tuleks muuhulgas arvestada ka järgmiste hoonekonstruktsioonide seisukorda puudutavate aspektidega:

- Kas hoone staatika (lagede maksimaalne kandevõime, kandvad seinad) on piisav suure lauskoormusega ruumide (serveriruumi, arvutuskeskuse, UPSi jms) sisseseadmiseks nendes hoone osades, kus nende töö oleks kõige ökonoomsem ja IT-turbe seisukohast kõige mõttekam (vt M 1.13z Kaitset vajavate ruumide paigutus ja M 1.47 Eraldi tuletõkked)?
- Kas olemasolevaid või täiendavalt vajalikke juurdepääsuteid (koridore, trepikodasid, lifte) on võimalik kasutada ja sisse seada vastavalt meetmes M 2.17 Sisenemisreeglid ja reguleerimine ?
- Kas juurdepääsuteed võimaldavad suure turbevajadusega hoone osi eraldada madala turbevajadusega hoone osadest selliselt, et näiteks koolitusruumid ja arendustegevusse kaasatud ruumid oleksid teineteisest lahutatud?
- Kas olemasolevaid või täiendavalt vajalikke juurdepääsuteid (koridore, trepikodasid, lifte) on alati võimalik kasutada ka suuremate IT-komponentide transportimiseks? Kui see pole võimalik, võib riistvara rikke tagajärjel kujuneda olukord, kus süsteemi taaskäivituses tekib pikk viivitus.
- Kas hoonele kehtivad ehituslikud piirangud (servituudid, muinsuskaitse nõuded jne), mis võiksid takistada hoone vajadusekohast kasutamist? Eriti hoolikalt tuleks uurida kolmandatele isikutele antud servituute, sest nendest võivad tekkida vastuolud kaitstud juurdepääsuga alade moodustamisel.
- Kas ruume on võimalik liigendada vastavalt M 1.8 Ruumide tuleohutus ja M 1.51 Tulekoormuse vähendamine ?
- Kas meetmeid M 1.3 Juhtmestuse kohandamine ja M 1.39 Tasandusvoolude vältimine varjes on võimalik rakendada vastuvõetavate kuludega?
- Kas hoonel on välimine piksekaitse? Kui on, kas see mõjutab üksikasju meetmete M 1.25 Liigpingekaitse ja M 1.39 Tasandusvoolude vältimine varjes ellurakendamisel?

Rendipindade puhul tuleb lisaks arvestada ka järgnevate aspektidega:

Kas rentnikul on võimalik saada kõik õigused hoone sisseseadmiseks vastavalt oma vajadustele? Milliseid õigusi ja reservatsioone soovib rentija säilitada?

Kas rendilepingu lõppedes on rentnik kohustatud turvalisust tagavad ehituslikud muudatused kõrvaldama? Planeerimisfaasis peab olema kindlaks tehtud, et võimalike lisakulude kartuses ei loobutaks vajalikest turvameetmetest.

Kui hoonet kasutavad paralleelselt ka kolmandad isikud, tuleb välja selgitada, kui palju mõjutab või koguni takistab see erinevate meetmete ellurakendamist.

Kas rentnik saab õiguse kaasa rääkida kolmandate isikute poolt kasutatavate ruumide korduval väljarentimisel? Võib juhtuda, et hoone uusi kaaskasutajaid tuleb turvalisuse aspektist hinnata kriitilisemalt kui eelnevaid kaaskasutajaid.

Kontrollküsimus:

- Kas sobiva hoone valimisel arvestatakse ka turvaspektidega?

M 2.335 Infoturbe eesmärkide ja strateegia kehtestamine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond

Rakendamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT turbespetsialist

Ametiasutuse või ettevõtte ülesannete ja eesmärkide täitmisel on edu tagamiseks oluline faktor infoturve. Infoturbe puhul ei ole tegemist mitte ühekordse projekti, vaid kestva protsessiga ning sellega peavad oma tööprotsesside käigus arvestama kõik töötajad. IT-turbe protsesside juurutamine ja rakendamine kuulub ettevõtte või ametiasutuse juhtorgani kohustuste hulka. Esimese sammuna tuleb määrata sobivad IT-turbe eesmärgid ja koostada vastav strateegia. Lisaks strateegilistele juhtnööridele tuleb ettevõtte või ametiasutuse korrapärase ja turvalise IT-toega töö võimaldamiseks välja töötada ka kontseptsioonide üldnõuded ja organisatsioonilised raamtingimused.

IT-turbe eesmärgid

Turbeprotsesside juurutamise alguses tuleb hoolikalt määratleda IT-turbele seatavad eesmärgid. Vastasel korral tekib oht, et hakatakse välja töötama erinevaid IT-turbe kontseptsioone, mis ei arvesta ametiasutuse või ettevõtte tegelike vajadustega. IT-turve aitab kaasa ettevõtte või ametiasutuste peamiste eesmärkide ja ülesannete täitmisele. IT-turbe eesmärkide sõnastamise aluseks on seega vastava institutsiooni peamised eesmärgid ja tähtsamad tööprotsessid. Sobivad ja realistlikud IT-turbe eesmärgid on aluseks kõikide järgnevate IT-turbeprotsessi etappide juurutamisel. Eesmärgid peavad olema reaalsed, veenvad, mõistetavad ja arvestama praktilise tööga. Seatud eesmärkide alusel töötatakse hiljem IT-turvakontseptsiooni loomise käigus välja IT-süsteemide, IT-komponentide ja võrkude turbevajadus ning määratakse, milliseid meetmeid tuleb selle tagamiseks võtta. IT-turbemeetmete võtmisel tuleb reeglina leida alati kompromiss kulude ja keerukuse vahel. Mõistlike IT-turbe eesmärkide sõnastamiseks peaks olema arusaadav, milline info ja millised tööprotsessid aitavad kaasa ülesannete täitmisele ning kui kõrgelt tohib hinnata nende osatähtsust.

IT-turbe eesmärke peab kandma ja nende eest vastutama ettevõtte või ametiasutuse juhtkond. Eesmärgid peab välja töötama ja dokumenteerima organisatsiooni vastav IT-turbeüksus koostöös juhtkonnaga. Olenevalt organisatsiooni konkreetsest struktuurist on mõistlik kaasata protsessi nõustamiseks ka suuremate organisatsiooniüksuste (nt osakondade või valdkondade) juhid. Detailse kirjelduse, kuidas ja kui täpselt IT-turbe strateegia ja eesmärgid tuleb kirja panna, leiate BSI standardist nr 100-2 „IT etalonturbest lähtuv tegutsemisplaan”, ingliskeelne variant on kättesaadav veebiaadressil https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html)

IT-turvastrateegia ajakohasuse säilitamine ja tõhustamine

IT-turbe eesmärkide ja strateegia puhul tuleb regulaarselt kontrollida, kas need on jätkuvalt ajakohased ja tegelikele oludele vastavad. Eriti tähtis on kontrollida IT-turvaeesmärke ja -turvastrateegiat kehtivate raamtingimuste, tööprotsesside või IT-keskkonna muutumise korral ning vajaduse korral neid ka vastavalt kohandada. IT-turbe protsess on pikemas perspektiivis edukas vaid juhul, kui juhtkond kontrollib regulaarselt ka IT-turbe strateegia toimimist ja tõhusust. Kontrollide põhjal selgunud täiendamisvajadused tuleb turbeprotsessi sisse viia.

Kontrollküsimused:

- Kas IT-turbe eesmärgid on välja selgitatud?
- Kas on juurutatud adekvaatne IT-turbe protsess?
- Kuidas tagatakse IT-turbe eesmärkide ja turvastrateegia ajakohastamine?

M 2.336 Koguvastutus infoturbe eest juhtkonna tasemel

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond

Rakendamise eest vastutavad: ametiasutuse/ettevõtte juhtkond

IT turvalisus on juhtide pärusmaa!

Ettevõtete ja ametiasutuste juhtimine on tegevused, millega kaasneb suur vastutus. Juhtimisvastutus ei puuduta mitte ainult eesmärkide, nagu nt ärilise edukuse saavutamist, vaid ka potentsiaalsete riskide võimalikult varajast tuvastamist ja minimeerimist. Lisaks muudele ohtudele tuleb tegeleda ka sellistega, mis tekivad ebapiisava IT turbe tagajärjel. Piisava IT turbeastme tagamine on keerukas ülesanne. See eeldab süstemaatilist lähenemist, pidevat ja eesmärgile orienteeritud IT turbeprotsessi. Iga institutsiooni juhtkonna ülesanne on see protsess algatada, seda juhtida ja kontrollida. Väiksemate institutsioonide puhul tegeleb kõnealuse valdkonnaga tihti personaalselt üks kindel juhtkonna liige. Keskmise suurusega ja suurtes institutsioonides delegeeritakse IT turbega seotud ülesanded erinevatele IT turbe eest vastutavatele töötajatele. Olenevalt institutsiooni suurusest ja omapärast kaasatakse IT turbe protsessidesse veel ka täiendavaid inimesi, kelle puhul kujutab nimetatud valdkond endast kas põhitööd või siis täiendavat tööülesannet. Turbevaldkonna erinevate ülesannete adekvaatseks juhtimiseks oleks organisatsioonis mõistlik luua sobiv struktuur. Koguvastutus jääb siinkohal alati juhtorgani kanda, sõltumata sellest, kui paljudele inimestele turbealaseid ülesandeid delegeeritakse.

Juhtkonna tasandi motivatsioon

Juhtkonda tuleks regulaarselt teavitada puuduliku IT turbega kaasnevatest võimalikest ohtudest ja nende tagajärgedest. Selleks on soovitatav tõsta juhtkonna teadlikkust seoses järgmiste punktidega (vt M 3.44 Juhtkonna teadlikkuse tõstmine infoturbe alal):

- tuua välja turbega seotud riskid ja nendega seotud kulud;
- selgitada IT turvaintsidentide mõju igapäevastele kriitilise tähtsusega tööprotsessidele;
- juhtida tähelepanu seadusest ja lepingutest tulenevatele turbekohustustele;
- anda ülevaade institutsiooni tegevusvaldkonnale ettenähtud standardsetest IT turbelahendustest.

Vaatamata sellele, et turbealaste eesmärkide saavutamise eest vastutab esmajoones juhatus, peavad kõik institutsiooni töötajad kõnealust vastutust siiski ka jagama ja selles protsessis aktiivselt kaasa lööma.

Seetõttu on tähtis, et järgitaks alljärgnevaid põhimõtteid:

- **koguvastutuse võtmine IT turbe eest** – IT turbe initsiatiiv peab tulema ametiasutuse või ettevõtte juhtkonnalt. Ametiasutuste ja ettevõtete juhtkonnad peavad aktiivselt toetama IT turbega seotud ülesandeid;
- **IT turbe integreerimine** – IT turve peab moodustama kindla osa kõikidest protsessidest ja projektidest, kus kasutatakse IT-lahendusi. Sellele lisaks tuleb kõiki protsessis osalejaid informeerida piisavalt IT turbega seotud protsessist ja neid selleks motiveerida, et vastavatest nõuetest ka kinni peetaks;

- **vastutusalade kindlaksmääramine** – ametiasutuse ja ettevõtte juhtkond peab nimetama ametisse IT turbe eest vastutavad töötajad ning tagama neile piisava koolituse ja andma nende käsutusse vajalikud ressursid;
- **juhtimine ja kontrollimine –** juhtkond peab tegelema aktiivselt IT turbega seotud protsesside algatamise, juhtimise ja kontrollimisega. Selleks peab juhtkond olema teadlik võimalike IT turvaintsidentidega kaasnevatest tagajärgedest, juhtkond peab määrama turbega seotud eesmärgid ja looma raamtingimused, mis võimaldaksid püstitatud eesmärke realiseerida;
- **reaalsete eesmärkide püstitamine** – absoluutset IT turvet ei ole olemas. Seetõttu on oluline, et turbealased eesmärgid püstitataks selliselt, et neid oleks ühelt poolt võimalik saavutada vastuvõetavate kulutustega (personali-, aja- ja rahakuluga) ning teiselt poolt oleks võimalik tagada, et turbega seotud ohte vähendataks piisavalt;
- **eeskujuks olemine** – juhtkonnal on IT turbe valdkonnas täita eeskuju andev funktsioon. Siia alla kuulub muu hulgas tõsiasi, et juhtkond peab ka ise kõikidest ette antud turbereeglitest korrektselt kinni pidama;
- **pidev täiustamine** – IT turvalisuse haldamiseks kasutatavaid elemente tuleb pidevalt kontrollida, et välja selgitada, kas need on jätkuvalt sobivad ja toimivad piisavalt tõhusalt. Tuvastatud kitsaskohad tuleb sihikindlalt kõrvaldada ja võimalikud täiendused pidevalt ellu rakendada. Muu hulgas on tähtis tunda võimalikult vara ära tulevikuga seotud arengud, muutunud raamtingimused ja potentsiaalsed ohud.
- **suhtlemine ja teadmised** – juhtkond ja IT turvaosakond peavad töötajaid motiveerima ja hoolitsema selle eest, et töötajad läbiksid piisava koolituse ning oleksid valdkonnast piisavalt teadlikud. Töötajatele tuleb selgitada eelkõige nii tehniliste kui ka organisatoorsete turbemeetmete sisu ja eesmärke. Meetmete rakendamise planeerimisse tuleks kaasata ka IT kasutajad. Seeläbi on võimalik kaasata töötajate ideid ja hinnata kavandatavate turbemeetmete rakendatavust.

Kontrollküsimused:

- Kas ametiasutuse või ettevõtte juhtkond on vastutuse IT turbe eest selgelt enda kanda võtnud?
- Kas ametiasutuse või ettevõtte juhtkond on määranud töötajad, kes vastutavad IT turbe eest?

M 2.337 Infoturbe integreerimine üleorganisatsioonilistesse tegevustesse ja protsessidesse

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond

Rakendamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT turvaosakonna meeskond

IT-alane turve peab olema integreeritud kõikidesse tööprotsessidesse. Kõikide vajalike IT turbeaspektide nõuetekohane rakendamine peab olema tagatud mitte ainult uute projektide, vaid ka käimasolevate rakenduste puhul. Suuremates institutsioonides on tihti kasutusel kõikehõlmav riskihaldussüsteem. Kuna IT-ga seotud riskid kuuluvad olulisimate operatsiooniriskide alla, tuleks IT-alaste ohtude haldamine viia kooskõlla juba olemasolevate haldusmeetoditega. Siinkohal on oluline, et organisatsiooni sees erinevates allüksustes kehtestatavad tööeeskirjad ja töökohustusi puudutavad kokkulepped ei läheks omavahel vastuollu. Põhjalikke seletusi ja konkreetseid meetmeid IT turbe organisatoorse poole kujundamise kohta leiate IT etalonturbe kataloogidest. Seetõttu tuuakse alljärgnevalt välja vaid mõningad näited tähtsamate üldkehtivate IT turbemeetmete kohta.

Vastutusalade määramine ja funktsioonide lahutamine

IT turbega seotud organisatoorse poole vastutusalad ja kompetentsid peavad olema täpselt määratletud ja töötajate vahel üheselt ära jagatud. Lisaks tuleb kõikide tähtsamate funktsioonide puhul kehtestada töötajate kindel asendamise kord.

Teabe liikumise kindlaksmääramine

Teabe liikumist kajastavad reeglid tuleb planeerida, kirjeldada, teatavaks teha ja juurutada. Kõikide ülesannete ja töörollide jaoks tuleb kehtestada reeglid, kes peab keda teavitama, keda tuleb teavitada erinevate sündmuste korral ning mida täpselt peaks edastatav info sisaldama.

Tööprotsesside, info, IT-rakenduste ja IT-süsteemidega seotud vastutuse kehtestamine

Kõikide olulisemate tööprotsesside, info, IT-rakenduste ja IT-süsteemide, samuti hoonete ja IT-ruumide puhul tuleb määrata töötajad, kes nende eest vastutavad. Olenevalt tegevusvaldkonnast ja kohapeal rakendatavast sõnavarast võib vastavaid töötajaid nimetada kas info valdajateks, tööprotsesside eest vastutajateks või ka spetsialistideks. Nimetatud spetsialistid peavad oma tööga toetama IT turvastrateegia väljatöötamist ja rakendamist (vt lisaks M 2.225 Teabe, rakenduste ja IT-komponentide alaste vastutuste kinnistamine).

Infoturbealase koolituskontseptsiooni koostamine

IT turve puudutab eranditult kõiki töötajaid. Iga töötaja peab oma vastutustundliku ja tagajärgedega arvestava tegevuse läbi kaasa aitama võimalike kahjude vältimisele ja eduka turbe saavutamisele. See nõue ei puuduta mitte ainult alalisi töötajaid, vaid ka kõiki teisi institutsiooni heaks töötavaid inimesi, seega nt ka uksehoidjaid ja praktikante. Lisaks tuleb turbevaldkonna puhul arvestada ka selliste isikutega, kes pääsevad tööprotsessidele, rakendustele ja IT-süsteemidele ligi väljastpoolt, nt väljasttellitud teenuse osutamisega tegelevate töötajatega. Tähtsamad turbemeetmed, millega personali haldamise puhul tuleb arvestada, st alustades personali valikust ja töölevõtmisest kuni nende ümberasumiseni mõnda teise valdkonda või töötajate institutsioonist lahkumiseni on koondatud moodulisse

B 1.2 Personal . Lisaks tuleks kõik töötajad viia kurssi oma tööülesannete raames kehtivate turbemeetmetega. Töötajate teadlikkust seoses IT turbeaspektidega tuleb regulaarselt tõsta, et nad oleksid oma igapäevatöös infoga ümberkäimisel teadlikud nii võimalikest ohtudest kui ka vastavatest kaitsemeetmetest. Teavitamisprotsessi tuleb kaasata ka organisatsiooni juhtkond (vt B 1.13 Infoturbe teadlikkus ja -koolitus).

IT-turbeaspektide integreerimine tööprotsessidesse

Juhatusel peab olema ülevaade tööprotsesside jaoks kriitilise tähtsusega infost, erinevate valdkondade tööülesannetest ja tööprotsessidest. Vastutavad spetsialistid ja IT turvaosakond peavad kehtestama konkreetsed reeglid olulisemate turbeaspektidega ümberkäimiseks (nt kehtestama kaitsemeetmed, tegelema info liigitamise ja märgistamisega).

Õigused ja volitused

Väärtuste kaitsmiseks tuleb täpselt reguleerida, millistel põhimõtetel leiab aset sissepääs ruumidesse, juurdepääs IT-süsteemidele ja rakendustele ning juurdepääs infole (vt M 2.6 Sissepääsuõiguste andmine ; M 2.7 Süsteemi ja võrgu pääsuõiguste andmine ; M 2.8 IT-rakendustele ja andmetele pääsuõiguste andmine ja M 2.220 Pääsu reguleerimise suunised).

Muudatuste haldus

Muudatuste haldus tegeleb riistvara- ja tarkvaramuudatuste, samuti protsesside muudatuste planeerimisega. Organisatoorsete reeglitega on tarvis tagada, et selle käigus järgitaks kõiki vajalikke turbeaspekte (vt M 2.221 Muudatuste haldus).

Konfiguratsiooni haldus

Konfiguratsiooni haldus hõlmab kõiki meetmeid ja struktuure, mis on vajalikud erinevate objektide seisundi seireks, tegeledes nt objektide identifitseerimise, inventari loetelu loomise ja uuendamisega kuni kasutuselt kõrvaldamiseni välja.

Vaadeldavad objektid (konfiguratsioonielemendid) võivad olla nii terved infrastruktuuri valdkonnad, konkreetsed IT-rakendused ja IT-süsteemid kui ka nende üksikud komponendid (nt dokumentatsioonid). Konfiguratsiooni halduse raames tuleb juurutada protsessid ja reeglid, millega kirjeldatakse, kuidas peaks haldama informatsiooni, mis kajastab rakendatavate konfiguratsioonielementide omadusi, ning kuidas tuleks hallata infot, mis kajastab turbe seisukohast olulisi rikkeid, probleeme ja muudatusi, mis on seotud muudatustega konfiguratsioonielementides. Tüüpilised tegevused on nt IT-süsteemide loetelu ajakohastamine või muudatuste sisseviimine turvet kajastavas dokumentatsioonis pärast muudatuste sisseviimist IT-rakendustes. Konfiguratsiooni halduse kohta leiate täiendavat infot moodulist B 1.9 Riist- ja tarkvara haldus .

Kontrollküsimused:

- Kas turvet puudutavate otsuste langetamisse kaasatakse piisaval määral ka IT turbe eest vastutav töötaja või IT turvaosakonna meeskond?
- Kas IT turbe seisukohast olulisi organisatsioonilisi reegleid ja protsesse kontrollitakse ja täiendatakse regulaarselt?

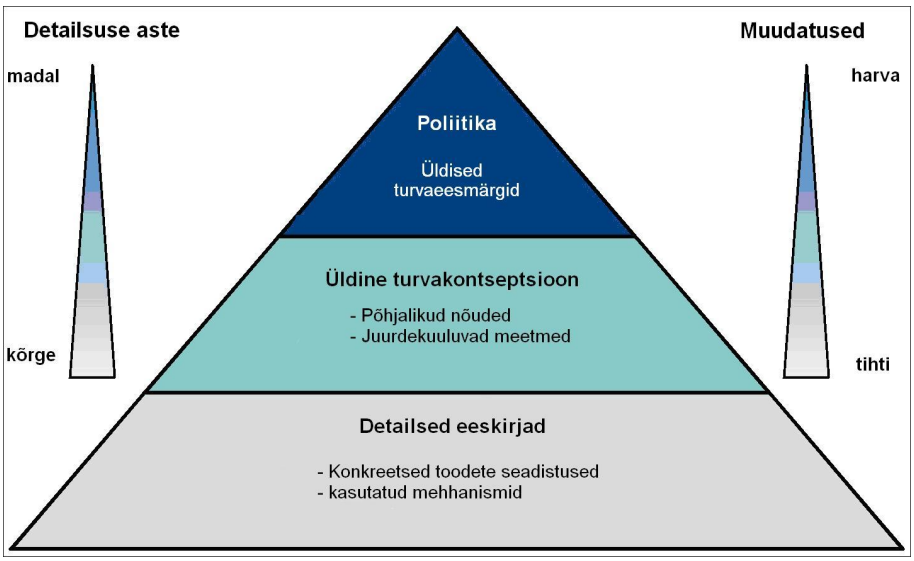
M 2.338z Sihtrühmakohase infoturbepoliitika koostamine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT turvaosakonna meeskond
Rakendamise eest vastutavad: IT turvaosakonna meeskond

IT-turvet kajastavate teemade sihtrühmakohane käsitlus
Soovitud turbeastme saavutamise üks olulisi edutegureid on vastutustundlikud ja kompetentsed töötajad, kes suudavad koordineeritult koos töötada. Tuleb arvestada, et erinevad sihtrühmad, nagu nt juhtkond, IT kasutajad, administraatorid ja IT turbeeksperdid täidavad erinevaid tööülesandeid, mistõttu on tegemist ka erineval tasemel eelteadmistega. Ettevõtte või ametiasutuse juhtkond peab võtma koguvastutuse, püstitama eesmärgid ja kehtestama raamtingimused. Administraatorid seevastu peavad süsteemide käsitsemiseks ja turvaliseks konfigureerimiseks olema kõrge tehnilise kvalifikatsiooni ja paljude detailsete teadmistega. IT turbe eest vastutavad töötajad peavad olema suutelised looma IT etalonturbe kataloogide alusel kõikehaarava IT turvakontseptsiooni. Kui sellega soovitakse katta kõik IT turbe valdkonnad, tuleb arvestada, et vastavas IT turvakontseptsioonis saab olema päris palju lehekülgi. IT turvakontseptsiooni sisu sihtrühmakohane ettevalmistus ja inimesteni vahendamine moodustab tähtsa osa IT turvaosakonna tööst. Eesmärk on saavutada olukord, kus kõik töötajad oleksid teadlikud neile kehtivatest IT turbeaspektidest ja neid järgima. Selleks on soovitatav koostada erinevad turbepoliitikad või koguni põhjalikud osakontseptsioonid, mis puudutaksid erinevaid IT turvet puudutavaid teemasid olenevalt sihtrühma vajadustest. Niimoodi on võimalik tagada, et töötajatele edastatakse täpselt selline info, mida nad ka reaalselt teatud teema kohta teadma peavad. Turvalisuse seisukohast kriitilistes valdkondades töötavate IT-süsteemide või IT-teenuste jaoks, mille konfigureerimine või kasutamine on keeruline, võib nt administraatorite sihtrühmale koostada eraldi IT-süsteemi turvapoliitikad, mis sisaldaksid muu hulgas ka tehnilisi juhiseid. IT kasutajate sihtrühmale loodavad teemakäsitlused seevastu ei tohiks koormata töötajaid liigsete detailidega, kuna need võivad juhtida tähelepanu olulistelt asjadelt hoopis kõrvale, muuta teema arusaamatuks ja tekitada segadust.

Poliitikate hierarhiline ülesehitus
Poliitikate sõnastamisel on ennast õigustanud lähenemine, mis jagab töö mitme eri tasandi vahel. Esimesel tasandil tuleks sõnastada lühidalt ja konkreetselt üldised IT turvaeesmärgid ja IT turvastrateegia, koostades vastava IT turvapoliitika (vt M 2.192 Infoturbepoliitika koostamine). Strateegia ei sisalda veel ühtki tehnilist detaili, selle peab vastu võtma juhtkond ning selles tuleks teha võimalikult vähe muudatusi. Järgmisel tasandil tuleks eelneva info põhjal koostada põhjapanevad tehnilised turbenõuded. Üldise turvakontseptsiooni alla kuuluvad dokumendid, kus kirjeldatakse erinevaid IT turbega seotud aspekte (nt interneti kasutamise poliitika või viirusetõrje kontseptsioon), kuid ei mainita veel ühtki konkreetset toodet. Kolmandal tasandil kirjeldatakse tehnilisi detaile, konkreetseid meetmeid ja toote eripärasid kajastavaid seadistusi. See sisaldab palju dokumente, mida muudetakse regulaarselt ning reeglina loevad neid ainult erinevate valdkondade eest vastutavad eksperdid.

Alljärgneval joonisel on kujutatud erinevate tasanditega seotud töid graafiliselt.



Joonis. Poliitikate hierarhiline ülesehitus

Spetsiaalsete IT turvapoliitikate sisu

Spetsiaalsete IT turvapoliitikate sihtrühmakohasel koostamisel võib lähtuda järgmistest teemadest:

- käitumisreeglid ja turbealased suunised IT kasutajatele,
- käitumisreeglid ja turbealased suunised administraatoritele,
- tulemüürid (vt M 2.70 Turvalüüsi (tulemüüri) kontseptsiooni väljatöötamine),
- viirusetõrje (vt M 2.154 Viirusetõrje kontseptsiooni loomine),
- avariiplaanid,
- andmevarundus (vt M 6.33 Andmevarunduskontseptsiooni loomine),
- arhiveerimine (vt M 2.243 Arhiveerimiskontseptsiooni väljatöötamine),
- e-posti ja interneti kasutamine,
- väljasttellimine (vt M 2.251 Väljasttellimisprojektide turvanõuete spetsifitseerimine).

IT kasutuse turvapoliitika

IT turvapoliitika üldisi nõudeid on tihti soovitatav konkretiseerida IT kasutusele suunatud turvapoliitika abil, st vastav eraldi turvapoliitika peab aitama tähtsamad tervet organisatsiooni hõlmavad IT turvakontseptsiooni meetmed ilma koormavate tehniliste detailideta kokku võtta ja kõigile arusaadavaks muuta. Vastav poliitika peaks kirjeldama üldkehtivaid reegleid seoses IT kasutamisega ning peaks aitama mõista IT turvakontseptsiooni.

IT kasutusele suunatud üldises poliitikas võib puudutada järgmisi teemasid:

- kaitset vajava infoga ümberkäimine (informatsiooni valdajate kindlaksmääramine, info liigitamiskohustus selle kaitsevajaduse järgi),

- kohalduvad seadused ja ettekirjutused,
- tähtsamate töörollide lühikirjeldused (nt IT turbe eest vastutav töötaja, administraator, kasutaja),
- personali koolitamine,
- töötajate asendamise reguleerimise kohustus,
- IT haldamisele seatavad nõuded (soetamine, kasutamine, hooldamine, audit ja utiliseerimine),
- peamised turbemeetmed (sissepääs ruumidesse ja juurdepääs IT-süsteemidele, krüpteering, viirusetõrje, andmevarundus, avariiplaanid),
- spetsiifiliste IT-teenuste kasutusreeglid (andmete edastamine, interneti kasutamine).

Näidispoliitikad
Erinevaid näiteid poliitikate ja kontseptsioonide kohta on võimalik leida RIA kodulehelt ISKE teema „Dokumendid” alt.

Kontrollküsimused:

- Millised on seni institutsioonis eksisteerinud IT turbepoliitikad?
- Kas töötajad on asjaomaste IT turbepoliitikatega kursis?

M 2.339z Ressursside ökonoomne kasutamine infoturbeks

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond
Rakendamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT turbespetsialist

IT kasutuseks vajalike ressursside eraldamine
IT turbe üks peamisi eeldusi on IT hästi toimiv käitamine. IT käitamiseks peab olema võimalik kasutada piisaval hulgal vajaminevaid ressursse. Reeglina tuleb enne seda, kui kehtestatud IT turbemeetmed saavad efektiivselt tööle hakata, lahendada tüüpilised IT käitamisega seotud probleemid (väike eelarve, ülekoormatud administraatorid, vähestruktureeritud ja halvasti hooldatud IT-kooslus). Seda, kas eraldatud ressurssidest piisab, näeb näiteks selle põhjal, kas IT kasutajatele suudetakse pakkuda piisavalt tugiteenust ning kas kõikvõimalik riist- ja tarkvara läbib ettenähtud testimisprotseduurid.

Ressursside eraldamine IT turbeks
IT turve eeldab piisava finants- ja personaliressursi ning sobiva sisseseade olemasolu. Nimetatud vahendid peab IT turvaosakonna meeskonnale vajaminevas mahus eraldama vastava ettevõtte või ametiasutuse juhtkond. IT turvaosakonna meeskonnal on soovitatav koostada IT turbealaste eesmärkide põhjal loetelu ressurssidest, mis on vajalikud kõikide sõnastatud meetmete rakendamiseks. Selline loetelu on ühelt poolt abiks juhtkonnale ressursside jagamise üle otsustamisel, kuid aitab samal ajal ka planeerida vajalikke projekte ning kehtestada projektide tähtaegu.

Juurdepääs välistele ressurssidele
Organisatsioonisisesed IT turvaeksperdid on reeglina oma igapäevatööga nii ülekoormatud, et uute ülesannete või edasiarenduste puhul ei ole neil aega, et kõiki turvalisust mõjutavaid faktoreid piisavalt analüüsida ja neid omakorda turbemeetmeteks vormistada. Sellesse valdkonda kuuluvad nt seadusemuudatused, uute IT-süsteemide kasutuselevõtmine ja uuemate tehnika vallas toimunud arengute jälgimine. Kuhjuvate tööülesannete korral tuleb palgata kas täiendavaid töötajaid, mis on tihti küllaltki raske, või kasutada väliste ekspertide teenuseid.

Vajaduse korral tuleb organisatsiooni IT turvaekspertidel koostada vastav ülevaade, mille alusel saaks juhatus eraldada neile vajalikud ressursid. Eesmärk on tagada kõikide vajalike turbemeetmete ellurakendamine, ükskõik kas väliste või institutsioonisiseste ekspertide abil.

Ressursside eraldamine IT turvalisuse eest vastutavatele töötajatele

Ilma korralikult toimiva IT turvalisuse organisatoorse pooleta ei ole isegi kõige kallimatest tehnilistest lahendustest mitte mingisugust kasu. Kogemused on näidanud, et üks efektiivsemaid turbemeetmeid on nimetada ametisse IT turvaekspert. Pärast eraldi IT turvalisuse eest vastutava töötaja ametisse nimetamist langeb enamikes organisatsioonides märgatavalt IT turvaintsidentide arv.

Selleks, et IT turvaeksperdil oleks ka reaalselt võimlaik IT turbeastet tõsta, peab tal olema:

- piisavalt aega, et oma tööülesandeid täita;
- küllaldane ülevaade kõikidest igapäevatöö protseduuridest, eri valdkondade tööülesannetest ja projektidest;
- piisav juurdepääs kõigile vajalike ressurssidele.

Väiksemates organisatsioonides on võimalik, et IT turvaeksperdi ülesanded võtab enda kanda mõni inimene lisaks oma põhitööle.

Ressursside eraldamine IT turvaosakonna meeskonnale

IT turvaosakonna meeskond tuleks moodustada siis, kui üksainus IT turvaekspert ei ole enam suuteline haldama kõiki igapäevatöö protsesse ja kõikvõimalikke projekte, st juhul, kui organisatsioon on saavutanud teatud suuruse. IT turvaprotseduuride esmakordne juurutamine on tihti seotud suuremate ressursikuludega. Seetõttu on otstarbekas võimaldada IT turvaosakonna meeskonnal kasutada selles tööetapis täiendavat personaliressurssi.

IT turvastrateegia majanduslikud aspektid

IT turvastrateegia puhul tuleks juba algusest peale arvestada ka selle majanduslike aspektidega. Planeeritavate IT turbemeetmete valimisel tuleks arvestada ka käsutada olevate ressurssidega. Kui teatud meetmete rakendamiseks ei jätku piisavalt tehnilisi lahendusi või personali, tuleb muuta strateegiat.

Paljudel juhtudel on võimalik leida teistsuguseid meetmeid, mis suudavad tagada enam-vähem sama kõrge turbeastme nagu soovitud. Kui aga sõnastatud turvaeesmärgid ja olemasolevad finantsilised, tehnilised või personaliressursid on siiski liiga erinevad, tuleb nii turvaeesmärgid kui ka igapäevased tööprotsessid uuesti põhjalikult läbi vaadata. Sellistel juhtudel tuleb ebakõladest teavitada ka juhtkonda, et neil oleks vajaduse korral võimalik võtta abistavaid meetmeid.

IT turvameetmete kindlaksmääramisel tuleks alati konkreetselt välja tuua ka nende rakendamiseks vajalik rahaline ja personaliressurss. Lisaks tuleks kindlaks määrata ka vastutavad töötajad ja muud kontaktisikud ning kehtestada täpsed ajaplaanid ja materjalid, mida on tarvis soetada. Kõikide planeeritavate turvameetmete puhul on lisaks soovitatav dokumenteerida, kas IT turbe jaoks planeeritud ressursid eraldati kokkulepitud ajakava kohaselt ning põhjused, miks projekti elluviimisel on tekkinud kõrvalekaldeid. Ainult niimoodi saab tõrkeid ära hoida ja tagada, et kõikvõimalikud parandused on piisavalt jätkusuutlikud.

Ressursside eraldamine IT turbe kontrollimiseks

Kõiki IT turvameetmeid tuleb regulaarselt kontrollida, et teha kindlaks, kas need toimivad piisavalt hästi ja täidavad oma eesmärki. Ka selleks tuleb eraldada vajalikud ressursid. Üldjuhul ei tohiks turvameetmete toimimist ja sobivust kontrollida need töötajad, kes tegelesid turvameetmete väljatöötamisega. Organisatsioonisisese lühinägelikkuse vältimiseks võib selleks otstarbeks kaasata väliseid eksperte. Vastuse leidmine küsimusele, kas IT turbele on eraldatud piisavalt ressursse, on reeglina palju raskem kui tehniliste aspektide kontrollimine.

Kontrollküsimused:

- Kas nõuetekohase IT käituse jaoks on eraldatud piisavalt ressursse?
- Kas IT turvalisust puudutavaid kontrolle viiakse läbi regulaarselt?
- Kas IT turvameetmete kindlaksmääramisel toodi välja ka andmed nende elluviimiseks vajalike ressursside kohta?
- Kas IT turbele planeeritud ressursid eraldati ka reaalselt kokkulepitud tähtaegade kohaselt? Kas meetmete ellurakendamisel esines viivitusi, mille tagajärjel polnud pikema aja jooksul võimalik tagada eesmärgiks seatud turbeastet?
- Kas IT turbe eest vastutavatel töötajatel või IT turvaosakonna meeskonnal on võimalik täita oma turbealaseid tööülesandeid, või takistavad selle funktsiooni täitmist nt igapäevased tööülesanded või muud projektid?

M 2.340 Õiguslike raamtingimuste järgimine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond
Rakendamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, organisatsiooni juht, ülemused

Infotöötluse puhul on tarvis järgida üksjagu seadustest või ka lepingutest tulenevaid raamtingimusi. Nimetatud tingimused võivad olenevalt institutsiooni liigist, tegevusvaldkonnast ja igapäevatöö protsessidest suuresti erineda.

Infotöötluse tüüpilised valdkonnad, mille puhul kohandatakse spetsiaalseid seadustest tulenevaid tingimusi, on näiteks järgmised:

- isikuandmete kaitse,
- krüptograafiliste protseduuride kasutamine,
- intellektuaalse omandi kaitse,
- IT-süsteemide nõuetekohane käitamine.

Olenevalt asukohamaast, kus parasjagu infot töödeldakse, ja info spetsiaalsest kasutusvaldkonnast võib kohalduda veel mitmeid muid seadusest tulenevaid eeskirju. Nende kõikide üleslugemine ajaks IT etalonturbe kataloogid lõplikult lõhki. Mõningates IT etalonturbe teemades on toodud näiteid erinevate riikide või eri tegevusvaldkondade seaduste kohta, mis puudutavad nt krüptograafiat, väljasttellimist või arhiveerimist. Kuna nimetatud näidete puhul võib kehtida palju täiendavaid seadustest tulenevaid raamtingimusi, tuleb arvestada, et näited ei suuda kajastada täielikku infot ning samuti võivad need olla juba aegunud. Infotöötlemist, IT-süsteemide ja sinna juurde kuuluva füüsilise infrastruktuuri turvalist käitamist kajastavad seadustest ja lepingutest tulenevad kohustuslikud eeskirjad tuleb välja selgitada ja dokumenteerida. Siinkohal tuleb jälgida, et seadustest tulenevad eeskirjad võivad riigi ja regiooni tasandil erineda. Seega tuleb iga asukoha puhul järgida neid seadusi, mis kehtivad selles konkreetses asukohas. Samuti on tarvis arvestada, et olenevalt IT-süsteemide kasutusotstarbest (bürookasutusest, protsessijuhtimisest) võivad samuti kehtida erinevad ettekirjutused. Eriti oluline on, et kõik rakendatavad IT kasutusmeetodid ja protseduurid, kõik installeeritud IT-süsteemid (riistvara ja tarkvara) ning kogu IT-süsteemide käitamiseks vajalik füüsiline infrastruktuur vastaksid seadustest tulenevatele eeskirjadele. Arvestada tuleb ka kõikide seadusemuudatustega ja institutsiooni jaoks olulised muudatused ellu viia.

Kontrollimine ja rakendamine

Seaduste järgimise puhul lasub vastutus institutsiooni kohapealsel juhtorganil ja seetõttu on ta kohustatud hoolitsema selle eest, et vajalikud seadused oleksid teada ning et nendest loodaks dokumentatsioon. Erinevate valdkondade puhul võib asjakohase vastutuse delegeerida ka mõnele vastutavale töötajale. Näiteks ettevõtte andmekaitsespetsialist peaks vastutama selle eest, et ettevõttes järgitaks seadustest tulenevaid andmekaitse-eeskirju, samuti peaks ta tegelema institutsioonis vajalike reeglite loomise ja järgimisega, mis puudutavad isikuandmetega

ümberkäimist. IT-juhatus peaks hoolitsema litsentsihalduse defineerimise ja selle dokumentatsiooni eest. Loomulikult vastutavad seadustest tulenevate eeskirjade järgimiseks kehtestatud reeglite rakendamise ja kontrollimise eest ka kõik töötajad ja eriti juhtivpersonal (vt M 3.2 Uute töötajate kohustamine eeskirju järgima).

Kontrollküsimused:

- Kas kõik seadustest tulenevad olulised kohustused on teada ja dokumenteeritud?
- Kas seadustest tulenevate eeskirjade järgmiseks on kindlaks määratud töötajate vastutusalad ja volitused?

M 2.341 SAP kasutuselevõtu planeerimine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator, IT-juht

Enne SAP süsteemi installeerimist ja kasutuselevõttu tuleb läbi viia laialulatuslikud planeerimistööd. Hoolikas planeerimine ei ole vajalik ainuüksi turbeaspektide jaoks. Ka protsessid ja protseduurid, mida SAP süsteemiga soovitakse automatiseerida ja toetada, tuleb täies ulatuses, korrektselt ja vajaminevates detailides läbi töötada. Ainult nii on võimalik tagada, et SAP süsteemi juurutamine osutub edukaks. Suurte süsteemide puhul tuleb planeerimisfaasi pikkust kalkuleerides arvestada, et isegi mitmekuuline tähtaeg ei pruugi olla piisav. Andmekaitse eest vastutav töötaja ja töötajate esindus tuleks antud protsessi kaasata juba kontseptsiooni loomise faasis. SAP süsteemidega töödeldakse reeglina alati ka isikutega seotud andmeid, nt HR-mooduliga või logimise raames (vt allpool). Teiselt poolt jällegi on neid tarvis kaasata seetõttu, et nad saaksid osaleda tööprotsesside muutmises. Iga SAP süsteemi planeerimisele tuleb läheneda individuaalselt, kuna iga SAP süsteemi kasutusvaldkond on erinev. Erinevate kasutusvaldkondade tõttu tuleks individuaalselt läheneda ka tootmissüsteemide (*production system*) alla liigitatavate testimis- ja vastuvõtusüsteemide ja arendussüsteemide planeerimisele. Siinkohal on tarvis jälgida, et muuhulgas arvestataks SAP süsteemide omavaheliste sõltuvussuhetega. Eriti kehtib see ühe kindla SAP süsteemi erinevate alamversioonide korral (arendus, testimine ja vastuvõtmine, tootmine), kuid ka erinevatest SAP süsteemidest moodustuva koosluse puhul. Seetõttu tuleb läbi viia üldine planeerimine, mis arvestaks individuaalsete süsteemide koostalitlusvõimega.

Planeerimisfaasi kontseptsioonid

Järgnevalt on toodud nimekiri SAP süsteemi turbealastest osakontseptsioonidest, mis tuleks koostada planeerimisfaasis ning mida tuleks pidevalt täiendada. Antud nimekiri ei ole täielik ning seda tuleb sobitada kohapealsete olude ja nõudmistega, kuid sõltumata olukorrast tuleb ilmtingimata luua järgmised SAP süsteemi turbealased osakontseptsioonid:

- Tehnilise konfiguratsiooni planeerimine
- Halduskontseptsioon
- Kasutajate haldamise kontseptsioon
- Volituste kontseptsioon
- Ressursside planeerimine
- SAP süsteemimaastiku planeerimine
- Auditeerimis- ja logimiskontseptsioon
- Muudatuste halduse kontseptsioon
- Varunduskontseptsioon
- Avariikontseptsioon

Üldjuhul tuleb kontseptsiooni loomise raames arvestada ametiasutuses või ettevõttes kehtivate turvakontseptsioonidega.

Tehnilise konfiguratsiooni planeerimine

Eelpool nimetatud kontseptsioonidele tuginedes tuleb planeerida tehniline teostus ehk SAP süsteemikonfiguratsiooni ellurakendamine (*customizing*). Selleks tu-

leb koostada projektipõhine rakendamisjuhis ehk IMG (*Implementation Guide*), millega kehtestatakse ABAP-pinus hädavajalikud tehnilised konfigureerimissammud. Vajalikud sammud soovitud konfiguratsiooni saavutamiseks valitakse reeglina välja SAP etalon-IMG alusel (vt M 4.258 SAPi ABAP-pinu turvaline konfiguratsioon). Iga üksiku Java-pinu jaoks ei eksisteeri eraldi IMG-mehhanismi, küll aga tuleb soovitud konfiguratsiooni saavutamiseks siiski planeerida ka vajalikud konfigureerimissammud (vt M 4.266 SAP Java protokollistiku turvaline konfigureerimine). Tehnilise konfiguratsiooni planeerimise käigus tuleb arvestada, et tarvis on luua ka mehhanismid, mis lubaksid protseduure ennistada, et reageerida juurutamise käigus aset leidnud muudatustele. Planeerimisfaasis võib vajalike tehniliste konfiguratsioonide määramiseks ja väljatöötamiseks kasutada SAP süsteemidokumentatsiooni. Selleks võib kasutada abiportaali *SAP Help Portal* help.sap.com. Pärast installeerimist saab tehnilise konfiguratsiooni vajadusel sobival moel ümber kohandada.

Halduskontseptsioon

SAP süsteemi hästi läbimõeldud halduskontseptsioon tõstab suurel määral selle turvalisust. Halduskontseptsioonis tuleb kindlaks määrata töötajate haldusalased ülesanded. Tehniline ellurakendamine peab suutma tagada, et iga töötaja saaks tegelda ainult nende tööülesannetega, milleks ta on kohustatud. Üldjuhtudel tuleks siinkohal arvestada järgnevalt toodud soovituste ja aspektidega. Kõikidel juhtudel tuleb luua ka kontseptsioon SAP süsteemi jaoks installeeritud pinude (*stacks*) nagu nt ABAP ja Java jaoks. Ilmtingimata tuleb vältida olukordi, kus mõni pinu on küll installeeritud, kuid selle halduskontseptsiooni ei ole loodud.

Haldusülesannetega seotud funktsioonide lahutamine

Suurte ettevõtete ja ametiasutuste puhul on soovitatav jagada haldamine mitme töötaja vahel, et erinevad funktsioonid teineteisest lahutada. Reeglina tuleks funktsioonide lahutamisel baashaldus ning rakenduste ja moodulite tasandi haldus teineteisest eraldada. Täiendavalt on soovitatav lahutada vähemalt kasutajahalduse administraatorite, õiguste haldamise, süsteemilogi haldamise ning varundus- ja muudatuste halduse funktsioonid. Sõltuvalt sellest, kui palju personaliressurssi on võimalik kasutada, võib funktsioonide lahutamisega ka jätkata nt kas üksikute liideste (nt RFC, ICF, SOAP) või teenuste (nt pakktöötluse) alusel. Kontseptsiooni planeerimisse tuleks kaasata ka tööprotsesside ja info eest vastutavad töötajad. Ainult niimoodi on võimalik tagada, et kontseptsioonis arvestatakse kõigi tööprotsessidest tingitud vajadustega. Töötajate haldusülesannete lahutamisel tuleks siiski ka arvestada, et ABAP-pinu ja Java-pinu jaoks pole loodud nii detailset aluskonfiguratsiooni, mis võimaldaks eelpool kirjeldatud üksikasjalikku lahutamist. Seega tuleb arvestada lauaulatuslike konfigureerimistöödega, mis võimaldaksid detailsemat lahutamist.

Funktsioonide lahutamine väikestes institutsioonides

Väikestes ettevõtetes ja ametiasutustes pole eelpool kirjeldatud funktsioonide lahutamine võimalik juba piisava personaliressursi puudumise tõttu, sest tihti töötab sellistes asutustes vaid üks administraator. Sellistel juhtudel tuleks siiski hoolikalt hinnata võimalikke tagajärgi seoses institutsiooni seest alguse saavate võimalike rünnetega või puudulike süsteemiteadmistega. Süsteemi turvalisuse tagamiseks võib sellistel juhtudel rakendada regulaarseid turvakontrolle, mis tellitakse väljast. Üldjuhul tuleb riskide minimeerimise otstarbel kindlaks määrata ka sisekontrollide läbiviimine. Siinkohal tuleb arvestada, et ka niisuguste kontrollide kehtestamine ja läbiviimine vajab haldamist. SAP süsteemi ABAP-pinu ei tohi administreerida kasutaja, kellel on SAP_ALL õigused. Selline administreerimis-

variant kätkeb endas paljusid turvariske. Kui baashaldusega tegeleb ainult üks administraator, võiks kaaluda järgmise lahenduse rakendamist:

- Haldamiseks kasutatava kontoga seotakse administreeritavad objektid profiili SAP_ALL alusel, luues vastava profiilikoopia.
- Profiilikoopiast kustutatakse kõik administreeritavad objektid, mida ei lähe tarvis baashalduses, st reeglina sellised õigused, mis on seotud kas rakenduste või moodulitega.

Seeläbi ei ole administraator saanud automaatselt kõiki rakendustega seotud õigusi. Isegi neil juhtudel, kus kasutatakse ainult ühe administraatori teeneid, on soovitatav halduskontseptsioonis kindlaks määrata, milliseid haldusülesandeid on administraatoril lubatud ja milliseid ülesandeid on tal keelatud täita. Ülejäänud administreeritavaid objekte tuleb käsitleda vastavalt vajadusele. Sellise lähenemise abil on võimalik nt tagada, et teatud haldusoperatsioone saab administraator läbi viia alles siis, kui eelnevalt on läbitud vastav loataotlemise protseduur. Halduskontseptsioonis tuleks kindlaks määrata ka avariiolukordade haldamiseks vajalikud protseduurireeglid ja tegutsemisjuhised.

Kasutajate halduskontseptsioon

Ühe ainsa SAP süsteemi haldamine

Kasutajate halduskontseptsiooni keerukus sõltub suurel määral sellest, kas korraga tuleb hallata ühte või mitut SAP süsteemi. Juhul kui hallata tuleb vaid ühte süsteemi, peaks kasutajate halduskontseptsiooniga leidma vastused järgmistele küsimustele:

- Millistest põhimõtetest lähtutakse kasutajanimede andmisel, tagamaks, et kasutajanimed oleksid üheselt mõistetavad?
- Millised on erinevate töötajate õigused seoses kasutajate haldamisega?
- Millistel otstarvetel rakendatakse erinevaid kasutajatüüpe?
- Kuidas toimub kasutajate jagamine erinevatesse kasutajarühmadesse?
- Kuidas kaitstakse privilegeeritud standardkasutajaid?
- Millised kasutajad kuuluvad kasutajarühma SUPER?
- Milliseid protsesse nähakse ette kasutajate haldamiseks (nt taotlemine, loa andmine, loomine, muutmine, kustutamine)?

Siinkohal tuleb silmas pidada, et kõigi halduseks vajalike tööde jaoks tuleb määratleda asjakohased protsessid (nt kasutajate loomine, töörollide muutmine või sidumine kasutajatega) ja need täies ulatuses kuni detailideni välja töötada. Lisaks tuleb kõikide protsesside puhul määratleda töötajate vastutusalad. Niimoodi välistatakse turvaaukude tekkimine, mis on tingitud vastutuse ebaselgest kehtestamisest või vajalike protsesside poolikust väljatöötamisest.

User Management Engine

Java-pinu puhul on küll võimalus rakendada erinevaid kasutajasalvesteid, kuid üldjuhul on soovitatav kasutada siiski UMEd (*User Management Engine*), kuna selle konfigureerimisvõimalused on kõige paindlikumad. Reeglina tuleks UME

konfigureerida selliselt, et sinna juurde kuuluvat ABAP-pinu rakendataks kasutajasalvestina. Niimoodi tagatakse, et Java- ja ABAP-pinu loovad ühesugused kasutajakontod ühesuguste nimedega ühesuguse kasutaja põhikirje (*user master record* -i) alusel.

Mitme SAP süsteemi haldamine

Kui korraga on tarvis hallata mitut SAP süsteemi, määrab suures osas kasutajate haldamisega seotud administratiivsete tööde mahu ja keerukuse selleks loodud kasutajahalduse kontseptsioon. Tuleb otsustada, kas rakendatakse detsentraliseeritud või tsentraliseeritud kasutajahaldust. Sellekohane otsus sõltub muuhulgas SAP süsteemi kasutusvaldkonnast ning kõikide sellega seotud süsteemidega kaasnevatest nõuetest.

Lisaks eelpool kirjeldatud aspektidele tuleb sellisel juhul kasutajate haldamise kontseptsioonis leida vastused järgnevatele küsimustele:

- Milliste süsteemide peal hallatakse milliseid kasutajakontosid (juhtiva süsteemi definitsioon)?
- Kuidas toimub kasutajakontode jaotamine erinevate süsteemide vahel?
- Millised süsteemid vajavad või nõuavad eraldi kasutajahaldust?

Tsentraliseeritud kasutajahaldus

Tsentraliseeritud kasutajahalduse rakendamine on mõistlik neil juhtudel, kus on tegemist võimalikult homogeenset liiki kasutajatega (nt ametiasutuse või ettevõtte siseringi kasutajatega), kellel on juurdepääs erinevatele SAP süsteemidele. Siinjuures on oluline, et erinevate juurdepääsuvariantide turbenõuetes ei tohiks olla liiga suuri erinevusi. Juhul kui kasutajate kooslus ei ole homogeenne (nt kui tegemist on ametiasutuse- või ettevõtte siseringi kasutajatega, partnerettevõtete kasutajatega, ametiasutuse või ettevõttega kaudselt seotud kasutajatega), oleks erinevate kasutusvaldkondade alla liigituvate kasutajate tarbeks mõistlik luua erinevad haldussaared (st vajalik arv tsentraliseeritud kasutajahaldusega süsteeme). Langetades otsust tsentraliseeritud kasutajahalduse kasuks või kahjuks, tuleb kindlasti arvestada ka tehniliste raamtingimustega. Näiteks kui SAP süsteemi puhul soovitakse rakendada tsentraliseeritud kasutajahaldust ehk CUAd (*Central User Administration*), eeldab see toimiva ALE-maastiku olemasolu (vt M 5.128 SAP ALE (IDoc/BAPI) liidese kaitse). Sellisel juhul on kasutajatele õiguste andmist võimalik hallata ka tsentraliseeritult ning neid on võimalik üle kanda ka teistesse SAP süsteemidesse (vt M 4.259 ABAP-pinu turvaline kasutajate haldus ja M 4.267 SAP Java pinu turvaline kasutajate haldus .

SAP infoallikad

Täiendavat infot SAP süsteemide kasutajahalduse täiendavate dokumentatsioonide kohta leiate M 2.346 SAP dokumentatsiooni kasutamine .

Volituste kontseptsioon

Õiguste kontseptsioonid määravad kindlaks funktsioonide ja andmete juurdepääsud. Seetõttu on õiguste kontseptsioonil suur tähtsus SAP süsteemide juurdepääsude ja andmete turvalisuse tagamisel. Sel põhjusel peab õiguste kontseptsiooni väljatöötamisele eelnema hoolikas, vajadustest lähtuv planeerimistöö (vt M 2.342 SAP pääsuõiguste planeerimine).

Ressursside planeerimine

SAP süsteem suudab ametiasutuse või ettevõtte tööd optimaalselt toetada ainult sellisel juhul, kui olemasolevad arvutiressursid on kooskõlas kasutusvaldkonna ja selleks vajaliku SAP tarkvaraga ja nende poolt ressurssidele esitatavate nõuetega. Ressursse kajastavas plaanis tuleb seetõttu täpselt paika panna vajaminev riistvara. Olulised teemad on muuhulgas:

- Vajaminevate arvutite arv
- Arvutite CPUd ja salvestid
- Vajaminev kõvaketaste maht
- Võrgu jaoks vajalik ribalaius
- Vajalikud võrgusegmendid ja võrguühenduse elemendid.

SAP infoallikad

Infot ressursside planeerimiseks vajaliku SAP dokumentatsiooni kohata leiate meetmest M 2.346 SAP dokumentatsiooni kasutamine .

SAP süsteemimaastiku planeerimine

SAP süsteem koosneb alati mitmetest erineva ülesandega komponentidest, mis kasutavad omavaheliseks sideks võrgu infrastruktuuri. SAP süsteemi turvalisust saab positiivselt mõjutada juba ainuüksi süsteemimaastiku arhitektuuri valimisega. Sama kehtib ka vastupidi, st ebapiisavalt planeeritud ja ülesehitatud süsteemimaastik võib viia turvaprobleemide tekkimiseni. Kuna turbe seisukohast soodne süsteemimaastik sõltub suurel määral SAP süsteemi kasutusvaldkonnast ja salvestatavate andmete kaitsevajadusest, on IT-etalonturbe moodulis võimalik esitada ainult sellekohaseid üldsoovitusi. Reeglina pakub siiski ka SAP soovitusi, kuidas erinevate kasutusvaldkondade jaoks soodsat süsteemi üles ehitada. Üldjuhul tuleks kasutus planeerida selliselt, et komponentide vahel toimiksid ainult sellised juurdepääsud, mis on ilmtingimata vajalikud. Eriti oluline on teineteisest lahutada tootmissüsteem, testimis- ja vastuvõtusüsteem ning arendussüsteem. Vastava planeerimistööga tuleb tagada, et SAP süsteemi tootmisandmeid ei oleks võimalik salvestada muutmata kujul testimis-, vastuvõtu- või arendussüsteemidesse ja neid seal muutmata kujul kasutada. Kui seda pole võimalik tagada, tuleb testimis- ja vastuvõtusüsteeme kaitsta selliselt, et säiliks nendes süsteemides kasutatavate andmete konfidentsiaalsus. Süsteemimaastiku kujundamisel tuleb muuhulgas leida vastused järgnevatele küsimustele:

- Millistele arvutitele tuleb installeerida vajaminevad komponendid?
- Kus asuvad võrgutehnilisest vaatevinklist vaadatuna üksikud arvutid ja komponendid?
- Milliseid komponente on tarvis kaitsta (sisemiste, välimiste) juurdepääsude eest vastavate tulemüüride või marsruuteritega?
- Millistele komponentidele on (sisemistel, välimistel) kasutajatel tarvis otse ligi pääseda? (Sellest vajadusest tingituna ei ole vastavaid komponente võimalik täies ulatuses kaitsta tulemüüride või marsruuteritega).

- Millised komponendid tuleb paigutada oma juurdepääsu eripära tõttu demilitariseeritud tsooni?
- Milliste vahenditega on võimalik tagada kogu SAP süsteemi käideldavust?

SAP infoallikad

Täiendavaid juhiseid spetsiaalsete kasutusvaldkondade kohta leiate meetmetest M 2.343 SAP süsteemi portaalilahenduse kaitse ja M 2.344 Interneti SAP süsteemide turvaline kasutamine .

Auditeerimis- ja logimiskontseptsioon

Auditeerimis- ja logimiskontseptsioon peab kindlaks määrama, millised SAP süsteemi tegevused ja millised kasutajate tegevused peaksid kajastuma logis. Lisaks tuleb siinkohal arvestada järgnevate aspektidega:

- Kellel on õigus muuta auditeerimise ja logimise seadistusi?
- Kuhu kohta salvestatakse logifailid?
- Kellel on juurdepääs koostatud logifailidele?
- Kuidas kontrollitakse koostatud logifaile?
- Kes, millises mahus ning milliste ajavahemike tagant viib läbi turvakontrollid (auditid)?

SAP süsteem pakub laialdasi võimalusi sisemiste sündmuste ja kasutajate tegevuse logimiseks (vt M 4.270 SAP logimine). Lisaks süsteemiseire tagamisele, mida logimisega soovitakse saavutada, tuleb SAP süsteemi turvalisust regulaarselt kontrollida ka vastavate auditite käigus. Sellekohaseid auditeid võivad läbi viia nii administraatorid (enesekontrolliks) kui ka muud kontrollijad. Kontrollijad võivad olla valitud teistest osakondadest (IT-turvaosakonnast, kontrolliosakonnast) või ka väljastpoolt (IT-audiitorite, audiitorite, järelvalveorganisatsioonide hulgast) (vt M 2.347 SAP süsteemi regulaarsed turvakontrollid). Siinkohal tuleb arvestada, et SAP süsteemi turvalisuse adekvaatseks hindamiseks ei piisa ainult audiitorite endi poolt läbiviidud kontrollidest.

Muudatuste halduse kontseptsioon

SAP süsteemi turvalisuse tagamiseks on oluline seda regulaarselt värskendada paikade, kuumparanduste ja täienditega. Programmeerimisel tehtud vigu on võimalik kõrvaldada ainult süsteemi regulaarse värskendamise teel. Kuna muudatuste haldamise protsessid on ABAP- ja Java-pinu puhul suurte tehniliste erinevustega, tuleb koostada kaks eraldi kontseptsiooni. Kontseptsioonide koostamisel tuleb leida vastused järgmistele küsimustele:

- Millise protsessi alusel toimub süsteemi värskendamine süsteemivariantides arendus, testimine ja vastuvõtmine, tootmine?
- Kuidas tagatakse, et installeeritavad värskendused ei mõjutaks negatiivselt igapäevast kasutust?
- Milliste ajavahemike tagant leiab aset värskendamine?
- Kelle on õigus viia läbi värskendusi tootmissüsteemis?

- Milliste muudatuste halduse protsesside puhul tuleb läbi viia kontrolliprotseduurid?
- Kuidas tagatakse, et värskendamise õigust ei antaks vaid ühele isikule?
- Kuidas tuleks piirata juurdepääsu värskendamiseks vajalikele funktsioonidele ja tööriistadele?
- Kuidas toimub muudatuste logimine, et vastavad tegevused oleksid jälgitavad?

Transportsüsteem

ABAP-pinu muudatused viiakse sisse nn transportsüsteemi abil. Selleks võib ka mitu SAP süsteemi liita üheks transpordiühenduseks (transportimisdomeeniks). Muudatuste haldamise kontseptsiooni väljatöötamisel tuleb seega koostada ka vastav transportimiskontseptsioon. Selleks tuleb muuhulgas selgitada välja järgnevad asjaolud ning leida vastused järgnevatele küsimustele:

- Kellel on õigus algatada transportimine?
- Transportimisloa saamise protseduur peab olema sõnastatud võimalikult selgelt, st kindlaks peavad olema määratud kvaliteedieesmärgid, millest tuleb enne uute paikade transportimist täpselt kinni pidada.
- Kellel on õigus transporditud sisu paigaldada?
- Kuidas leiab aset transport ühest süsteemist teise?
- Millistel põhimõtetel tuleks defineerida protsesside järjekord, et selles osaleksid erinevad isikud, mis võimaldaks rakendada vajalikke kontrollietappe?
- Arendajate poolt läbiviidav otsene transportimine arendussüsteemidest testimis- ja vastuvõtusüsteemidesse või tootmissüsteemidesse peavad olema välistatud.
- Millisel määral on vajalik tagada transporditavate failide terviklust?
- Kuidas tuleks kindlustada jälgitavus? (Küsimus: kes, kunas ja mida tegi?)
- Transportimismaastiku puhul on tarvis planeerida: Millised instantsid ja usaldusisikud on asjasse segatud? Millisest allikast millisesse sihtkohta tohib transportida?

Täiendavat infot ja teemakohaseid soovitusi leiate meetmetest M 2.221 Muudatuste haldus , M 4.272 SAP transportsüsteemi turvaline kasutamine ja M 4.273 SAP Java protokollistiku tarkvara levitamise turvaline kasutamine .

Varunduskontseptsioon

SAP süsteemi varunduskontseptsiooni puhul ei eksisteeri ühtki erinõuet. Varunduskontseptsioonis tuleb muuhulgas leida vastused järgnevatele küsimustele:

- Millal leiab aset erinevate komponentide ja andmete varundamine?
- Kellele antakse sellekohased volitused?
- Kellele antakse volitused andmete taastamiseks?
- Kellel on juurdepääs arhiveeritud varundatud andmetele?
- Kus toimub varundatud andmete turvaline hoiustamine? Siinkohal tuleb pöörata erilist tähelepanu sellele, et varundatud andmed peavad olema tootmisandmetest ruumiliselt eraldatud.

Kindlaks tuleb määrata vastused ja protseduurid ning need ellu rakendada. Erandlike protseduuride vältimiseks tuleks SAP varunduskontseptsioon integreerida olemasoleva varundusprotseduuri alla. Hästitoimiv varunduskontseptsioon on eriti oluline hädaolukorraks valmisoleku puhul (vt M 6.97 SAP süsteemi valmisolek hädaolukorraks).

Avariikontseptsioon

SAP süsteemide avariikontseptsioon peab sõnastama igapäevatööd ohustavad hädajuhtumid ja sinna juurde kuuluvad avariiprotseduurid. Siinkohal tuleb arvestada vähemalt järgnevate avariiolukordadega:

- SAP serveri avarii
- SAP süsteemi andmebaasi avarii
- SAP süsteemi kompromiteerimine
- Transportimissüsteemi (ABAP) avarii või tarkvara jagamise (Java) avarii
- Terve arvutuskeskuse avarii

Üheselt on tarvis kindlaks määrata avariiolukordades kehtivad volitused (vt M 6.97 SAP süsteemi valmisolek hädaolukorraks) ning avariiprotseduuride läbiviimine tuleb siduda konkreetsete isikutega. Soovitatavalt tuleks regulaarselt läbi viia avariiõppusi ja nende käigus saadud kogemused protsessidesse sisse töötada.

Täiendavad kontrollküsimused:

- Kas SAP kasutust on piisavalt planeeritud?
- Kas kõik kasutusvaldkonnad on teada ja läbi töötatud?
- Kas SAP jaoks koostatud turvalisuse osakontseptsioonid on kooskõlas olemasolevate turvakontseptsioonidega?
- Kas planeerimistöödesse kaasati ka töötajate esindus, andmekaitsespetsialist ja IT-turbespetsialist?
- Kas tootmissüsteemid on arendus-, testimis- ja vastuvõtusüsteemidest isoleeritud?
- Kas on planeeritud viia regulaarselt läbi avariiõppusi?

M 2.342 SAP pääsuõiguste planeerimine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator, IT-juht

Tähtsamate mõistete selgitus

SAP süsteemi õigustega juhitakse kasutajate pääsuõigusi. Tööandmete turvalisus sõltub seetõttu suurel määral otseselt sellest, kuidas on tehtud erinevate õiguste seadistused. Soovitud turbe tagamiseks on sel põhjusel tarvis õiguste andmist hoolikalt planeerida ja ellu rakendada.

Volitused

SAP süsteemi funktsioonid (nt programmid või raportid, üldistatult kogu SAP süsteemide rakendused) käivitatakse erinevate tehingute (*transactions*) abil, mis võimaldavad andmetega läbi viia erinevaid operatsioone või tegevusi (nt kirjutada, lugeda, kustutada). Tehingute vahendusel käivitatud rakendused kontrollivad enne käivitumist, kas vastaval kasutajal on olemas asjakohased volitused, mis lubavad tal nimetatud rakenduse abil andmetega vastavat operatsiooni läbi viia.

Volitusobjektid

Kontrollimehhanism on üles ehitatud nn volitusobjektidele, mis on varustatud volitusväljadega. Konkreetse volituse all võib seega mõista teatud volitusobjekti, mille volitusväljadesse on tehtud vastavad sissekanded. Tehingu käivitamisel kontrollib SAP tuum algul, kas kasutaja on üleüldse volitatud vastavat tehingut käivitama. Pärast käivitamist võib vastav tehing läbi viia ka veel täiendavaid volituste kontrollimisi. Kontrollimisel selgitatakse, kas kasutajal on õigused, mis on tuletatud vajaminevast volitusobjektist. Kui see on nii, kontrollitakse järgnevalt volitusvälju, et teha kindlaks, kas need sisaldavad vajaminevaid väärtusi või väärtuste kombinatsioone. Siinjuures võib tehing kontrollida ka mitut volitust. Kontrollitavad volitused määratakse kindlaks programmikoodiga. Tehingu käivitamisel kontrollib SAP tuum iga kord volitusobjekti S_TCODE. Rakenduste käivitamisel kontrollitakse volitusobjekti S_PROGRAM. Reaalse kontrolli viib seega alati läbi SAP tuum ning seda ka siis, kui kontrolli algatab kas programmikood või tehing.

Organisatsiooni allüksused

Rakenduste vaatevinklist on eelkõige olulised selliste volitusobjektide volitusväljad, mis on tarvis luua organisatsiooni allüksuste baasil. Sellistel juhtudel volitavad nad läbi viima kas mõnda tööülesannet või tehingut teatud valdkonnas, milleks võib olla nt raamatupidamine (ettevõtetes on siinkohal tihti tegu äritegevuse juurde kuuluva üksusega, nt tütarettevõtte raamatupidamise allüksusega).

Töörollide ja profiilide loomine

Kasutajatele volituste andmisel liigitatakse kasutajad erinevate nn töörollide vahel. Rollidega määratakse kindlaks erinevad tehingud, mida teatud rollide alla kuuluvatel kasutajatel on lubatud käivitada. Kuna iga tehingu puhul leiab aset teatud, programmikoodi poolt kindlaksmääratud volitusobjektide kontrollimine, võib iga rolli jaoks tuletada oma profiili (st volituste kogumi), mis sisaldab kõiki volitusobjekte, mida võib tehingu puhul enamasti vaja minna. Protsess, mille käigus toimub rolli õigusteprofiili ja selles sisalduvate tehingute loomine, leiab aset automatiseeritud kujul profiiligeneraatori (Transaction PFCG) vahendusel.

Tehingute kontrollmärgistus

Tehingute kontrollmärgistuse abil on võimalik juhtida seda, milliste volitusobjektide puhul, mida tehing kontrollib, viib SAP tuum läbi reaalse kontrolli. Kontrollmärgistuse abil on seega võimalik määrata volitusobjektid, mis jäetakse teatud tehingu käivitamisel kontrollimata. Sellistel juhtudel jääb loodud õiguste profiilis

ära ka volituse andmine profiili generaatori poolt. Kontrollmärgistustega tegeleb tehing SU24, st siin koostatakse ka volitusobjektidele üksikute volitusväljade väärtused, mille profiili generaator kannab profiilide jaoks loodud volitustesse. Tegu on soovituslike väärtustega. Profiili generaatori poolt loodavad profiilid tuleb sõltuvalt olukorrast vahel ka veel käsitsi üle töötada.

Volituste andmise planeerimise erinevad tööetapid

Rollide defineerimine

SAP süsteemi volituste andmine on mitmeastmeline protsess. Esmalt tuleb kindlaks määrata vajaminevad töörollid. Rollide määramise puhul on oluline, et need kajastaksid lõpuks ka reaalselt ettevõttes või ametiasutuses leiduvaid töökohti või ametikohti. Samas tuleks arvestada, et rollide jaotamist ei ole tarvis teha eraldi kõikide töötajate kohta, sest vastasel korral läheks rollide arvukus liiga suureks ja kaoks vajalik ülevaatlikkus. Õiguste kontseptsioon toimib või ei toimi vastavalt sellele, kui hästi on rollid algselt defineeritud, ning sellele, kui hästi ja detailselt on rollid välja töötatud.

Volituste profiilide loomine

Pärast seda, kui rollid on välja töötatud, on tarvis neile profiili generaatoriga luua vastavad volituste profiilid. Rolliprofiilides loodavate volituste ulatust mõjutab kontrollmärgistuste konfiguratsioon. Ka seda on tarvis hoolikalt planeerida, kuna kontrollide väljalülitamine tähendab alati ka teatud määral turbe langust. Loodud profiilid ja neile antud volitused tuleb üle kontrollida ja neid vajadusel kohandada.

Rollide sidumine kasutajatega

Volitused seotakse kasutajatega seeläbi, et kasutajate puhul määratakse kindlaks, milliste rollide alla nad liigituvad ning seejärel käivitatakse nn kasutajavõrdlus. Selle protsessiga salvestatakse rolliga seotud volituste profiilis kajastuvad volitused kasutaja põhikirjesse (*user master record* -isse).

Volituste kontseptsioon

SAP süsteemi volituste kontseptsiooni puhul on tarvis luua kaks verisooni: üks ABAP-pinu ja teine Java-pinu jaoks. Siinkohal tuleb arvestada, et Java-pinu volituste süsteem ja ABAP-pinu volituste süsteem on kardinaalselt erinevad. Sellele vaatamata tuleb kontseptsiooni loomisel läbi töötada ühesugused küsimused. Olulised teemad on siinkohal:

- Milliseid rolle on tarvis?
- Millistel rollidel lubatakse käivitada erinevaid SAP süsteemi funktsioone (nt algatada tehinguid, käivitada programme või koostada raporteid)?
- Millistel rollidel on õigus ligi pääseda erinevatele SAP süsteemi andmetele?
- Milliseid erinevate volitustega administratiivseid rolle läheb tarvis planeeritava halduskontseptsiooni ellurakendamiseks?
- Kas rakendused kasutavad lisaks SAP standardsele volitustesüsteemile veel ka teisi volitusi? Vastavate volitustega tuleb kontseptsioonis eraldi arvestada ning nende kasutus tuleb planeerida.
- Millised õiguste haldamiseks vajalikud protsessid (nt taotlemine, loa andmine, loomine, muutmine, kustutamine) tuleb defineerida koos kaasnevate vastutusaladega?

- Kas volituste kontseptsioonis on arvestatud piisavalt tööfunktsioonide lahutamise põhimõtetega? Siinkohal mängib eriti tähtsat rolli ka seadustest tulenevate ettekirjutuste järgimine.
- Kas muudatuste haldamise puhul on arvestatud ka potentsiaalsete riskidega, mis võivad kaasneda liiga laialdaste volituste andmisega?

Tuleb arvestada, et kõikide tegevuste jaoks, mis on seotud õiguste valdkonnaga, tuleb defineerida vastavad protsessid ja need omakorda detailselt välja töötada. Lisaks tuleb kõikide protsesside puhul määratleda töötajate vastutusalad. Niimoodi välistatakse turvaaukude tekkimine, mis on tingitud vastutuse ebaselgest kehtestamisest või vajalike protsesside poolikust väljatöötamisest.

Volituste planeerimise raamtingimused

Rollide ja nendega seotud volituste defineerimine peab ühelt poolt lähtuma institutsiooni vajadustest, kuid teiselt poolt tuleb siia kaasata ka sellised tingimused, mis on kehtestatud erinevate seadustega, mis võivad käsitleda teemasid nagu nt ettevõtluse kontroll ja läbipaistvus , andmetöötlusel põhinevaid raamatupidamissüsteeme või riiklikku andmekaitseseadust . Seetõttu on ilmtingimata vajalik läbi viia põhjalik planeerimistöö. Mida detailsemalt on teada erinevatele rollidele esitatavad nõuded, seda paremini on hiljem võimalik neile jagada volitusi. Siinkohal tuleb arvestada ka rollide vajaliku lahutamisega. Rollid ja seega ka volitused on soovitatav välja töötada vastavalt organisatsiooni sees kehtivale hierarhiale ning selles leiduvatele tasanditele ja ametikohtadele. Niimoodi on nt võimalik tagada, et kui töötaja vahetab organisatsiooni sees tegevusvaldkonda, pole tal enam võimalik kasutada oma seni kehtinud volitusi.

Vastutavate instantside kaasamine

Muuhulgas on oluline, et ettevõtte või ametiasutuse sees nimetataks ametitesse töötajad, kes peavad vastutama informatsiooni ja protsesside eest (andmete omanikud või protseduuride eest vastutavad töötajad), kes vastutavad organisatsiooni teatud kindlate andmete eest. Näiteks finantsidega tegeleva osakonna juhataja (ingl *Chief Financial Officer, CFO*) peaks vastutama finantside ja nende järelvalve eest. Kõikide valdkondade vastutavad töötajad tuleb ilmtingimata kaasata vajaminevate rollide, volituste ja protsesside planeerimisse, sest ainult neil on olemas vajaminev erialane kompetents. Administraatorid ei ole reeglina võimelised rolle ja volitusi rakenduste tasandil üksi planeerima. Volituste planeerimise käigus tuleb leida vastused järgnevatele küsimustele:

- Millised volitused liigituvad kriitiliste õiguste alla (st lubavad teostada SAP süsteemi kriitilise tähtsusega operatsioone, mis on seotud kas administratiivsete, õiguslike või majanduslike aspektidega)?
- Millistele töörollidele tohib anda kriitilise tähtsusega volitusi, profiile või rolle?
- Millistele töörollidele tohib anda kriitilise tähtsusega volitusväljade erinevaid väärtusi?

Täiendavaid juhiseid kriitilise tähtsusega volituste väljatöötamise kohta leiate M 4.261 Kriitiliste SAP volituste turvaline rakendamine .

ABAP-pinu

ABAP-pinu ja Java-pinu jaoks loodavad kontseptsioonide detailid on väga erinevad. ABAP-pinu puhul peab volituse haldamine toimuma mitte käsitsi, vaid profiili

generaatori abil. Üldjuhul on soovitatav käsitsi haldamisest kindlasti loobuda, kuna selle tagajärjel tekivad tihti õiguste väärkonfiguratsioonid. Profiili generaatori abil kindlustatakse, et kasutajad saavad ainult sellised volitused, mis on vajalikud rollijaotusel põhinevate tehingute läbiviimiseks. Seetõttu on eriti oluline, et kontseptsioonid, protsessid ja toimingud oleksid kooskõlas profiili generaatori kasutamisega.

JAVA-pinu

JAVA-pinus seevastu ei ole valikuvõimalusi, kuna kasutada tuleb Java 2 Enterprise Edition (J2EE) spetsifikatsiooni volituste mehhanismi. Siinkohal tuleb arvestada, et antud standardi võimalusi aitab täiendada *User Management Engine* (UME) (vt M 4.260 SAP-volituste haldus , M 4.262 SAP-volituste lisakontrollide konfigureerimine ja M 4.268 SAPi Java pinu pääsuõiguste turvaline konfiguratsioon).

SAP infoallikad

Täiendavat infot SAP dokumentatsioonide kohta, mida on võimalik kasutada volituste kontseptsioonide koostamisel, leiate M 2.346 SAP dokumentatsiooni kasutamine .

Volituste haldamise planeerimine

Volituste haldamine eeldab planeerimistööd, mille käigus töötatakse välja soovitud halduskontseptsioon. Peamiselt tuleb nende tööde käigus arvestada sellega, millised on erinevate töötajate tööülesanded seoses volituste haldamisega. Siinkohal on soovitatav teemale läheneda rollide baasil (vt M 4.260 SAP-volituste haldus *)* , et loodud rolle oleks hiljem võimalik siduda konkreetsete kasutajatega ja seega ka isikutega. Tööde käigus tuleks jälgida, et ühele ja samale isikule ei antaks kokkusobimatuid rolle (tuleb arvestada tööülesannete lahutamisega). Kuna organisatsioonis on volituste haldamiseks tihti võetud kasutusele juba terve rida erinevaid rolle, tuleb süsteem nende põhjal sobival moel üles ehitada. Näiteks ei eksisteeri reeglina mitte paljusid üksikuid rolle nimega administraator, vaid pigem on siiski tegu rollidega nagu kasutajate administraatorid, rollide administraatorid, volituste administraatorid, arendajad, *Help-Desk* -töötajad või transpordikorraldajad. Seetõttu ei ole SAP poolt algselt defineeritud rolle reeglina võimalik otse üle võtta ning neid tuleb mugandada.

Täiendavad kontrollküsimused:

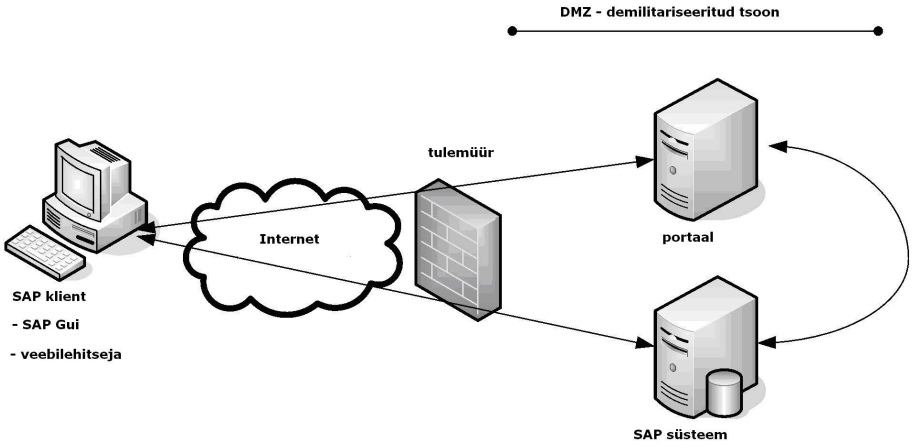
- Kas rollid ja volitused on planeeritud adekvaatselt?
- Kas planeerimise käigus arvestati rakenduste eripäradega kaasnevaid volitusi ja volitusmehhanisme?
- Kas planeerimistöödesse kaasati ka tööprotsesside eest vastutavad töötajad?
- Kas kõikide protsesside jaoks on planeeritud ka volituste haldamine ning kas sellega seoses on kindlaks määratud kõik vastutusalad?

M 2.343 SAP süsteemi portaalilahenduse kaitse

Algatamise eest vastutavad: IT-juht, IT-turvaosakond, arendusosakonna juht

Rakendamise eest vastutavad: administraator, arendaja

SAP süsteeme rakendatakse üha enam ka portaalilahendustes. Järgneva näite puhul on lähtutud olukorrast, kus on tegemist organisatsioonisisese ametkonna- või ettevõtteportaaliga, mille juurdepääs on lahendatud SAP süsteemi baasil. Käesolev meede ei käsitle mitte ametkonna- või ettevõtteportaali turvalisust, vaid SAP süsteemi turvalisust portaali keskkonnas. Internetis rakendatavate SAP süsteemide kohta leiate täiendavat infot M 2.344 Interneti SAP süsteemide turvaline kasutamine . Portaalilahenduste juurdepääs toimib reeglina HTTP vahendusel ning kasutajatel tuleb selleks rakendada brauserit.



Joonis: Portaalilahenduse SAP süsteem

Portaalilahenduse puhul tehakse tihti valesid oletusi nagu kasutaks portaal juurdepääsu SAP süsteemile, mis on portaalile „järgi ühendatud“. Kasutajate otsene juurdepääs SAP süsteemile poleks sellisel juhul ilmtingimata vajalik. Reeglina leiab portaalis aset siiski vaid ümbersuunamine SAP süsteemi, mille tagajärjel liiguvad kasutajate päringud seega otse SAP süsteemi. Antud tõsiasi on tihti arusaadav isegi kasutaja jaoks, kuna brauseris avatud portaalileheküljel kuvatavad andmed asuvad raami sees. Seetõttu tuleb ka portaalilahenduste puhul rakendada meedet M 2.344 Interneti SAP süsteemide turvaline kasutamine .

Üldised aspektid

Üldjuhul on SAP süsteemide portaalilahenduste puhul olulised järgmised põhiaspektid:

- Võrgu ja süsteemi ülesehituse arhitektuur (vt M 2.341 SAP kasutuselevõtu planeerimine).
- Kommunikatsiooni turvamine (vt M 5.125 SAP-süsteemi siseneva ja väljuva kommunikatsiooni kaitse).
- Rakenduste turve internetikasutuses.
- Rünnete tuvastamine (*Intrusion Detection* süsteemid).
- Failide kaitsmine viiruste eest üles- ja allalaadimisel (vt M 4.271 SAP süsteemi viirusetõrje).

Eriti hoolikalt tuleb siinkohal käsitleda järgnevaid, otseselt portaalilahendusega kaasnevaid aspekte:

Süsteemijuurdepääsu piiramine

Kõik SAP süsteemid, mida kasutatakse brauserite ümbersuunamise abil, peavad olema kasutajatele ligipääsetavad. Antud faktiga tuleb arvestada riskide hindamisel ning see mõjutab SAP süsteemi asukoha valikut võrgus, kuna see tuleb paigutada näiteks demilitariseeritud tsooni. Kõnealuste SAP süsteemide juurdepääse tuleb piirata tulemüüriga, võimaldades juurdepääse ainult läbi selliste portide, mis kasutavad kas HTTPd või HTTPSi. Sõltuvalt konkreetsest lahendusest tuleks SAP süsteemi juurdepääs vajadusel suunata läbi *Reverse Proxy*, et välistada otsene juurdepääs SAP süsteemile.

Dialoogipääsu piiramine

Reeglina tuleks portaalilahenduse abil kasutatavate SAP süsteemide SAPGui-juurdepääse lubada ainult piirangutega. Eriti oluline on SAPGui-juurdepääsu keelamine sellistele kasutajatele, kelle juurdepääsud leiavad aset ainult portaali ja brauseri vahendusel. Juhul kui port-juurdepääs ei ole tulemüüriga piiratud, võib siinkohal rakendada nt kasutajate tüüpi „Internetikasutajad“. Tuleb arvestada, et SAPGui-juurdepääsu peab olema võimalik kasutada administraatoritel ning selleks tuleb teha tulemüürile vastav konfiguratsioon. Alternatiivse lahendusena võib kasutada ka eraldi administreerimisvõrku.

Internet Transaction Server (ITS)

Juhul kui SAP süsteemide juurdepääsuks ei kasutata Internet Transaction Server-it (ITS-i), tuleks ITS juurdepääs desaktiveerida, kuna selle poolt pakutav juurdepääsulahendus sarnaneb SAPGui-juurdepääsule. Kasutades SAP Web Application Server-i versiooni, mis on vanem kui versioon 6.40, tuleb ITS installeerida eraldi komponendina (WGate, AGate). Sellistel juhtudel tuleks need komponendid jätta kas installeerimata või deinstalleerida. ITS on integreeritud alates versioonist 6.40, seega tuleb vastavad teenused ABAP-pinus (nt *webgui*) ja Javapinus (nt *mi* või *me*) desaktiveerida. ABAP-pinus toimub see seeläbi, et desaktiveeritakse ICF-teenus „webgui“ (vt M 5.127 SAP Internet Connection Framework (ICF) kaitse). Java-pinus (vt M 4.266 SAP Java protokollistiku turvaline konfigureerimine) tuleb rakendused „mi“ ja „me“ desaktiveerida *Deploy* -teenusega.

Autentimine/ *Single Sign-On*

Reeglina on portaali ja SAP süsteemi vahelise pääsu konfiguratsioonina kasutusel *Single Sign-On* . Seetõttu on vajalik tagada, et samade nimedega kontod oleksid mõlemas süsteemis seotud ühe ja sama isikuga. Kui seda pole võimalik tagada, tuleb rakendada portaali nn *User-Mapping* -mehhanismi. SAP süsteemi juurdepääsu loomisel kasutatakse sellisel juhul salvestatud kontoinfot. Vastava lahenduse puhul tuleb pidevalt jälgida, et *User-Mapping* -info oleks kogu aeg värske.

Volitused

Portaalilahenduste puhul võib juhtuda, et portaalikeskkonnas töötavad rakendused (*frontend* -rakendused), loovad ise otsese juurdepääsu SAP süsteemiga. Sõltuvalt rakenduse disainist kasutatakse juurdepääsu loomiseks kas mõnda tehnilist kontot või sisseloginud kasutaja kontot. Sellisel kontol tohib lubada SAP süsteemis kasutada ainult selliseid ABAP-funktsioonigruppe, mis on vajalikud portaalilahenduse toimimiseks. Peamiselt tuleb jälgida seda, et SAP süsteemis hoitavate kasutajate volitused oleksid võimalikult minimaalsed. Planeerimistöödel tuleks lähtuda sellest, et *frontend* -rakenduste volituste kontroll võib teatud tingimustel ka mitte toimida. Juhul kui kasutaja suunatakse portaali poolt ainult ümber, tekib tal otsene juurdepääs SAP süsteemile. Seetõttu tuleks SAP süsteemide volitused sisse seada alati selliselt, et käivitada oleks võimalik ainult selliseid funktsioone,

mida võimaldavad portaalirakendused. Eriti oluline on see neil juhtudel, kus ei ole võimalik välistada portaalikasutajate dialoog-juurdepääse.

Rakenduste seansside haldus

Kõikide ABAP- ja Java-pinu rakenduste puhul, mida kasutatakse läbi portaali, tuleks juurutada turvaline seansihaldus. Rakendused tuleb programmeerida selliselt, et pärast kasutaja väljalogimist muutuks tema seansiinfo ilmtingimata kehtetuks. Tuleb arvestada, et portaalist väljalogimisega ei kaasne automaatselt SAP süsteemist väljalogimine. Selline olukord kujutab endast probleemi neil juhtudel, kus klient-arvutit kasutab mitu erinevat isikut, kuna igal järgneval kasutajal võib tekkida sõltuvalt olukorrast võimalus pääseda ligi eelmise kasutaja andmetele SAP süsteemis.

SAP infoallikad

Automaatse väljalogimise korraldamiseks võimaldab SAP süsteem kasutada programmeerimisraamistikke (nt Business Server Pages, BSP). Sellega tuleks arvestada isiklike arenduste puhul, kui otsustatakse, millist tehnoloogia ehk raamistik tuleks juurutada.

Täiendavad kontrollküsimused:

- Kas SAP süsteemi kohta on läbi viidud riskide hindamine, mis põhineb reaalsetel SAP süsteemi juurdepääsudele esitatud nõudmistel?
- Kas juurdepääs süsteemile on piiratud hädavajaliku miinimumini?
- Kas dialoog-juurdepääsude kasutamine on tõkestatud, kui neid ei vajata?
- Kas kasutatavad rakendused on varustatud turvalise seansihaldussüsteemiga, mis töötab ka portaalilahendustes?

M 2.344 Interneti SAP süsteemide turvaline kasutamine

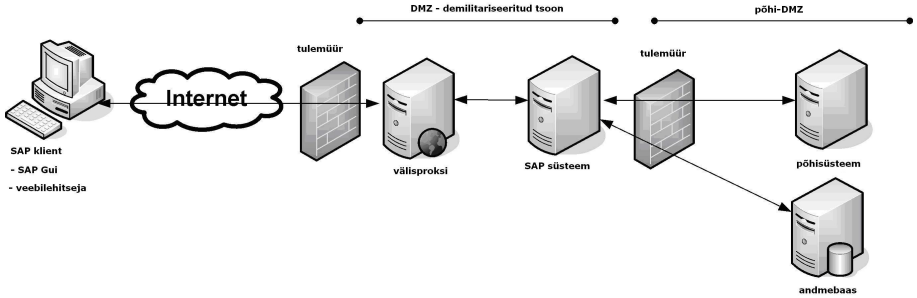
Algatamise eest vastutavad: IT-juht, IT-turvaosakond, arendusosakonna juht

Rakendamise eest vastutavad: administraator, arendaja

SAP süsteeme rakendatakse üha enam ka internetilahendustes. Reeglina on sellistel juhtudel installeeritud kas teatud täiendavad rakendused, või siis rakendatakse neid Interneti portaalilahendustes (vt M 2.343 SAP süsteemi portaalilahenduse kaitse) „ *Backend* -süsteemidena“. Internetilahenduste juurdepääs toimib reeglina HTTP vahendusel ning kasutajatel tuleb selleks otstarbeks rakendada brauserit. Seetõttu tuleb internetilahenduste puhul lisaks arvestada ka järgnevate aspektidega:

Süsteemi juurdepääsu piiramine lähtuvalt riskide hindamisest

Kõik SAP süsteemid, mille juurdepääs toimib otse läbi Interneti, on avatud kõrgetele riskidele. Antud asjaoluga tuleb arvestada riskide hindamisel. Kõnealuste SAP süsteemide juurdepääse tuleb piirata tulemüüriga, võimaldades juurdepääse ainult läbi selliste portide, mis kasutavad kas HTTPd või HTTPSi. Üldjuhul kehtivat SAP süsteemi internetipõhisele juurdepääsule samasugused nõuded nagu kõikidele teistele süsteemidele, nt nagu veebiserveritele (vt B 5.4 Veebiserver). Seetõttu tuleks järgida ka asjakohaseid nõudeid, mis kehtivad võrku ühendatud internetiühendusega süsteemidele. Muuhulgas võib nt olla mõistlik panna SAP süsteemi juurdepääs toimima läbi välisproksi või rakenduste tulemüüri (vt B 3.301 Turvalüüs (tulemüür)).



Joonis: SAP süsteem Internetis

Kommunikatsiooniliidese kontrollimine ja turvamine

Rakenduste kasutamist võimaldatakse läbi HTTP baasil toimivate liideste. Nii süsteemirakenduste kui ka tavaliste rakenduste puhul tuleb läbi viia riskide hindamine. Lisaks oleks mõistlik läbi viia ka veebiliidese turvakontroll, et tuvastada võimalik ohupotentsiaal seoses tüüpiliste veebi baasil toimuvate rünnetega. Üldjuhul tuleks arvestada, et HTTP-liidese vahendusel võivad toimuda ka RFC-juurdepääsud. Seetõttu tuleks sisse lülitada ainult sellised teenused, mida läheb ka kindlasti tarvis ning ka need tuleks omakorda läbi kontrollida, et selgitada, kas neid sobib Internetis kasutada või mitte.

Dialoogipääsu piiramine

Välistada tuleks võimalus kasutada SAPGui-juurdepääsu SAP süsteemidele otse läbi Interneti ning juurdepääse tuleks omakorda piirata protokollidega HTTP ja HTTPS.

Internet Transaction Server

Juhul kui SAP süsteemide juurdepääsuks *Internet Transaction Server* -it (ITS-i) ei kasutata, tuleks ITS juurdepääs desaktiveerida, kuna selle poolt pakutav juurde-

pääsulahendus sarnaneb SAPGui-juurdepääsule. Kasutades SAP *Web Application Server* -i versiooni, mis on vanem kui versioon 6.40, tuleb ITS installeerida eraldi komponendina (WGate, AGate). Sellistel juhtudel tuleks nende installeerimisest lihtsalt loobuda. ITS on integreeritud alates versioonist 6.40, seega tuleb vastavad teenused ABAP-pinus (nt *webgui* , vt M 5.127 SAP Internet Connection Framework (ICF) kaitse) ja Java-pinus (nt *mi* või *me* , vt M 4.266 SAP Java protokollistiku turvaline konfigureerimine) desaktiveerida. Juhul kui ITSi soovitakse kasutada, tuleks hoolikalt kontrollida SAP süsteemi volitusi, veendumaks, et need võimaldavad käivitada tõepoolest ainult lubatud funktsioone. Pistelistest kontrollidest sellisel juhul ei piisa. Kontrollimisprotsess võib olla sõltuvalt olukorrast küllaltki mahukas töö. Eriti oluline on siinkohal desaktiveerida kõik tehingud, mille kasutamist soovitakse tõkestada, kuna see välistab nende võimaliku kasutuse ka kriitiliste volituste kombinatsioonide toel. Kuna SAP süsteemis võib esineda mitu tuhat tehingut, tähendaks see väga mahukat konfigureerimistööd, mida pole reeglina võimalik tagada. Seetõttu tuleb ohupotentsiaal hoida hoolikalt läbimõeldud volituste kontseptsiooni abil võimalikult madalana.

Autentimine/ *Single Sign-On*

Interneti baasil toimivad *Single Sign-On* juurdepääsud tuleks aktiveerida selliste süsteemide vahel, mille puhul on lubatud kasutada interneti juurdepääse. Väliste süsteemide jaoks tuleks usaldussuhete konfigureerimisest loobuda, kuna nende puhul ei ole võimalik tagada piisavat turvalisust.

Volitused

Peamiselt tuleb jälgida seda, et SAP süsteemis hoitavate kasutajate volitused oleksid võimalikult minimaalsed. Kasutajate puhul, kes ei vaja SAPGui-juurdepääse, on soovitatav kasutada kontosid, mille tüübiks on kas kommunikatsiooni- või internetikasutajad.

Interneti juurdepääsuga SAP süsteemide andmete valideerimine

Interneti juurdepääsuga SAP süsteemide andmete edastamisel süsteemidesse, mille ei ole Interneti juurdepääsu, nt nagu see leiab aset päringute puhul või andmete transportimisel, tuleb andmed enne *Backend* -süsteemi edastamist esmalt valideerida.

Kättesaadavad andmed

Juhul kui sisemise SAP süsteemi andmeid soovitakse teha kättesaadavaks läbi SAP süsteemide, mis on varustatud Interneti juurdepääsuga, tuleks eelnevalt selgitada järgmisi asjaolusid:

- Tuleks välja selgitada, kas vastavaid andmeid on tõepoolest tarvis kättesaadavaks teha otseste, läbi Interneti toimivate juurdepääsude vahendusel või saaks olukorra lahendada hoopis andmete eksportimise ja importimisega teatud kindlate ajavahemike tagant. Sellega välistatakse välised juurdepääsud sisemistele süsteemidele.
- Andmete eksportimisel tuleks kontrollida, kas eksportida on tarvis kogu infot või läheb reaalselt tarvis ainult teatud kindlat osa. See piirab Interneti juurdepääsuga SAP süsteemi salvestatud andmeid.

Eksport/importlahenduste puhul tuleb jälgida, et need välistavad rakenduste otsese integreerimise (nt CRM või SRM süsteemide jaoks), mistõttu ei saa enam

kasutada otsese integreerimisega kaasnevaid eeliseid. Lisaks on tarvis tegeleda andmetranspordi konfigureerimisega ja hoolitseda selle haldamise eest. Seetõttu saab antud varianti kasutada vaid lihtsate lahenduste puhul.

Täiendavad kontrollküsimused:

- Kas SAP süsteemi kohta on läbi viidud riskide hindamine, mis arvestas piisavalt internetiühenduse valdkonnaga?
- Kas juurdepääs süsteemile on piiratud hädavajaliku miinimumini?
- Kas on võimalik kasutada ainult vajalikke teenuseid?
- Kas pakutavad teenused on edukalt läbinud turvakontrolli?

M 2.345 SAP süsteemi väljasttellimine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: IT-juht, IT-turvaosakond
SAP süsteemi väljasttellimisel tuleb arvestada järgnevaga:

- Väljasttellimise partneri puhul tuleb rakendada nõudeid, mis on kajastatud B 1.11 Väljasttellimine (Outsourcing) .
- Erilist tähelepanu tuleb pöörata vastavate protsesside sujuvale integreerimisele, et näiteks töid teostav partner annaks tööde tellijale ka tagasisidet. See puudutab muuhulgas ka selliseid protsesse, mis on seotud kasutajate ja nende volituste haldamisega.
- Kõikide SAP süsteemiga kaasnevate ülesannete kohta on soovitatav koostada asjakohane tabel. Sellesse tabelisse tuleks üles märkida ülesanded, mida peavad täitma väljasttellitud teenuse osutaja poolt palgatud töötajad ja ka sellised ülesanded, mida peavad täitma organisatsiooni enda töötajad. Vastutavad töötajad tuleb dokumenteerida. Järgnev tabel on toodud ainult ühe võimaliku näitena, see ei kajasta mitte mingil juhul täielikku loetelu ning seda tuleks kindlasti muuta vastavalt kohapealsetele oludele. Loetletud ülesannetes on reeglina tarvis sisse viia täiendavad alajaotused.

Ülesanne	Vastutav osapool
SAP süsteemi planeerimine	Ettevõte / ametiasutus (siiski tuleks kaasata ka väljasttellitud teenust osutav partner)
Volituste kontseptsiooni koostamine	Ettevõte / ametiasutus
SAP süsteemi installeerimine	Väljasttellitava teenuse osutaja
SAP süsteemi aluskonfiguratsioon	Väljasttellitava teenuse osutaja (peab täitma ettevõtte või ametiasutuse poolt planeerimisfaasis väljatöötatud ettekirjutusi)
Moodulite ja rakenduste tasandite konfiguratsioonid	ettevõte / ametiasutus (vastavalt planeerimisfaasis väljatöötatud ettekirjutustele)
Baashaldus – kasutajate loomine	Väljasttellitava teenuse osutaja (vastavalt ettevõtte või ametiasutusega sõlmitud lepingule, rollide lahutamisel väljasttellitava teenuse osutaja)
Baashaldus – volituste haldamine	Väljasttellitava teenuse osutaja (vastavalt ettevõtte või ametiasutusega sõlmitud lepingule, rollide lahutamisel väljasttellitava teenuse osutaja)
Rakenduste haldus – kasutajate loomine	Ettevõte / ametiasutus (vastavalt organisatsioonisisesele kinnitamisprotseduurile)
Rakenduste haldus – volituste haldamine	Ettevõte / ametiasutus (vastavalt organisatsioonisisesele kinnitamisprotseduurile)

Selgitused:

- Arvutite käitamisega ja SAP süsteemi baashaldusega tegeleb reeglina väljasttellitava teenuse osutaja. Rakenduste haldusega tegeleb reeglina see osapool, kes teenust väljastpoolt sisse ostab. Siinkohal on oluline, et väljasttellitud teenuse osutajale antaks edasi vajalik informatsioon nõuete kohta, mis puudutavad rakenduste (turbealaseid) eripärasid. Ainult niimoodi on võimalik tagada adekvaatne baashaldus.
- Turbe valdkonnas peaksid regulaarselt aset leidma asjakohased kooskõlastused. Nende kokkusaamiste käigus on võimalik arutada ka teenuse osutaja poolt turbeastme suurendamiseks tehtud ettepanekuid ja võimalikke tellijapoolseid muudatusi väljasttellitava teenuse osutamise tingimustes.
- Riskide hindamise käigus on tarvis arvestada asjaoluga, et väljasttellitava teenuse osutaja saab kasutatava SAP süsteemi andmete üle täieliku kontrolli. Turbe seisukohast tuleb antud asjaolu kõikide ametiasutuste ja ettevõtete puhul hinnata kriitiliseks. Vajalike kontrollide olemasolu kontrollitakse muuhulgas nt ka Sarbanes Oxley keskkonnas.
- Tundlike andmete töötlemisel, millele rakenduvad erinõuded kas tulenevalt erinevatest seadustest või mille puhul nõutakse konkreetselt hoolikalt ümberkäimist, peab sellekohast vastutust jagama ka väljasttellitud teenuse osutaja. Sellistel juhtudel tuleb väljasttellitava teenuse osutajat kohustada saladusi hoidma ning sõlmida vastavad lepingud.
- Kasutajate ja volituste haldamise puhul on mõistlik kaasata volituste planeerimisse ka üks väljasttellitavat teenust osutava partneri töötaja, kuna see on ainuke viis, kuidas väljasttellitava teenuse osutajal on võimalik tagada piisav turve ka rakenduste puhul.

Täiendavad kontrollküsimused:

- Kas SAP süsteemi jaoks on koostatud adekvaatne väljasttellimise kontseptsioon?
- Kas ülesannete laialijagamine on turbe seisukohast mõistlik ning kas kõikide ülesannete puhul on kindlaks määratud vastutusalad ja dokumenteeritud nende eest vastutavad töötajad?
- Kas kasutajate ja volituste haldamiseks planeeritud protsessid suudavad tagada, et teenuse väljasttellimisel pole võimalik endale volitusi kokku koguda?

M 2.346 SAP dokumentatsiooni kasutamine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator, IT-juht, arendaja

SAPga kaasneb väga suur dokumentatsioon ja väga laialdane info. Saadaoleva dokumentatsiooniga peavad eriti täpselt kursis olema administraatorid, kes peavad ennast regulaarselt kurssi viima ka võimalike täiendustega. Keskne koht, mille kaudu saab hankida SAPd puudutavat informatsiooni, on SAP Service Marketplace (http://service.sap.com). Siinkohal tuleb arvestada, et brauseris peab olema sisse lülitatud JavaScript ning enamasti viiakse läbi ka autentimine. Erandiks on SAP Help Portal, mille kaudu saab hankida erinevate toodete dokumentatsiooni. SAP Service Marketplace sisaldab endas viiteid ka täiendavatele infoallikatele. Järgnevalt on välja toodu mõningad näited:

- SAP Service Marketplace pakub infot SAP kohta või täiendava tarkvara kohta. Oluline on siinkohal ka turvet puudutav info, mis on kättesaadav kiirlingi alt "/security". Siit on võimalik endale tellida ka SAP Security Newsletter, mis edastab turbealast infot meili teel. Lisaks on olulised veel ka SAP toodete turvajuhised, mis on kättesaadavad kiirlingi alt "/securityguide". Käesoleva konteksti puhul on eriti oluline SAP NetWeaver-i turvajuhis.
- Kõikide toodete juhendid ja laiaulatuslik dokumentatsioon on kättesaadav abiportaalist SAP Help Portal (http://help.sap.com).
- Eraldi arendajate jaoks vajaliku informatsiooni jaoks on loodud keskkond SAP Developer Network (http://sdn.sap.com). Selle kasutamiseks tuleb end registreerida, mis on tasuta.

Järgnevalt on toodud ülevaade olulisematest SAP dokumentidest käesoleva mooduli üksikute meetmete lõikes. Dokumentide asukohaks, kui pole öeldud teisiti, on SAP Help Portal.

M 2.341 SAP kasutuselevõtu planeerimine

Kasutajate haldamine

Detailsemat infot SAP süsteemide kasutajahalduse kohta leiate SAP dokumendist „Identity Management", peatükist „Users and Roles (BC-Sec-USR)", alalõikudest „User Maintenance" ja „Central User Administration", samuti lõigust „User Management Engine".

Ressursside planeerimine

SAP ressursside planeerimise (tuntakse ka nime all *Sizing*) kohta pakub laialdast informatsiooni Service Marketplace. Teema alt „Solution Life-Cycle Management" leiate muuhulgas alateemad „Quick Sizer Tool" ja „Sizing Guidelines". Nimetatud info on abiks ressursside planeerimisel. Detailseid juhiseid soovitatava süsteemimaastiku kohta leiate reeglina kasutatavate SAP toodete turvajuhistest, mis on kättesaadavad ka Service Marketplace keskkonnas lühendi alt nimega „securityguide". Detailsemat infot SAP transpordisüsteemi kohta leiate dokumendi „SAP Netweaver Technical Operations Manual" erinevatest „Software Change Management" lõikudest, mis käsitlevad ABAP- und Java-pinu kirjeldusi. Täpsemat infot Audit Information System-i (AIS-i) kohta leiate SAP juhisest nr 451960.

M 2.342 SAP pääsuõiguste planeerimine

Detailsemat infot, mida kasutada volituste kontseptsiooni koostamisel, leiate SAP dokumendi „Identity Management“ peatüki „Users and Roles (BC-Sec-USR)“ alalõigust „SAP Authorization Concept“.

M 2.349 Turvaline SAP süsteemi tarkvara arendamine Täiendavaid nõuandeid *Debugging* -volituste kohta leiate SAP juhistest nr 13202 ja 65968.

M 4.256 SAP süsteemi turvaline installeerimine

Detailsemat infot operatsioonisüsteemide turvamise kohta leiate SAP dokumendi „SAP NetWeaver Security Guide“ alalõikudest „SAP System Security Under UNIX/LINUX“ ja „SAP System Security Under Windows“.

M 4.258 SAPi ABAP-pinu turvaline konfiguratsioon

IMG

Infot IMG dokumentatsiooni kohta leiate SAP dokumendist pealkirjaga „Customizing (BC-CUS)“, kus on toodud lõik „Sissejuhatus (IMG).

Profiilid

Täpsemat infot profiilidega ümberkäimise kohta leiate SAP dokumendi „Configuration“ alalõigust „Profiles“.

Süsteemi muudetavus

Süsteemi muutmise teema kohta leiate täpsemat infot SAP dokumendi „Transport Organizer (BC-CTS-ORG)“ alalõigust „Setting the System Change Option“.

Mandaadid

Administraatorid peavad olema väga täpselt kursis mandaatide konfigureerimise võimalike tagajärgedega. Asjakohase detailsema dokumentatsiooni leiate SAP dokumendi „Transport Organizer (BC-CTS-ORG)“ alalõigust „Mandaatide juhtimine“.

Operatsioonisüsteemi käsud

Operatsioonisüsteemide käskude (*commands*) turvaliseks muutmise kohta leiate täpsemat infot SAP dokumendi „SAP NetWeaver Security Guide“ alalõikudest „Logical Operating System Commands“ ning dokumendi „Configuration“ alalõigust „External Operating System Command: Contents“.

Single Sign-on

Täpsemat infot *Single Sign-On* protseduuride kohta leiate SAP dokumendi „SAP NetWeaver Security Guide“ alalõigust „User Authentica-tion and Single Sign-On“ ning dokumendist „Using Logon Tickets“.

SNC

SNC kohta leiate täpsemat infot SAP dokumendi „SAP NetWeaver Security Guide“ alalõigust „Transport Layer Security“.

M 4.259 ABAP-pinu turvaline kasutajate haldus

Kasutajate haldamine

Täiendavaid juhiseid SAP süsteemide kasutajate haldamise kohta leiate SAP dokumendi „Identity-Management“ alalõigust „First Installation Procedure“.

Standardsed kasutajad

Detailsemat infot standardsete kasutajatega ümberkäimise kohta leiate SAP dokumendi „SAP NetWeaver Security Guide“ alalõigust „Protecting Standard Users“.

M 4.260 SAP-volituste haldus

Volituste haldamine

Täpsemat infot volituste haldamise ülesehitamise ja olulisemate volituste kohta SAP dokumendi „Identity Management“ alalõigust „Organizing Authorization Administration“.

Profiili generaator

Täpsemat infot volituste haldamise kohta profiili generaatori abil leiate SAP dokumendi „Identity Management“ alalõigust „Role Maintenance“.

M 4.261 Kriitiliste SAP volituste turvaline rakendamine

Volituste kontrollid

Üldiseid juhiseid volituste kontrollide kohta leiate SAP dokumendi „Identity Management“ alalõigust „Authorization Checks“. Kriitiliste volituste identifitseerimiseks on hädavajalik omada piisavaid teadmisi protsessi aluseks oleva volituste kontrollide kohta.

Süsteemivolitused

Täiendavat infot SAP süsteemivolituste kohta leiate SAP dokumendi „Identity Management“ alalõigust „Protective Measures for Special Profiles“.

M 4.262 SAP-volituste lisakontrollide konfigureerimine

Volituste kontrollide desaktiveerimine

Täiendavat infot SAP süsteemivolituste desaktiveerimise kohta leiate SAP dokumendi „Identity Management“ alalõikudest „Authorization Checks“ ja „Reducing the Scope of Authorization Checks“.

Volitusgrupid

Täiendavat infot volitusgruppide konfigureerimise kohta leiate SAP dokumendi „ALV Grid Control (BC-SRV-ALV)“ alalõigust „Assigning and Maintaining Authorization Groups“.

M 4.263 SAP sihtpunkti kaitse

Täpsemat infot sihtkohtade juurdepääsude juhtimise kohta leiate SAP dokumendi „RCF/ICF Security Guide“ alalõigust „Controlling Access to RFC Destinations“.

M 4.264 SAP süsteemide tabelite otsemuudatuste piiramine

Detailsemat infot parameetreid puudutavate tehingute kohta leiate järgnevatest allikatest:

- SAP dokumendi „RFC Security Guide“ alalõigust „Authorization Object S_TABU_DIS (Table Maintenance)“
- Sissejuhatuse dokumentatsioonist (IMG, Transaction SPRO) teema alt „SAP Web Application Server/ Süsteemi administreerimine/ Kasutajad ja volitused/ Ridadega seotud volitused“
- SAP dokumendi „Volitused mySAP HR“ alalõigust „Rakenduseülesed volitusobjektid“.

Täiendavat infot parameetritehingute ja volituste kohta leiate tehingu SE93 kontekstis järgnevatest SAP dokumentidest:

- SAP dokumendi „ABAP-Programming (BC-ABA)“ alalõigust „Parameter transaction“
- SAP dokumendi „Identity Management“ alalõigust „Authorization Checks“.

M 4.265 SAP süsteemi pakktöötluse turvaline konfigureerimine

Täiendavat infot pakktöötluse kohta leiate SAP dokumendi „Background processing“ alalõigust „Authorizations for Background Processing“.

M 4.266 SAP Java protokollistiku turvaline konfigureerimine

JAVA-pinu teenused

Java-pinu teenuste ja nende funktsioonide kohta leiate juhiseid asjakohastest käsiraamatutest nagu nt SAP dokumendi „SAP NetWeaver-i tehniline kasutusjuhend“ alalõigust „SAP Web Application Server (JAVA) administreerimine“ ning sinna juurdekuuluvatest dokumentidest nagu „Arhitektuuri käsiraamat“, „Administreerimise käsiraamat“ ja „Arendaja käsiraamat“.

HTTP PUT

HTTP PUT problemaatika kohta leiate täiendavat infot SAP juhisest nr 606733.

M 4.269 SAP süsteemi andmebaasi turvaline konfiguratsioon

SAP soovitused andmebaasi turvaliseks muutmise kohta leiate SAP dokumendi „Operating System and Database Platform Security Guides“ alalõigust „Database Access Protection“. Soovitused on toodud erinevate andmebaasitoodete lõikes.

M 4.270 SAP logimine

Süsteemiseire funktsioonid

Süsteemiseire funktsioonide täpsemad seletused leiate SAP dokumendist „Tools for Monitoring the System“.

Muudatuste jälgimine

Täiendavat infot muudatuste jälgimise kohta leiate SAP juhisest nr 1916 ja seal näidatud täiendavatest allikatest.

M 4.271 SAP süsteemi viirusetõrje

Täpsemat infot arvutiviiruste tõrjeks loodud programmidele vajalike liideste kohta leiate SAP dokumendist „SAP Virus Scan Interface“. Informatsiooni erinevate toodete kohta, mida on võimalik liideste abil ühendada, leiate SAP Service Marketplace keskkonna kiirlingi „securitypartners“ alateemast „Partners for Virus Scan interface (NW-VSI)“.

M 4.272 SAP transportsüsteemi turvaline kasutamine

Täpsemat infot transportsüsteemi kohta leiate SAP dokumentidest „Change and Transport System – Overview (BC-CTS)“ ja „Transport Management System (BC-CTS-TMS)“.

M 4.273 SAP Java protokollistiku tarkvara levitamise turvaline kasutamine

Täpsemat infot tarkvara levitamise kohta Java-pinus leiate SAP dokumendist „SAP NetWeaver Java Development Infrastructure“.

M 5.125 SAP-süsteemi siseneva ja väljuva kommunikatsiooni kaitse

SNC

Täpsemaid juhiseid SNC-konfiguratsiooni kohta leiate SAP dokumendi „Administration Manual“ alalõigust „Configuring SNC (SAP J2EE Engine to ABAP Engine)“. Täiendavaid juhiseid leiate veel ka SAP dokumendi „Network and Transport Layer Security“ alalõigust „Secure Network Communications (SNC)“.

SSL

Täpsemat infot SSLi installeerimise ja konfiguratsiooni kohta leiate SAP dokumendi „System Security“ alalõigust „Configuring the SAP Web AS for Supporting SSL“ ning SAP dokumendi „Administration Manual“ alalõigust „Configuring the Use of SSL on the SAP J2EE Engine“. Infot SSLi kaitsmise kohta Java-pinu sisemiste LDAP juurdepääsude puhul leiate dokumendist „Configuring SSL Between UME and LDAP Directory (SAP NW‘04)“.

M 5.126 SAP RFC liidese kaitse

Ülddokumentatsioon

Detailsemat infot RFC-kommunikatsiooni kohta leiate SAP dokumendi „RFC/ICF Security Guide“ alalõigust „RFC Scenarios“.

Trusted Systems

Täiendavat infot teema kohta „Trusted Systems“ leiate SAP dokumendi „RFC/ICF Security Guide“ alalõigust „Authorization Object S_RFCACL“ ding dokumendi „Components of SAP Communication Technology“ peatüki „RFC“ alalõigust „Trusted System: Trust Relationships Between the SAP Systems“.

Sideinfo fail

Täiendavat informatsiooni *sideinfo* faili kohta leiate SAP dokumendi „Components of SAP Communication Technology“ alalõigust „Introduction to RFC Client Programs“ ja dokumendi „SAP Gateway“ alalõigust „Side Information Tables“.

Väline RFC-Server

Täpsemat infot väliste RFC-serverite kohta leiate SAP dokumendi „RFC/ICF Security Guide“ alalõikudest „Security Measures - Overview (RFC)“ ja „RFC Communication between SAP Systems and External (Non-SAP) Systems“. Infot RFC SDK kohta leiate dokumendist „Components of SAP Communication Technology“ alalõigust „The RFC API“ ja alalõigust „Contents of the RFC SDK“.

SAP Gateway

Täiendavat infot SAP Gateway kohta leiate SAP dokumendi „SAP Gateway“ alalõigust „Security Settings in SAP Gateway“.

M 5.127 SAP Internet Connection Framework (ICF) kaitse

Täiendavat infot ICFi kohta leiate SAP dokumendi „Components of SAP Communication Technology“ peatüki „Internet Communication Framework“ alalõigust „Administration: HTTP Communication Using the SAP System as a Server“ ja SAP dokumendi „RFC/ICF Security Guide“ alalõigust „RFC Scenarios“.

M 5.128 SAP ALE (IDoc/BAPI) liidese kaitse

Täpsemat infot ALE-liideste kaitsmise kohta leiate SAP dokumendist „Security Guide ALE (ALE Applications)“.

M 5.129 SAP süsteemide HTTP teenuste turvaline konfiguratsioon

SOAP

Täiendavat infot SOAP-liidese kohta leiate SAP dokumendi „Components of SAP Communication Technology“ peatüki „Internet Communication Framework“ alalõigust „SOAP Framework“.

Content-Server-liides

Täiendavat infot Content-Server-liidese kohta leiate SAP dokumendi „SAP Content-Server Security Guide“ ja dokumendi „Knowledge Provider (BC-SRV_KPR)“ alalõigust „SAP Content Server HTTP 4.5 Interface“.

M 6.97 SAP süsteemi valmisolek hädaolukorraks

Täpsemat infot *Backup* -i kohta leiate juhendist „SAP NetWeaver Technical Operations Manual“. ABAP-pinu kohta leiate infot alalõikudest „Backup and Restore“ ja „Creating a Homogeneous System Copy“, Java-pinu kohta alaõigust „Backup and Recovery of the SAP Web Application Server (Java)“.

Täiendavad kontrollküsimused:

- Kas SAP kättesaadavat dokumentatsiooni on kasutatud?
- Kas kättesaadavat SAP dokumentatsiooni kontrollitakse regulaarselt võimalike uuenduste osas?

M 2.347 SAP süsteemi regulaarsed turvakontrollid

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator, IT-turvaosakond, audiitor

SAP süsteemi turvalisust on pikemas perspektiivis võimalik tagada ainult piisavate regulaarsete kontrollide abil. Need võimaldavad tuvastada ja kõrvaldada nii väärkonfiguratsioone kui ka igasuguseid muid kitsaskohti. Turvakontrollid peaksid toimuma regulaarselt ning neid peaksid läbi viima erinevad inimesed. Näiteks administraatorid peaksid kontrolle läbi viima suhteliselt lühikeste ajavahemike tagant (umbes kord kuus). Selleks on soovitatav välja töötada kontrollnimekiri, et kontrollprotseduur lähtuks kindlatest põhimõtetest. Väiksemad tuvastatud probleemid saavad administraatorid reeglina ise kohe ära parandada, suurematest probleemidest tuleb teavitada vajalikke instantse vastavalt selleks kehtestatud protseduurireeglitele. Keskmise pikkusega ajavahemike tagant (mitme kuu möödudes) peaksid turvakontrollid läbi viima mõned teised organisatsioonisisesed töötajad (IT-turvaosakonna töötajad, IT-revidendid). Pikkade ajavahemike tagant oleks mõistlik läbi viia kontrollid, mis teostatakse väljaspool organisatsiooni töötavate isikute poolt. Kontrollide puhul tuleb arvestada järgmiste aspektidega:

- Turvet puudutava info regulaarne kogumine - Administraatorid ja IT-turbe eest vastutavad töötajad peavad ennast regulaarselt kursis hoidma nende vastutusalasse jäävate süsteemide võimalike muudatuste ja uuendustega. Selleks tuleb ennekõike regulaarselt tutvuda SAP infoallikatega.
- SAP infoallikad - M 2.346 SAP dokumentatsiooni kasutamine
- Revisjoni teostavate kasutajate volitused - SAP kasutajakontodele, mis võimaldavad organisatsioonivälistel isikutel kontrollida süsteemi konfiguratsiooni, tuleks volituste määramisel anda vaid lugemisõigused. Revisjoni jaoks loodud kasutajatel ei tohi olla õigust viia sisse muudatusi. AP-pinus ei tohi revisjoni jaoks loodud kasutajaid liigitada profiili alla SAP_ALL. Juhul kui revisjonide läbiviimiseks loodud kasutajate volitusi ei ole võimalik piirata lugemisõigusega, tohivad juurdepääsud leida aset vaid siis, kui järgitakse nelja silma printsiipi.
- SAP infoallikad - Süsteemi kontrollimiseks pakub SAP kasutada ka nende endi poolt loodud auditeerimissüsteemi (*Audit Information System,* AIS). Süsteem võimaldab kasutada erinevaid rolle ja volitusi, mida saab siduda revisjoni jaoks loodud kasutajakontoga. Rollide valik on reeglina koostatud selliselt, et need võimaldavad kasutada ainult lugemisõigusega juurdepääse. Rollidega saab tutvuda profiili generaatoris (Transaction PFCG), kasutades otsingut “SAP*AUDITOR*”.
- AIS-i juurdepääsu konfigureerimine - Kontrollide läbiviimiseks võib rakendada auditeerimise infosüsteemi AIS (*Audit Information System*). AIS-ist on loodud erinevaid versioone: Transaction SECR ja rollidel põhinev versioon. Transaction SECR võimaldab kontrolle osaliselt automatiseerida. Lisaks saab AISi abil kontrolli tulemusi dokumenteerida ja fikseerida kontrolli puhul tuvastatud seisundi (valgusfoori põhimõte: punane, kollane, roheline). Pakutavatest kontrollivõimalustest on soovitav välja valida ja defineerida teatud kogus kontrolle (*Top 10 Security Reports*), mis kontrolliprotseduuri raames läbi töötatakse. Kontrolli käigus selgitatakse välja, milline on hetke konfiguratsioon võrreldes etalonkonfiguratsiooniga. Siinkohal tuleb arvestada, et AISi kasutades muutuvad nähtavaks kriitilise tähtsusega süsteemikonfi-

guratsioonid. Seetõttu peab vastav juurdepääs olema piiratud ainult volitatud kasutajatega (S_TCODE, Transaction SECR). Vastupidiselt Transaction SECR versioonile kasutab rollidel põhinev AIS juba eelnevalt väljatöötatud rolle, volitusi ja programme, mis võimaldavad anda kasutajale vajalikud volitused auditite läbiviimiseks süsteemi ja moodulite tasandil. Eelkõige kasutatakse seda äritegevusele suunatud auditite tarbeks. Rollidel baseeruv AIS tuleb sisse seada ja konfigureerida vastavalt kohapealsetele oludele.

- SAP infoallikad - Täiendavat infot leiate antud teema kohta M 2.346 SAP dokumentatsiooni kasutamine .
- Süsteemimuutmise muudatuste kontrollimine - Süsteemimuutmise seadeid (*System Change Options*) tuleb regulaarselt kontrollida. Selleks võib kasutada tehingut SE03 „Administration/System Change“. Kontrollida tuleks globaalseid seadistusi ja iga mandaadi seadistusi (vt M 4.258 SAPi ABAP-pinu turvaline konfiguratsioon). Java-pinu puhul on võimlaik süsteemi muudetavust konfigureerida süsteemiseadistuse abil.
- *Security Auditlog* - *Security Auditlog* sisaldab endas turvalisust puudutavaid logisissekandeid. Seetõttu tuleb regulaarselt tegelda nende analüüsimisega. Logiandmete analüüsimiseks võib kasutada tehinguid SM20, SM20N või RZ27_Security, kusjuures võiks eelistada tehingut SM20N, kuna sellel on parem kasutajaliides. Tehingute SM20 ja SM20N kasutamiseks tuleb eelnevalt kindlaks määrata analüüsi ulatus tehinguga SM19 ning sisse lülitada *Auditlog* (vt M 4.270 SAP logimine).
- Profiili parameetrid - Profiili parameetrite seadistusi tuleb võrrelda planeeritud etalonväärtustega (vt M 4.258 SAPi ABAP-pinu turvaline konfiguratsioon *)* . Kehtivaid profiiliparameetreid on võimalik vaadata ka otse tehinguga SM20N. Alternatiivse lahendusena võib kasutada ka RSPARAM raportit, mis toimib tehinguga SE38.
- Kasutajainfosüsteem - Kasutajainfosüsteemiga (Transaction SUIM) tuleks läbi viia regulaarseid kontrolle. Selle käigus on oluline järgnev turbealane info:

1. Vääralt sisseloginud kasutajad - Need võivad vihjata ründekatsetele.
2. Kasutajate sisselogimisandmed ja paroolide muudatused. - Sellega on võimalik tuvastada kasutajaid, kes pole mitte kunagi ennast sisse loginud või kes pole mitte kunagi muutnud oma parooli neil juhtudel, kus süsteem seda automaatselt ei nõua.
3. Tehingute käivitamiseks vajalike kriitiliste volitustekombinatsioonidega kasutajad. Kasutajate volitusi tuleks võrrelda volituste kontseptsiooniga.
4. Kriitiliste volitustega kasutajad - Kasutajate volitusi tuleks võrrelda volituste kontseptsiooniga.
5. Kasutajate, rollijaotuse, rollide, profiilide ja volituste muudatuste tõendamine. - Siinkohal tuleks eriti hoolikalt kontrollida võimlaikke muudatusi administratiivsetes objektides.

- Ligipääsetavad SAP *Gateway* -d - SAP süsteemi poolt ligipääsetavaid teiste SAP süsteemide SAP *Gateway* -sid saab määrata tehinguga RSGWLST. Tehing näitab ära nii ühendus- kui ka juurdepääsuvõimlaused. Eemalasuvates *Gateway* -des saab vaadata faili “secinfo” seadistusi, mille abil määratakse kindlaks volitused eemalasuvate SAP *Gateway* -dega kontakti loomiseks

ja registreerimiseks. Lisaks on võimalik kontrollida ka eemalasuvate ligipääsetavate SAP *Gateway* -de registreeritud RFC-serveriprogramme. Sellise info analüüs eeldab siiski vastavaid tehnilisi teadmisi. Kuna tehinguga RSGWLST on võimlaik hankida informatsiooni ka tundliku süsteemiinfo kohta, tuleb selle tehingu juurdepääsu piirata. Lokaalse süsteemi SAP *Gateway* seisundit on võimalik kontrollida tehinguiga SMGW (*Gateway Monitor*).

- *Single Sign-On* (SSO) võimaluste kontrollimine - SAP süsteemi sisselogimiseks tuleb kasutajatel sisestada kehtiv autentimisinfo (nt kasutajanimi / parool, sertifikaat), mille järgselt on neil võimalik ennast sisse logida teistesse SAP süsteemidesse, kasutades selleks SSO mehhanismi, mille puhul ei nõuta korduvat autentimisinfo sisestamist. Tehinguga STRUST on võimalik vaadata teiste SAP süsteemide sertifikaate, mida lokaalne süsteem aktsepteerib SSO-juurdepääsude puhul. Siia nimekirja peaksid olema kantud ainult usaldusväärsed süsteemid. Alternatiivse lahendusena võib kontrollimiseks kasutada ka tehinguid SSO2 või SSO2_ADMIN.
- Regulaarne volituste kontrollimine - Volituste täiemahuline käsitsi kontrollimine pole reeglina võimalik, sest nende arv on selleks liiga suur. Seetõttu on ilmtingimata vaja töötada välja sobiv volituste kontseptsioon. Kuid ka selle olemasolul tuleb siiski regulaarselt kontrollida, kas volituste sisu ühtib kontseptsiooniga. Selleks võib olulisemate kasutajarühmade puhul läbi viia pistelisi kontrolle (vt lõiku „Kasutajainfosüsteem“ eespool). Volituste kontseptsioon peab suutma tagada selliste protsesside rakendamise, mis suudaksid tõkestada volituste kokkukuhjamist.
- SAP infoallikad - Lisaks võib rakendada tööriistu, kuhu on integreeritud nii muudatuste kui ka riskide haldamine, mis võimaldab nt vähendada kasutajate volitustega seotud probleemidest tingitud petmisi. SAP võimaldab selleks kasutada nn „SAP GRC Access Control-i“, mis kontrollib konfigureeritud volitusi lähtuvalt sellest, kas kasutajatele on antud volitusi, mida tuleks turbe seiskohalt liigitada kriitiliste hulka. Tavapäraselt leiavad sellised kontrollid aset ka Sarbanes-Oxley-keskkonnas, kuid üldjuhul võib neid siiski soovitada igale ametiasutusele ja ettevõttele. Kontroll peab suutma antud vaatevinklist kriitilisi volitusi, mis on seotud tehingutega (näiteks SE80, SE16, SQVI või kasutajate jaoks kriitilise tähtsusega volitusobjekte, nt S_PROGRAM, S_USER_GRP, S_TABU_DIS, S_RFC, S_USR_RFC) tuvastada ja esile tuua. Sarnaseid kontrollitööriistu võib leida ka teistelt tootjatelt.
- Uuenduste (*updates*) värskuse kontrollimine - SAP süsteemi installeeritud täiendite puhul tuleb kontrollida nende värskust. Selleks võib kasutada tehingut SPAM. Süsteemi hetkel paigaldatud paikade (*patches*) versioone tuleb võrrelda saadaolevate paikadega. See eeldab, et kontrollijal on teada, millised paigad on SAP süsteemi jaoks hetkel saadaval. Kontroll peab tuvastama ka täienditega seotud vigu või hoiatavaid teateid. Siinkohal tuleb arvestada, et hoiatavaid teateid võib esineda ka siis, kui uuenduste seisundit (*Update Status*) kajastav indikaatorvärv on roheline.
- Sideliideste turvalisuse kontrollimine - kontrollida tuleks erinevate sidet võimaldavat liideste turvalisust (vt M 5.125 SAP-süsteemi siseneva ja väljuva kommunikatsiooni kaitse). See puudutab nt ABAP-pinu RFC-, ICF- ja ALE-liideseid ja Java-pinu liideseid. Eriti hoolikalt tuleb siinkohal kontrollida, kelle on antud administraatori volitused ning milliseid teenuseid ja funktsioone on võimalik kasutada.

Täiendavad kontrollküsimused:

- Kas SAP süsteemis viiakse regulaarselt läbi turvakontrolle?
- Kas volitusi kontrollitakse regulaarselt vähemalt pisteliste kontrollidega?
- Kas SAP süsteemi on installeeritud kõige värskemad paigad?

M 2.348 Turvaline SAP-süsteemide kohandamine

Algatamise eest vastutavad: IT juht, IT turvaosakond,
Rakendamise eest vastutavad: administraator

SAP süsteemide kohandamise raames konfigureeritakse ja seatakse süsteem paika selliselt, et see suudaks pakkuda institutsioonile soovitud tuge. Antud protseduur nõuab reeglina küllaltki palju aega. Seetõttu tuleks arvestada järgnevaga:

- Mugandamise (Customizing) jaoks tuleb koostada eraldi kontseptsioon, mis peaks kirjeldama võimalikult täpselt SAP süsteemi soovitud seisundit ja mugandamise läbiviimiseks vajalikke protseduure.
- Kontseptsiooni koostamiseks tuleb läbi viia nõudmiste analüüs. Selle käigus tuleb välja selgitada valdkonnad, mida on tarvis kohandada, et saavutada soovitud süsteemikäitumine (vt M 2.341 SAP kasutuselevõtu planeerimine).
- Kohandamisprotsessi läbiviimiseks tuleb juurutada protsessid, mis annaksid tegevuse kohta tagasisidet ja võimaldaksid kontseptsiooni kohandamise käigus muuta (vt M 4.258 SAPi ABAP-pinu turvaline konfiguratsioon).
- Kohandamisega võivad tegelda ainult piisavate erialaste teadmistega ja usaldusväärsed isikud.
- Konfiguratsioonide kohandamist ei tohiks läbi viia tootmissüsteemis, vaid paigaldada kontrollitud kujul vastava transportimissüsteemi abil.

Täiendavad kontrollküsimused:

- Kas kohandamise jaoks on koostatud asjakohane kontseptsioon?
- Kas kohandamist viivad läbi usaldusväärsed isikud?

M 2.349 Turvaline SAP süsteemi tarkvara arendamine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator, arendaja

Ametiasutuse või ettevõtte spetsiifiliste nõuete täitmiseks võib SAP süsteemi funktsioone muuta või täiendada ka enda poolt loodud tarkvaraarendustega. Turbe seisukohast tuleb SAP süsteemide tarkvara arendamisel arvestada järgnevaga:

Tarkvaraarenduse protsess

Tarkvara arendamisega seotud protsesside jaoks on soovitatav aluseks võtta soovitused meetmest M 2.378 Süsteemiarendus .

Tootmissüsteemide arendajad

Kuna tootmissüsteemid (*production systems*) sisaldavad konfidentsiaalseid süsteemi- ja äriandmeid, ei tohi tarkvaraarendajatele võimaldada juurdepääsu tootmissüsteemidele. Eriti oluline on tagada, et tootmissüsteemis ei leiaks aset silumisprotsesse (*Debugging*). Veaanalüüsid tuleb läbi viia arendussüsteemides. ABAP-pinu jaoks tähendab see seda, et mitte ühelegi kasutajale ei tohi anda volitust S_DEVELOP. Tootmissüsteemides on keelatud kasutada tööriistu CATT ja eCATT (ABAP-pinus) ning *Engine Remote Debugging* (Java-pinu). Selle tõkestamiseks tuleb kasutada mandaate ehk vastavat Java-pinu konfiguratsiooni. Tarkvaraarendajatele võib tootmissüsteemide kuvamisõiguseid ja *Debugging* -õigusi anda vaid väga hästi põhjendatud erijuhtudel, nt tootmissüsteemide veaanalüüside läbiviimiseks ning sedagi ainult ilma modifitseerimisõiguseta. Turvalisus tuleb tagada lisaks ka veel täiendavate organisatoorsete meetmete abil.

SAP infoallikad

Täiendavat infot leiate antud teema kohta M 2.346 SAP dokumentatsiooni kasutamine . Uue tarkvara installeerimist arendajate poolt otse tootmissüsteemi tuleb takistada mitmeastmelise tarkvarale kasutusloa andmise kontseptsiooniga (vt M 4.272 SAP transportsüsteemi turvaline kasutamine ja M 4.273 SAP Java protokollistiku tarkvara levitamise turvaline kasutamine).

Majasiseste tarkvaraarenduste turbeettekirjutused

Tarkvaraarendajate tööd tuleks toetada sobivate turvaettekirjutuste väljatöötamisega. Arendajal on võimalik programmeerimise käigus turbenõuetega arvestada vaid juhul, kui vastavad nõuded on juba eelnevalt välja töötatud. Muuhulgas on soovitatav kehtestada järgnevad ettekirjutused:

- ABAP-Code peab alati kontrollima volitusi.
- ABAP-Code-i kasutatavad volitusobjektid ja isiklikult loodud volitusobjektid tuleb dokumenteerida ning lisaks tuleb need profiili generaatori jaoks tehinguga SU24 sisse töötada (vt M 2.342 SAP pääsuõiguste planeerimine).
- Java-Code-i rakendatavad teenused tuleb dokumenteerida.
- Java-rakenduste puhul tuleb dokumenteerida nn *Security Constraints* jaoks vajalikud rollid ja ettekirjutused (st rollid, mis on hädavajalikud rakenduste funktsioonidele ligipääsemiseks).
- ABAP-programmide puhul tuleks oma tarkvaraarenduste kontrollimiseks, muuhulgas nende turvalisuse ja SAP nimeandmise põhimõtete järgimise kontrollimiseks kasutada *ABAP Code Inspector* -it (*Transaktion SCI* -d). Eriti

kehtib see neil juhtudel, kus ABAP-programmide turvalisuse kontrollimiseks kasutatakse vaid enda loodud tarkvaraarendusi.

Kolmandate osapoolte poolt loodud tarkvara turve

Kolmandate osapoolte poolt loodud tarkvara tohib SAP süsteemi installeerida alles pärast põhjalikku vastuvõtuprotseduuri. Vastuvõtuprotseduuri käigus tuleb läbi viia ka turvakontrollid. Turbealased nõuded peavad olema detailselt välja toodud vastavas kohustuste nimekirjas. Ainult niimoodi on võimalik tagada rakenduste soovitud turvalisus.

Täiendavad kontrollküsimused:

- Kas tarkvara arendamisprotsessidesse on integreeritud ka turbeaspektid?
- Kas tarkvaraarendajatele edastatakse asjakohased turbealased ettekirjutused?
- Kas tarkvara installeeritakse alles pärast vastuvõtuprotseduuri läbimist, millega kaasneb muuhulgas ka turbeaspektide kontrollimine?

M 2.350 SAP süsteemi likvideerimine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator

Võttes vastu otsuse loobuda SAP süsteemi kasutamisest, kuna see asendatakse nt uuema süsteemiversiooniga, mis töötab uuel riistvaral, tuleb arvestada järgnevalt toodud punktidega. Rakendatavad meetmed peavad suutma tagada, et potentsiaalsel ründajal ei oleks võimalik kasutusest kõrvaldatud SAP süsteemi identiteeti oma huvides kurjasti ära kasutada. Kasutuselt kõrvaldamisega seotud protseduurid peavad seega tagama, et likvideeritava SAP süsteemi identiteet saaks kustutatud ja süsteem ise kasutuskõlbmatuks muudetud.

Andmekandjate kustutamine / utiliseerimine

Kõikide puudutatud arvutite andmekandjad tuleb enne taaskasutusse võtmist turvalisel moel kustutada (vt M 2.167 Andmete kustutamine või hävitamine). Ka riistvara utiliseerimise puhul tuleb tagada, et see vastaks kõigile turvanõuetele (vt M 2.13 Tundlike ressursside jäljetu hävitamine *)*.

Süsteemi kustutamine SAP kooslusest

Reeglina kasutatakse SAP süsteemi erinevate SAP süsteemide koosluses. Seetõttu sisaldavad ka ülejäänud süsteemid andmeid likvideeritava süsteemi kohta. Kõik viited likvideeritavale süsteemile tuleb allesjäänud SAP süsteemides ja komponentides kustutada. Muuhulgas on sellest puudutatud järgnevad valdkonnad:

- Identiteedid (st tehnilised kasutajad), mille all likvideeritav süsteem teostab oma juurdepääse
- Usaldussuhted
- Sihtkohad
- Transportsüsteemi konfiguratsioonid
- Tsentraliseeritult toimiva kasutajahalduse konfiguratsioonid
- Süsteemiseire (*Monitoring*) konfiguratsioonid

Siinkohal tuleb arvestada, et asjakohaseid viiteid võivad sisaldada ka väliste partnerite süsteemid. Seetõttu peab kasutuselt kõrvaldamise protsess muuhulgas hoolitsema ka selle eest, et vajalikud protseduurid viidaks läbi ka väliste koostööpartnerite juures.

Süsteemi kustutamine võrgukooslusest

Kustutada tuleb kõik võrgu- ja operatsioonisüsteemi tasandi viited. Muuhulgas on sellest puudutatud järgnevad valdkonnad:

- DNS-sissekanded,
- Tulemüüri reeglid,
- SAPGui/SAPLogon konfiguratsioonid (*System Lists*),
- Sissekanded failides „host“ ja „services“.

SAP Logon jaoks saadaolevate süsteemide nimekirjade puhul, mis salvestatakse faili *saplogon.ini* , on soovitatav kasutada tsentraalselt toimivat haldust ja vastav fail klientidele uuesti laiali jagada.

Täiendavad kontrollküsimused:

- Kas kõik SAP süsteemi hetkel kehtivad viited on dokumenteeritud?
- Kas kõikidel andmekandjatel olnud andmed on kustutatud turvaliselt?
- Kas väliseid partnereid on SAP süsteemi kasutuselt kõrvaldamisest informeeritud?

M 2.351 Salvestisüsteemide planeerimine

Algatamise eest vastutavad: asutuse/ettevõtte juhtkond, infoturbespetsialist

Rakendamise eest vastutavad: infoturbespetsialist, IT-juht

Põhjapaneva otsuste tegemine, millise salvestilahenduse peaks asutus endale valima, eeldab vajaduste analüüsi. Esmalt tuleb välja selgitada, milliseid tulevasi rakendusi peaks salvestilahendus suutma toetada ning millist olemasolevat riistvara soovitakse uue salvestilahendusega kas täiendada või asendada.

Olulisemad võrdlusaspektid on siinkohal käideldavusele, jõudlusele ja mahule esitatavad nõuded. Tavapäraste käideldavusnõuete korral tuleks täiendavalt välja selgitada, kui keerulist süsteemi on asutus suuteline käitama. SAN-süsteemide kasutuselevõtuga kaasneb ka uue baastehnoloogia juurutamine. Seetõttu tuleb arvestada, et sellise tehnoloogia kasutuselevõtu planeerimine ja selle juurutamine on küllaltki töö- ja ajamahukas. Juhul kui salvestisüsteemi hakatakse kasutama virtualiseeritud serverikeskkondades, tuleb arvestada nt täiendavate teguritega nagu WWN- ja võrguaadresside määramine, mis tekitab samuti tööd juurde.

NAS-lahendused on välja töötatud põhimõttel, et neid oleks võimalikult lihtne integreerida juba olemasolevasse IT-keskkonda ja need keskenduvad failipõhiste juurdepääsude kasutamisele. Seetõttu oleks neid mõistlik kasutada juhtudel, kus faile ja failipõhiseid rakendusi on tarvis konsolideerida kõrgema kvaliteediga, kuid siiski pigem kergesti hallatavate salvestilahendustega.

Neil juhtudel, kus serverite salvestiruumi on tarvis kiiresti asendada tsentraalse salvestiga, kuid kus pikemas perspektiivis tuleb arvestada, et käideldavusele seatavad nõuded aina suurenevad, võib kaaluda selliste salvestisüsteemide rakendamist, mis kujutavad endast SAN- ja NASsüsteemide kombinatsiooni. Selliseid salvestisüsteeme on võimalik esimeses väljaehituse astmes käitada (väga kõrgekvaliteediliste) NAS-lahendustena. Sisemiste komponentide juurdelisamisega saab neid muuta täiendavate serverite ning vajaduse korral ka liiasusega salvestusvõrkude SAN-lahendusteks.

Juhul kui vaadeldavate süsteemide hulgast on mõne süsteemi puhul juba ette teada, et selle käideldavusega seotud turbevajadus võib lähimas tulevikus muutuda kõrgeks või koguni väga kõrgeks, mistõttu oleks tarvis erinevates asukohtades rakendada liiasusega salvestisüsteeme, tuleks kasutusele võtta SAN-tehnoloogia. Neil juhtudel tuleb ilmtingimata hoolitseda selle eest, et salvestisüsteem toetaks SAN-protokollide kasutamist. Sellise tehnoloogiaga on võimalik üles ehitada täies mahus liiasusega ja kõrge käideldavusega salvestilahendusi.

Asutuse valik, millega otsustatakse juurutada vastavalt kas NAS- või SAN-salvestilahendus, tuleb sobival viisil dokumenteerida. Seepärast on soovitav juba salvestilahenduse planeerimise ja kontseptsiooni koostamise etapis koostada esmalt üldkontseptsioon. Üldkontseptsioonis tuleks kirjeldada kõiki selles meetmes kajastatavaid valdkondi nagu salvestilahendusele esitatavad nõuded, riistvara ja tarnijate valimine, taristu planeerimine jmt. Samuti tuleb salvestilahenduste kasutamiseks koostada asjakohane turvakontseptsioon.

Planeerimise etapis tuleb muu hulgas kindlaks määrata, kuidas hakatakse loodavat salvestilahendust integreerima asutuse tööprotsessidega. Nõnda toimides saab juba piisavalt varakult aimu sellest, kas ja kuidas tuleb tööprotsesse kohandada või muuta. Sellega on võimalik kui mitte vältida, siis vähemalt lühendada juurutamise ja kasutamise etapis tekkivaid viivitusi.

Salvestilahenduse planeerimise etapis tuleb kehtestada ka reeglid, kuidas hakatakse ümber käima tarkvara erinevate versioonidega juhul, kui tarkvara versioone ei hallata seni veel tsentraalselt. Nõnda saab vältida kõikvõimalikke ühilduvusprobleeme ja asutus saab endale olukordades, kus saavad teatavaks uued turvaaugud või vead, luua kiiresti enda süsteemist ülevaate ja otsustada, kas uutele turberiskidele on tarvis reageerida.

Riistvara valimine

Salvestilahenduse valikul on olulised järgmised nõuded:

- rakenduste jaoks hetkel vajaminev ja tulevikus eeldatav salvestiruum (mahtuvusnõuded);
- rakenduste salvestamiskiirusega seotud nõuded (jõudlusnõuded);
- rakenduste tõrkekindlusega seotud nõuded (käideldavusnõuded);
- andmete konfidentsiaalsuse ja tervikluse tagamisele esitatavad nõuded, millest lähtutakse võimalike riistvarapõhiste krüpteerimistehnoloogiate juurutamise üle otsustamisel (turbenõuded);
- Secure-Operating-süsteemide kasutamise võimalus. Sellised spetsiaalsed operatsioonisüsteemid võimaldavad lihtsustada turbekonfiguratsioone ja kahandada seeläbi nii vigade tõenäosust kui ka käsitsi tehtavate haldustööde mahtu.

Salvestilahenduste planeerimiseks on oluline välja selgitada, milliste tööprotsesside ja rakenduste jaoks on salvestilahendust tarvis kohe praegu ja milline saab olema salvestisüsteemi prognoositav kasutusvaldkond tulevikus, st millised on salvestisüsteemile pikas perspektiivis esitavad nõudmised seoses süsteemi jõudluse, tõrkekindluse ja salvestusmahu kasvuga. Prognoosi koostamisel tuleks arvestada, et igasugused hinnangud tuleks anda võimalikult suure varuga. Kogemused näitavad ikka ja jälle, et isegi väga suure varuga planeeritud salvestusmahud osutuvad juba lühikese aja möödudes tegelikest vajadustest palju väiksemateks.

Salvestilahenduste planeerimisel tuleb arvestada ka andmevarunduse valdkonnaga, sest vajamineva salvestiruumi prognoos mõjutab otseselt ka andmevarunduskeskkonna ülesehitust. Siinkohal tuleb tagada, et pärast salvestilahenduse väljaehitamist ja andmevarundusseadmete ühendamist jääks andmete varundamisele ja varundatud andmete tagasipaigaldamisele kuluv aeg sellistesse piiridesse, mis vastaks asutuse allüksustes kehtestatud käideldavusnõuetele.

Rakendustele esitatavad nõuded

Ühte ja sama salvestilahendust kasutab andmete salvestamiseks reeglina korraga palju servereid ja rakendusi. Salvestilahendusele esitatavad käideldavus-, terviklus- ja konfidentsiaalsusnõuded määratakse kindlaks kõige suurema turbevajadusega rakenduse alusel.

SAN-süsteemi tehnilist teostust planeerides tuleks kontrollida, kas asutuses kehtivad käideldavusnõuded vastavad tingimustele, mille puhul võiks vähemalt planeerimise etapis kaaluda ka avariikindla SAN-süsteemi juurutamist (M 2.354 Kõrge käideldavusega SAN-konfiguratsiooni kasutamine).

Juhul kui asutus kasutab rakendusi, mille andmetele seatakse eriti kõrgeid konfidentsiaalsusnõudeid, tuleb planeerimise etapis arvestada, et neid andmeid on tarvis kaitsta krüpteeringuga nii SAN-süsteemis transportides kui ka andmekandjates. Nende teguritega tuleb arvestada hilisema turvaanalüüsi ja riskianalüüsi raames.

Toodete, tootjate ja tarnijate valimine

Erinevast põlvkonnast või erinevatelt tootjatelt pärit toodete kasutamine aitab üldjuhul suurendada süsteemi keerukust, kuid olenevalt olukorrast võib sellega kaasneda ka probleeme. Seetõttu on soovitatav püüelda siiski süsteemide homogeensuse suunas. Ka koostööpartnerite valikul tuleks arvestada, et paigaldamisel, katsetamisel ja käitamisel tekkivaid probleeme suudetakse reeglina palju kiiremini ja efektiivsemalt lahendada siis, kui nendega tegeleb ainult üks kindel teenuseosutaja.

Teiselt poolt jällegi võib liiga suur sõltuvus kindlatest tootjatest või tarnijatest tekitada ka probleeme. Toodete valimisel mängivad olulist rolli tihti ka majanduslikud aspektid. Kõik need asjaolud tuleks enne uute toodete soetamist läbi kaaluda. Täiendavalt tuleks arvestada ka sellega, et paljud tootjad garanteerivad enda tootelahenduste laitmatu toimimise ja vajaliku tugiteenuse ainult teatud kindlate riist- ja tarkvarast koosnevate kombinatsioonide korral. Seetõttu tuleks uurida toodetele väljastatud sertifikaate, et saada teavet, millised on toodetele sobivad kasutuskeskkonnad ja tutvuda tootjapoolsete kinnitustega toodete

ühilduvuse ja koostalitlusvõime kohta. Tootjad avaldavad sellekohast teavet nn ühilduvusmaatriksites (Compatibility Matrix).

Salvestikomponentide tootjad pakuvad enda tugiteenuseid sageli läbi kaughoolduse juurdepääsude. Tootjaid valides tuleks välja selgitada, millised on tootjate tehtavate hooldustööde tingimused. Kui hooldustöödeks kasutatakse kaughooldust, peab asutus tagama, et kaughoolduse juurdepääs oleks turvaline (M 5.33 Kaughoolduse turve). Eriti hoolikalt tuleks tutvuda õigusalaste raamtingimustega selles riigis, kust kaughooldust tegema hakatakse, sest võib juhtuda, et pääsuandmed võidakse edastada ka õiguskaitseorganitele, nt luureagentuuridele, ilma et SAN-süsteemide käitajat sellest teavitataks. Täiendavate spionaaži vältimist puudutavate küsimustega pöörduge vastavate riiklike organite poole.

Tsentraalsete haldussüsteemide kasutamine

Ühtse haldusrakenduse kasutamine ressursside tsentraalseks seireks ja haldamiseks lihtsustab olulisel määral salvestilahenduste haldamist. Eriti möödapääsmatu on tsentraalselt toimiva haldussüsteemi kasutamine suurte salvestilahenduste puhul, sest nõnda on haldamine kõige efektiivsem. Varem oli tsentraliseeritult toimiva halduse juurutamine erinevate toodetega kaasnenud tootjapoolsete haldusmehhanismide tõttu heterogeensetes salvestuskeskkondades küllaltki keeruline.

Tänu SNIA (Storage Network Industry Association) väljastatud standardile SMI-S (Storage Management Initiative Specification) on salvestitootjatel nüüdsest oma tooteid palju lihtsam tsentraalselt toimiva haldussüsteemi alla koondada. Samuti võimaldab SMI-S läbi heterogeensete võrkude kasutada baasfunktsioone nagu Storage Provisioning ja LUN Masking.

SMI-S-i versioon 1.6 sisaldab hulgaliselt turvaseadistusi, mille peamine eesmärk on kaitsta autentimismehhanisme ja konfidentsiaalsust. Täiendavate turbefunktsioonide väljatöötamise kallal töötatakse. SNIA on avaldanud ka SMI-S-i seniste versioonide põhjaliku tehnilise dokumentatsiooni.

Täiendava materjalina on SNIA avaldanud teavet ka selle kohta, kuidas saab väljavalitud tootja pakkuda SMI-S-i nõuetele vastavat riist- ja tarkvara. Seda teavet tuleks salvestilahenduse planeerimisel ka kasutada.

Juhtudel, kus planeeritakse SMI-S-i juurutamist, tuleks haldussüsteemi ja salvestilahenduse vahelise side turvamiseks rakendada vähemalt järgmisi turvamehhanisme:

- **krüpteering**: side täielik krüpteerimine turvaliste krüpteerimismehhanismi-

dega (vt meede M 2.164 Sobiva krüptoprotseduuri valimine)

- **autentimine**: soovitatakse kasutada autentimisprotseduuri HTTP Digest Access Authentication. Seevastu autentimisprotseduuri HTTP Basic Authentication tuleks kasutada üksnes juhtudel, kus autentimist turvatakse juba kas HTTPS-i või mõne krüpteerimismeetodiga.

Võrguühenduse planeerimine

SAN-süsteemi sisekomponentide omavaheliseks ühendamiseks tuleks kasutada Fibre-Channel-võrku. Ka siis, kui kasutatakse iSCSI-d, tuleks töökindluse tagamiseks luua siiski eraldi võrk.

Juhtudel, kus NAS-lahenduste või SAN-komponentide (salvestusseadmed, SAN-kommutaatorid jmt) haldamiseks ja kontrollimiseks on tarvis need ühendada LAN-i, tuleks vastavat LAN-i käitada eraldi haldusvõrguna. **Nõnda arvestatakse järgmiste turbe-eesmärkidega:**

- asjasse mittepuutuvatel kasutajatel puudub haldusandmete ja haldustegevuste luuramise võimalus.
- võimalik on kasutada protokolle (eriti SNMP versiooni 1), mille puhul on küll teada, et need ei ole turvalised, kuid alternatiivide puudumise tõttu tuleb neid käitamise kontrollimiseks siiski kasutada.
- õiguste haldamine muutub sellise võrgu piires palju ülevaatlikumaks.
- spetsiaalseid kontrollimeetmeid nagu Intrusion-Detection-süsteeme on võimalik rakendada palju ülevaatlikumalt ja efektiivsemalt.

Ebaturvalisi protokolle tuleks vältida ja nende asemel kasutada SNMP-d alates versioonist 3. Praktikas kasutatakse siiski sageli veel süsteeme, mis ei toeta versiooni 3 kasutamist ja seetõttu ollakse sunnitud kasutama protokolli vanemaid versioone. Neil juhtudel tekivad aga täiendavad ohud, mida peavad vastutavad isikud endale teadvustama. Neid ebaturvalisi protokolle tuleks kasutada üksnes muudest võrkudest eraldatud ja turvatud haldusvõrkudes. Samas ei tohiks ka neil juhtudel vastavaid protokolle rakendada mitte püsiva, vaid ajutise lahendusena ning pikas perspektiivis tuleks hakata kindlasti kasutama üksnes selliseid seadmeid, mis toetavad ka SNMP-protokolle alates versioonist 3.

Taristu

Enne SAN-lahenduse soetamist ja kasutuselevõtmist tuleb planeerimisel arvestada ka mitmete taristut puudutavate teguritega.

SAN-süsteemi komponentide füüsiliseks asukohaks tuleb valida piiratud juurdepääsuga serveriruum või arvutuskeksus. Serveriruumide taristu turvet käsitlevaid soovitusi leiate moodulist B 2.4 Serveriruum ja arvutuskeskuste kohta moodulist

B 2.9 Arvutuskeskus .

Üldise, süsteemide paigalduskoha turbe kõrval tuleks tähelepanu pöörata ka sellele, kas paigalduskohas on olemas salvestilahenduse käideldavusnõuete tagamiseks vajalik kliimaseade ja elektritoide. SAN-süsteemi üksikute komponentide paigaldamise asukohad tuleb hoolikalt läbi mõelda. Näiteks tuleks leida sobivad asukohad, kuhu oleks nii turbe kui ka kasutusmugavuse seisukohalt kõige mõttekam üles seada andmevarundusseadmed, mis eeldavad kas regulaarset või perioodilist käsitsi sekkumist (nt lindikassettide väljavõtmist või vahetamist).

Samuti tuleks ruumide peale laiali jagatud SAN-konfiguratsiooni puhul kontrollida, kas kõikidele seadmetele on võimalik tagada katkematu elektritoide. Tavalisse jaotusruumi võib olla tarvis paigaldada SAN-kommutaator, mis võimaldaks ühendada väljaspool asuvaid servereid. Sellisel juhul tuleb ka vastav jaotusruum, nagu ka kõik serverid, varustada UPS-i ja avariitoiteallikaga. Soovitusi SAN-süsteemide hädaolukordadeks ettevalmistuse kohta leiate meetmest M 6.98 Salvestisüsteemide valmisolek hädaolukorraks .

Protsessid

Salvestilahendus tuleb integreerida keskse IT-komponendina kõikide IT-juhtimisprotsessidega. Eriti oluline on kohandada NAS- või SAN-süsteemide käitamine asutuse igapäevaste tööprotsesside seire- ja eskalatsiooniprotseduuridega. Eraldi protseduuridena tuleb juurutada tootjapoolsed seiret ja tööprotsessside käigushoidmist võimaldavad teenused. Selle käigus tuleb alati arvestada IT-turvapoliitika ja muude asutuses kehtestatud ettekirjutustega.

Personal

Enne kasutuselevõttu tuleks välja selgitada, kui palju ja milliste teadmistega töötajaid läheb tarvis salvestilahenduse käitamiseks. Juhul kui vajalike teadmistega personali ei ole piisavalt, tuleb vajalike koolitustega alustada õigel ajal.

Kontrollküsimused

- Kas vajaduste analüüsiga on välja selgitatud, millised on käideldavus-, jõudlus- ja mahtuvusnõuded praegu ja millised on need lähitulevikus?
- Kas asutuse valik, millega otsustati kasutusele võtta kas NAS- või SAN-salvestilahendus, on sobival moel dokumenteeritud?
- Kas salvestilahenduste kasutamise jaoks on koostatud turvakontseptsioon?
- Kas salvestisüsteemidele vajalikku taristut on analüüsitud ja kas see on kohandatud sobivaks?
- Kas NAS- või SAN-süsteemi käitamine on asutuse igapäevaste tööprotsesside seire- ja eskalatsiooniprotseduuridesse sobivalt sisse töötatud?

M 2.352 Kohtvõrgu salvesti (NAS-süsteemi) turvapoliitika väljatöötamine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT-turvaosakond

Rakendamise eest vastutavad: IT-turvaosakond

NAS-süsteem kui toimingute ja tööprotsesside tsentraalne andmesalvestuskoht on iga institutsiooni jaoks määrava tähtsusega. Süsteemi turvalist ja nõuetekohast käitamist saab tagada ainult siis, kui seadmete paigalduste asukohad, haldamine ja käitamine on integreeritud olemasolevatesse turvatehnilistesse nõuetesse. Kõige olulisemad antud valdkonna turvatehnilised nõuded ja eesmärgiks seatav turbeaste tekivad organisatsiooniülese turvapoliitika baasil ning need tuleks sõnastada ja kokku võtta eraldi NAS-süsteemide turvapoliitikana. Eesmärgiks on üldise ja üldkehtiva turvapoliitika nõuete konkretiseerimine NAS-süsteemide tarbeks. NAS-süsteemide turvapoliitikat koostama hakates tuleks esmalt läbi töötada M 2.316 Serveri turvapoliitika kehtestamine . Nimetatud meetmes kirjeldatakse serverifunktsiooniga IT-süsteemide üldisi turvameetmeid. NAS-süsteemide turvapoliitika loomiseks on tarvis välja tuua NAS-süsteemi planeeritava kasutusvaldkonna spetsiifika. NAS-süsteemide üldise haldus- ja konfigureerimisstrateegia valikul („liberaalne“ või „piirangutega“) tuleks lähtuda töödeldava info ja sellele ligipääsu võimaldavate rakenduste kaitsevajadusest. Lisaks tuleb NAS-süsteemide turvapoliitika väljatöötamise käigus pöörata erinevates etappides tähelepanu järgnevatele punktidele:

- Installeerimist ja konfigureerimist puudutavad nõuded peavad jääma kooskõlla meetmega M 4.274 Salvestisüsteemide turvaline aluskonfiguratsioon). Sellega seoses on tarvis välja töötada täiendavad protseduurid ja ettekirjutused:
- Välja tuleb töötada esmakordse installeerimise protseduur, mis tuleb ka dokumenteerida. Juhul kui esmapaigalduse teeb tootjafirma või tarnija, tuleb lasta endale saata vastav dokumentatsioon.
- Kui lahendus näeb ette kaughooldust, mida teostab kas tootja või teenusepakkuja, tuleb koostada kaughooldust käsitlevad organisatsioonilised ja tehnilised eeskirjad.
- Koostada tuleb juurdepääsude kontrollimise kontseptsioon. NAS-süsteemide puhul toimub see reeglina vastavate pääsuloendite (Access Control Lists) abil. Juurepääsude täiendava kaitse tagamiseks võib rakendada ka nn Storage Security Appliances, mis lülitatakse läbipaistvate proksidena klientide ja NASi vahele.
- Juhul kui NAS-süsteem kasutab integreeritud veebiserverit ka muudel otstarvetel kui ainult siseringi konfigureerimistööriistana, tuleb takistada selle rakendamist erineva usaldusväärsusega võrgutsoonides. NAS-süsteemi on lubatud nt kasutada samaaegselt nii intraneti failiserverina kui ka intraneti veebiserverina. NAS-süsteemi ei tohi kasutada samaaegselt intraneti failiserveri ja veebiserverina.
- NAS-süsteemide turvapoliitika peab sõnastama turvalise haldamise ja turvalise käitamise nõuded (vt M 4.275 Salvestisüsteemide turvaline kasutamine).

- Sõltuvalt kasutusvaldkonnast tuleb kindlaks määrata, kuidas kasutatakse krüpteeringut (standardid, võtmete pikkused).
- Välja tuleb töötada käitamiseks ja hoolduseks sobilike tööriistade kasutusnõuded ja ettekirjutused integreerimiseks olemasoleva võrguhaldussüsteemi alla (vt M 2.359 Salvestisüsteemide seire ja haldamine).
- Välja tuleb töötada tarkvara uuendamise ning konfiguratsiooni muutmise volitused ja protseduurid. Muudatused tuleb dokumenteerida.
- NAS-süsteemi kasutamine tuleb sisse töötada institutsiooni viirusetõrjekontseptsiooni, st tuleb luua reeglid, mille alusel toimub viirusetõrjetarkvara installeerimine ja konfigureerimine ning varustamine digitaalallkirjade täienditega.
- Välja tuleb töötada asjakohane andmevarunduskontseptsioon (vt B 1.4 Andmevarunduspoliitika), mis lähtub NAS-süsteemile kehtestatud turbeastmest ning mis tuleb viia kooskõlla organisatsiooniülese andmevarunduskontseptsiooniga.
- Turvaintsidentide lahendamiseks vajalike eeskirjade väljatöötamisel tuleks lähtuda moodulist B 1.8 Turvaintsidentide käsitlus . Sellel lisaks on tarvis:
- Koostada eeskirjad töötõrgetele ja tehnilistele vigadele reageerimiseks (kohalik tugi, kaughooldus)
- Koostada eeskirjad spetsiifiliste turvaintsidentidega ümberkäimiseks (nt pahavara, volitamata juurdepääsud, ootamatult kõrge CPU-ressursside kasutus),
- Koostada NAS-süsteemide avariiplaanid, milleks tuleb lisaks integreerimisele organisatsiooni üldise avariiplaani alla arvestada veel ka M 6.98 Salvestisüsteemide valmisolek hädaolukorraks .

NAS-süsteemide turvapoliitika peab olema kättesaadav kõigile asjaosalistele. Seda tuleb regulaarselt uuendada.

Täiendavad kontrollküsimused:

- Kas NAS-süsteemide kasutamise kohta on koostatud vastav turvapoliitika?
- Millal viimati uuendati turvapoliitikat?
- Kas turvapoliitika kirjeldab NAS-süsteemide sisseseadmise, käitamise ning tõrgete kõrvaldamise nõudeid?

M 2.353 SAN-salvestivõrgu turvapoliitika väljatöötamine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT-turvaosakond

Rakendamise eest vastutavad: IT-turvaosakond

SAN-süsteem kui teatud üksikute või ka paljude toimingute ja tööprotsesside tsentraalne andmesalvestuskoht on iga institutsiooni jaoks määrava tähtsusega. Süsteemi turvalist ja nõuetekohast käitamist saab tagada ainult siis, kui SAN-süsteemide planeerimine, paigalduste asukohad, haldamine ja käitamine on integreeritud olemasolevatesse turvatehnilistesse nõuetesse. Peamised turvatehnilised nõuded ja eesmärgiks seatud turbeastme nõuded tulenevad tervet organisatsiooni hõlmavast turvapoliitikast ning nende nõuete rakendamiseks ja täpsustamiseks tuleks antud kontekstis välja töötada eraldi spetsiaalne turvapoliitika. Turvapoliitikaks vajalike asjakohaste nõuete väljatöötamisel tuleb aluseks võtta SAN-süsteemi salvestatavate andmete kaitsevajadusi kajastav dokumentatsioon. Ainult vastava dokumentatsiooni abil on võimalik välja selgitada andmetele kehtivad erinevad käideldavus-, terviklus- ja konfidentsiaalsusnõuded ning tuvastada vajamineva tehnilise ja organisatoorse ressursi maht. Kuna SAN-süsteemide jaoks on tarvis luua eraldiseisev võrk, tuleb SAN-süsteemide turvapoliitika väljatöötamisel esmalt lähtuda meetmest M 2.279 Marsruuterite ja kommutaatorite turvapoliitika koostamine . Nimetatud meetmes tutvustatakse üldisi turvameetmeid IT-komponentide jaoks, mis võimaldavad sisevõrgus juurdepääsu andmetele või teistele süsteemidele. Täiendavad teemad, millele tuleb SAN-süsteemi turvapoliitika väljatöötamise raames tähelepanu pöörata, on muuhulgas järgmised:

SAN-süsteemi planeerimist puudutavad ettekirjutused:

- Välja tuleb töötada ettekirjutused tehnilise infrastruktuuri tarbeks, mille alla seatakse üles vastavad SAN-süsteemid. Ruumide infrastruktuur, kuhu SAN-süsteemi komponendid paigaldatakse, peab olema nende käitamiseks sobiv, et tagada SAN-süsteemi käideldavusnõuete täitmine.
- Tuleb koostada väliste töötajate poolt (hoolduse eesmärgil) kasutatavate juurdepääsude reeglid. Kuna teenusepakkujatega sõlmitavates SAN-komponentide seire- ja hooldusleping utes nõutakse reeglina salvestisüsteemi otsest ühendust kas tootja või teenusepakkuja seiresüsteemiga, tuleb kehtestada reeglid selliste juurdepääsude kontrollimiseks ja logimiseks.
- Juhul kui käideldavusele seatakse väga kõrged nõuded, tuleb nõuda avariikindlate SAN-konfiguratsioonide kasutamist. Juhul kui on tarvis tagada SAN-süsteemi eriti kõrge käideldavus, tuleb välistada võimalikud veaallikad (*Single Points of Failure, SPoF*), mis võiksid avarii korral endaga kaasa tuua terviksüsteemi avarii. Niisuguse konfiguratsiooni kasutamist tuleks toetada spetsiaalsete testimissüsteemidega, mille peal oleks võimalik läbi proovida kõik muudatused ja tarkvaratäiendid.

Administraatorite tööd puudutavad ettekirjutused:

- Dokumenteerida tuleb põhimõtted, mille alusel antakse administraatoritele SAN-komponentide ja terviksüsteemi haldamisvolitused. Kui võimalik, tuleks välja töötada töörollide jaotuse kontseptsioon.
- Koostada tuleks erinevad administraatorite rollid, millele antakse vajalikud volitused vastavalt nende tööülesannetele. Eriti oluline on miinimumini piiratud volituste andmine rutiinsete süsteemihaldusülesannete (nt *Backup* -i) puhul. Administraatorite kasutajanimed seotakse konkreetsete rollidega. Võimalike vigade vähendamiseks tohib administraatori kasutajanime alt tööd teha vaid siis, kui see on ilmtingimata vajalik.
- Administraatorite juurdepääse tuleb kaitsta vähemalt tugevate paroolidega, vajadusel ka spetsiaalsete, kasutajate autentimist võimaldavate kaitsemeetmetega.
- SAN-süsteemide haldamiseks ja kontrollimiseks vajalikke administraatorite ning revidentide juurdepääse tuleks lubada kas ainult kohapeal läbi otseühendusega konsooli, läbi eraldiseisva haldusvõrgu või läbi krüpteeritud ühenduse. SAN-ressursside juurdepääse tuleb piirata, määrates kindlaks ligipääsetavad süsteemid, ning neid tuleks kontrollida nt turvalüüside abil.
- IT-süsteeme, mida rakendatakse halduskonsoolidena või revisjonide tarbeks tuleb kaitsta parimal võimalikul moel viiruste ja pahavara eest.
- Tööülesannete jaotamisega, ettekirjutuse ja kasutusreeglitega ning kõikide SAN-komponentide konfiguratsioonide dokumentatsiooni pideva täiendamisega tuleb tagada, et administraatoritel ei oleks võimalik SAN-süsteemides algatada protsesse või teha selliseid seadistusi, mille tagajärjel võiksid tekkida kas ebakõlad, avariid või andmekaod. Olulised muudatused tuleb dokumenteerida. Selleks on soovitatav juurutada muudatuste haldamise protseduur, mis võib põhineda nt ITIL-dokumendikogul.
- Kindlaks tuleb määrata muudatuste valdkonnad, mille puhul tuleb rakendada nelja silma printsiipi.

SAN-süsteemi installeerimise ja konfigureerimise nõuded:

- Dokumenteerida tuleb esmakordsel installeerimisel läbitav protseduur. Kuna paljudel juhtudel teeb esmapaigalduse kas tootjafirma või tarnija, tuleb lasta endale saata vastav dokumentatsioon.
- Pärast installeerimist tuleb kontrollida, kas *Default* -seadistustes esineb võimalikke turvariske, desaktiveerida LAN-liideste SAN-kommutaatorite ja salvestiseadmete ebaturvalised teenused ja kontrollida, kas standardsed kasutajanimed ja paroolid on muudetud.
- Funktsiooni „Süsteemikonsool SANi kasutamiseks“ rakendumisala tuleks piirata võimalikult vähestele seadmetele. Nende seadmete LANi kaudu töötavaid juurdepääsusid SAN-komponentidele tuleks lubada eranditult vaid krüpteeritud ühenduste kaudu. Selliste seadmete juurdepääsuõigusi omavate kasutajate ring tuleks hoida võimalikult väiksena. Konsooli kasutamise ja konfigureerimise reeglid ning juurdepääsuliikide piirangud tuleb dokumenteerida.
- Välja tuleb töötada reeglid, mis sätestavad dokumentatsiooni nõuetekohase koostamise, hooldamise ja dokumentatsiooni vormi (nt protseduurireeglid

administratiivsete ülesannetega seotud kasutajatunnuste loomiseks, kasutusjuhendid igapäevatöös vajalikele töö- ja kontrolliprotseduuridele).
- Ka SAN-süsteemi sees tuleks rakendada spetsiifilisi segmenteerimismeetodeid (vt M 5.130 Salvestisvõrgu (SAN-i) kaitse segmenteerimise abil). Sellega saavutatakse SAN-süsteemi koostisosade parem kaitse nii konfidentsiaalsuse kui ka konfiguratsiooni tervikluse ja süsteemi käideldavuse osas.

Turvalise käitamise nõuded:

- SAN-süsteemi haldus tuleb muuta turvaliseks seeläbi, et haldamiseks vajalikud juurdepääsud leiavad aset läbi spetsiaalsete ühenduste (st eraldiseisva haldusvõrgu, sõltuvalt olukorrast ka läbi salvestivõrgu enda).
- Vajadusel tuleb teha valik sobivate tööriistade hulgast, mis võimaldaksid SAN-süsteemi komponente käitada, hooldada ja integreerida olemasoleva võrguhaldussüsteemi alla. Nimetatud tööriistade jaoks tuleb välja töötada turvalise konfiguratsiooni nõuded. Võimalusel tuleks kasutada ainult krüpteeritud ühendusi ning mittevajalike liideste ja teenuste kasutamine tuleks tõkestada.
- Juhul kui soovitakse kasutada tootja poolt pakutavaid kaughoolduse või kaugseire võimalusi, tuleb välja töötada ettekirjutused, mis sätestaksid selleks vajalike juurdepääsude turvanõuded. Näiteks tuleks sätestada, kuidas peaksid aset leidma ühendused läbi VPNi või kuidas peaksid toimima otseühendused ning lisaks tuleks nõuda, et institutsioonile saadetaks antud tegevuste kohta mõistetaval kujul esitatud logiandmed.
- Üheselt tuleb kindlaks määrata töötajate volitused seoses tarkvaratäiendite laadimise ja konfiguratsiooni muudatuste sisseviimisega. Vastava protseduuri teostusviis tuleb dokumenteerida. Niipea kui on teada, et käideldavusele seatakse väga kõrged nõuded, tuleb nõuda, et muudatusi ja täiendeid kontrollitaks enne tootmissüsteemi installeerimist alati eelnevalt asjakohases testimissüsteemis.
- SAN-süsteemi käitamise raames tuleb logida kõik haldamisega seotud tegevused. Sellele lisaks tuleb koostada salvestisüsteemide haldamise ja seire kontseptsioon (vt M 2.359 Salvestisüsteemide seire ja haldamine).
- SAN-süsteemide andmevarundust puudutavad nõuded tuleb viia kooskõlla institutsiooni üldise andmevarunduse kontseptsiooniga (vt B 1.4 Andmevarunduspoliitika). Eriti kõrgete konfidentsiaalsusnõuete puhul tuleb siinkohal kindlaks määrata ka volitused seoses varukoopiate tegemisega.
- Kuna SAN-süsteemide töö on määrava tähtsusega, tuleb nende avariiplaan (vt M 6.98 Salvestisüsteemide valmisolek hädaolukorraks) sisse töötada üleorganisatsioonilisse avariiplaani.
- Vastutused ja protseduurid tuleb kindlaks määrata ka revisjonide ja auditite jaoks. SAN-süsteemide revisjon tuleb integreerida kõikehõlmava revisjoni kontseptsiooni alla.

Täiendavad kontrollküsimused:

- Kas SAN-süsteemide kasutamise kohta on koostatud vastav turvapoliitika?
- Millal viimati uuendati SAN-süsteemide turvapoliitikat?
- Kas turvapoliitikas on sõnastatud ka turbeaste?
- Kas turvapoliitika kirjeldab SAN-süsteemide sisseseadmise, käitamise ning tõrgete kõrvaldamise nõudeid?

M 2.354z Kõrge käideldavusega SAN-konfiguratsiooni kasutamine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT-turvaosakond

Rakendamise eest vastutavad: IT-turvaosakond, IT-juht

Juhul kui süsteemidel ja rakendustel, mis salvestavad oma andmeid SANsüsteemidesse, on seoses käideldavusega väga kõrge kaitsevajadus, tuleb kaaluda kõrgkäideldavust tagava SAN-konfiguratsiooni kasutamist. Mõiste „kõrgkäideldavus“ all peetakse siinkohal silmas suurt vastupanuvõimet potentsiaalsetele kahjulikele sündmustele, mida nimetatakse teisisõnu veel ka avariikindluseks (disaster tolerance).

Institutsioonis salvestatud andmete puhul tähendab see seda, et SAN-komponentidega ehitatakse üles selline salvestisüsteem, mis:

- Hoiab andmeid kahes eraldi asukohas.
- Tagab mõlema asukoha SAN-komponentide omavahelise ühenduse, kuid ei muuda süsteeme teineteisest sõltuvaks.
- Suudab tagada, et ühes asukohas tekkinud kahjustus ei too endaga kaasa teise asukoha süsteemikomponentide märkimisväärset funktsioonide langust.

Sellise arhitektuuri vajalikkuse üle saab otsustada järgmiste näitajate abil:

- Maksimaalne taaskäivitusaeg (ingl tihti RTO: recovery time objective), määrab kindlaks ajavahemiku, mis võib IT-süsteemil kuluda funktsioonide taastamiseks piisaval määral, et tagada igapäevatöös vajalike protsesside toetamine pärast seda, kui on leidnud aset mõni kahjutekitanud sündmus.
- Maksimaalne vastuvõetav andmekadu (ingl tihti RPO: recovery point objective).

Viimase kasutuskõlbliku ja tervikliku andmekogumi võrdlemisel andmekogumiga, mis on jäänud alles pärast kahju tekitanud sündmuse toimumist, saab leida „kaduma läinud töö“ hulga. Maksimaalne vastuvõetav andmekadu kirjeldab põhimõtteliselt taastamistööde mahtu või nende keerukust, mis jääb institutsiooni jaoks vastuvõetavatesse piiridesse.

- Puudutatud keskkond kirjeldab kahjutekitanud sündmuse ruumilist ulatust.

Asukoht jääb kasutuskõlblikuks vaid juhul, kui kahjutekitanud sündmus ei mõjuta mitte mingisugusel määral asukohas olevaid süsteeme.

SAN-salvestisüsteemid on kõrgkäideldavust pakkuvate IT-lahenduste võtmetehnoloogiaks. Piisava jõudlusega omavaheliste ühenduste abil on SAN-süsteeme võimalik paigutada erinevatesse ruumidesse ka väga suurte vahemaade taha, mis suudab kaitsta neid isegi väga laiaulatuslike mõjude eest. Suure jõudlusega omavahelisi ühendusi on võimalik kasutada maksimaalse andmekao minimeerimiseks.

Rakenduste maksimaalset seisakuaega seevastu on SAN-süsteemide konfiguratsioonidega võimalik mõjutada ainult väga vähesel moel. Kuna seisakuaega mõõdetakse eranditult kasutajate vaatevinklist, ei sõltu see mitte ainult salvestatud andmete käideldavusest, vaid ka kogu ülejäänud IT-infrastruktuuri (serverite, võrgu, arvutite) käideldavusest, mida SAN-komponendid andmetega varustavad.

Erinevad konfigureerimisvõimalused

SAN-süsteemide kõrgkäideldavuse tagamiseks on võimalik kasutada erinevaid konfiguratsioone.

Peegeldamine läbi serveri

Kõige lihtsam meetod SAN-süsteemi kõrgkäideldavuse saavutamiseks tuleb serverile, mis salvestab oma andmeid SAN-süsteemi, külge ühendada teine, eraldatud ruumis asuv salvestisüsteem. Kõik serverile kirjutatavad andmed salvestatakse mõlemas salvestisüsteemis. Antud lahenduse puuduseks on tõsiasi, et „Salvesti“ konfigureerimine toimub omakorda osaliselt serveril. Seetõttu toimub jällegi ka haldamine serverikaupa. Tsentraalset toimiva haldussüsteemi võimalustest tuleb sellise lahenduse puhul kahjuks loobuda. Lisaks on tarvis luua palju keerulisem juhtmestik kui teiste lahenduste puhul, sest kõik serverid tuleb ühendada mõlema salvestisüsteemiga. Lihtsustatult kokkuvõttes tuleb lisaks serveri ja salvestisüsteemi ühendusliinile luua ka veel teine liin, mis ühendab serveri otse eraldiseisvas ruumis asuva teise salvestisüsteemiga.

Replikeerimine

Replikeerimiseks on võimalik kasutada kas serverit või salvestisüsteemi. Serveri baasil toimivad lahendused pannakse reeglina tööle kas eraldi tarkvara, rakenduste või ka operatsioonisüsteemi abil. Sellised lahendused kasutavad kahjuks väga palju CPU, põhimälu ja ribalaiuse ressurssi. Salvestisüsteemi baasil toimiva replikeerimise puhul ühendatakse serverid salvestisüsteemiga, mis ühildab oma andmemahu kas täies ulatuses või vastavalt selle konfiguratsioonile eraldiseisvas ruumis asuva salvestisüsteemi andmemahuga.

Sünkroonne replitseerimine

Juhul kui kaks süsteemipaigalduse asukohta asuvad teineteisele piisavalt lähedal, võib kõne alla tulla ka andmete sünkroonne replikeerimine. Andmete sünkroonne replikeerimine tähendab, et iga serveri juurdepääsu puhul, mille käigus kirjutatakse serverile andmeid, loeb serveri otsene salvestusketas vastava protseduuri lõppenuks alles siis, kui ka teine, eraldiasuv salvestisüsteem on esimesele salvestisüsteemile saatnud kinnituse andmete eduka kirjutamise kohta. Serveri poolt vaadatuna muutuvad sellise lahenduse puhul kõvaketta kasutamist vajavad juurdepääsud aeglasemaks, kuna kirjutamisega tegeleb kaks kettasüsteemi ning protsessile lisandub signaali levimisele kuluv aeg, mil see liigub salvestisüsteemist asukohast A salvestisüsteemi asukohas B.

Asünkroonne replitseerimine

Andmete asünkroonse replikeerimise puhul hoolitseb salvestisüsteemide spetsiaalne tarkvara selle eest, et asukoha A salvestisüsteem edastaks muutunud andmed regulaarselt asukohas B paiknevale salvestisüsteemile. Sellega ühendatakse serveri külge salvestisüsteem, mis seda ei pidurda. Täiendavaks eeliseks on antud lahenduse puhul veel ka see, et ametiasutus või ettevõte ei ole enam sunnitud täpselt identseid salvestisüsteeme avariiolukorraks kahes

asukohas varuks hoidma. Põhiasukohas kasutatakse sellisel juhul suure jõudlusega süsteemi. Teises asukohas võib seevastu kasutada soodsama hinnaga süsteemi, millele vaatamata on ka võimaliku avarii puhul siiski tagatud kõikide põhiülesannete täitmine. Asünkroonse replikeerimise puuduseks on tõsiasi, et teises salvestisüsteemis on alati tegemist vanema andmehulga versiooniga kui põhisalvestisüsteemis. Andmekao suurus põhisüsteemi võimaliku avarii korral sõltub kasutatavast tehnoloogiast.

Salvestisüsteemide sünkroonne replikeerimine on mõttekas vaid neil juhtudel, kus on loodud ka liiasusega serverisüsteemid, mis suudavad käitamise otse üle võtta. Tõenäosust, et ühe asukoha salvestisüsteemi tabab täielik avarii, kuid sinna külge ühendatud (nt SAN-süsteemi) serverid ja võrgukomponendid jäävad sellest puudutamata, tuleb hinnata pigem väikeseks. Lisateavet replikeerimise kohta leiate meetmest M M 3.92w Salvestisüsteemide kasutamise põhiterminid .

Kõrgkäideldavust pakkuva SAN-konfiguratsiooni planeerimisel tuleb alustuseks läbi töötada kogu institutsiooni IT avariiolukordadeks valmisoleku kontseptsioon. SAN-süsteemi ja selle külge ühendatud süsteemide käideldavusnõuded tuleb kirjalikult fikseerida.

Kõrgkäideldava SAN-süsteemi planeerimine, mis arvestab institutsiooni riskipoliitika nõuetega, on alles esimene samm teel kõrgkäideldava lahenduse suunas. Samaaegselt tuleb tegelda ka kogu institutsiooni IT-keskkonna edasiarendamise planeerimisega ja avariiolukorraks valmisoleku planeerimisega. Kõrgkäideldav SAN-süsteem on mõttekas vaid juhul, kui ka serverid on taaskäivitamiseks valmis ning kui kasutajad saavad andmetele ligi pääseda läbi töökorras arvutustehnika ja korralikult toimiva võrgu.

Siinkohal tuleb arvestada, et kõrgkäideldavat SAN-süsteemi on tarvis toetada testimis- ja konsolideerimissüsteemiga. Kõrgkäideldavust pakkuva konfiguratsiooni ülesehitamisel ei tohi konfiguratsioonimuudatusi ja tarkvaratäiendeid mitte kunagi installeerida otse tootmissüsteemidesse. Institutsioon peab looma süsteemid, mille peal oleks võimalik kõiki muudatusi enne kasutuselevõtmist läbi testida. Ainult niimoodi on võimalik tagada, et administratiivsed sekkumised ei mõjuks igapäevastele tööprotsessidele negatiivselt.

Salvestite virtualiseerimine kõrge käideldavuse otstarbel

Kõrge käideldavusega salvesti virtualiseerimine võimaldab luua täieliku kõrge käideldavusega salvestilahenduse, mis suudab automaatselt reageerida tõrkeolukordadele.

Kõrge käideldavusega salvesti virtualiseerimine põhineb virtualiseerimisseadmel (appliance). Vastav seade võimaldab hallata salvesti kõiki osi tsentraalselt

ning see realiseeritakse kõrge käideldavusega salvestilahenduse jaoks nn klastrina. Klastrid ja salvestisüsteemid paigutatakse sealjuures tuleohutuse seisukohalt eraldi tsoonidesse. Valitav arhitektuur peaks suutma tagada, et andmed oleksid mõlemas salvestisüsteemis kogu aeg ühtlaselt olemas (peegeldamine). Seevastu salvestite virtualiseerimislahendus on üles ehitatud liiasusega ning ühe salvestisüsteemi tõrke korral töötavad teised seadmed (appliances) edasi.

Virtualiseeritud ja kõrge käideldavusega salvestilahenduse funktsioonide tööd tuleb enne kasutuselevõttu katsetada ja nende kasutamist hädaolukorraks ettevalmistuse raames ka harjutada (vt moodul B 1.3 Hädaplaanimine), et veenduda, kas see suudab tagada hädaolukordades piisava jõudluse. Katsetuste ja harjutamiste käigus tuleb erilist tähelepanu pöörata andmekadude tekkimise riskile. Katsetused ja harjutamine tuleb korraldada selliselt, et need ei kahjustaks asutuse andmeid.

Kontrollküsimused:

- Kas salvestilahendusele esitatavad kõrgkäideldavuse nõuded on fikseeritud kirjalikult?
- Kas replikeerimismehhanismid vastavad kõrgkäideldavuse nõuetele?
- Kas salvestilahenduse suure käideldavusega konfiguratsioon suudab täita eesmärgiks seatud käideldavusnõudeid?
- Kas asutusel on olemas katsetamis- ja konsolideerimissüsteem?

M 2.355 Salvestisüsteemi tarnija valimine

Algatamise eest vastutavad: IT-juht, ametiasutuse / ettevõtte juhtkond, infoturbespetsialist

Rakendamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, infoturbespetsialist, IT-juht

Pärast salvestisüsteemile esitatavate nõuete väljatöötamist tuleb leida sobiv tarnija. Võimalike tarnijate vahel valides tuleb pöörata tähelepanu palju rohkematele kriteeriumitele kui ainult riistvaralahendus ja selle hind.
Võimalikud valikukriteeriumid on järgmised:

tehnilised nõuded;
majanduslikud tingimused (soetamine liising, Storage-on-Demand-lahendused);
senised suhted tarnijatega;
seni tarnijatega sõlmitud raamlepingud;
laiapõhjalised tugiteenused.

Tuleb arvestada, et tarnija abi võib olla minna vähemalt käitamisega seotud probleemide lahendamisel ning päris kindlasti läheb abi tarvis ka riistvara hädaolukordade puhul. Seetõttu tuleb salvestilahenduste soetamise ja kasutuselevõtuga seotud tingimuste ja hinna kõrval arvestada ka pakutavate tugiteenuste ja nende tingimustega.

Hooldustingimused fikseeritakse tarnijaga kirjalikult teenusetasemeleppes (Service Level Agreements, SLA). Seetõttu peaksid kogutavad hinnapakkumised sisaldama lisaks riistvara ja tarkvara hindadele ka teavet vastavate SLA-de kohta, mis võimaldaks tulevasel kliendil juhul, kui kõne alla tuleb mitu tarnijat, tervikpakette omavahel võrrelda.

Selles kontekstis on oluline hinnata ka täiendavaid tegureid nagu pakkuja hooldusvõimekus, mis võib sõltuda nt sellest, kui palju on pakkujal erinevaid teeninduspunkte ja kus need asuvad. Valikul võib saada määravaks nt asjaolu, kas pakkujal on olemas tsentraalselt toimiv teabeliin või kas pakkujal on soovitud süsteemi jaoks ette näidata piisav arv asjakohaste sertifikaatidega töötajaid. Asutused peaksid muu hulgas arvestama ka meetmega M 2.356 Lepingud SAN teenusepakkujatega .

Juhtudel, kus salvestilahendusi mitte ei soetata, vaid nt liisitakse, tuleb lepingus fikseerida ka see, kuidas kantakse andmed lepingu lõppedes üle uutesse süsteemidesse ning millistel tingimustel ja millise tasu eest toimub kõikvõimalike muude tehniliste ja organisatoorsete küsimuste lahendamine.

Terviklahendustega, mille puhul soetatakse kõik vajaminev ühelt kindlalt tarnijalt, võivad kaasneda teatud eelised ja seda just keeruliste süsteemide puhul,

mistõttu tuleks seda ka eelistada. Paigaldamisel, katsetamisel ja käitamisel tekkivaid probleeme suudetakse reeglina palju kiiremini ja efektiivsemalt lahendada siis, kui nendega tegeleb ainult üks kindel pakkuja.

Erinevate tootjate komponentide kombineerimine võib salvestilahenduste soetamisel anda märgatava kulude kokkuhoiu. Samas on oluline analüüsida, kas esialgne kulude kokkuhoid jääb püsima, kui arvestada sinna juurde ka kõik juurutamise ja kasutamisega seotud kulud (aluskonfiguratsioon, proovikäitus, andmete üleviimine; hooldus, tugiteenus probleemide lahendamisel).

Kontrollküsimused

- Kas lepingus kirjeldatud teenused on üheselt mõistetavad ja mõõdetavad?
- Kas tarnijate valikukriteeriumid ja valiku tegemine on arusaadavalt dokumenteeritud?
- Kas lepingu lõppemine on täpselt reguleeritud?

M 2.356 Lepingud SAN teenusepakkujatega

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT-turvaosakond, IT-juht

Rakendamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT-turvaosakond, IT-juht

Ainult vähesed institutsioonid suudavad ise tagada SAN-komponentide tehnilise toe nii igapäevastes tööprotsessides kui ka avariiolukordades. Seetõttu peavad paljud tegema oma valiku sobivate tootjate ja tarnijate hulgast, mida edaspidi nimetame kokkuvõtlikult teenusepakkujateks. Järgnevalt kirjeldatud aspektid on mõeldud abivahendina ning neid võib kasutada lepingu koostamisel kontrollnimekirjana. Lepingupunktide liik, ulatus ja detailsus sõltuvad teenuse ostja käideldavusnõuetest ja ka konkreetse SAN-süsteemi keerukusest.

Teenusepakkujalt tuleks alati nõuda kõikide oluliste seaduste ja ettekirjutuste järgimist, eriti aga riikliku andmekaitseseaduse järgimist, samuti tuleks teenusepakkujat kohustada järgima kõiki organisatsioonilisi ja tehnilisi meetmeid, mis on seotud IT-turbega. Nimetatud meetmed peavad vastama vähemalt IT-etalonturbe tasemele ning vajadusel tuleks teenusepakkujat kohustada järgima veel ka täiendavaid teenuse ostja poolt kehtestatud turbenõudeid. Lisaks nimetatud üldistele kohustustele on soovitatav kõik kokkulepitavad teenused lepingusse kirja panna selliselt, et nende täitmist oleks võimalik nii hinnata kui ka kontrollida. Muuhulgas võib nt olla vajalik kokku leppida, et teatud probleemide ilmnemisel on teenusepakkuja kohustatud nelja tunni jooksul saatma kohapeale oma kvalifitseeritud töötaja. Selline, tellija konkreetseid vajadusi kajastav kokkulepe võib olla mõnikord palju kasulikum kui nn „Kuldklient“ kõik ühes teenus, kuna viimased võivad seada tellija poolt oodatud kvaliteeditingimustele palju ebameeldivaid erandeid nagu nt puhkepäevadel tugiteenus ainult telefoni teel. Lepingus peaks olema fikseeritud ka SAN-süsteemide avariikontseptsiooni koostamine. Eriti tuleb selgitada, kes vastutab erialase sisu eest ja millised on tellijapoolsed osaluskohustused. Siinkohal on tungivalt soovitatav, et teenuste tellija investeeriks piisavalt palju aega ettevalmistustöödesse ja selgitaks võimalikult täpselt välja oma vajadused. Lepingu tagantjärele täpsustamine ja täiendamine, mis osutub vajalikuks kirjeldatud teenuste erineva tõlgendamise tõttu, tähendavad tellijale sageli kulutuste märgatavat suurenemist.

Kui tegemist on teenuste väljasttellimisega, arvestage ka mooduliga B 1.11 Väljasttellimine (Outsourcing) , pilvtehnoloogiaga seotud salvestilahenduste puhul mooduliga B 1.17 Pilvteenuse kasutamine ja eelkõige meetmega M 2.541 Pilvteenuseosutajaga sõlmitava lepingu koostamine.

Järgnevalt on välja toodud loetelu erinevatest teemadest, mida võiks kasutada nii lepinguprojekti hindamisel kui ka selle koostamisel:

Organisatsioonilised reeglid ja protsessid

- Kommunikatsioonikanalite ja kontaktisikute määramine.
- Tööaegade kindlaksmääramine (nt päevatöö, öötöö, mida loetakse tööks nädalavahetustel ja puhkepäevadel).
- Protsesside, tööprotsesside ja vastutusalade kindaksmääramine.

- Probleemide ja kriiside lahendamiseks kasutatavad protseduurid, vajalike volitustega kontaktisikute nimetamine.
- Teenusetarnija juurdepääsuvõimalused tellija IT-ressurssidele.
- Teenusetarnija personali sissepääsuõigused ja pääsuõigused seoses tellija ruumide ja IT-süsteemidega.
- Andmehulkade üleandmine lepinguliste suhete lõppemisel, andmete kustutamine teenusepakkuja salvestusvahendite tagastamisel.

Personal

- Vajadusel tuleb määratleda väliste töötajate jaoks loodavate töökohtade tingimused.
- Töötajate omavahelise asenduskorra määramine ja kooskõlastamine.
- Täiendõppemeetmete planeerimine.

Valmisolek hädaolukorraks

- Vajalikud tegevused rikkeolukorra esinemisel.
- Reageerimisajad ja eskalatsiooniastmed.
- Tellija osaluskohustus avariiolukordade lahendamisel.
- Asendus- või varusüsteemide kasutamist puudutavad kokkulepped.
- Eriti olulised võivad olla vääramatut jõudu puudutavad regulatsioonid. Näiteks tuleks kokku leppida, kuidas tagada andmete ja süsteemide käideldavus juhul, kui teenusetarnija personal on otsustanud hakata streikima (nt täiendavate välise personali kaasamine).

Juriidilised raamtingimused

- Lepingus peavad olema fikseeritud teenuseosutaja iga töötaja kohustus järgida kehtivaid norme, seadusi ja muid kokkulepitud täiendavaid turvameetmeid. Vajadusel tuleb sõlmida eraldi leping konfidentsiaalsusnõuete kohta.
- Reguleerida tuleb kolmandate osapoolte, teenusetarnija tütarettevõtete ja allhankefirmade kaasamine projekti. Reeglina pole mõistlik neid automaatselt kõrvale jätta, selle asemel tuleks kehtestada mõistlikud reeglid.
- Süsteemide, tarkvara ja liideste osas tuleb kokku leppida omandi- ja autoriõigused. Tuleb saavutada kokkulepe, kas teenusetarnija võtab üle olemasolevad kolmandate osapooltega sõlmitud lepingud (riistvaraga varustamine, teeninduslepingud, tarkvaralitsentsid jne).
- Teenusetarnijaga tuleb kokku leppida, kuidas toimitakse juhul, kui teenuse lepingut tahetakse lõpetada, kuid teenuseosutaja poolt kasutatud tööriistu, protseduure, skripte ja pakkprogramme soovitakse edasi kasutada.
- Täpsustada tuleks tingimusi, mis kehtivad lepingulise suhte lõppemisel, nt teenusetarnija vahetuse või maksejõuetuse puhul.
- Tuleb jälgida, et tellijale jääks õigus katkestada lepingulisi suhteid piisavalt paindlikult.
- Teenusetarnijale peab kehtestama kohustuse, et pärast tellimuse lõppemist peab ta tagastama kogu tellijale kuuluva riist- ja tarkvara, kaasa arvatud salvestatud andmed ning kustutama turvalisel moel kogu salvestatud informatsiooni.

- Tuleks määrata, milline on poolte vastutus kahjude korral. Siinkohal peab teenuse tellija pöörama ka piisavalt tähelepanu sanktsioonidele või kahjunõuetele, mida rakendatakse siis, kui teenust ei osutata kokkulepitud kvaliteediga.
- Esmalt tuleks kindlaks määrata, kuidas oleks võimalik kahjusid tõestada, st kuidas oleks võimalik tuvastada kahjude tekitajaid.
- Kuidas mõõdetakse näiteks mainekahju?
- Kuidas hinnata kohustuste eiramist, millele vaid juhuse tõttu ei järgnenud tõsiseid kahjustusi?
- Kahjutasude nõudmise õigus on väärtusetu, kui see ületab teenusepakkuja maksevõimet ja teenusepakkuja kuulutab välja maksevõimetuse.

Muudatuste haldamine ja testimisprotseduurid

- Tuleb välja töötada tingimused, mis võimaldaksid tellijal kohanduda uute nõuetega. Tuleb kehtestada reeglid, kuidas tuleb ümber käia tellija muutunud nõuetega.
- Tuleb kokku leppida uue tarkvara ja riistvara testimisprotseduuride osas. Siinkohal tuleks kaasata järgnevad punktid:
- Täiendite ja süsteemi kohandamiste reeglid.
- Tellija ja teenusetarnija vastutusalad testimiskontseptsioonide väljatöötamisel ja testide läbiviimisel.
- Vastuvõtuprotseduurid. Ikka ja jälle esineb olukordi, kus teenuseosutaja viib tootmissüsteemi kas ette teatades või ette teatamata sisse muudatusi, kuid sõltuvalt olukorrast võivad sellega kaasnevad riskid ja vastutus jääda täielikult teenuse tellija kanda.

Teenuseosutaja kontrollimine

- Sisseostetava teenuse kvaliteeti tuleb regulaarselt kontrollida. Tellijal peavad olema selleks vajalikud info-, juurdepääsu- ja pääsuõigused. Juhul kui auditeid ja Benchmark -teste peaksid läbi viima sõltumatud kolmandad osapooled, peab see olema lepingus fikseeritud.

Täiendavad kontrollküsimused:

- Kas kõik kokkulepped on kirjalikult fikseeritud?
- Kas leping sisaldab üheselt mõistetavaid ja mõõdetavaid teenuste kirjeldusi?

M 2.357 Salvestisüsteemide haldusvõrgu ehitus

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator

Kõrgete turvanõuetega SAN- või NAS-komponentide haldamine ja seire peab olema piisavalt ette valmistatud. Vajalike nõuete täitmiseks on tihti kõige ülevaatlikumaks, efektiivsemaks ja majanduslikult soodsamaks lahenduseks luua eraldiseisev LAN, mida kasutatakse eranditult vaid haldusülesannete täitmiseks. Nimetatud haldusvõrku ühendatakse PCd, mida kasutatakse ainult kriitilise tähtsusega komponentide haldamiseks. Nimetatud võrgu sees tuleks haldamiseks kasutada ainult turvalisi protokolle (ssh-d telneti asmele ja https-i http asemel). Kui haldusvõrgud eraldatakse tootmisvõrgust vähemalt loogiliselt, veel parem kui füüsiliselt, on mõeldav ka ebaturvaliste protokollide, eriti paljudes tootmiskeskkondades ikka veel peaaegu asendamatu SNP version 1 kasutamine.

Kontseptsioon/ planeerimine

- Kõige lihtsam viis, kuidas hakata niisugust võrku üles ehitama, on võtta kasutusele eraldi kommutaator.
- Kõik administraatorite kliendid seotakse nende võrguliideste abil haldusvõrguga.
- Kõik kõrgema kaitsevajadusega serverid ja süsteemid (aktiivsed võrgukomponendid, salvestisüsteemid) varustatakse täiendava võrguühendusega, mis liidab nad haldusvõrguga.
- Käitamistarkvara ja rakenduste haldusjuurdepääsud seotakse serverites võimaluse korral alati eraldi haldusvõrgu võrguaadressiga.

Haldusvõrgus tuleks kasutada privaatseid aadresse (vastavalt RFC-standardile nr 1918). Selliste aadresside marsruutimist „ametlikus“ võrgus ei toimu, mistõttu tuleb ühendust ametliku võrguga, juhul kui selle rakendamiseks esineb vajadus, alati kaitsta NAT (Network Address Translation) ja muude tulemüüri kasutamist nõudvate kaitsemeetmetega. Haldusvõrgus tuleks kõikide IT-komponentide jaoks tagada ühtse kellaaja kasutamine, rakendades ka pisteliselt või pidevalt vastavat NTP-serverit. Seeläbi kergendatakse logide analüüsimist ja võimaldatakse anda hinnanguid sündmustele, mille mõjusid on täheldatud mitmel erineval komponendil. Tarvis on luua ülevaade saadaolevatest ressurssidest, mida on võimalik kasutada salvestisüsteemi ülesehitamiseks. Siia alla kuulub nii personaliressurss, mis on vajalik asjakohase kontseptsiooni loomiseks ja ellurakendamiseks, st võrgu käitamiseks, kui ka selleks vajaminev finantsressurss.

Tulemused fikseerimine

Lisaks on tarvis välja selgitada, kas haldusvõrgus on tarvis rakendada täiendavaid seiremeetmeid. Näiteks on võrgu-IDdega võimalik täiendavalt luua ülevaadet, kas võrgus leiab aset keelatud tegevusi või mitte. Samuti võiks sellises võrgus rakendada tsentraalselt toimivat logimist, kus üks konkreetne instants toimib tsentraalse logiserverina ja haldab kõikide serverite ja salvestisüsteemide logiandmeid. Siinkohal tuleb arvestada, et sõltuvalt olukorrast tuleb selliste meetmete rakendamine eelnevalt kooskõlastada töötajate esindusorganiga. Keerukama ülesehitusega haldusvõrgu puhul tuleks planeerimistöös ja kontrollimisel toetuda moodulile B 4.1 Heterogeensed võrgud .

Rakendamine

Esmalt tuleks välja selgitada, millisel kujul on tootmisvõrku ning selles asuvaid statsionaarseid servereid ja muid seadmeid (aktiivseid võrgukomponente,

salvestisüsteeme) võimalik laiendada (vt M 2.139 Olemasoleva võrgukeskkonna läbivaatus ja M 2.140 Võrgu hetkeolukorra analüüsimine). Seejärel tuleks välja selgitada loodava haldusvõrgu nõuded seoses võrgus asetleidva kommunikatsiooniga ning määrata kindlaks tulevase võrgu kaitsevajadus. Haldusvõrgu turvalisust puudutavate nõuete väljaselgitamisel tuleb lähtuda olemasolevatest IT-protseduuridest, mida soovitakse haldusvõrgu kaudu haldama hakata.

Kasutamine

Proovikäitamise raames tuleb läbi viia kontroll, mille käigus testitakse rakendatavaid turvameetmeid ja luuakse alus vastava võrgu käitamiseks vajaliku dokumentatsiooni väljatöötamiseks. Tüüpilisteks kontrollküsimusteks, mille järel võib lahenduse tootmissüsteemis kasutusele võtta, on:

- Kas haldusvõrk on tootmisvõrgust läbivalt eraldatud?
- Kas kõikjal kasutatakse võimalikult turvalisi teenuseid (secure shell-i, https-i)? Kas antud teenuste ebaturvalised variandid (telnet, http) on hallatavates seadmetes desaktiveeritud?
- Kas valdkondade kohta, kus ebaturvaliste teenuste kasutamisest ei ole võimalik loobuda, on olemas ülevaade ja asjakohane dokumentatsioon?
- Kas kõikide PCde, serverite, aktiivsete võrgukomponentide jms Default kasutajatunnused ja paroolid on muudetud?

Väljavahetamine

PCde või muu riistvara väljavahetamisel, või isegi, kui need eemaldatakse võrgust ainult lühikeseks ajaks parandustöödeks, tuleb tagada, et sinna ei oleks salvestatud siseinfot (paroole, logiandmeid, sisedokumente jms).

Valmisolek hädaolukorraks

Hädaolukordadeks peab olema ette valmistatud plaan, mis tagab tootmisvõrgu jätkuva töö ka neil juhtudel, kui haldusvõrgus peaks tekkima avarii.

Täiendavad kontrollküsimused:

- Kas haldusvõrk on tootmisvõrgust füüsiliselt või tulemüüridega kontrollitult eraldatud?
- Kas spetsiaalsete jälgimis- ja logimismeetmete kasutamine on kooskõlastatud töötajate esindusorganiga?

M 2.358 Salvestisüsteemide süsteemisätete dokumenteerimine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator

Salvestisüsteemi seadistuste dokumentatsioon hõlmab endas tehnilisi ja organisatsioonilisi ettekirjutusi ning kirjeldab institutsioonile iseloomulikku konfiguratsiooni. Vastav dokumentatsioon on aluseks tavarežiimis haldamisele ning muudatuste planeerimisele ja ellurakendamisele. Lisaks on pidevalt värskena hoitav dokumentatsioon aluseks ka avariiolukordadeks ettevalmistamisele. Avariiolukordades peab olema võimalik kasutada asjakohaseid olulisi andmeid. Siinkohal on tarvis siiski arvestada, et süsteemi seadistust puudutavad andmed on konfidentsiaalsed, mistõttu tuleb neid piisavalt kaitsta volitamata kasutuse eest.

Dokumentatsiooni sisu

Dokumenteerida tuleks eelkõige järgnev informatsioon:

Organisatsiooni käsitlev info:

- Väljatöötatud rollide ja sinna juurdekuuluvate volitusteprofiilide kirjeldused.
- Salvestisüsteemi administreerimisõigusega kasutajad koos oma rolliliigitustega.
- Kasutajatunnuste ja nende õiguste loomise aeg ning vajadusel ka info nende aegumise kohta ja muud selgitused.
- Kasutaja kontaktandmed ja kasutaja seotus organisatsiooniga.
- Ettekirjutused andmete varundamise ja hädaolukorraks valmisoleku kohta.

Tehnikat käsitlev info:

- Salvestisüsteemide asukohad koos infoga seadmete tüübi, kasutusvaldkonna ja kasutajateringi kohta.
- Salvestisüsteemide loogilised ja füüsilised jaotumised erinevate serverite alla.
- Salvestisüsteemide kõik võrguühendused (SAN, LAN, kaugseireks võibolla ka WAN)
- Loetelu seadmetest, mis ekspordivad andmeid läbi NAS-liidese.
- Loetelu kõikidest halduseks kasutatavatest liidestest (In-Band ja Out-Band). See peaks muuhulgas sisaldama ka ülevaadet, millised liidesed on aktiivselt kasutuses ja milliseid teenuseid nendega kasutatakse.

Haldamist käsitlev info:

- Graafiline kujutlus võrkudest (SAN, LAN, vahel ka WAN) ja konfigureeritud ühendustest salvestisüsteemide, serverite ja haldamiseks kasutatava PC vahel.
- Kogu vajalik info liideste ja teenuste aktiveerimiseks ja desaktiveerimiseks.
- Andmevarunduseks hädavajalikud seadistused.
- Logimisseaded.
- Soovitatav on koostada ka väike kokkuvõte (nö kokaraamatu stiilis) olulisematest või regulaarselt läbi viidavatest haldustegevustest.

Dokumentatsiooni regulaarne kontrollimine

Organisatsiooni puudutav dokumentatsioon tuleks reeglipäraselt (vähemalt iga 6 kuu tagant) üle kontrollida, et välja selgitada, kas dokumentatsioon ja hetkel

kasutajatele välja jagatud õigused langevad kokku ning kas õiguste jagamine on kooskõlas turvanõuete ja kasutajate kohustuslikele tööülesannetega. Tehnikat käsitlevat dokumentatsiooni tuleks kontrollida veelgi tihedamini, kuna see on aluseks hädaolukordadeks ettevalmistamisel.

Täiendavad kontrollküsimused:

- Kas volitatud kasutajate, kasutajarühmade ja nende õiguste profiilide kohta on olemas vastava dokumentatsioon?
- Kas dokumentatsiooni andmed on värsked?
- Millal toimus viimati vastava dokumentatsiooni andmete kontrollimine?
- Kas dokumentatsioon (ka paberkandjal olev dokumentatsioon) on volitamata isikute juurdepääsu eest piisavalt kaitstud?

M 2.359 Salvestisüsteemide seire ja haldamine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator

Võimalike vigade ja turvaprobleemide kiire tuvastamine eeldab salvestisüsteemide töö pidevat jälgimist. Kui serverite seire puhul tuleb konkreetselt jälgida ainult serverit, siis salvestisüsteemide puhul tuleb korraga pöörata tähelepani nii serveritele kui ka salvestitele. Erinevatest allikatest pärit andmete analüüsi lihtsustamiseks tuleks kasutada kas vajadusel või pidevalt NTP-serverit, et tekitada kõikides seadmetes ühtsed kuupäevad/kellaajad. Salvestisüsteem võib koosneda paljudest erinevatest komponentidest. Jälgida tuleb andmeid, mis kajastavad salvestisüsteemi riistvara seisundit, salvestisüsteemi vaba salvestusruumi ning transpordikanaleid kajastavaid andmeid (IP ja FC). Selliste andmete efektiivne analüüs võib toimuda ainult automatiseeritult vastavate programmide abil. Selleks on tarvis kokku koguda suur hulk andmeid ja neid analüüsida. Olulisematele süsteemiteadetele kiiremaks reageerimiseks võib need teadetefiltritega välja filtreerida. Antud kontekstis tuleb tegeleda järgmiste komponentide seirega:

- Rakendused, mis tegelevad salvestisüsteemis andmete töötlemisega või mis täidavad abifunktsioone. Siia alla kuulub nii turvatarkvara kui ka viirusetõrjetarkvara.
- Rakenduste poolt töödeldavad kasutajaandmed, mis transporditakse seejärel serverist läbi salvestusvõrgu salvestisüsteemidesse.
- Andmete transportimiseks vajaminev võrgu riistvara.
- Andmete salvestamiseks vajaminev salvestusriistvara (kettasüsteemid, lindiajamid).
- Võrk. NAS-süsteemi puhul peaks seire alla kuuluma TCP/IP-võrk, SAN-süsteemi puhul tuleks kontrollida salvesti sisevõrku ning lisaks sellele veel ka juhtimiseks ja haldamiseks kasutatavat kohapealset võrku.

Lisaks ressursside seirele peaks olema võimalik tsentraliseeritud kujul tegeleda ka terviksüsteemi üksikkomponentide haldamisega. Salvestisüsteemide juhtimiseks ja kontrollimiseks kasutatavaid süsteeme nimetatakse tihti salvestihaldussüsteemideks.

NAS haldus

NAS süsteemide seire, kui tegu on eranditult vaid NAS süsteemiga, on muudetud vägagi lihtsaks. Kuid vaatamata sellele, et niisugune tegevus võib esmapilgul näida „hooldusvaba“, tuleb ka siin rakendada vajalikud tehnilised ja organisatsioonilised seiremeetmed. Võimalusel tuleks NAS süsteem integreerida mõne lihtsa võrgu-haldussüsteemi alla, et oleks võimalik vähemalt kontrollida, kas NAS süsteemi on parasjagu võimalik kasutada ning kas sellel on piisavalt salvestiruumi.

SAN haldus

SAN süsteemide seireks on võimalik kasuta In-Band-Management ja Out-Band-Management mehhanisme. In-Band Management mehhanismi kasutatakse liidestes ja võrgus, mis tegelevad andmete transportimisega SAN-seadmete vahel.
Konfiguratsiooni- ja seirevõimalused on In-Band-Management mehhanismi puhul tihti küllaltki laialdased ja mugavad, kuna selle aluseks olev tarkvara sobib väga hästi kokku tootega ning tootjad on siinkohal püüdnud luua teatud iseseisvust.
Out-Band Management mehhanism kasutab täiendavaid liideseid, tavaliselt TCP/IP-võrguühendusi. Infokogumise protokollina rakendatakse väga laialdaselt

SMNP-d. Out-Band-Management mehhanism pakub (samuti) üldlevinud standardite kasutamist ning kergendab erinevatelt tootjatelt pärit toodete kombineerimist. Kuna Out-Band-Management mehhanismi puhul rakendatakse tihti ebaturvalist SNMP versiooni nr 1, tuleb haldamiseks luua eraldiseisev LAN (vt M 2.357 Salvestisüsteemide haldusvõrgu ehitus). Juhul kui käideldavusele esitatakse kõrgendatud nõudeid, tuleks neid kahte omavahel kombineerida. Juhul kui korraga rakendatakse nii In-Band- kui ka Out-Band-Management mehhanisme ja seiret, kergendab ja kiirendab niisugune täiendav võrguühendus võimalike probleemide seiret ja diagnoosimist.

Tsentraliseeritud kontroll

Suurte installeeritud süsteemide ning eriti SANi puhul, mille komponendid on jaotatud eri asukohtade vahel, peaks olema loodud tsentraalne koht, kuhu edastatakse kõik oluline käitamisega seotud info. Soovitatav on kasutada programme, mis võimaldavad ülevaatlikku jälgimist graafilisel kujul. Niisugune haldussüsteem muutub keerulise süsteemi liideseks. Selle efektiivseks kasutamiseks on tarvis piisava asjakohase koolitusega personali.

Juhul kui salvestilahendus soetatakse teenusena välistelt teenuseosutajatelt, tuleb nendega sõlmida teenusetaseme lepingud (SLA). Neil juhtudel peaks asutus kehtestama ka tingimused, kuidas teenuste taset kontrollitakse (nt regulaarse aruandluse ja kontrollidega) ja millist teavet on teenuseosutaja kohustatud teenuse tellijale edastama.

Kontrollküsimused:

- Kas on olemas tsentraalne koht, kuhu edastatakse erinevate salvestisüsteemide informatsioon?
- Millised probleeme või rikkeid kajastavad näitajad on kaasatud seire alla?
- Kas olulisemate teadete filtreerimiseks ja paremini esiletoomiseks kasutatakse teadetefiltreid?
- Kas salvestisüsteemi seirega tegelevad töötajad on läbinud piisava asjakohase koolituse ja on võimelised õigesti käsitlema teateid ning suudavad tuvastada probleeme juba nende varajases staadiumis?

M 2.360 Salvestisüsteemide turvaaudit ja aruanded

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT-turvaosakond

Rakendamise eest vastutavad: IT-turvaosakond, administraator, audiitor

Salvestisüsteemide turvalisust puudutavate kontrollide ulatus ja läbiviimise sagedus sõltub konkreetsetest andmetest, mida vastavas salvestisüsteemis töödeldakse. Keerukamate süsteemide puhul, kus suur hulk rakendusi salvestab oma andmeid salvestisüsteemi, tuleb teha tööprotsesside analüüs ning määrata selle põhjal kindlaks nende kaitsevajadus. Selle käigus tuleb välja selgitada ka peamisi tööprotsesse toetavate rakenduste ja andmete kaitsevajadus, et töötada välja nõuded turvaauditite sageduse ja kontrollisügavuse kohta. Nagu alati, kehtib ka siin põhimõte, et kogu süsteemile kehtivate ettekirjutuste väljatöötamise aluseks võetakse süsteemi üksikosadele kehtivad kõige rangemad nõuded. Kõikide turvalisust puudutavate tegevuste kontrollimiseks tuleb sisse seada vastav seireprotsess. Sellise protsessiga peab olema kindlaks määratud, milliseid turvaaruandeid tuleb regulaarselt koostada. Kuna salvestisüsteemid võivad olla väga keerulise ülesehitusega, peavad turvaaruanded koguma erinevatest allikatest asjakohaseid andmeid ja neid ka analüüsima. Lisaks peab olema kindlaks määratud, kuidas reageeritakse ettekirjutustest kõrvalekaldumistele. Turvaaruandeid peaksid kasutama audiitorid informatsiooni saamiseks.

Auditi sisu

Auditi käigus võrreldakse turbealaseid ettekirjutusi hetkel kehtivate seadistuste ja värskete andmetega. Niisuguse auditiga kontrollitakse, kas nõutud turbealastest ettekirjutustest ja protsessidest peetakse kinni või mitte.

Turvaauditite eesmärk

Auditi puhul on oluline silmas pidada, et selle eesmärgiks ei tohiks olla mitte süüdlaste leidmine, vaid faktide väljaselgitamine, vt M 2.182 IT-turvameetmete regulaarne läbivaatus .

Turvet käsitlevad aruanded

Auditi tulemuste kajastamiseks võib koostada ka lihtsa võrdlustabeli, kus kõrvutatakse kehtestatud nõudeid ja hetkeolukorda. Aruanne peaks asjakohaselt ja lühidalt välja tooma ettekirjutused (nt turvapoliitikast tulenevad nõuded) ja loetlema iga ettekirjutuse kohta audititest saadud järeldused. Kui kehtestatud nõuete ja hetkeolukorra vahel leitakse kõrvalekaldumisi, mille võimalikud vastuabinõud kohe teada, tuleks need üles märkida otse turvaaruandesse.

Audiitorite sõltumatus

Auditeid peaksid läbi viima sõltumatud audiitorid, st töötav personal ei tohiks ennast ja oma tööd ise auditeerida. Audiitorid vajavad oma töö tegemiseks sügavaid teadmisi salvestisüsteemidest ka siis, kui salvestisüsteemi administraatorid on neile auditeerimise käigus toeks. Vastavaid teadmisi tuleb regulaarselt asjakohaste koolitustega omandada ja täiendada.

Volituste andmine audiitoritele

Neil juhtudel, kus audiitorid peaksid oma tööd tegema iseseisvalt ja administraatoritepoolse abita, tuleks kõikide salvestisüsteemi komponentide jaoks sisse seada roll „Audiitor“. Sellisele kasutajarollile tuleks anda kõikide salvestisüsteemi seadistuse ja logifailide kasutamiseks vaid volitused read only. Neil juhtudel, kus institutsioon ei ole omalt poolt kehtestanud konkreetseid ettekirjutusi, peaks audiitor läbi töötama vähemalt järgmised kontrollivaldkonnad:

- Salvestisüsteemi tehnilise varustuse ja organisatoorse töö reeglite kohta peab olema koostatud asjakohane turvakontseptsioon.

- Salvestatud andmete kaitsevajadusega kaasnevad nõuded käideldavusele ja konfidentsiaalsusele peavad olema välja töötatud ja dokumenteeritud vastavalt töötajatele.
- Pärast kasutuselevõtmist peavad algparoolid olema välja vahetatud kõikides komponentides (salvestites, varundusseadmetes, vahel ka SAN-kommutaatorites), halduseks kasutatavates PCdes ja täiendavas tarkvaras.
- Kõiki komponendid (salvestid, varundusseadmed, vahel ka SAN-kommutaatorid) peavad olema üles seatud volitamata sissepääsu eest kaitstud ruumidesse, kus on olemas vajalik infrastruktuur (voolutoide, kliimaseade).
- Salvestisüsteemi haldamiseks vajalikud juurdepääsud peavad leidma aset eranditult läbi eraldiseisva haldusvõrgu.
- Haldusvõrk peab olema kaitstud tulemüüriga, viirusetõrjetarkvaraga ning vajadusel ka IDS-iga.
- Haldamiseks tohib kasutada ainult turvalisi ühendusi (nt https-i, ssh-d).
- Juurdepääsud salvestisüsteemidele ja nende andmetele peavad olema piisavalt kaitstud ja organisatsiooni ülejäänud võrgustsobival moel eraldatud.
- Kui andmete kaitsevajadus seda nõuab, peab andmete transportimine ja salvestamine toimuma krüpteeritult.
- Logi peab olema korraldatud selliselt, et logis kajastuksid andmed veasituatsioonide ja väärkasutamise katsete kohta. Logiandmeid tuleb regulaarselt kontrollida.
- Aluskonfiguratsioon ja olulised hilisemad muudatused selle konfiguratsioonis peavad olema dokumenteeritud. Salvestisüsteemide topoloogia ja salvestisüsteemi LAN-ühenduste kohta peab olema koostatud võrguplaan ning see peab olema värske. Nimetatud dokumentatsioon peab olema kättesaadav ka hädaolukorras.
- Pärast võimalike muudatuste sisseviimist kontrollitakse salvestisüsteemi turvalisust puudutavad seadistused veelkord üle.
- Regulaarselt tuleb kontrollida, kas andmevarundusega seotud protsessid toimivad rikkevabalt ning kas salvestusvahendid on töökorras.

Täiendavad kontrollküsimused:

- Kas salvestisüsteeme kontrollitakse regulaarselt?
- Kas audiitorid on kursis institutsiooni poolt kehtestatud ettekirjutustega?
- Kas salvestisüsteemide kohta koostatakse regulaarselt turvaaruandeid?

M 2.361 Salvestisüsteemide kasutuselt kõrvaldamine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator

Olukorras, kus salvestisüsteemi või salvestisüsteemi üksikuid kõvakettaid ei lähe enam tarvis, tuleks kõige esimese asjana tagada, et kõik süsteemi salvestatud andmed kantakse sobival moel üle teistesse süsteemidesse. Seejärel on tarvis veenduda, et süsteemist kustutataks turvalisel moel kõik kasutajaandmed ja konfiguratsiooniandmed.

Üksikute andmekandjate väljavahetamine

Juhul kui kõvaketastes, võibolla ka ainult mõnes üksikus, esineb defekte, mille tõttu otsustatakse need välja vahetada, tuleb tagada, et tootja töötleks väljavahetatavaid kõvakettaid selliselt, et neist ei oleks enam võimalik andmeid kätte saada. Ka neil juhtudel, kus ilmneb, et salvestisüsteemi kõvaketas on muutunud defektseks, tuleb kindlasti tagada, et sellel andmekandjal olnud andmed ei satuks kolmandate isikute kätte. Neil juhtudel, kus andmetele kehtib kõrge kaitsevajadus, tuleks kas tootja või vahendajaga kokku leppida kõnealuste ketaste asjakohane füüsiline hävitamise osas. Nimetatud tegevuse kohta peab tootja või teenuseosutaja esitama institutsioonile ka tõestuse.

Kõvaketta kustutamine

Vigaste kõvaketaste väljavahetamisel, mida on kas võimalik või koguni planeeritakse edasi kasutada, tuleb sinna salvestatud andmed kustutada sellisel moel, mis välistaks nende taastamise (vt M 2.167 Andmete kustutamine või hävitamine). Keerukamate salvestisüsteemide SAN- ja NAS-ketaste kustutamiseks läheb tarvis keerukamat tootjate poolt pakutavat kustutustarkvara. Sellistel juhtudel võib kustutamiseks palgata mõne hooldusega tegeleva ettevõtte. Selleks tuleb väljavalitud teenusepakkujaga sõlmida vastava teenuse kohta kirjalik leping. Ka selle kohta peaks teenuseosutaja esitama institutsioonile vastava tõestuse.

Salvestisüsteemi kasutuselt kõrvaldamine

Kui tekib vajadus salvestisüsteem kasutuselt kõrvaldada, tuleks esmalt koostada protseduur, mille alusel toimub vastavate andmete üleviimine. Siinkohal on tarvis tagada, et kõik salvestisüsteemis olevad andmed kantaks sobilikul kujul üle teistesse salvestisüsteemidesse. Sobival kujul tähendab siinkohal seda, et vastava protsessi käigus peavad olema täidetud kõik nõuded, mis tulenevad kõnealuse institutsiooni tegevusest ja ka seadustest, nt andmete säilituskohustusega seotud nõuded jms. Soovitatav on planeerida üleminekuaeg, mille käigus saab igapäevaselt kasutada juba uutesse süsteemidesse ülekantud andmeid, kuid samal ajal jääb alles ka juurdepääs vanale salvestisüsteemile, kuna see võimaldab lahendada probleeme, mida kohe alguses võib-olla ei suudetud ette näha. Seega võib kasutajaandmed lõplikult kustutada alles pärast üleminekuaja lõppemist. Kogu vajamineva protsessi jaoks tuleks koostöös tootja või tarnijaga välja valida sobiv protseduur, mis arvestaks ka andmete kaitsevajadusega. Kahtluste korral tuleks kõikide salvestisüsteemi ketaste puhul valida samasugune protseduur, mida rakendataks ka üksikute ketaste väljavahetamisel.

Haldust kajastava info kõrvaldamine

Konfiguratsioonist tuleb kõrvaldada NAS süsteemide või LUN-ide IP-aadressid ning ka sarnane SAN komponente puudutav info. Samuti on tarvis tagada, et turvaliselt saaks kõrvaldatud ka igasugune muu haldamist kajastav info. Siia alla kuulub nt selline info, mida salvestab süsteemis haldustööriistana kasutatav veebiserver.

Litsentsivõtmete haldamine

Tarkvaralitsentside (nt viirusetõrjetarkvara puhul) on tarvis kontrollida, kas neid läheb enam tarvis või mitte, et lõpetada õigeaegselt ebavajalike toodete sisseostmine.

Dokumentatsioon

Andmete üleviimise ja kustutamise kohta on tarvis koostada lõppdokumentatsioon. Kontrollida tuleks hädaolukorraks ettevalmistamise planeerimist kajastavat dokumentatsiooni. Uue konfiguratsiooniga tuleb kooskõlla viia ka riketejärgseks süsteemi taaskäivitamiseks vajalik funktsioonide sõltuvusahel. Avariiolukordades kasutatavad dokumentatsioonis ja käitamist kajastavas dokumentatsioonis ei tohi kajastuda viiteid kasutuselt kõrvaldatud salvestisüsteemide kohta.

Kontrollküsimused:

- Kas vabanevatelt kõvaketastelt kustutatakse tundlikud andmed täielikult?
- Kas kustutamiseks rakendatav protseduur vastab salvestatud andmete kaitsevajadusele?
- Kas kõikidest olulistest dokumentidest eemaldatakse kasutuselt kõrvaldatud süsteemi kajastavad viited?

M 2.362 Sobiva salvestisüsteemi valik

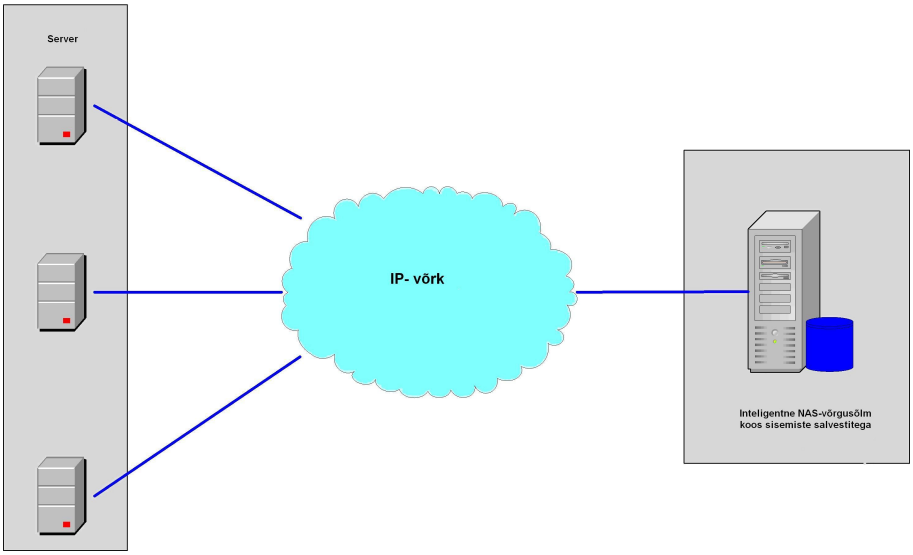
Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT-turvaosakond

Rakendamise eest vastutavad: IT-juht, IT-turvaosakond

Jõudmaks põhjendatud otsuseni, milline konkreetne salvestisüsteem tuleks antud kasutusvaldkonna tarbeks muretseda, tuleks ennast täpselt kurssi viia NAS- ja SAN-tehnoloogia tehniliste põhimõtetega ja selgitada välja nende potentsiaalne sobivus konkreetse institutsiooni jaoks. Otsuste aluseks olnud põhjendused tuleb kirjalikult fikseerida.

Network Attached Storage

NAS süsteemid on spetsiaalsed serverid, mis võimaldavad rakendada oma salvestiruumi nagu oleks tegu kasutusvalmis failisüsteemiga. Failisüsteemina pakutakse enamasti valida kas Windows-i (SMB/CIFS) või Unix-i (NFS) vahel. NAS süsteeme on väga lihtne integreerida olemasoleva võrgu infrastruktuuri alla. Neid on võimalik ühendada institutsiooni võrku nagu ühendatakse kliente või servereid. Seetõttu on NAS süsteemid tihti loodud eraldiseisvate süsteemidena (ingl *appliances*). Tootja juurest lahkudes on nad juba kasutusvalmis ning pärast mõningaid elementaarseid andmesisestusi, nt võrguseadistuste sisestamist on neid võimalik ka kohe kasutusse võtta. NAS süsteemide baastarkvarana rakendatakse tavaliselt vastava kasutusvaldkonna jaoks minimeeritud ja optimeeritud standardseid operatsioonisüsteeme (tihti Unixit või Linuxit, mõnikord ka Windowsi).



Joonis: NAS - Network Attached Storage

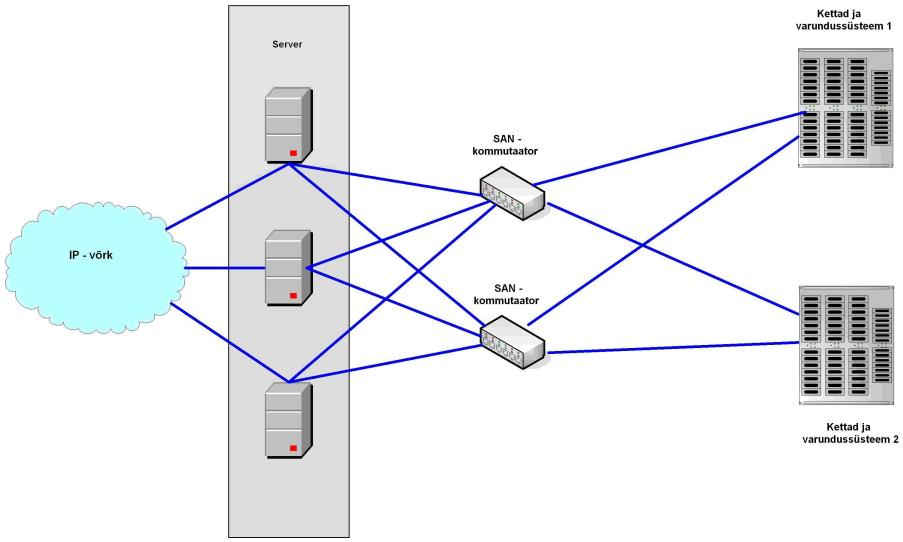
Lihtne ühendusviis on aga samas ka NAS süsteemide puuduseks, kuna *Network Attached Storage* süsteemid ühendatakse Ethernet tehnoloogia abil serveritega, täpsemalt öeldes klientidega. Selleks kasutatavad TCP/IP-protokollid on suhteliselt väikese läbilaskevõimega, kuid kasutavad seejuures küllaltki suurt protokolli üldkulu (ingl *overhead*). Seega ei ole nad loodud kiireteks suurte salvestite juurdepääsudeks. NAS süsteemide kasutamine võib LANile tähendada suurt koor-

must. Paljude rakendusnäidete puhul võib siiski täheldada, et üldjuhul on ühe gigabitine Ethernet-ühendus piisavalt kiire, et välistada sobiva LANi arhitektuuri puhul pudelikaelte tekkimine. Standardsete võrkude ja protokollide kasutamine tekitab SAN süsteemide puhul samasuguseid kitsaskohti nagu neid võib kohata Unixi või Windowsi alla töötavate serverite puhul. Standardsed NAS lahendused ei sobi just ilmtingimata kõige paremini salvestisüsteemiks sellistele rakendustele, mis ei põhine failide kasutusel. Siia alla kuuluvad kõik suuremad andmebaasid ja näiteks ka Microsoft Exchange-Server. Kui sellist rakendust soovitakse kasutada NAS süsteemi all, tuleks eelnevalt kontrollida, kas on võimalik soetada spetsiaalseid tooteid, mis on konkreetselt niisuguse kasutusvaldkonna jaoks optimeeritud. NAS süsteem võib tihti asendada tervet rida erinevaid servereid. Vaatamata sellele, et riistvaralised kulud on siinkohal reeglina palju suuremad kui üksikute serverite ülesehitamisel, mille on mitu ja/või suuremat kõvaketast, võib sellega märgatavalt tõsta süsteemi käideldavust. Selgeid eeliseid pakub aga tihti esinev võimalus seadet igapäevase kasutuse käigus konfigureerida või paigaldada sellel täiendavat salvestusruumi pakkuvat riistvara nii, et sellega ei kaasne tööseisakuid. Näitajate paranemine kaasneb ka andmevarunduse vallas. Süsteemile otse külge ühendatud andmevarundusseadmed (arhiveerimiseks vajalikud lindiajamid, „JukeBox-id“) suudavad vohama läinud serverimaastiku andmehulkadest varukoopiate tegemist lihtsustada, kiirendada ja stabiilsemaks muuta. Lihtsamate NAS süsteemide puuduseks on asjaolu, et süsteemi avarii puhul on tagajärjed palju tõsisemad kui ühe üksiku serveri avarii puhul ning tõsiasi, et avarii puhul ei ole võimalik olukorda institutsioonis hoitava varusüsteemiga kiiremas korras lahendada.

Storage Area Networks

SAN süsteemid koosnevad ketaste alamsüsteemidest, andmevarundussüsteemidest ja eraldiseisvast võrgu infrastruktuurist. Ketaste alamsüsteemid liidavad enda sees tervet hulka kõvakettaid. Siinkohal tehakse vahet, kas ühendamine leiab aset vaid ühise korpuse ja ühise voolutoite baasil (JBOD = *Just a Bunch of Disks*) või rakendatakse spetsiaalset lülitusseadet, nn RAID-Controller-it, mis ühendab RAID-tehnoloogia abil (RAID = *Redundant Array of Independent Discs*) füüsilised kõvakettad kokku virtuaalseteks kõvaketasteks. Sellel lisaks on veel olema ka intelligentsed RAID-Cotroller-id, mis suudavad pakkuda veel ka täiendavaid teenuseid. Mitmete füüsiliste kõvaketaste liitmisel üheks virtuaalseks üksuseks, nimetatakse ka salvesti virtualiseerimiseks RAIDi abil, on võimalik füüsiliste kõvaketaste osava kombineerimise teel tõsta süsteemi rikkekindlust või jõudlust või ka mõlemat. RAID-Controller näitab ära ainult kokku liidetud kõvakettad (virtuaalsed kõvakettad või loogilise *Volume*) ning jagab andmed, mis tuleks niisuguse kõvaketta peale kirjutada, üksikute füüsiliste kõvaketaste vahel ära. Nimetatud funktsiooni on võimalik kasutada ka serverites spetsiaalse rakenduse *Volume Manager* abil, kuid tuleb arvestada, et seeläbi tõuseb serveri töökoormus. Andmete jagamise korraldamiseks eksisteerib erinevaid süsteeme, nn RAID-Level-eid. Kui RAID-Level toetab info salvestamist liiasusega, jäävad andmed isegi pärast ühe kõvaketta avariid siiski alles ning neid on võimalik taastada. Ketta-alamsüsteemi üksikuid kõvakettaid on tihti võimalik välja vahetada ka jooksva töö käigus (ingl *hot swap*). Ketta-alamsüsteemid pakuvad võimalust koostada kõik osakomponendid liiasusega, mis aitab suurendada süsteemi käideldavust. Täiendavaks eeliseks on tõsiasi, et sobilike konfiguratsioonimehhanismide abil on võimalik rakenduse jaoks eraldatud salvestusruumi vastavalt selle vajadusele muuta. Ketta-alamsüsteem annab rakendusele vaid vajamineva salvestiruumi. Isegi neil juhtudel, kus andmed

salvestatakse liiasusega, läheb ikkagi tarvis täiendavat andmete varundamist, kuna salvestisüsteemi salvestatud liiasusega andmemahud ei suuda parandada võimalikke loogilisi defekte. Andmevarundussüsteemidena on võimalik kasutada lindiajameid, optilisi andmekandjaid ning ka spetsiaalseid kõvakettasüsteeme. Ka need seadmed integreeritakse otse salvestivõrgu alla. SAN süsteemid kasutavad oma enda võrguriistvara ning enda rakendusotstarbega kokkusobivaid kiireid võrguprotokolle. Tihti kasutatakse fiiberoptilisi kaableid (süsteeminimetus: *Fibre Channel* , FC). Lihtne *Storage Area Network* koosneb kas ühest *Fibre Channel Switch* -sit või *Director* -ist (suuremad *Switch* -id, mis on varustatud rohkemate funktsioonidega, kannavad tihti nimetust *Director*), ühest või mitmest ketta-alamsüsteemist ja serveritest, mis ühendatakse nn HBA-ga (*Host Bus Adapter* -iga) *Fibre Channel Switch* -i külge. *Fibre Channel* võrgud kasutavad spetsiaalset massmälu kasutuseks mugandatud protokolli, mis võimaldab suuri edastuskiirusi ja on seetõttu väga sobiv kasutamiseks salvestisüsteemides. Samuti on võimalik kasutada iSCSI seadmeid. iSCSI „pakib“ salvestusprotokollid, st massisalvesti juhtkäsklused ja sinna juurde kuuluvad andmed IP-pakettidesse. iSCSId rakendatakse juhtudel, kus serveritest soovitakse luua iSCSI *Host-Bus-Adapter* -i abil virtuaalseid *End-to-End* -ühendusi juurdepääsuks salvestisüsteemidele, ilma et oleks tarvis käitada eraldiseisvaid salvestusvõrkusid. Olemasolevaid võrgukomponente (LAN-kommutaatoreid) saab ära kasutada ning serverite ja salvestusseadmete vaheliseks ühenduseks ei ole tarvis rakendada mitte mingisugust uut võrgutehnoloogiat ega ka olemasolevast tehnoloogiast erinevat riistvara. Mõistet SAN kasutatakse järgnevalt mõlema tehnoloogia puhul. Kohtades, kus on tarvis eristada, kasutatakse mõisteid Fibre Channel SAN või FC-SAN ning vastavalt kas iSCSI-SAN või IP-SAN. SAN süsteemide üheks suurimaks eeliseks on nende avariikindlus (ingl *disaster tolerance*). Olulist rolli mängib siinjuures *Multi-Pathing* kontseptsioon, mida SAN süsteemid pidevalt järgivad. Juhul kui serveril on võimalik ketta-alamsüsteemini jõuda läbi mitmete *Host Bus Adapter* -ite ja läbi erinevate võrguühenduste, on võimalik kahe süsteemi vaheline andmeedastus ära jagada mitme andmetee vahel. Kasutades serverites mitmeid *Host Bus Adapter* -eid ja kuvades virtuaalseid kõvakettaid ketta-alamsüsteemi mitmetes liidestes, saavutatakse salvestisüsteemi edastuskiiruse ja käideldavuse efektiivne kasv. Kui serveris kasutatakse kahte või rohkem *Host Bus Adapter* -it, jaotatakse koormus ühe adapteri avarii korral ümber teistele HBAdele. Selline operatsioonisüsteemile ja rakenduste jaoks läbipaistev *Faiolver* tõstab serveri käideldavust. Kõikide SAN süsteemi komponentide varustamine liiasusega aitab luua väga kõrge avariikindlusega süsteem (vt M 2.354 Kõrge käideldavusega SAN-konfiguratsiooni kasutamine). Seega on väiksemate *Storage Area Network* -ide puhul mõeldav, et organisatsiooni territooriumil kasutatakse üksteisest väga kaugel paiknevates asukohtades ehituselt samasugust ketta-alamsüsteemi, mis kumbki on ühendatud kahe, jällegi omakorda eraldi installeeritud kommutaatoriga. SAN süsteemide liiasusega varustatud ühenduste loomiseks, peab serveritel olema vähemalt üks *Host Bus Adapter*, et iga *Host Bus Adapter* oleks ühendatud ühega kahest võimalikust SAN-kommutaatorist.



Joonis: SAN - Storage Area Network

Üksikute liinide, ühe kommutaatori või koguni ühe ketta-alamsüsteemi avarii puhul jääb terviksüsteem selle negatiivsest mõjust puutumata. SAN süsteemide kujundamisel on küllaltki kerge välja töötada liiasusi, mis suudavad tagada, et üksikute komponentide nagu nt sideliinide, kommutaatorite või koguni ketta-alamsüsteemi avarii ei too endaga kaasa terviksüsteemi jõudluse langust. Väga kõrgete käideldavusnõuete puhul on võimalik antud ülesehitust laiendada selliselt, et kõikide liiasusega varustatud komponentidega SAN süsteemid seatakse üles üksteisest väga kaugel asuvatesse (kuni 100 km) ja tehniliselt autokraatlikesse arvutuskeskustesse. Niimoodi on võimalik ekstreemjuhtudel, nt terve arvutuskeskuse avarii puhul tagada, et kasutajate jaoks ei tähenda niisugune avarii ei tööseisakut ega ka ressursside vähenemist. Täiendavat liiasust on võimlaik lisada *Cluster* -serveri kasutamisega, mis jagab ühe loogilise masina kahe või rohkema füüsilise serveri vahele laiali. Selleks tuleb rakendus installeerida kahele või rohkemale serverile. Vastavad serverid töötavad ühtede ja samade kasutajaandmetega. Juhul kui ühes serveris peaks aset leidma rike, võtab teine server automaatselt avariilise serveri töö enda kanda. SAN lahenduste positiivsed omadused maksavad küllaltki palju raha ja on keerulised. Võrreldes *Direct Attached Storage* meetodiga läheb samasuguse salvestiruumiga SAN süsteemi juurutamine mitmeid kordi kallimaks. Lisaks sellele on SAN süsteemi planeerimine ja ülesseadmine piisavalt keerukas ettevõtmine, et institutsioonil on selle tarbeks kindlasti soovitav kaasata abijõudusid väljastpoolt.

Kokkuvõte

NAS salvestisüsteem kujutab endast failidel põhinevat juurdepääsu, SAN süsteem aga plokkidel põhinevat juurdepääsu. SAN rakendub „sügavamalt“ ja pakub kõikvõimalikke tehnilisi lahendusi andmete salvestamiseks. NAS kujutab endast institutsiooni serverimaastiku laiendust.

Kombineeritud seadmed

Viimasel ajal on ilmunud müügile ka seadmeid, mis kujutavad endast NAS ja SAN lahenduste segu. Niisuguste süsteemide sisemine ülesehitus vastab kõikidele SANi kriteeriumitele. Väljapoole suunatult on neid siiski võimalik käitada ka NAS süsteemidena. Lisade ja vastavate konfiguratsioonidega on niisuguseid sal-

vestisüsteeme võimalik käitada ka segarežiimis. Nii võib üks ja sama seade toimida ühelt poolt mõningate Ethernet -ühendustel töötavate rakenduste jaoks kui Filer , st kui intelligentne võrgusõlm, mis võimaldab kasutada erinevaid failiteenuseid ning teiselt poolt võib sama seade töötada ka teiste serverite jaoks läbi Fibre Channel -i või iSCSI toimiva „puhtakujulise salvestina“.

Täiendavad kontrollküsimused:

- Kas salvestisüsteemide ja salvestusvõrkude planeerimisel on institutsiooni vastutavate töötajate jaoks piisavalt selgelt välja toodud erinevat liiki salvestisüsteemidega kaasnevad võimalused ja ka nende piirid?
- Kas otsuste aluseks olnud põhjused, miks teatud salvestisüsteemi kasuks otsustati, on dokumenteeritud?

M 2.363 SQL-injektsiooni kaitse

Algatamise eest vastutavad: IT-turvaosakond, IT-juht

Rakendamise eest vastutavad: administraator, rakenduste arendaja

Vältimaks SQL-injektsioonide ärakasutamist (vt G 5.131 SQL-injektsioon) või vähemalt raskendamaks nende läbiviimist, tuleb tarvitusele võtta terve rida erinevaid kaitsemeetmeid. Kõnealused meetmed puudtavad rakenduse kõiki komponente, rakendust ennast ja serverit kuni andmebaaside haldussüsteemideni (DBMS) välja.

Rakenduste programmeerimise meetmed

Üheks olulisemaks meetmeks, mille abil saab SQL-injektsioone vältida, on rakenduse poolt läbiviidav sisestuste ja parameetrite hoolikas kontrollimine ja filtreerimine. Andmete puhul tuleks kontrollida, kas nende tüüp vastab oodatud andmetüübile. Juhul kui oodatakse numbritest koosnevaid parameetreid, saab neid kontrollida PHP (PHP: *Hypertext Preprocessor*) funktsiooniga *is_numeric()*. Filtreerimine seevastu peaks hea seisma selle eest, et ignoreeritaks erinevaid märke nagu viitemärke (‘), semikooloneid (;) ja topeltsidekriipsusid (–). Turvaline on kasutada *Stored Procedures* või *Prepared SQL-Statements* (Java = PreparedStatement-klassi, PHP-MySQL = mysql_real_escape_string()-funktsiooni). Neid võimaldavad kasutada paljud andmebaaside haldussüsteemid (DBMS-id) ning need on algselt loodud selleks, et optimeerida sagedamini esinevate päringute kasutamist. Niisuguste parameetriteks muudetud *Statement* -ide eeliseks on see, et parameetreid ei ole enam võimalik otseselt liita SQL-Statement-i alla. Need edastatakse andmebaasi hoopis SQL-Statement-ist eraldi. *Statement* -ide ja parameetrite kokkuliitmise teeb ära DMBS ise, kusjuures eelpool nimetatud märgid maskeeritakse automaatselt. Selleks, et potentsiaalsetele ründajatele ei antaks ette rünnakuteks avatud kohti, tuleks eriti pöörata tähelepanu sellele, et rakendused ei saadaks väljapoole veateateid, mis võimaldaksid ründajal teha järeldusi kasutatava süsteemi või selle taga oleva andebaasi struktuuri kohta.

Serveri meetmed

Serveri kõige olulisemaks kaitsemeetmeks on operatsioonisüsteemi tugevdamine Rünnatavate kohtade minimeerimiseks võetakse tarvitusele järgnevad abinõud:

- Mittevajalike teenuste desaktiveerimine.
- Mittevajalike kasutajakontode kustutamine.
- Oluliste turvapaikade installeerimine.
- Kõikide serveri tööks mittevajalike koostisosade kustutamine.
- Sellel lisaks tuleks kaaluda *Application-Level-Gateway* (ALG) kasutamist (vt M 5.117 Andmebaasiserveri integreerimine turvalüüsi koostisse). ALG-d suudavad rakenduse tasandil kontrollida andmeid, mis liiguvad veebibrauseri ja rakenduse vahel ning takistavad kahjulike andmete jõudmist serverisse.

Üheks täiendavaks turvameetmeks on ka *Intrusion-Detection* -süsteemide (IDS-ide) ja *Intrusion-Prevention* -süsteemide (IPS-ide) kasutuselevõtmine. IDS süsteemid analüüsivad võrgu kaudu liikuvat andmevahetust ja suudavad tuvastada potentsiaalselt ohtlikke andmeid. Selleks rakendatavad analüüsitehnikad jagunevad kategooriatesse väärkasutus (*Misuse*) ja anomaaliate tuvastamine (*Anomaly Detection*). *Misuse Detection* analüüsitehnika püüab tuvastada teadolevaid ründemustreid. *Anomaly Detection* lähtub seevastu põhimõttest koguda infot lubatud

käitumismustrite kohta ja tuvastada nende kõrvalekaldumised rünnetena. IDS on võimeline ründeid tuvastama ja suudab edastada hoiatusi, IPS seevastu on suuteline algatama ka asjakohaseid vastureaktsioone. Reaktsioon võib seisneda nt selles, et toimub ühenduse blokeerimine, andmete hülgamine või andmete muutmine. Kõrgendatud turvanõuete puhul tuleks välja selgitada, kas IDSi või IPSi kasutamine on konkreetsel juhul õigustatud.

Andmebaasi meetmed

Samamoodi nagu operatsioonisüsteemi puhul, tuleb ette võtta ka andmebaasi tugevdamine. Andmebaasi puhul tähendab see nt järgmist:

- Ebavajalike *Stored Procedures* eemaldamine.
- Mittevajalike teenuste desaktiveerimine.
- Ebavajalike kasutajakontode ja *Default Account* -ide kustutamine.
- Oluliste turvapaikade installeerimine.

Antud kontekstis tuleks andmebaasi juurdepääsuks luua spetsiaalne kasutajakonto, mis peaks hakkama saama võimalikult väheste pääsuõigustega. Sellele lisaks tuleks tundlikke andmeid nagu paroole hoida andmebaasis võimalusel ainult krüpteeritud kujul. Paljud tootjad on enda poolt välja töötanud nn kitsaskohtade skannerid, mis on võimelised skaneerima nii rakendusi kui ka andmebaase võimalike turvaaukude nagu nt SQL-injektsioonide suhtes. Põhimõtteline näide protseduuri kohta, kuidas koostada turvalist koodi, kasutades PHPd ja MySQLi:

PHP-s takistab funktsioon mysql_real_escape_sting() märkide ülekandmist MySQL-andmebaasi. Funktsioon maskeerib edasiantavast stringist saadud märgid nagu nt viitemärgid ja takistab seeläbi SQL-injektsiooni.

Järgneva süntaksi asemel:

```
$query = "SELECT * FROM users
WHERE username=
‘ ". $_POST[‘username’] . „
AND password=
‘ ". $_POST[‘password’] . “”;
```

tuleks kasutada hoopis järgnevat süntaksit:

```
$query = "SELECT * FROM users
WHERE username=
‘ ". mysql_real_escape_string($_POST[‘username’]) . „
AND password=
‘ ". mysql_real_escape_string($_POST[‘password’]) . “”;
```

Näide turvalise koodi kohta kasutades ASP-d koos ADO und SQL-serveriga:

Prepared Statement -i kasutamine eelneva näite baasil näeks antud juhul välja järgmine:

```
$query = "SELECT * FROM users WHERE username=?
AND password=?"
Set cmd = Server.CreateObject(“ADODB.Command”)
cmd.CommandText = query
cmd.CommandType = adCmdText
Set param = cmd.CreateParameter(“”,adVarChar, adParamInput,
nMaxUsernameLength, strUsername)
```

```
cmd.Parameters.Append
Set param = cmd.CreateParameter(“”,adVarChar, adParamInput,
nMaxUsernameLength, strPassword)
cmd.Parameters.Append
Set rs = cmd.Execute()
```

Siinkohal on tarvis silmas pidada, et eelnevalt välja toodu koodinäited püüavad näitlikustada vaid SQL-injektsioonide vältimise üldisi põhimõtteid.

M 2.364 Halduse planeerimine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: IT-juht, administraator

Organisatsioonilised meetmed

Enne Windows Server-ite juurutamist tuleb teha põhjalik planeerimistöö, et kasutuselevõtmine saaks toimuda reguleeritult ja turvaliselt, ning et oleks tagatud ka selle edasine turvaline käitamine. Windows Server-ite planeerimisele ja administreerimisele kehtivad nõuded tuletatakse kasutusvaldkonna kirjeldustest ja kasutusotstarbe määratlustest. Käitamise raames ette võetavad administratiivsed muudatused võivad endaga kaasa tuua turvalisust ohtu seadvaid kõrvalmõjusid.

Haldamise planeerimisel tuleb lähtuda turvapoliitikast tulenevatest ettekirjutustest (vt M 2.316 Serveri turvapoliitika kehtestamine). Selles peaks muuhulgas sisalduma ka ettekirjutused, mis kehtestavad nõude, et serverit on keelatud rakendada kasutaja töökohaarvuti funktsioonides.

Sissepääs ja juurdepääs

Haldamine võib toimuda koha peal läbi serveri konsooli, mõnest teisest LAN-i ühendatud arvutist, või ka mõnest väljaspool asuvast arvvutist nt VPN-i vahendusel.

Administraatorite ülesannete ja volituste planeerimisel tuleb välja töötada sissepääsuõiguseid puudutavad reeglid (vt M 2.6 Sissepääsuõiguste andmine). Siinjuures tuleb järgida eelnevalt välja töötatud tööülesannete jaotust (vt M 2.5 Vastutuse ja ülesannete jaotamine). Ebavajalikke serverini viivaid sissepääsuõigusi tuleb vältida.

Tüüpilised administratiivsed ülesanded

Ülesannete loetelu

- Sündmuste kuva (event viewer -i) jälgimine
- Tarkvara installeerimine, hooldamine ja deinstalleerimine
- Windowsi komponentide lisamine/muutmine/eemaldamine
- Täiendite laadimine (Windows Update)
- Koormuse kontrollimine
- Riistvara töö jälgimine
- Rakenduste ja teenuste toimimise jälgimine
- Failisüsteemi hooldamine
- Volituste kohandamine vastavalt muutnud nõuetele
- Kasutajate ja gruppide haldamine, uue kasutajate ja gruppide loomine, muutmine ja kustutamine
- Organisatsiooniüksuste disaini (OU Design-i) kohandamine
- Muudatuste või kohanduste tegemine Active Directory -s
- Andmetest varukoopiate tegemine
- Võrguühenduste kontrollimine
- Viirusetõrje läbiviimine ja selle hooldamine
- Registreerimisandmebaasi hooldamine
- Kuupäeva/kellaaja/ajatsoonide haldamine

Sissehitatud haldusalased standardgrupid

Lokaalsed turvagrupid

Windows Server-ite haldamine nõuab laiautuslikke volitusi ning seetõttu läheb tarvis sobivat volituste kontseptsiooni. Standardse installeerimisprotseduuri tagajärjel luuakse haldamise jaoks järgnevad lokaalsed turvagrupid:

Süsteemi poolt defineeritud turvagrupp	Server 2003	Server 2008	Tähendus halduse jaoks
Administraatorid	X	X	Täielik juurdepääs kõigile valdkondadele, turbe seisukohast väga kriitiline
Põhikasutaja	X	X	Laiaulatuslik juurdepääs süsteemi seadistusele koos mõningate piirangutega: põhikasutajatel ei ole nt volitusi võtta enda omandisse üle faile, laadida või eemaldada seadmete draivereid, hallata turvet ja protokolle, installeerida teenuseid.
Varunduse operaatorid	X	X	lugemis- ja kirjutusõigusega juurdepääs kõigile failidele

Remote Assistance teenusepakkujad	X	X	volitused ainult Active-Directory keskkonnas, kaugpöördusega on lubatud osa võtta konsooliseansist (Shared Desktop), mille kaudu saavad samasugused õigused nagu sisselogitud kasutajal. Kaughalduse otstarbeks ebasobiv, paremini sobib selleks Remote Desktop.
Abiteenuse osutajate grupp	X		selle grupiga võivad administraatorid määrata ühiseid volitusi kõikide support -rakenduste jaoks, võib põhjustada suurt turvariski
Võrgukonfiguratsioonioperaatorid	X	X	õigus hallata ühenduste seadistusi kaustas Network Connections
Printimise operaatorid	X	X	printerite ja printimise ootejärjekordade haldamine
Jõudlusprotokolli kasutajad	X	X	konsooli Jõudlus (perfmon.exe) haldamine
Distributed COM-kasutajad	X	X	konsooli Komponentide teenused haldamine
Süsteemiseire kasutajad	X	X	kirjutusõigusega juurdepääs jõudlusnäitajatele ja -logidele

Kasutajad	X	X	lubatud on sisselogimine liikmeserveritesse ja eraldiseisvatesse serveritesse
Remote Desktop -i kasutajad	X	X	grupp, mis on loodud Remote Desktop sisselogimisvõimaluste juhtimiseks
TelnetClients	X		grupp, mis on loodud Telneti sissevalimisvõimaluste juhtimiseks
Tiražeerimise (replication) operaator	X	X	operatsioonisüsteemi poolt kasutatav grupp, mida ei tohi rakendada kasutajate puhul
Külalised	X	X	registreerimata kasutajatele mõeldud ressursijuurdepääsude juhtimine, mida ei tohi rakendada kasutajate puhul
Krüptograafia operaator		X	selle grupi liikmed on volitatud tegelema krüptograafiliste protsessidega
IIS_USRS		X	Integreeritud grupp Internet Information Services kasutamiseks

Teadmiseks:

Domeenikontrollerite standardsed grupid võivad eelpooltoodutest osaliselt erineda.

Minimaalselt vajalike volituste kombineerimise printsiip

Windows Server-tes operatsioonisüsteemis on administraatorite tööülesannete täitmiseks loodud erinevad turvagrupid nagu nt grupp Administraatorid , millele on antud täielik haldusalane juurdepääs kõigile serveri valdkondadele, mistõttu mõjutavad need grupid väga olulisel määral ka Windows Server-ite turvalisust.

Windows Server-ite erinevate kasutusvaldkondade puhul, nt rakendades seda failiserverina tuleks turvagruppide loomisel lähtuda põhimõttest, et turvagruppide-

le ei peaks andma täielikke haldusõiguseid. Erinevate haldusega seotud ülesannete täitmisel, nt andmetest varukoopiate tegemisel saab rakendada erinevaid haldusgruppe nagu nt gruppi Varunduse operaatorid , mis aitab Windows Server-ite erinevate valdkondade ohtusid piirata. Alati tuleb lähtuda põhimõttest, et jagatavate volitusekombinatsioonide hulk tuleb hoida võimalikult väike, mistõttu tuleks nt kaaluda, kas haldusega seotud ülesannete täitmiseks piisaks võibolla piiratud õigustega turvagrupist nimega Põhikasutajad (vt M 5.10 Piiratud õiguste andmine). Olemasoleva võrgu puhul tuleks välja selgitada, kas vajalikke ülesandeid saab täita Active Directory-s või kohapealsetes serverites olemasolevate turvagruppidega (siinkohal tuleks arvestada G 2.115 Standardsete turvagruppide ebapädev kasutamine Windowsi alates Server 2003-st). Standardgruppide valikuta aitab suurendada administreerimiseks kasutatavate lisakomponentide installeerimine.

Sellekohasteks näideteks on turvagrupp nimega Terminaliserveri kasutajad, kui on installeeritud terminaliserveri teenused või turvagrupp DHCP-Administraatorid, kui on installeeritud DHCP-teenus. Olemasolevatele turvagruppidele toetumine ei ole alati sobiv, kuna nende volitusi pole võimalik hallata. Seetõttu on kehtestatud haldusülesannete täitmiseks soovitatav kasutada selleks spetsiaalselt kohandatud turvagruppe. Vigade vältimiseks tuleks täpselt kindlaks määrata, milliste haldusalaste ülesannete täitmiseks kasutatakse volitusi, mis on antud grupile nimega Administraatorid. Näiteks failisüsteemi täielikku juurdepääsu saab standardse seadistuse alusel muuta ainult läbi grupi nimega Administraatorid (vt M 4.149 Windows'i faili- ja ühiskasutusõigused), teiselt poolt jällegi on grupil nimega Administraatorid alati Remote Desktop -i abil juurdepääs ka kõigile serveritele, ning need volitused ei sõltu grupist nimega Remote Desktop-i kasutajad . Suuremates keskkondades tuleks alati eelistada võimalikult väikeste haldusalaste juurdepääsuõigustega gruppe. Vajadusel võib volitusi suuremate juurdepääsuõigustega gruppide abil suurendada.

Isedefineeritud grupid

Isedefineeritud gruppide mõjudega arvestamine

Vajalike halduslaste ülesannete täitmiseks on võimalik ka ise luua turvagruppe, mis sisaldavad vajaminevaid volitusi. Iseloodud gruppe on võimalik täiendada vastavalt eelpool toodud juurdepääsu taseme loetelule. Planeerimisega tuleks takistada programmide tahtmatut käivitamist liiga laialdaste halduslaste volituste tõttu, kuna seeläbi saavad programmid juurdepääsu serveri kriitilise tähtsusega osadele ning võivad seeläbi kahjustada serveri turvalisust.

Haldamiseks kasutatavad kasutajakontod

Kasutamise ja haldamise lahutamine

Vaadeldes eraldi iga isiku poolt IT-keskkonnas volitustega kasutajakonto alt läbiviidavaid tööülesandeid, tuleb administraatorite jaoks sisse viia põhimõtteline eristamine ja välja selgitada:

- Millised ülesanded on seotud IT-süsteemi kasutamisega?
- Millised ülesanded on seotud IT-süsteemi haldamisega?

Kaks eraldi kontot

Antud lähenemise teostuseks on soovitav ühe isiku jaoks luua kaks eraldi kontot.

Kuna Windows Server enda olemasolevad standardsed grupid ei sunni otseselt otsustama kasutaja ja administraatori vahel, tuleks igapäevatööks luua üks kasutajakonto ja haldusülesannete täitmiseks teine halduskonto ning neid vastava põhimõtte alusel ka kasutada.

Eesmärk jagada võimalikult piiratud volitusi

Kasutajakontode loomiseks ja kõrvaldamiseks on tarvis luua kindlaksmääratud ja dokumenteeritav protsess. Eriti oluline on see haldusülesannetega seotud kontode puhul. Eesmärgiks on alati see, et kasutajaseansiks vajalik sisselogimine Windows-Server-arvutisse või Windows-haldusarvutisse toimuks võimalikult väheste volitustega, kõige parem kui täiesti tavaliste kasutajaõigustega. Selle tagamiseks võib rakendada mitut erinevat lähtepunkti:

- Sekundaarne serverisse sisselogimine - Hallatavasse serverisse logitakse esmalt sisse täiesti tavaliseks kasutajaseansiks, mille volitused on piiratud ning serveri haldamiseks vajalikke tööriistasid saab hakata kasutama alles sekundaarse sisselogimise järel (execute as. . . või runas), st pärast sisselogimist haldamiseks loodud kasutajakonto alt. Sellistel juhtudel on tarvis kaaluda, kas tavalistele kasutajatele tohiks lubada ennast kohapeal serverisse sisse logida (standardseadistus) või tuleks selleks luua hoopis eraldi turvagrupp.
- Haldusjaama sisseseadmine - Haldusjaama rakendamisel on soovitav kasutada Active Directory (vt M 2.229 Active Directory planeerimine). Haldusjaama logitakse sisse kasutajakonto alt, millel on antud arvutis ainult väga vähesed volitused (nt grupp Kasutajad). Hallatavatele serveritele pääsetakse vastavate tööriistade abil (vt allpool) ligi haldusjaama vahendusel. Selleks on kas kasutajakontole antud vajalikud volitused, või toimub juurdepääs sekundaarse sisselogimise abil. Seeläbi ei ole enamikel juhtudel tarvis täielikku haldusalaste volitustega siselogimist.
- Laiendatud volitustega sisselogimine kohapeal - Antud lahenduse puhul tuleks takistada serveritesse sisselogimist kohapeal, tehes erandi vaid administreerimisega seotud väljavalitud kasutajakontodele puhul. Nimetatud kasutajakontod peavad olema kohandatud täpselt nende ettenähtud eesmärgi täitmiseks. Samuti on soovitatav rakendada niisuguste kontode puhul täiendavaid piiranguid, nt sessiooni kestvuse piiranguid. Alates Windows Server 2008 on riskid UAC-ga piiritletud (vt M 4.340 Windows kasutajakonto haldamise (UAC) kasutamine alates Windows Vistast). Asjakohased strateegiad on soovitav kirja panna Windows Server-ite keskkondade käsitleva poliitika erinevatesse strateegiatesse.

Konfiguratsiooni muutmine

Igapäevase kasutuse käigus ja hoolduseks ette nähtud ajal

Planeerimistööde käigus tuleb arvestada faktiga, et käideldavuse ja usaldusväärsuse seisukohast vaadelduna tuleb jooksva kasutuse käigus sisseviidavaid konfiguratsiooni muudatusi pidada kriitilisteks (vt M 4.78 Konfiguratsioonimuudatuste hoolikas teostamine). Seetõttu tuleb haldusalaste ülesannete planeerimisel vahet teha ülesannetel, mida täidetakse jooksva töö käigus ja ülesannetel, mida saab täita ainult spetsiaalselt hoolduseks ette nähtud ajal. Kõik see sõltub suuresti Windows Server konfiguratsioonist, selle täiendavatest serverirakendustest ja nõuetest, mis esitatakse süsteemi käideldavusele. Konfiguratsiooni muudatuste

sisseviimisel tuleks eelistada spetsiaalselt hoolduseks ette nähtud aegasid, kuna sõltuvalt olukorrast võib jooksva kasutuse käigus tekkida vajadus kutsuda esile serveri taaskäivitus.

Haldamiseks kasutatavad tööriistad

Üheks oluliseks aspektiks on erinevatele serveritele sobivate haldusalaste tööriistade väljavalimine. Windows Server 2008-ga tootja poolt kaasa antud tööriistu saab väga hästi integreerida operatsioonisüsteemi turvamehhanismide alla, mis võimaldab luua ka tervikliku käitamiskontseptsiooni. Peamised haldamiseks kaasa pandud komponendid on järgmised:

- Microsoft Management Console (MMC) - Peaaegu kõiki komponente tuleb hallata eraldi MMC-Snap-In-iga. MMC-ga saab läbi haldusjaama hallata eemalasuvate serverite komponente. Paljud kolmandate tootjate poolt loodud tööriistad kasutavad MMCd haldusalase liidesena.
- Server Manager - Alates Windows Server 2008-st on tsentraalselt toimivad haldusfunktsioonid koondatud tarkvaratööriista Server Manager alla. Server Manageri jaoks on MMC Snap-In'ina saadaval ka Server Manageri konsool.
- Kaughaldus Remote Desktop -i vahendusel - Remote Desktop -i kasutamine võib vähendada serveri turvalisust, mõjutades selle terviklust ja konfidentsiaalsust, vt G 5.132 RDP-seansi kompromiteerimine. Sellele lisaks kaasnevad ka kõrgendatud nõudmised organisatoorsele tööle.
- Konsoolid, mis nõuavad IIS-i (Internet Information Services) kasutamist. Neid on tarvis kasutada rakendusserveri administraatoritel ning osaliselt läheb neid tarvis ka sertifitseerimisteenuste läbiviimisel. Peale selle baseerub veebi baasil ka paljude kolmandate tootjate poolt loodud konsoolide kasutamine. Siinkohal tekib täiendavaid ohtusid, mille kaitseks võib sõltuvalt olukorrast olla tarvis kasutusele võtta täiendavaid kaitsemeetmeid.
- Käsuviiba käsud - Paljusid Windows Server-ite komponente on võimlaik hallata käsuviiba (command prompt) käskudega. Tegu on võimsate tööriistadega. Kuna käskude süntaks on osaliselt väga keeruline, kaasneb nende rakendamisega märkimisväärne väärkasutuse ja väärkonfiguratsioonide oht. Nende kasutamine peaks keskenduma juhtudele, kus ei ole piisavas mahus võimalik rakendada GUI-baasil toimivaid tööriistu. Mõningaid seadustusi saab seevastu tõesti teha ainult vastavate käsuviibalt sisestavate käskudega.

Mõnikord on konkreetne rakendusjuhtum ka eraldi dokumentides välja toodud ning neid kajastavad nt Microsoft Knowledge Base , Windowsi abi või ka muud tootjate poolt veebis avaldatud dokumendid. Konkreetse kasutusvaldkonnaga seotud garantiitingimuste ja tootjapoolse tugiteenuse ulatusega on soovitav ennast juba varakult kurssi viia. Käsuviiba käskude rakendamine on sobilik neil juhtudel, kus erinevaid protsesse on tarvis väga paindlikult automatiseerida, nt skriptide abil. Enne skriptide kasutuselevõtmist tuleb need läbi katsetada testsüsteemides (vt M 2.367 Käskude ja skriptide kasutamine alates Windows Server 2003-st). Mõningad kolmandate tootjate konfigureerimise standardprotseduurid ja haldusprogrammid võivad nõuda Windows Server 2008 konfiguratsiooni täiendavat muutmist, nt juhtudel, kui on tarvis kasutada IIS-komponente või .NET-Framework-i. Selle tagajärjel võib langeda serveri turvalisus. Kasutuselevõtu üle otsustamisel tuleks

kontrollida ka nende sobivust (vt B 1.10 Tüüptarkvara). Haldusega seotud ülesannete täitmisel tuleks vältida 16-bitiste programmide kasutamist.

- Kaughaldus
- Juurdepääs üle LAN-i - Tootega kaasas olevad Remote -tööriistad võimaldavad LAN-i piires Windows Server -itele efektiivselt juurdepääsu. Tavapärase turbeastme täitmiseks piisab, kui on täidetud kõik Windows Server-ite IT-turvapoliitika nõuded. Turvapoliitikas peaksid kajastuma ka selged ettekirjutused, milliseid Remote -tööriistu, nt Remote Desktop -ühendusi lubatakse LAN-is kasutada.
- Juurdepääs läbi turvalüüside - Turvalüüsidel põhinevate juurdepääsude kasutamine peaks põhinema KP-turvapoliitikal. Remote -tööriistu võib kasutada nii mõnes teises LAN-i ühendatud arvutis kui ka väljaspool, nt Interneti vahendusel. Kaugpöördusel toimivate juurdepääsude puhul, mis saavad alguse väljaspool turvalüüsidega kaitstud IT-keskkonda, tuleb autentimise protseduur ja andmeedastus varustada krüpteeringuga. Selleks on soovitav kasutada HTTPS-i või VPN-i. Lisaks on soovitav võimaldada väljastpoolt tulevatele klientide juurdepääs ainult teatud vähestele arvutitele. Selleks tuleb halduskontspetsiooni kaasata kõik puudutatud komponendid (nt turvalüüsid, VPN-lüüsid).

Kaugpöördusel toimiva halduse planeerimisel tuleb kaugpöörduse jaoks koostada ka oma turvapoliitika. Selleks tuleb vastavalt kohandada ja täiendada organsatsiooni üldkehtivaid IT-turvapoliitikaid.

Välised teenusepakkujad

Eraldi turvagrupid

Spetsiaalselt väljasttellimisele kehtivad nõuded (vt B 1.11 Väljasttellimine (Outsourcing)) ja väliste teenusepakkujatega sõlmitavates lepingutes rakendatavad kokkulepped tuleb sisse töötada volituste kontseptsiooni (vt eespool). Välistele teenuseosutajatele tuleb luua eraldu turvagrupid, andes neile vaid sellised Windows Server piiratud volitused, mis on nende tööks hädavajalikud. Olemasolevad standardsed grupid ei ole sellistel juhtudel enamasti sobivad. Enne andmevarunduse teenuse tellimist tuleks nt kontrollida, kas turvagrupiga Varunduse operaatorid kaasnevad volitused pole selleks otstarbeks mitte juba liiga laialdased. Haldusega seotud kontode sisselogimisandmete edastamine ning ühtse paroolipoliitika kehtestamine on eriti keeruline neil juhtudel, kui teenusepakkuja ülesandeid täitev isik ei tööta kohapeal (vt G 2.111 Pääsuõiguste kuritarvitamine teenusepakkuja vahetumisel). Juhul kui lisaks kõigele muule kasutatakse ka Active Directory, pole domeeni piires väliste teenusepakkujate jaoks võimalik läbi suruda erinevaid paroolipoliitikaid. Seetõttu tuleb antud valdkond lahendada organisatoorsete meetmete abil ning kirjutada vastavad nõuded sisse juba IT-turvapoliitikasse.

Paikade ja täiendite paigaldamine

Windows Server-ite võimaldab täiendeid paigaldada regulaarselt ja automaatselt. Siinkohal tuleks läbi kaaluda võimalikud ohud, mis tekivad automaatsel taaskäivitusel ja juhtudel, kus täiendid ei puugi kokku sobida juba eelnevalt installeeritud programmidega. Kõrge kaitsevajadusega serverite puhul tuleks antud funktsioon desaktiveerida. Tavapärase kaitsevajaduse puhul tuleks Automatic Update

funktsiooni kasutamise otsus langetada vastavalt konkreetsele olukorrale. Automaatseid täiendeid ei tuleks hankida otse Internetist. Nende haldamiseks ja installeerimise heakskiitmiseks tuleks kasutada tarkvara jagamissüsteemi (nt Windows Server Update Service, WSUS, näiteks M 4.417 Paikade haldus WSUS-iga alates Windows Server 2008-st). Siinkohal tuleb koostada reeglid, milliseid täiendeid ja paikasid tohib installeerida automaatselt ning millised täiendid ja paigad peavad eelnevalt saama administraatori heakskiidu. Kõikidel juhtudel tuleb rakendada meedet M 2.273 Turvalisust mõjutavate paikade ja värskenduste kiire paigaldamine ja tagada selle ettekirjutuste järgimine. Enne Service Pack-ide paigaldamist keskkonda tuleks koostada asjakohane Roll-out -strateegia (serverite järjekord, ka võimalik Rollback). Siinkohal tuleb arvestada et Service Pack -id võivad sisaldada teatud uusi funktsioone, mis tuleb serverile installeerida teatud kindlate rollide alla. Üheks sellekohaseks näiteks on Service Pack 1-e uus turvagrupp Distributed COM-users.

Dokumentatsioon

Dokumentatsiooni kontseptsioon

Haldamise planeerimistööde hulka kuulub ka dokumentatsiooni kontseptsiooni puudutavate nõuete väljatöötamine. Kontseptsioon peaks olema tihedalt kooskõlas muudatuste haldamisega (vt M 2.221 Muudatuste haldus).

Ülesanded, volitused ja administraatorite tööriistad

Dokumentatsiooni tuleb üles märkida administraatorite tööülesanded, tööülesanneteks vajaminevad tööriistad koos nende jaoks vajalike volitustega (ka ressursivolitused), et nende jätkuv kasutamine oleks tagatud ka personali väljalangemise korral (vt G 1.1 Personali väljalangemine ja M 2.31 Volitatud kasutajate ja õiguste profiilide dokumenteerimine .

Töökontode paroolid

Töökontode paroolide dokumenteerimiseks tuleb koostada sobiv asjakohane kontseptsioon. Antud paroolid on kriitilise tähtsusega ning seetõttu peab neile kehtima range juurdepääsukontroll (nt seif, mitmekordne krüpteering ja neljasilmaprintsiip).

Administratiivsete skriptide kasutamisel tuleb dokumentatsiooni vastavalt täiendada. Dokumenteerimiskohustuse alla kuuluvate konfiguratsioonide ja kasutusvaldkondade puhul võib kasutada skriptide testimiskeskkonna dokumentatsiooni (vt M 4.240z Serveri testimiskeskkonna rajamine).

Täiendavad kontrollküsimused:

- Kas IT-osakonna töötajatel on loodud nii tavalised kui ka haldusülesannete täitmiseks ette nähtud kasutajakontod?
- Kas kaughoolduse läbiviimine on korraldatud piisavalt turvaliselt?
- Kas täiendite paigaldamise kohta on vastu võetud reeglid, mis tagavad selle tegevuse piisava turvalisuse?
- Kas hoolduse läbiviimiseks on kehtestatud spetsiaalsed hooldusajad?

M 2.365 Süsteemiseire planeerimine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator, vastutav spetsialist, audiitor

Sündmuste logid

Windows Server 2003 käitamise raames koostatakse mitmekesiseid ja põhjalikke sündmuste logisid. Vastavate logide peamiseks eesmärgiks on tuvastada ja tagada korrakohane töö ning tegeleda ka veaanalüüsiga. Logid võetakse tihti aluseks revisjonide ja muude hindamiste käigus.

Logimise põhimõtted

Protokollide sisust sõltuvad nende säilitamiskohustuse kestvus ning andmekaitsekohutusega seotud aspektid. Logimise põhimõtted peaksid vastama seadustest tulenevatele ettekirjutustele ja suutma minimeerida logiandmete väärkasutust ning sellega kaasnevaid ohtusid ja riske (vt M 5.9 Serveri logi , M 2.64 Logifailide kontroll ja M 2.110 Andmeprivaatsuse suunised logimisprotseduurides).

Seire ja logimise põhimõtted

- Logisid tuleks lasta koostada ainult vajaminevas mahus. Nende koostamine nõuab ressurssi ja salvestiruumi. Rakendada tuleks vältimise põhimõtet.
- Kõrgemad turbenõuded nõuavad üldjuhul ka laiaulatuslikumat seiret.
- Logisid tuleb koostada põhjendatud, kindlaksmääratud eesmärkidel ning need peavad lähtuma eesmärgist.
- Seire ja logimine peab teenima organisatsiooni huvisid ning selle läbiviimine peab olema kooskõlastatud töötajate esinduse ja andmekaitsespetsialistiga.
- Logisid tuleb kaitsta volitamata juurdepääsu, manipuleerimise ja hilisema täiendamise eest.
- Logisid tuleb regulaarselt ja kohe esimesel võimalusel analüüsida.
- Logide korrektse analüüsimise tarbeks tuleb koostada täpsed ja sünkroonsed ajasisestused ning defineerida selleks vajalikud formaadid, liidesed ja protseduurid.
- Logide analüüsimise tarbeks vajalike põhimõtete väljatöötamisel tuleks lähtuda moodulist B 1.8 Turvaintsidentide käsitlus .
- Logid tuleks pärast maksimaalse säilituskohustuse tähtaja ületamist kustutada.

Seirepoliitika

Seirepoliitika kehtestamine

Serveri seirepoliitika koostamisel tuleb aluseks võtta Windows Server 2003 seirepoliitika ning teha vastavad mugandused. Seirepoliitikas määratakse kindlaks, kes peaks jälgima erinevaid sündmusi ning millised reaktsioonid peaksid järgnema teatud sündmustele kindlaksmääratud reaktsiooniaja raames ning kuidas tuleks logiandmetega ümber käia. Windows Server 2003-le kaasa pandud turvamaalide failid asuvad kaustas *%SystemRoot%\Security\Templates*. Neid on võimalik vaadata halduskonsooliga MMC (Snap-In *Turvamallid*) ning need on mõeldud ülevaate saamiseks ja orienteerumiseks. Seire alla kuuluvad kasutajad ja sündmused määratakse kindlaks *Grupipoliitikate* -Snap-In-is. Dokumenteeritud peaks olema, kas ning kui jah, siis millistel põhjustel tuleks järgmiste kategooriate puhul logida õnnestunud ja/või ebaõnnestunud sündmusi:

- Sisselogimiskatsed
- Sisselogimisel esinenud sündmused
- Kontode haldamisega seotud sündmused
- Active Directory juurdepääsud
- Objektijuurdepääsud
- Volituste kasutamine
- Protsesside tagantjärele monitoorimine
- Süsteemisündmused
- Poliitikate muudatused

Objekti seire

Seire aktiveerimine

Objektjuurdepääsude (nt andmete) seire korraldamisel puhul tuleb jälgida, et see peab olema sisse lülitatud nii serveri seirepoliitika kui ka väljavalitud objektide omadustele kehtiva seirepoliitika rakendamise raames. Windows Server 2003 lubab administraatoritel nt faile enda omandisse üle võtta ning lubab neid edastada ka kolmandatele osapooltele, st ka nende algsele omanikule. Viimane seetõttu ainult piiratult võimeline niisuguseid tegevusi tuvastama. Seetõttu tuleks niisuguseid, seire alla kuuluvaid objekte kajastavaid sündmusi analüüsida võimalikult usaldusväärselt.

Sündmuste logid

Logisid on võimalik käsitsi vaadata ja hallata *Sündmuste kuva* -ga. Iga üksik sissekanne sisaldab veel ka täiendavat, detailsemat infot ning selget sündmuste ID-d, mille kohta on olemas põhjalikud kirjeldused. Sündmuste kuva konfiguratsioon peab olema määratletud. Selleks tuleb arvestada järgmiste aspektidega:

- Rollide lahutamine - Sündmuste logide salvestamise asukoht võib mõnikord standardsest seadistusest *%SystemRoot%\system32\config* ka erineda, nt juhtudel, kus administraatoritele ei tohi jätta võimalusi mõjutada logide analüüsimist. Selles kaustas asub ka register. Seetõttu ei ole mõttekas administraatoritelt juurdepääsu selle kaustale ära võtta. Alates versioonist Windows Server 2003 on võimalik volitusi piirata sündmuste kuva logide juurdepääsu alusel. Erinevate logide pääsuloendid (*Access Control List* , ACL) määratletakse turbekirjelduskeele abil (*Security Descriptor Definition Language* , SDDL) registri parameetris *CustomSD*. Alternatiivse lahendusena saab haldamist ja seiret teineteisest lahutada ka mõne süsteemihalduse tööriista abil, mille kasutamiseks vastavale administraatorile volitusi ei anta.
- Logide suurus ja nende säilitamine - Logifailide maksimaalne suurus peab olema kooskõlas nende ülekirjutamisega, võimalike sündmuste oodatava mahuga ja logimise alla kuuluva seire kestusega. Juhul kui konfiguratsiooniks valitakse „Sündmusi mitte kunagi üle kirjutada," tuleb tagada, et logifail ei muutuks liigas suureks, kuna see võib hakata süsteemi pärssima. Vastasel korral võib juhtuda, et serveri töö jääb seisma ja server lülitab ennast välja, muidugi eeldusel, et turvaseadistused on niimoodi tehtud. Eesmärgiks seatud käideldavust ei suudeta sellistel juhtudel alati tagada.

- Olulised logid - Sündmuste logid sisaldavad vähemalt järgmisi logisid: süsteem, rakendus ja turvalisus. Sõltuvalt serveri rollist ja funktsioonist võivad kajastuda ka järgnevad täiendavad logid nagu kataloogiteenus, DNS server ja andmete tiražeerimisteenus. Täiendavad failipõhised logid, millega peab sõltuvalt serveri rollist ja funktsioonist arvestama on IIS-logid, RRAS-logid ja RADIUS-logid
- Sündmuste tüübid - Logides võivad kajastuda vead, hoiatused, informatsioon, õnnestumiste seire, ebaõnnestumiste seire.

Logides kajastatud sündmuste seireinstrumendid

Seireinstrumendid

Logisid on võimalik analüüsida vastavalt vajadusele kas käsitsi (nt *Sündmuste kuva* abil), kasutaja poolt defineeritud skriptide abil (nt *Eventlg.pl* , *Eventquery.vbs*), spetsiaalsete tööriistadega (nt *Dumpel.exe* , *Auditusr.exe* , *EventCombM* T) või täisautomaatsete haldustööriistadega (nt *Microsoft Operations Manager 2005,* MOM 2005). Nendele lisaks on saadaval ka teiste tootjate lahendusi.

Viited allikatele:

Tööriist	Allikas
Eventlg.pl	Windows 2000 Resource Kit, Supplement 1
Eventquery.vbs	Windows 2000 Resource Kit, Supplement 1
Dumpel.exe	Windows 2000 Server Resource Kit, Supplement 1
Auditusr.exe	Windows Server 2003 mit SP1 koostisosa
EventCombMT	Microsoft Windows Server 2003 Resource Kit Tools

Need tooted katavad sellised seirevajadused, mille puhul võib Windows Server 2003 enda vahenditest vajaka jääda. Siia alla kuulub näiteks teavitamine SMTP abil, reageerimine sündmustele reaalajas või ligikaudne kohtulik analüüs kahtlaste sündmuste tuvastamiseks ja põhjustajate leidmiseks.

Käideldavuse seire

Windows Server 2003 või selle teenuste käideldavuse seire puhul tuleb arvestada, et usaldusväärset seiret ja automaatset eskalatsiooni suudab tagada ainult sõltumatu kolmas süsteem. Seirepoliitikas peaks muuhulgas olema dokumenteeritud ka rakendatava seire liik.

- Automatiseeritud seire. Käsitsi seire ja analüüsimine ei ole soovitav. Käsitsi seire ja analüüsid on suure veapotentsiaaliga ja subjektiivsed, neis esineb inimestest tingitud kõikumisis ning on ainult piiratud kujul kättesaadavad. Käsitsi seirele ja analüüsimisele tuleks eelistada automatiseeritud seiret ja analüüsi. Lähtuda tuleks sobivuse põhimõttest. Detailsemaid kirjeldusi soovitatud lahenduste kohta leiate Microsofti turvaseire ja rünnete tuvastamise planeerimise käsiraamatust. Ka neil juhtudel, kus Windows Server 2003-e

turvaseire puhul on kõrgeimaks prioriteediks seatud sündmuste kuva turvalogi, ei tohi jätta tähelepanuta teisi sündmusi ja nende logimist, mis on samuti turbe seisukohast olulised. Sündmuste logides kajastatud andmed tuleks regulaarselt viia seosesse teiste andmetega nagu nt puhkusepäevadega, puhkepäevadega, kellaaegadega jms, et tuvastada kõrvalekaldumisi „normaalsest“ kasutustest.

- System Monitor. System Monitor pakub oma jõudlusi kajastavate logide ja hoiatustega usaldusväärset infot ressursside nagu nt põhimälu, protsessori, võrgu ja kõvaketta ruumi käideldavuse kohta reaalsel ajahetkel. Määratletud väärtuse ületamisel on see võimeline väljastama automaatse hoiatuse. Sellega on võimalik toetada serveri käideldavuse kindlustamist. Pikema ajavahemiku jooksul kogutud jõudlust kajastavate logide statistiline analüüs võimaldab analüüsida võimalikke trende ja aitab kaasa riistavara õigeaegsele ja vajadustest lähtuvale moderniseerimisele. System Monitoriga on võimalik jälgida ka printimise ootejärjekordi.
- Riistvara - Riistvarakomponentidega, mis soetati spetsiaalselt käideldavuse tõstmiseks (nt puhvertoiteallikad, temperatuuri jälgimine), seotud sündmused või logiandmed tuleb kaasata seiresse.
- Rakendused - Rakendused võivad dokumenteerida turvalisuse seisukohast olulist infot rakenduste logis, sündmuste kuvas või oma enda logides. Selline info ja/või logid tuleb samuti kaasata seiresse.

Dokumentatsioon

Seirepoliitika kui dokumentatsioon

Dokumentatsioonina kasutatakse seirepoliitikat. Lisaks tuleks Windows Server 2003 süsteemi efektiivse seirepoliitika tarbeks koostada asjakohased turvamallid (.inf failid). Täiendavate tööriistade kasutamisel tuleb dokumenteerida ka veel jälgitavad objektid ja logitud sündmuste tüübid.

Täiendavad kontrollküsimused:

- Kas seire ja logimise põhimõtetest peetakse kinni?
- Kas turvapoliitika baasil on loodud Windows Server 2003-e jaoks eraldi seirepoliitika?
- Kas lisaks turvalogile ja sündmuste kuvale analüüsitakse veel ka täiendavaid logisid?
- Kas seire raames saadud tulemusi rakendatakse ka tuvastamata kitsaskohtade leidmiseks ja koolituse eesmärgil?
- Kas töökontod on kaasatud regulaarsesse seiresse, mis tuvastab võimalikku väärkasutust, nt ebaõnnestunud katsete seiresse?

M 2.366 Windows Serveri turvamallide kasutamine

Algatamise eest vastutavad: IT-juht, infoturbeosakond
Rakendamise eest vastutavad: administraator

Windows Server 2003 turvaparameetrite konfigureerimiseks on võimalik kasutada *turvamalle* . Kuna enamikus süsteemi valdkondadest esineb turvalisuse seisukohalt olulisi aspekte, tuleb malle käsitleda kui olulisi ja tõhusaid administreerimisvahendeid. Nende abil on võimalik parameetreid standardiseerida ja tsentraalselt administreerida. Tähtsaimad mallide tööriistad on turvakonfiguratsiooni redaktor (inglise k *Security Configuration Editor* , SCE) ja turvakonfiguratsiooni viisard (inglise k *Security Configuration Wizard* , SCW, mis on olemas alles alates remondipaketist 1).

Turvamallid

Erinevalt administratiivsetest mallidest (M 2.368 Administratiivsete mallide kasutamine alates Windows Server 2003-st) sisaldavad turvamallid parameetrite konkreetseid väärtusi. Turvamalli aktiveerimine lokaalse süsteemi turvapoliitikas muudab süsteemi konfiguratsiooni koheselt. Kõik malli seadistused aktiveeritakse koheselt ning konfigureeritakse konkreetse väärtusega.

Windows NT-4,0-mallide migreerimine

Windows NT 4.0 malli tüüpi (failid laiendiga *pol*) ei tohiks *Windows Server* 2003-ga enam kasutada. Seda tüüpi olemasolevad turvamallid tuleks grupipoliitika objektidena uuesti luua. *Windows Server 2003 Resource Kit* programmi *Gpolmig.exe* kasutades on võimalik vähendada selleks tehtavaid kulutusi.

Üldised ettevaatusabinõud turvamallide kasutamisel

Ohtude kataloogi punktis G 3.81 Turvamallide väär kasutamine alates Windows Server 2003-st on loetletud mõned ohud. Hoolika planeerimise ja rakendamise ning põhireeglite järgimisega on võimalik kindlustada turvamallide soovitav mõju sihtsüsteemis.

Nõuete analüüs

Kõigepealt tuleks kindlaks määrata arendustööks ja testimiseks vajaminevad kulutused. See sõltub erinevalt konfigureeritud sihtsüsteemide arvust, seadistuste liigist ja arvust mallis, samuti ettenähtud strateegiast mallide jagamisel sihtsüsteemidele. See tuleks eelnevalt nõuete analüüsi käigus välja selgitada, milles tuleb järgida ka olemasolevaid IT-koosluse turvasuuniseid.

Testimiskeskkond

Igal juhul on soovitatav testimis- ja arenduskeskkonna olemasolu või vähemalt ajutiselt isoleeritud testimisserver. Mida suurem on seadistuste ja sihtkonfiguratsioonide arv, seda suuremad on kulutused testimiskeskkonnale. Mida rohkem sarnaneb testimisserveri konfiguratsioon teatud kindlas valdkonnas potentsiaalsete sihtserverite tegelikule konfiguratsioonile, seda paremini on võimalik ette ennustada malli mõju nimetatud valdkonnale. Tehnilised kulutused üksikseadistustele, nagu näiteks paroolide pikkusele, on väikesed ning seotud väiksemate ohtudega (testimiskeskkond ei ole siin just tingimata vajalik). See kehtib eriti juhul, kui need kantakse grupeerimissuunistena automaatselt üle kõikidele asjakohastele serveritele ja klientidele.

Turvamallide levitamise ja aktiveerimise (*rollout*) strateegia töökeskkonnas

Turvamallide levitamine ja aktiveerimine töökeskkonnas (edaspidi ka *rollout*) on seotud suurte riskidega, eriti kui testimisel ei ole piisavalt mõistetav, millist mõju hakkavad kriitilised seadistused avaldama sihtserverile. Sel juhul on turvamal-

lide levitamisel ja aktiveerimisel esialgu vajalik piirduda vähemkriitiliste serveritega ning alles pärast edu saavutamist seda protsessi laiendada. Lisaks sellele tuleks planeerida ja testida niinimetatud tagasipöördumise (*rollback*) strateegia. Tagasipöördumine (*rollback*) tähendab, et serveri konfiguratsiooni on võimalik probleemide tekkimise korral viia tagasi endisesse seisundisse. *Rollout* - ja *rollback* -strateegiate rakendamisel tuleks tagada süsteemi staatuse kaitse ja usaldusväärne ennistamine. Paljudel juhtudel on kindlam jaotada suur hulk seadistusi mitme turvamalli vahel ja neid siis etappide kaupa rakendada. Turvamalle võib olla näiteks teatud kindlate *Windows Server* 2003 komponentide, asutuste ja ettevõtete valdkondade või turvaastmete jaoks (nt baasturvalisus ja kõrge turbeaste). Selline tegevusviis on edasiste mallide arendamiseks selgelt paindlikum, kuna sihipäraselt spetsiifilisi turvamalle on võimalik asendada, samal ajal kui kindlad põhiseadistused jäävad alles. Etapiviisilise rakendamise korral võib tekkida konfliktseid olukordi, kui kaks malli defineerivad ühte ja sedasama seadistust. *Rollout* -strateegiast oleneb, milline mall domineerib. Turvamalle võib rakendada käsitsi ühel serveril või saata need automaatselt mitmele serverile korraga. Käsitsi rakendamine toimub SCE või SCW konsoolide abil ning on soovitatav üksikutele kõrge turbeastmega serveritele, kuna nii on võimalik soovimatud mõjud kõige kiiremini avastada ja kõrvaldada. Automatiseerimine toimub skriptide või *Active Directory* abil. Viimane on etapiviisiliseks rakendamiseks kõige sobivam, kuna väikeste kulutustega on võimalik välja jagada terve rida malle ning määrata kindlaks parajasti domineeriv mall. On arusaadav, et enne turvamallide produktiivset rakendamist tuleb iga IT-valdkonna jaoks kontseptuaalselt kindlaks määrata sobiv strateegia. Turvamallid võivad *Windows Server* 2003 konfiguratsioonimuutuste ühiskasutusse andmise protsessi, samuti ka ettevalmistuskontseptsioone (M 4.281 Windows Server 2003 turvaline installeerimine ja ettevalmistus) oluliselt läbipaistvamaks muuta. Need tuleks kaasata M 2.221 Muudatuste haldus raames ühiskasutusse andmise protsessi.

Security Configuration Editor (SCE)

SCE koosneb standardinstallatsiooni kohaselt konsoolidest:

- *Lokaalne turvapoliitika* (*start* / *süsteemi juhtimine* / *haldus*): rakendab turvaseadeid otse lokaalsel serveril
- Turvamallid: koostab ja haldab turvamalle (*inf* -failid), ei vii serveril läbi konfiguratsioonimuutusi
- *Turvakonfiguratsioon ja –analüüs* : Turvaseadete modelleerimine ja süsteemi analüüs vahelelülitatava konfiguratsiooni andmebaasi abil, turvamallide eksport ja import, turvasuunistele vastavuse kontroll, modelleeritud turvakonfiguratsiooni aktiveerimine.

Turvamallide ning *turvakonfiguratsiooni-* ja *analüüsi* konsoolid käivitatakse *Microsoft Management Console* (MMC) kaudu.

SCE hõlmab keskseid turvaseadeid

SCE tööriistagrupi abil seadistatakse kõik *Windows* arvutite vahelise võrguliikluse autentimise ja signeerimise aspektid. Lisaks sellele kehtestatakse siin kõik

kesksed turvaseaded serverile, muuhulgas monitooringu suunised ja volitused failisüsteemis ja registreerimisandmebaasis. Domeenides sisaldavad SCE-konsoolid lisaseadeid *Kerberos* 'i ja teiste domeeni sätete jaoks. Kõik need seaded on võimalik salvestada turvamallidesse. Alati on soovitatav installeerida uusimad tootja poolt pakutavaid turvasätted.

Näidismallid

Windows Server 2003 juurde kuuluvad mõned erinevatele turvanõuetele vastavad turvamallid. Need paiknevad kaustas C:\ *Windows**security**templates* . Lisaks nendele on tootjalt võimalik hankida teisi dokumenteeritud malle.

Tagasipöördumine (*Rollback)*

Piiratud õigustega gruppide, süsteemiteenuste, sisselogimise ja failisüsteemi sätteid ei ole võimalik *rollback* 'i abil tühistada. Sellised sätted on võimalik mõnda teist turvamalli kasutades uuesti kehtestada. *Rollback* 'i variant kujutab endast *rollback* -mallide paralleelset väljatöötamist, mis asendab tegelike turvamallide sätted tõrke korral vähemkriitilisemate väärtustega. Eriti kriitilised on ressurssidele ligipääsetavust reguleerivad pääsuloendid (ACL) ja objektide kontrollseaded (SACL). Volituste kontseptsioonid, mida kujutatakse turvamallides, võivad malli kasutamisega olemasolevad volituste struktuurid pöördumatult hävitada (vt M 2.370 Volituste haldamine alates Windows Server 2003-st .

Iga serveri jaoks peaks olema oma turvamall

Iga serveri jaoks peaks olema siduvalt kindlaks määratud kõik sätted punktide all *Kontosuunised, Lokaalsed suunised* ja *Sündmuste protokollimine* . Seejuures tuleb arvesse võtta IT-turvasuuniseid ja vaadeldava IT-koosluse turvakontseptsioone, samuti IT-etalonturbe meetmeid. Lisaks sellele on soovitatav kasutada *Windows Server* 2003 standardseadeid, samuti ka selle juurde kuuluvaid turvamalle. Iga serveri jaoks peaks olemas olema kehtiv turvamall või turvamallide kogum. Serveri turvakonfiguratsioon peaks vastama turvamallide viimati dokumenteeritud seisule.

Kindlaksmääratud vastavusnõuded IT-koosluse IT-turvasuunistes.

Turvakonfiguratsiooni viisard (*Security Configuration Wizard* , SCW) kujutab endast turvakonfiguratsiooni redaktori (*Security Configuration Editor*, SCE) laiendust ja osalist lihtsustust. Kehtivad ühed ja samad põhimõtted. Nõuandeid ja soovitusi turvakonfiguratsiooni viisardi (SCW) kasutamiseks leiab IT-etalonturbe abivahendite alt.

Dokumenteerimine

Turvamallide minimaalseks dokumenteerimiseks piisab, kui iga serveri kasutatavad mallifailid (failid laienditega *inf* või *xml*), nende versioon ning enda loodud mallide puhul ka nende sisu esitada süsteemi dokumentatsioonis. Vastava turvamallide versioonihalduse ja pääsukontrolli olemasolu korral peaks olema võimalik kindlaks teha, kes, millal ja milliseid turvamalle muutis. Kui turvamallide ettevalmistamine toimub *Active Directory* abil, tuleb dokumenteerida kõik ülejäänud faktorid, millest sõltub serveri või serverite seadistuste efektiivsus, nt *Organization Unit* (OU), *Windows Management Instrumentation* , WMI filtrid. Alati peab olema arusaadav, kust mingi turvaseade pärineb. Selle alusel peaks toimuma dokumentatsioonide ja vajadusel testimise kontseptsioonide, mõned skriptide ning turvamallidega seoses oleva valmisoleku ja tagasipöördumise (*rollback*) strateegiate loomine. Dokumentatsiooni tuleks rakendada ka süsteemi- ja turvaprotokollide regulaarse analüüsi planeerimiseks.

Turvamallid - sobiv alus süsteemi dokumentatsiooni koostamiseks

Turvakonfiguratsiooni viisardi (SCW) turvamallide jaoks on kaasas transformatsiooni ja laadilehe failid mallide kuvamiseks ning väljatrükkimiseks (*C:\WINDOWS\security\msscw\transformfiles*). Sellest piisab serveri rollide baasdokumentatsiooniks süsteemi dokumentatsiooni koostamise raames.

Aktiivsete seadete dokumenteerimiseks sobib hästi GPMC-konsool (*Group Policy Management Concole*), juhul kui rakendust leiab *Active Directory.* Rühmapoliitika objektide (*Group Policy Objects* , GPO), RSoP (*Resultant Set of Policy*) ja rühmapoliitika moodulite jaoks saab raportid trükiformaadis HTML-faili eksportida (soovitav objekt markeerida / menüü *Toiming* / *Salvesta rapo*rt . . .).

Täiendavad kontrollküsimused:

- Kas rakendatakse turvamalle ja kas neid kaasatakse muudatuste halduse testimise ja ühiskasutusse andmise protsessi?
- Kas turvamallide seaded põhinevad tootja käesoleval ajal kehtivatel turvasoovitustel?
- Kas turvamallide rollout - ja rollback - strateegia või rollback -mallid on planeeritud ja testitud?
- Kas turvamallide failid alluvad versiooni- ja pääsukontrollile?
- Kas kasutusel on Windows NT 4.0 vananenud mallid?

M 2.367 Käskude ja skriptide kasutamine

Algatamise eest vastutavad: IT-juht, infoturbeosakond
Rakendamise eest vastutavad: administraator

Praktikas kasutatakse käske ja skripte tihti väikeste ülesannete täitmiseks, nt mingi parameetri kehtestamiseks ja kuvamiseks. Skriptid on võimsad töövahendid, mille kasutamine võimaldab käskude automaatset täitmist. Kahjupotentsiaal nende vale ja asjatundmatu kasutamise puhul võib olla üksikute käskudega võrreldes mitmekordne. Seepärast tuleb skripte kasutada kaalutletult, et nende mõju oleks kontrollitav ja mõistetav. Kui aktsepteeritakse planeerimis-, kavandamis- ja hoolduskulusid, on skriptide abil võimalik administratiivseid ülesandeid lihtsustada ja standardiseerida.

Käsk

Käskude all mõistetakse programmide käivitamist välja abil Käivitamine. . . või andmesisestuse käsurea kaudu. Seda nimetatakse traditsiooniliselt ka “DOSbox”. Kõike, mida saab käivitada CMD-käsurealt, nimetatakse käsuks. Seejuures tuleb teha vahet varjatud käskude ja CMD-käsurea juhtimiskonstruktide, operatsioonisüsteemi ja teiste tootjate käskude vahel. Käske saab koondada loetavatesse failidesse (pakktööde fail, spetsiaalne skript-fail).

Skript

Skript on klaartekstfail, mida saab koostada suvalise tekstiredaktoriga (nt notepad.exe). Skriptis sisalduvad juhendid sooritatakse käivitamisel vastava interpretaatori poolt. Windowsi all kasutatakse skripte peamiselt administratiivsete tööde automatiseerimiseks. Eelkõige lihtsustavad need pidevalt korduvate administratiivsete ülesannete sooritamist. Kui nende sooritamine toimub automaatselt, nt Plaanitud tegumid kaudu, funktsioneerivad need ka administraatori äraolekul. Skriptide korduvkasutus tagab sooritatud ülesannete jälitatavuse ja ühtlase kvaliteedi.

Nõuded

Skriptide interpretaatoritele, tarkvaraga kaasasolevatele skriptidele ja tarnija lisapakettides sisalduvatele skriptidele (nt MBSA, Support Tools, Ressource Kit), samuti ise välja töötatud skriptidele peaks laienema samad nõuded kui tüüptarkvarale (vt B 1.10 Tüüptarkvara). Nõudeid ja tingimusi skriptide väljatöötamiseks ja rakendamiseks tuleb analüüsida ja selle põhjal siduvad parameetrid kindlaks määrata (vt M 2.83 Tüüptarkvara testimine). Skriptide väljatöötamise ja hooldusega tohivad tegelda ainult kvalifitseeritud spetsialistid. IT-süsteemi kriitilises talitluskeskkonnas ei tohi skripte kirjutada ega hooldada administratiivne personal, keda ei ole skriptide programmeerimise alal piisavalt koolitatud ning kellel on vähe kogemusi (vt G 2.67 Pääsuõiguste puudulik haldus). Eriti administreerimise ja selle automatiseerimise valdkonnas tuleb kindlalt tagada, et instrumentide või keerukate skriptide näol ei rakendataks keelatud või mitte aktsepteeritud tarkvara. Mitte teadaoleva päritoluga tarkvara rakendamisest tuleb loobuda.

Turvasuunised

Skriptide kasutamise raamistik tuleks sätestada turvasuunistes. Minimaalselt tuleb sätestada, millisel eesmärgil, millisest allikast pärinevaid skripte ja milliseid skriptide keskkondi või keeli tohib kasutada. Lisaks sellele tuleb kindlaks määrata skriptide arendusele ja vastuvõtmisele esitatavad nõuded teatud kindlates kasu-

tusvaldkondades. Kui turvasuunistes ei ole sätestatud teisiti, kehtivad turvameetmed B 1.10 Tüüptarkvara . Tuleb silmas pidada, et nt sisselogimisskriptid, ei ole teatud juhtudel iga kasutusvaldkonna jaoks efektiivsed ja praktilised. Põhimõtteliselt tuleks keelata mittesigneeritud skriptide kasutamine. Signatuuride aluseks on turvasertifikaadid. Tootja skriptid on juba signeeritud. Soovitatav on luua oma sertifikaadid sertifitseerimiskeskuse mallidest. Signeerimiseks kasutatakse Crypto-API spetsiaalseid programmeerimisobjekte, millele juurdepääs on võimalik skriptide abil. Lähemat informatsiooni pakub Windows Server 2008 Windows SDK.

Põhimõtted

Allapoole ühilduvuse probleem

Tuleb arvestada, et skriptid on küll reeglina ülespoole ühilduvad, kuid nende edasi arenedes uute funktsioonide kasutuselevõtu tõttu ei ole nad tihti allapoole ühilduvad.

Turvakontekst käivitamise ajal

Skriptide käivitamine toimub alati käivitaja turvakontekstis, st neil on käivitamise ajal käivitaja volitused. Kui skripte käivitatakse läbi teenuse või protsessi, on skriptidel selle teenuse või protsessi volitused. Paljudele funktsioonidele, millele on skriptide abil juurdepääs, vajatakse administratiivseid volitusi, mis laienevad üksikutele objektidele või kogu serverile.

Programmilähtetekstis mitte paroole kasutada

Kui skriptid (nt sisse-/väljalogimise skriptid) või teenused (nt seoses andmevarundusega) antakse kasutajate käsutusse, ei tohi skripti kehtimise ajal anda lubamatuid laiendatud volitusi või sisestada administratiivseid paroole. Tihti toimub skriptide jaotamine ja käivitamine domeenidesse sisselogimisel või Active Directory grupeerimissuuniste kaudu automaatselt. Tuleb tagada, et administratiivsete skriptide programmi lähtekoodid jääksid kasutaja eest varjatuks ning et skripti käivitamine ei häiri kasutamist. Vastavad seadistused paiknevad nt tarkvaraga kaasasolevates administratiivsetes mallides - Administratiivsed mallid \ Süsteem \ Skriptid.

Süsteemis sisalduvad võimalused skriptide loomiseks:

Käsurida

Windows Server 2008 ja hilisemate versioonide standardinstallatsioon sisaldab mitmeid võimalusi skriptide loomiseks ja käivitamiseks:

- Käsurida/CMD-kest ja pakktöötlusfailid (BAT, CMD). Tegemist on tootja skripti keskkonnaga, mis sisaldab ka dokumentatsiooni. Vanemate versioonide pakkprogrammeerimise võimalused olid piiratud, nüüd on need aga väga laialdased (nt on käsutuses FOR -käsk). Installeerimine ei ole vajalik.
- Microsoft Visual Basic Scripting (VBScript) ja JScript.VbScript on lihtne skriptikeel. Sellel puuduvad installeeritud administreerimisfunktsioonid. Need käivitatakse alles koos Windows Scripting Host (WSH) ja Windows Management Instrumentation (WMI) liideste, Active Directory Service Interface (ADSI) ja teiste operatsioonisüsteemi liidestega. Selleks tuleb objektid

kaasata skripti, mis valmistatakse ette liideste kaudu. Ilma põhjalike teadmisteta vastavatest objektimudelitest on nende kasutamine küll laialdaste mallide ja näidiste abil võimalik, kuid mitte soovitatav (nt sarnaste meetodite tõttu nagu GetObject versus CreateObjekt. Jscript 'i võib VBScript 'iga kasutusotstarbe poolest võrdseks pidada. Erinevus seisneb Java programmeerimiskeelele sarnanevas süntaksis. VBScript 'i ja Jscript 'i ei arendata enam edasi ja nendesse tuleb turvalisuse aspektist lähtudes suhtuda kriitiliselt.

- Windows Scripting Host (WSH) -Skriptide (nt vbs-või js-jailidena) käivitamine ja täitmine toimub CSript.exe (käsurea väljundi) või Wscript.exe (graafilise väljundiakna) kaudu. Nende kahe programmi abil käivitatakse WSH. WSH on standardile vastav keskkond, mis on ette nähtud skriptide töötlemiseks. Sellel on mõned programmifunktsioonid ning see loob võimaluse WSHga sobivatele keeltele laienduste järellaadimiseks (VBScript, Jscript). WSH on interpretaator. See on võimeline kasutama COM-objekte ning sellega seoses on tal juurdepääs tervele reale süsteemiliidestele (vt eestpoolt). Wscript.exe ja Cscipt.exe sisaldavad algelist silurit, mis võimaldab skripte testida. WSH-ga seoses on Windowsi jaoks ilmunud terve rida uuendusi ja veaparandusi, mis kõrvaldasid turvaprobleemid ning tegid osaliselt vajalikuks olemasolevate skriptide ülekirjutamise. Sellega tuleks WSH keskkonna skriptide arendamisel arvestada.
- Skriptimine Windows Management Instrumentation (WMI) abil. WMI sisaldab standardset juurdepääsu peaaegu kõikide Window s i ressurssside konfiguratsioonile, haldusele ja monitooringule. WMI on olemas juba aastast 1988 (Windows NT 4.0 SP4). WMI-l on keeruline arhitektuur, mis koosneb kolmest kihist (ressursid, arhitektuur, kasutajad) ning on objektile orienteeritult üles ehitatud. See juurutati DLLide kaudu pakkujakirjelduste (%SystemRoot%\system32\wbem) ja WMIteenuse (winmgmt.exe) jaoks. Juurdepääsuks Windowsi skriptide abil kasutatakse kokkusobivaid skriptide keskkondi nagu WSH või ActivePerl . Lisamooduliga wmimgmt.msc, WMItestimisprogrammiga wbemtest.exe või käsurea tööriista wmic.exe abil saab teostada WMI-konfiguratsioone või kontrollida käsutuses olevaid klasside definitsioone.
- Skriptimine Active Directory Service Interface (ADSI) abil. ADSI võimaldab Active Directory kataloogiteenuse skriptidel baseeruvat haldamist analoogselt WMI-tehnoloogiale.

Microsoft 'i skriptimise tööriistad, mis ei sisaldu standardinstallatsioonis:

- Tööriist Scriptomatic -Scriptomatic on tööriist skriptide loomiseks. Tööriist võimaldab kasutada WMId ja ADSId.
- Windows Power Shell.Windows Power Shell näol on tegemist täiustatud käsurea- ja skriptimiskeskkonnaga Windows platvormi jaoks, mis vahetab välja VBScript -i, JScript -i ja WSHi.

Paljudele Microsofti poolt pakutavatele tööriistadele ja skriptidele ei ole standardset tootetuge. See tuleb iga kord tootjaga läbi rääkida. Osaliselt anti tööriistad käsutusse õppe-eesmärgil, need ei oma või omavad ainult ebapiisavat veatöötlust ning ei anna optimaalset tulemust.

Windows Server 2008-ga kaasnevad uuendused

Windows PowerShell kujutab endast Windowsi platvormide jaoks edasiarendatud käsuviiba- ja skriptikeskkonda, mis asendab VBScripti, JScripti ja WSHd.

PowerShell kasutab .NET-objektimudelit ning sellesse on üle võetud mõned Unixist tuntud kontseptid, nt torud (pipes). Alates versioonist Windows Server 2008 pakutakse PowerShelli valikulise lisana, kuid versioonis Server 2008 R2 kuulub see juba standardsesse tarnekomplekti. Skriptide genereerimiseks on loodud tööriist Scriptomatic. See toetab nii WMI-d kui ka ADSI-d. Saadaval on ka PowerShelli jaoks mõeldud versioon. Paljudel Microsofti tööriistadel ja skriptidel üldine tootetugi puudub. Iga tootevaliku puhul tuleb tootjaga eraldi konsulteerida. Osa tööriistadest on saadaval üksnes õppe-eesmärgil, mistõttu on nende tõrkekäsitlus kas ebapiisav või puudub üldse ning nende töö ei ole koormusele vastavaks optimeeritud.

WSH blokeerimine

Kuritarvitamise ärahoidmiseks tuleb WSH blokeerida. Windowsi skriptimisvõimalusi kasutatakse kahjuks sageli ka kahjurvara levitamiseks (G 5.23 Pahavara). Seetõttu piiratakse või tõkestatakse sageli skriptide kasutamine klientidel. Klient-server süsteemis võib skriptide kasutamisest tulenev administratiivne ja organisatoorne kasu õigustada suurenenud riski ja sellele vastavalt ka turvalisuse tagamiseks tehtavaid suurenenud kulutusi . Kui kasutatakse vaid käsurea skripte, tuleks turvalisuse tõstmiseks WHS serveril blokeerida.

WSH blokeerimine on võimalik mitmel viisil.

1. Registrivõtme loomine

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\Enabled (Format Reg DWORD)

Väärtus viiakse nulli. Muudetud registreerimisseade peaks olema kujutatud administratiivses mallis.

2. Software Restriction Policy

Vastavate reeglitega võib ise failide Wscript.exe ja Cskript.exe või skriptfailide käivitumist takistada.

Alternatiivsed skriptide keskkonnad

Alternatiivsetel skriptid ei ole alati eeliseid

Alternatiivsed skriptide keskkonnad nagu Perl, KiXtart ja teised ei vähenda automaatselt ründepinda. Need omavad samuti juurdepääsu operatsioonisüsteemi funktsioonidele ja neil võib olla turvaauke. Kehtivad eelpool nimetatud nõuded ja põhimõtted.

Dokumenteerimine

Dokumenteerimine tarkvara arendamise ulatuses. Skriptid tuleb dokumenteerida sarnaselt muu tarkvaraarenduse dokumentatsioonile. Minimaalselt peaks olema dokumenteeritud nõuete kataloog, funktsionaalne kirjeldus, kasutajatugi, käivitustingimused ja versioonikontroll. Vastavate Windowsi komponentide või operatsioonikontseptsiooni dokumentatsioonis peab skripti nime ja versiooninumbri abil olema äratuntav, millist skripti kasutatakse.

Kontrollküsimused:

- Kas on olemas eeskirjad skriptide kasutamiseks organisatsiooni jaoks kriitilistel serveritel?
- Kas kõik ise loodud skriptid ning teiste tootjate tööriistad või skriptid on nõutaval viisil dokumenteeritud ja testitud?
- Kas skriptide ja tööriistade rakendamine on nõuetele vastavalt kinnitatud?
- Kas keskkond, kus skripte tohib käivitada, on küllaldaselt kaitstud väärkasutuse ja kahjurvara eest?

M 2.368 Administratiivsete mallide kasutamine

Algatamise eest vastutavad: IT-juht, infoturbeosakond
Rakendamise eest vastutab: administraator

Windows Group Policy on efektiivne ja mitmekülgne vahend erinevate Windows süsteemide, sealhulgas ka Windows Server 2008 konfigureerimiseks.

Vajalikud turvameetmed Windows Group Policy rakendamiseks
on kirjeldatud meetmetes M 2.231 Windowsi grupipoliitika planeerimine ja M 2.326 Windows Vista ja Windows 7 grupeerimissuuniste planeerimine .

Grupeerimissuuniste ja registri andmebaasi seos
Grupeerimissuuniste sätted mõjutavad registri andmebaasi. Enamik grupeerimissuuniste sätteid põhjustab muudatusi Windows süsteemi registri andmebaasis. Registri andmebaas kuulub Windows Server 'i kõige kriitilisemate komponentide hulka ning vajab seetõttu erilist kaitset ja hoolikat käsitlemist. Alati tuleks arvestada aspektidega "Testimine", "Turvamonitooring", "Tagasijooks" ja "Dokumentatsioon". Selleks on vaja kasutada sobivad tööriistu – Windows 'i registriredaktorist üksi ei piisa nimetatud aspektide katmiseks.

Registri andmebaasi muutused administratiivsete mallide abil
Grupeerimissuuniseid saab laiendada Microsofti ja kasutajate endi või teiste tarkvaratootjate defineeritud mallidega. Sellised niinimetatud administratiivsed mallid sisaldavad parameetrite seadistusi, mis kirjutavad sihipäraselt ja automaatselt registrivõtmeid registri andmebaasi.

Soovitav kasutada vaid administratiivseid malle
Registriandmebaasi võtmete muutmiseks on soovitatav kasutada vaid administratiivseid malle ja loobuda täielikult muudatuste käsitsi sisseviimisest. Muudatuste halduse raames tuleksid vähemalt käsitsi sisseviidud registrivõtmete muudatused kiiresti kasutaja defineeritud administratiivsesse malli sisse viia.

Administratiivsete mallide ühilduvus
Ühilduvus erinevate Windows versioonide mallide vahel
Iga Windowsi versiooniga ja peaaegu iga remondipaketiga on kaasas tootja administratiivsed mallid, mis sisaldavad uusi ja kõiki vanades versioonides sisalduvaid võimalusi. Uute sätete allapoole ühilduvus on mallides dokumenteeritud ja GPMC-konsoolil näha. Mitteühilduva Windowsi versiooni korral enamik sätetest ei toimi.

Grupeerimissuunised uusimale Windows'i versioonile
Loodavad grupeerimissuunised peaks alati põhinema uusimal Windowsi versiooni administratiivsel mallil, millel suuniseid tõenäoliselt rakendatakse. Vastavad mallid on saadaval Microsofti internetilehekülgedel kaustas 'adminpak.msi'.

Windows Server 2008-ga kaasnevad uuendused

Kasutusele võetud adm-tüüpi administratiivsed mallid võimaldavad süsteemi baasseadistuste, nt võrguparameetrite muutmise kõrval konfigureerida ka Office'i programme. Sellest hoolimata esineb adm-failide kasutamisel ka puudusi:

- puudub mitmekeelsete kohandamiste võimalus;
- kõik adm-failid on oma andmevormingu tõttu mitme kilobaidi suurused ning kui domeeni piires kasutatakse paljusid adm-faile, replikeeritakse need ka iga kord. See võib muuta andmemahud enneolematult suureks;
- administratiivseid malle ei saa tsentraalselt salvestada.

Selle piirangu tõttu muudeti alates versioonidest Windows Server 2008 mallifailide andmevormingut. Uus, XML-il põhinev andmevorming vähendab äsja loetletud puudusi. Tänu XML-vormingule muutusid mallide andmemahud oluliselt väiksemaks. Tsentraalse salvestuskoha kasutuselevõtt võimaldab mallifaile tsentraalselt salvestada ja hallata. Mallifailide lokaalne andmetee on %systemroot%\PolicyDefinitions\. Lisaks võeti kasutusele adml-vormingus keelepaketid. Need failid salvestatakse enamasti PolicyDefinitionsi kausta. Saksakeelse Windows Server 2008 puhul on peale keelest sõltumatute admx-failide olemas ka keelepõhised kaustad de-DE ja en-US. Mainitud adml-failid salvestatakse neisse kaustadesse.

Windows Server 2008 R2-ga kaasnevad uuendused

Grupipoliitikate haldamise redaktorprogrammis kuvatakse administratiivseid malle Administrative Templatesi andmetee nupukeste „Computer" ja „User configuration" all. Versiooniga Windows Server 2008 R2 võeti kasutusele uus kasutajaliides, mis pakub varasemast laiemat tooteomaduste konfigureerimise võimalust. Kogu saadaolevale teabele ja kommentaariväljadele pääseb nüüdsest juurde üheainsa registrikaardi all. Lisandunud on mitmerealiste märgijadade ja QWORD-tüüpi väärtuste tugi. Tänu võimalusele luua REG_MULTI_SZ-tüüpi registreerimisväärtusi, saab muu hulgas kasutada mitmerealisest tekstist koosnevaid sisestusi.

Kirjeldatud uuendused kehtivad ka Windows 7-ga töötavate süsteemide kohta, millesse on installitud kaugserveri haldustööriist RSAT.

Administratiivsete mallide kasutamine alates Windows Server 2008-st

Domeenikeskkonnas malle üldjuhul lokaalselt ei töödelda ega kasutata. Enamasti kasutatakse tsentraalset salvestuskohta ja tsentraalselt toimivat haldustööriista. See nn Central Store on kaust, mis tuleb uuesti koostada asukohas \SYSVOL\

domain\Policies. Pärast seda, kui kaust on loodud, kopeeritakse sellesse lokaalsete poliitikadefinitsioonide (PolicyDefinitions) sisu või msi-pakettidest pärit uued mallid. Malle saab töödelda grupipoliitikahalduse redaktorprogrammiga. Redaktorprogrammis saab ka näha kõiki tsentraalsesse salvestuskohta kopeeritud malle. Kuna redaktorprogramm analüüsib vaid seda andmeteed, on oluline Microsofti ette antud andmeteed alles jätta.

Olemasolevate administratiivsete mallide migreerimine

Windows Server 2008 toetab ka vanema tüübi administratiivseid malle. Süsteemi ebakõlade vältimiseks on sageli kõige mõistlikum kõik vanad adm-mallid

korraga uuteks migreerida. Erinevate kolmandate tootjate tarkvaralahenduste kõrval saab adm-mallide migreerimiseks kasutada ka Microsofti enda tasuta ning MMCga integreeritud tööriista ADMX.

Operatsioonisüsteemi värskendamine

Mallide sätted jäävad süsteemi värskendamisel alles. Pärast operatsioonisüsteemi värskendamist jäävad kõik sätted alles ning nende haldamine on võimalik operatsioonisüsteemi uuendatud administratiivsete mallidega. Kasutaja defineeritud mallid koos aktiveeritud sätetega jäävad muutumatuks ning nende haldamine võib toimuda nende juurde kuuluvates grupipoliitika objektides (“ Group Policy Objects ”, GPO).

Kasutaja defineeritud administratiivsete mallide rakendamine

Registri redigeerimine (Registry Tattooing)

Kasutaja defineeritud administratiivset malli rakendades kirjutatakse iga aktiveeritud parameetri jaoks vastav registrivõti jäädavalt registri andmebaasi. Selle eemaldamiseks on vaja registrit käsitsi redigeerida (Registry Tattooing). Efekti nimetatakse “mitte hallatav suunise säte”, samuti ka “ Registry Tattooing ”. Sellisel juhul saab GPMC-konsooliga muuta vaid registrivõtme väärtust, näiteks 1-lt 0-le “jah” või “ei” või 0x000D-lt 0x0020-le ooteperioodi muutmiseks, kuid võtit ennast enam muuta ei saa.

Redigeerimist ei toimu täielikult hallatavate mallide korral

“Redigeerimise efekt” puudub mõnedel Microsofti toodetega kaasasolevatel administratiivsetel mallidel. Neid nimetatakse “täielikult hallatavateks mallideks” ja nendest tulenevaid sätteid nimetatakse lühidalt “Suunised” (ingl k True Policies). Nende suuniste sätete täiendav haldamine toimub registrivõtmetes

HKEY_LOCAL_MACHINE\Software\Policies

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\ Current Version\Policies

HKEY_CURRENT_USER\Software\Policies

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies

ning need salvestatakse pol -failidena failisüsteemi. Policies -võtmetega ei tohiks kasutaja defineeritud administratiivseid malle kasutades manipuleerida. Enne rakendamist tuleks süsteemistaatus (ingl k Systemstate) varundada (vt M 6.99 Windows Serverite tähtsate süsteemikomponentide regulaarne varundus). Registri varundamisest üksi ei piisa, et komplikatsioonide korral ühe malliga endist seisundit taastada. Lisaks sellele tuleb sätete funktsionaalsust ja mõju isoleeritud testimissüsteemis kindlasti kontrollida. Seejuures tuleb silmas pidada kõiki Windowsi versioone, millega malli kasutatakse.

Rollout -strateegia

Kui sätteid rakendatakse mitmetele serveritele, tuleks rakendusprotsessi alustada töökeskkonna vähemkriitilises valdkonnas. Valdkonda tuleb pideva vaatluse ja kontrolli all hoides laiendada järk-järgult töökeskkonna kriitilisematele kihtidele. Kontrollifunktsiooni Active Directory keskkonnas omab GPMC-konsool või üksikul serveril RSOP-konsool.

Kasutaja defineeritud võtmete turvamonitooring

Iga selliselt loodud võtme jaoks tuleb turvaprotokollis fikseerida vähemalt kirjutamisõigused. Kirjutamisõigus tavapärastele kasutajakontodele tuleb deaktiveerida. Mõlemat on võimalik teostada käsitsi registri editoriga, skripti abil (vt M 2.367 Käskude ja skriptide kasutamine alates Windows Server 2003-st) või Windowsi turvamalli abil.

Kasutaja defineeritud administratiivsete mallide eemaldamine

Meetmed enne administratiivsete mallide eemaldamist

Administratiivsete mallide eemaldamine on seotud niisama suurte administratiivsete kuludega kui nende sisestamine. Kui ühte või mitut administratiivse malli parameetrit enam ei vajata, eemaldatakse need tavaliselt GPMC-konsoolist või asendatakse need modifitseeritud versiooniga. Selle käigus ei eemaldata ega nullita aga registrivõtmeid. Seetõttu tuleb enne turvamalli GPMC-konsoolist eemaldamist dokumenteerida kõik aktiivsed, GPMC-konsoolis nähtavad parameetrid ning omistada neile neutraalsed mittekriitilised väärtused. Mittekriitilised on väärtused, mis muudavad registrivõtme kehtetuks. Turvamall tuleks eemaldada alles pärast vastavat järelkontrolli GPMC- või RSOP-konsooli abil. Eksikombel eemaldatud turvamalli taassisestamisel ei kuvata GPMC-konsoolil olemasolevaid registriparameetreid ka mitte juhul, kui registrivõti või –võtmed on veel aktiivsed ja toimivad.

Mitte kasutuses olevad võtmed tuleb kustutada

Et välistada selliste mitte kasutatavate registrivõtmete väärkasutust, tuleb kõiki mitte enam kasutuses olevaid registrivõtmeid kaitsta tahtmatu kasutamise eest. See on tavaliselt võimalik vaid kustutamise teel. Kustutamine võib toimuda käsitsi registri redaktori või skripti abil. Alternatiivina võib takistada Windowsi turvamalli kaudu juurdepääsu võtmetele või karmistada monitooringu sätteid, mille kaudu tõuseb igatahes sissekannete sagedus turvaprotokolli ja kulutused revisjonile.

Dokumenteerimine

Rakendatud administratiivsete turvamallide uuendused tuleb dokumenteerida Administratiivsete turvamallide minimaalseks dokumenteerimiseks piisab, kui iga serveri kasutatavad mallifailid (failid laiendiga adm), nende versioon ning enda loodud mallide puhul ka nende sisu esitatakse süsteemi dokumentatsioonis. Vastava turvamallide versioonihalduse ja pääsukontrolli olemasolu korral peaks olema võimalik kindlaks teha, kes, millal ja milliseid turvamalle muutis. Lisaks sellele tuleb luua kõik aktiveeritud parameetrid, nende kehtivad väärtused ja aluseks olevad turvamallid. Kui turvamallide ettevalmistamine toimub Active Directory abil, tuleb dokumenteerida kõik ülejäänud faktorid, millest sõltub serveri või serverite seadistuste efektiivsus, (nt OU, turva- ja WMI-filtrid). Alati peab olema arusaadav, kust mingi registrivõti pärineb. Selle alusel peaks toimuma dokumentatsioonide ja vajadusel kontseptsioonide koostamine testimiseks, mõnede skriptide ning turvamallidega seotud valmisoleku ja tagasipöördumise strateegiate loomine. Dokumentatsiooni tuleks rakendada ka süsteemi- ja turvaprotokollide regulaarse analüüsi planeerimiseks. Kui rakendatakse Active Directory 't, sobib aktiivsete sätete dokumenteerimiseks hästi GPMC-konsool. Rühmapoliitika objektide (Group Policy Objects, GPO, RSoP (Resultant Set of Policy) ja rühmapoliitika moodulite jaoks võib raportid eksportida trükiformaadis HTML-faili (soovitud objekt markeerida / menüü Aktion / Raporti salvestamine . . .).

Kontrollküsimused:

- Kas registri andmebaasis on käsitsi lisatud võtmeid, mille haldamine ei toimu administratiivse turvamalli või selleks sobiva tööriista abil?
- Kas toimub kõigi kasutaja defineeritud administratiivsete turvamallide abil loodud registrivõtmete kirjutamisõiguse monitooring ning kas tavakasutajal puudub sellele juurdepääs?
- Kas administratiivsete turvamallidega konfigureeritud registreerimisvõtmete efektiivsus on testitud?
- Kas kõik administratiivsete turvamallide aktiveeritud sätted on serveri süsteemidokumentatsiooni kantud?

M 2.369 Turvalisusega seotud hooldustööde regulaarne läbiviimine

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: administraator

Regulaarsete hooldustööde läbiviimise põhimõtted

Hooldustööde läbiviimine on vajalik *Windows Server* 2003 korrashoiuks või selle funktsioonide ja ettenähtud rakendatavuse säilitamiseks. Hooldustöid tohib läbi viia vaid asjatundlik ja selleks volitatud personal ning see võib olla ka garantiilepingu nõue. Eriti välise personali kaasamisel hooldustöödesse tuleb järgida turvameetmes M 2.4 Hooldus- ja remonditööde reeglid esitatud nõudeid. Hooldustööde läbiviimine toimub regulaarselt ja plaanipäraselt hooldustööde plaani alusel, üldjuhul väljaspool normaaltööaega. Kui võrgukoormuse tasakaalustamiseks (*Network Load Balancing*, *NLB*) kasutatakse klastreid, on hooldustööde teostamine võimalik ka tööd katkestamata. Hooldustööde hulka kuulub konfigureerimine, puhastustööd, kuluvate komponentide ekspertiis ja uuendamine, riistvara täiendamine ning väikeste defektide kõrvaldamine. Seejuures tuleb järgida tootja ettekirjutusi (vt M 2.213 Tehnilise infrastruktuuri hooldus). Sellega kõrvaldatakse avastatud vead, viiakse sisse kohandused ja uuendused ning vajadusel valmistatakse laienduste abil ette uued funktsioonid ja rakendused. Laiendusi tohib sisse viia vaid pärast küllaldast testimist ning kirjalikku luba. Serveril tehtavad muudatused tuleb dokumenteerida. Hooldustöödele esitatavate nõuete ja läbiviimise koordineerimise ja dokumenteerimise kohustus lasub hooldustööde eest vastutaval isikul, enamasti administraatoril (vt B 1.9 Riist- ja tarkvara haldus ja M 2.34 IT-süsteemi muutuste dokumenteerimine).

Hooldustööde ettevalmistamine

Serveri rollide ja komponentide osakontseptsioonide abil peaks olema võimalik kindlaks määrata hooldust vajavad valdkonnad. Hoolduse seisukohalt tähtsate aspektide suhtes on võimalik saada informatsiooni vastavatest etalonturbe meetmest. Tuge muude hoolduse seisukohalt tähtsate aspektide suhtes mitmesuguste rakendusstrateegiate korral pakub *Windows Server* 2003 dokumentatsioonibiblioteek *Microsoft Operations Framework* (*MOF*). Teatud kindlaid hoolduse seisukohalt tähtsaid süsteemi omadusi on võimalik kindlaks teha vaid normaaltalitluse ajal. Seepärast tuleb süsteemimonitoris, võrgumonitoris, *Task Manager* 'is ja rollispetsiifilistes konsoolides sisalduv info õigeaegselt välja selgitada ja sellega arvestada. Erilist tähelepanu tuleb seejuures pöörata lehekülje tõrgetele seoses *swap file* 'iga ja protsesside vajadusele ressursside osas (vt M 2.365 Windows Server 2003 süsteemiseire planeerimine). Windows *System Resource Manager* (*WSRM*) võimaldab *Enterprice Edition* 'il või *Datacenter Edition* 'il defineerida ja juhtida rakenduste, protsesside ja teenuste ressursside kasutust. Hooldustööde käigus teostatavate sammude kohta tuleb koostada protokoll, mis sisaldab ka vastavat kuupäeva ja vastutavat isikut. Pärast hooldustööde läbiviimist tuleks see säilitada, et pärast oleks võimalik kindlaks teha, millest on tingitud reeglitest kõrvalekalded, nt sündmuste logi (*Event Viewer*) analüüsimisel. Sündmusevaaturi (*event viewer*) abil tuleb kontrollida, ega süsteemiprotokollis pole vigu ja hoiatusi. Igal juhul tuleb kindlaks määrata, mil määral on serveri turvaline funktsioneerimine nende sündmuste tõttu ohustatud. Kui hooldustööde tagajärjel on oodata kindlat tüüpi sündmuste suurenenud esinemissagedust, tuleks need valehäirete vältimiseks eelnevalt teatavaks teha. Teatud tingimustel võib see olla vajalik ka teiste protokollide osas, kui see neid puudutab. Lisaks sellele võib serveri tarkvara monitooringuks kasutada teisi tööriistu. Paljude tootjate riistvara juurde kuulub

ka nende arendatud monitooringu tarkvara, mis on võimeline edastama hoiatussignaale ja neid analüüsima. Olenevalt mudelist võib toimuda näiteks kõvaketaste, ventilaatori pöörete arvu, võrguosade pingete ja puhvertoiteallika monitooring. Tihti on kõrgekvaliteetsetel kõvaketastel niinimetatud varajane vigade avastamise funktsioon. See võimaldab kõvaketta õigeaegselt enne selle riket välja vahetada. Tuleb tagada, et hooldustööde läbiviimisel arvestataks kõigi nimetatud aspektidega (vt M 2.365 Windows Server 2003 süsteemiseire planeerimine .

Regulaarsed hooldustööd

Hooldustööde käigus tuleb kontrollida ja tagada, et riistvara oleks komplektne ning et see ei sisaldaks mingeid organisatsioonis keelatud komponente. Serveri töö turvalisuse tagamiseks peavad kõik seadmed ja teenused ilma tõrgeteta töötama. Seetõttu tuleb kontrollida nende nõuetele vastavat talitlust arvutihalduse teostamisel. Serveri aktuaalseid *süsteemi funktsioone* tuleb võrrelda dokumenteeritud konfiguratsiooni nõuetega ja nendega vastavusse viia. Seejuures tuleb eriti silmas pidada seadeid funktsioonide all *Laiendused*, *Süsteemi taastootmine* ja *Automaatvärskendused* . Kui kasutatakse turvamalle, tuleb kontrollida serveri vastavust turvamallide käibivale versioonile.

Paigad

Hooldustööde käigus on vaja kontrollida, kas kõik saadaolevad turvapaigad on installeeritud. Selleks võib kasutada tööriista *Security Baseline Analyser* (MBSA). Kõigepealt tuleks siiski kontrollida, kas MBSA suudab avastada kõiki olulisi paiku ning millised saadaolevad paigad on serverile tõepoolest olulised. Tavaliselt toimub vajalike turvauuenduste käivitamine võimalikult kiiresti. Kuna mõned paigad vajavad teatud tingimustel efektiivsuse saavutamiseks seadmete, teenuste või isegi serveri taaskäivitamist, saab neid uuendusi käivitada vaid hooldustööde käigus. Kõrvalekallete korral on nõutav põhjendus.

Kontod ja paroolid

Üleorganisatsioonilised kontode ja paroolide turvajuhendid kehtivad ka serverite lokaalsetele kontodele ja teenuskontodele. *Windows Server* 2003 süsteemi hooldustööde ja tervikluskontrolli käigus tuleks kontrollida, kas peetakse kinni kontode ja paroolide üleorganisatsioonilistest turvajuhenditest või volituste kontseptsiooni regulatsioonidest. Eriti hoolikalt tuleks kontrollida, ega ei eksisteeri kasutuses mitteolevaid lokaalseid kontosid või ei ole jagatud tühje paroole või paroole, mis ei vasta üleorganisatsioonilistele suunistele. Selleks võib kasutada tööriistu või *MBSA* skripte. Erilist tähelepanu tuleb pöörata ka ajutistele kontodele, mis olid või on ette nähtud kasutamiseks vaid piiratud ajavahemikus. Teenuskontodel on tihti laiendatud õigused ning need vajavad seetõttu erilist kaitset. Teenuskonto parooli muutmisel tuleb uus parool kanda vastava teenuse funktsioonidesse sakki *Logimine*. Järgnevalt on vajalik kõnealuste teenuste taaskäivitamine. Kui antud teenuseid vajatakse normaaltalitluse ajal, võib selliseid meetmeid rakendada vaid hooldustööde läbiviimisel (vt M 4.284 Teenuste rakendamine alates Windows Server 2003-st .

Andmekandjad ja andmekogumid

Lubamatud andmetüübid ja tarkvara

Tuleb kontrollida, et serveritel olevatel andmekogumites ei oleks lubamatuid andmetüüpe ja lubamatut tarkvara. Kõrvalekaldeid tuleb hallata organisatsiooni regulatsioonide alusel. Seejuures tuleb otsida ka krüpteeritud andmekogumeid, mis ei vasta organisatsiooni krüpteerimisjuhendile. Lubamatuid EFS krüpteeringuid on näiteks võimalik lokaliseerida tööriista *EFSInfo* abil (vt M 4.278 EFS-i turvaline kasutamine Windows Server 2003 keskkonnas).

Nõuded mälu kasutamiseks

Tuleb kontrollida ka mälu kasutamise nõuetest (nt maksimaalne kataloogi suurus või vanade andmete paigutamine välisele andmekandjale) kinnipidamist ning vajadusel rakendamist. Andmekandjate limiidid toetavad seda ülesannet, kuid lubavad siiski *Windows Server* 2003-le (kuni SP1 kaasa arvatud) ainult ühte piirangut kasutaja ja partitsiooni kohta. *Windows Server* 2003 R2 juurde kuuluvad laiendatud limiidihalduse ja andmete kontrolli läbiviimiseks võimsad ja mugavad tööriistad, millel on ka raporti esitamise funktsioon).

Kehtivad volitused

Kontrollida tuleb kehtivaid andmete, kinnituste, registreeringute ja printerite volitusi, et ei esineks kõrvalekaldeid reeglitest ning nõuetest. Suhteliselt staatiliste andmekogude ja süsteemi andmete korral soovitatakse jaotatud volituste dokumenteerimiseks ja kontrollimiseks inf-faile (*turvamallid*) ja *turvakonfiguratsiooni ning –analüüsi.* Andmekandjate hooldus hõlmab vaba salvestusmahu olemasolu kontrolli partitsioonidel, ketaste puhastamist ja fragmenteerimist. Nende teostamiseks on vaja planeerida piisavalt aega.

Peidetud andmevood

Olulised erinevused salvestatud andmete summa, arvutusliku ja veel käsutuses oleva andmemahu vahel kõvakettal võivad viidata soovimatutele peidetud andmevoogudele (*Alternative Data Streams*, *ADS*) NTFS partitsioonidel. Kui on viiteid peidetud andmevoogudele, tuleks pöörata tähelepanu asjaolule, kas kasutatav viirusetõrjetarkvara otsib peidetud andmevooge (vt M 2.157 Sobiva viiruseskanneri valimine). Kui kõvaketta hõivamine arvatavalt peidetud andmevoogudega on küllaltki suur, peaks järgneva analüüs, mis tuleks läbi viia sobivate kolmandate tootjate tööriistadega (vt G 2.116 Andmekadu andmete kopeerimisel ja teisaldamisel alates Windowsi Server 2003-st).

Visuaalne kontroll

Serveri riistvara visuaalne kontroll

Visuaalse kontrolli käigus tuleb visuaalselt kontrollida serveri välist keskkonda. Seejuures tuleb kontrollida kaableid ja pistikuid ning osade kinnitusi. Lisaks sellel tuleb kontrollida, kas kõik on puhas ja vajadusel puhastada õhutuskanaleid, ventilaatoreid ja jahutuskehasid.

Spetsiaalsed hooldustööd

Andmed kustutada

Kui hooldustööde käigus tuleb turvaliselt kustutada andmekandjaid, võib seda teha vaid kolmandate tootjate tööriistade abil (nt *VS - Clean*). Kui riistvara on paigaldatud varuga, näiteks *RAID-5* , topelt võrguosade ja klastrite kasutamisega, peab varukomponendi väljalangemisel selle viivitamatult asendama, vastasel korral tekib jälle väljalangemisoht. Kõik riistvaratootjad pakuvad oma toodetele uusimat informatsiooni, püsivara ja draivereid. On soovitatav end nende pakkumistega pidevalt kursis hoida ning oluliste muutuste korral uuendused hooldustööde käigus sisse viia.

Garantii- ja hooldusleping

Tuleb jälgida kinnipidamist garantii- ja hooldusleping tingimustest, et oleks tagatud õigeaegne hooldustööde läbiviimine lepingupartnertite poolt ning välditaks asjatuid seisakuid või kulusid. Seadmete soetamisest tuleb õigeaegselt vajalike protseduuride kaudu teada anda.

Täiendavad kontrollküsimused:

- Kas on olemas sobiv serveri hooldustööde läbiviimise plaan?
- Kuidas toimub läbiviidud hooldustööde tõendamine?
- Kas on läbi viidud andmekandjate puhastamine koos sellele järgnenud fragmenteerimisega?
- Kas vajalikud garantii- ja hooldusleping on veel kehtivad ning vastavad hetkel kehtivatele nõuetele.

M 2.370 Volituste haldamine

Algatamise eest vastutavad: IT-juht, infoturbe osakond:

Rakendamise eest vastutavad: IT-juht, administraator, vastutav spetsialist

Ülevaade olemasolevatest volituste kontseptsioonidest

Kontode, gruppide ja pääsuõigustega turvamudel ei piirdu sugugi vaid NTFS-failisüsteemi objektidega. Vastupidi, peaaegu kõikides operatsioonisüsteemi valdkondades võib anda pääsuvolitusi paljudele objektidele. Seega on võimalik volitusi igat liiki autentimist võimaldavatele kontodele üksikasjaliselt detailiseerida.

Windowsi volituste mudeli koosseisu kuuluvad:

- Kasutajakontod ja arvutikontod
- Süsteemikontod
- Varem defineeritud standardgrupid
- Grupi liikmed
- Grupisõltuvused (ainult Active Directory)
- Objektide pääsuõigused (Access Control List , ACL)
- Objektide pääsuõiguste kontroll (System Sccess Control List, SACL)
- Päringud

Järgmised volituste sätted ei kuulu ülalnimetatud volituste mudeli koosseisu:

- Internet Information Servises (IIS) ressursipõhised volitusmehhanismid;
- Süsteemiõigused (rights/privileges)
- Rollipõhine pääsuhaldus (Role Based Access Control, RBAC)

Koolitus

Et administraatorid omaks ülalnimetatud mehhanismide tundmiseks ja nende haldamiseks vajaminevaid teadmisi, tuleb neile korraldada vastavaid koolitusi ja teha kättesaadavaks erialane kirjandus. Vastasel korral ei ole võimalik tagada kasutuses olevate mehhanismide ning kogu Windows Server' ite turvalist talitlust. Olenevalt administraatorite ülesannetest tuleb neid koolitada ka vastavate komponentide alal, et oleks võimalik kalkuleerida ja ette planeerida volituste konfigureerimise mõju. Detailseid teadmisi operatsioonisüsteemi erinevate valdkondade üksikute volituste kohta leiab Windowsi online -abist ja tehnilise tugiteenistuse Microsoft Technet administraatoritele mõeldud infolehest.

Põhireeglid

Kasutajakontode ja administratiivsete kontode haldamine nõuab volituste ja turvamehhanismide alaseid põhiteadmisi ja teatud põhireeglite järgimist. Eriti hoolikas tuleb olla näiliselt väikeste muudatuste tegemisel töökeskkonnas ilma eelneva testimiseta, et mitte ohustada IT-süsteemi käideldavust.

Vähimad vajalikud volitused

Kõigi volituste andmisega seotud tegevuste läbiviimisel ja planeerimisel on vaja kinni pidada vähimate vajalike volituste andmise printsiibist (ingl k least privileges). Alati ei pea mingi spetsiifilise ülesande täitmiseks andma absoluutselt minimaalseid volitusi. Pigem ei tohiks ühele kontole anda “igaks juhuks” suuri volitusi, vaid

ainult volitusi, mis on vajalikud kontole defineeritud nõuete täitmiseks. Kui see on õigustatud, võib volituste laiendamine toimuda samm-sammult. Kui konto kasutajal ei ole vaja tegelda ressursside haldamisega, ei tohiks kontole ei tohiks anda täielikku juurdepääsu ressurssidele.

Simulatsioonitööriistad

Volituste konfigureerimisel on põhiliseks raskuseks mingi volituste konfiguratsiooni mõjude ennustamine. Volituste konfigureerimise mõjude ennustamiseks on olemas erinevaid simulatsioonitööriistu:

- Registrikaart Effective Authorisations - Objekti turvasätetes, nt failis, tekib võimalus simulatsiooniks, valides Add-ons / Effective Authorisations / Select. Simulatsioone tuleks läbi viia nii konfigureeritud turvagrupi kui ka pisteliselt kasutajakontodega, millel peaksid olema vastavad õigused.
- Konsool Resultant Set of Policies, RSOP - Start \ Käivita \ rsop.msc sisse trükkida. Active Directory kasutamisel saab seda protsessi RSOP-konsooli abil võrgus käivitada ja analüüsida ka eemalolevatel arvutitel.

Simulatsioonitööriistu tuleks volituste modelleerimise ja haldustööde läbiviimise protsessis intensiivselt kasutada. Soovitatav on formuleerida see konfiguratsioonimuudatuste kinnitamise protsessi käigus vastavas IT-turvasuunises.

Jagatud kontod ja unustatud paroolid

Kasutajakontosid ei tohi kasutada mitmed isikud (Account Sharing). See kehtib nii administratiivsete kui ka tavakontode suhtes. Kui administraator peab mõjuvatel organisatoorsetel põhjustel andma käsutusse jagatud konto, tuleb seda kui erandjuhtumit põhjendada ja dokumenteerida. Dokumenteerida tuleb kasutatud konto, paroolipoliitika elluviimise protseduur, volitused (ACL) ja kontrollseadete sätted (SACL) ning volitatud isikute ring. Väärkasutuse vältimine on siinkohal võimalik vaid organisatoorsel teel. Jagatud kasutajakontod tuleb sarnaselt administratiivsetele kontodele arvata kriitiliste kontode hulka ning süsteemiseire läbiviimisel sellega arvestada.

Parooli taastamise disketid

Tsentraalse autentimisega keskkonnas ei tohiks seda viisardit kasutada, kuna see ohustab sellise kontseptsiooni turvalisust. Parooli taastamise diskette ei tohi genereerida. See peab olema fikseeritud IT-turvapoliitikas ning seda võib näiteks keelata ka grupipoliitika alusel.

Kontrollküsimused:

- Kas on olemas oma volituste kontseptsioon?
- Kas administraatoritele korraldatakse volituste kontseptsioonide alaseid koolitusi ning tehakse neile kättesaadavaks vastavad erialaraamatud?
- Kas mingile objektile pääsuõiguse andmisest keeldumine kooskõlastatakse vastutava spetsialistiga?
- Kas volituste modelleerimisel ja haldustööde läbiviimisel tööprotsessis kasutatakse ettenägelikult simulatsioonitööriistu?
- Kas vaadeldavas IT-koosluses keelatakse või viiakse konto kasutamine mitme isiku poolt (Account Sharing) miinimumini?

M 2.371 Kasutamata kasutajatunnuste organiseeritud desaktiveerimine ja kustutamine

Algatamise eest vastutavad: IT-juht, infoturbeosakond, personaliosakond
Rakendamise eest vastutavad: administraator, vastutav spetsialist

Kui osutub vajalikuks mõne kasutajakonto deaktiveerimine või kustutamine, tuleb volituste dokumentatsiooni alusel kontrollida, milliseid volitusi vastav konto IT-keskkonnas omab ning millisteks autentimise protseduurideks seda vajatakse.

Kontode desaktiveerimine

Kasutamata kasutajakontod kujutavad endast turvariski ning need tuleb koheselt deaktiveerida. Kasutamata kasutajakontod võivad endas kätkeda turvariski. Seetõttu on soovitatav vähendada ründepinda ning kasutamata kontod desaktiveerida. Mida suuremate volitustega konto on (administratiivsed kontod), seda tähtsam on nende desaktiveerimine. Seetõttu tuleb infrastruktuuri regulaarselt kontrollida, et avastada aktiivseid kasutaja- ja administratiivseid kontosid, mida enam ei kasutata. Tähtis on ka, et selliseid kontosid ei kasutaks erinevad isikud. Alati peab olema võimalik kindlaks teha, kes, millal ja millist kontot kasutas.

Kontode kustutamine

Pääsuõigusi tuleb kontrollida ja konto pääsuloendist kustutada. Kui kasutajakonto kustutatakse, tuleb dokumentatsiooni abil üle kontrollida, milliseid pääsuõigusi kasutajakonto omab. Enne kontode kustutamist tuleb kontrollida, millistele objektidele on antud volitused (näiteks failide ühiskasutusse andmine). Pärast kustutamist tuleb veenduda, et kontod või täpsemalt nende turvatunnused oleksid pääsuõiguste loendist (Access Control List, ACL) eemaldatud.

Ettevaatust administratiivsete kontode kustutamisel

Administratiivsete kontode kustutamisel peaks kasutust leidma asendusregulatsioon, juhul kui administratiivsed ülesanded alles jäävad. Selle jaoks peaks juba enne kustutamist olema loodud ja võetud kasutusele asenduskonto. Kui seejuures ei toimita hoolikalt, võib tekkida suuri raskusi mõne ressursi haldamisel või täpsemalt öeldes ressurssidele juurdepääsu taastamisel. Seetõttu võib osutuda vajalikuks konto kõigepealt desaktiveerida ning alles pärast testimist kustutada. Enne kasutajakontode kustutamist tuleks defineerida protseduur, mis reguleeriks kasutaja poolt genereeritud andmete säilitamist ja / või edasi kasutamist. Vastasel juhul on andmeid võimalik vaid suurenenud kulutustega (administraatorid võtavad objektide halduse üle) või üldse mitte loetavaks muuta. See kehtib eriti väga konfidentsiaalsete või krüpteeritud andmete kohta. Vastavalt sellele tuleks enne kustutamist ka välja selgitada, milliste gruppide liige kasutaja oli, et kontrollida, kas ta äkki oli senini ainuke grupi liige, kes omas administratiivseid õigusi või volitusi ligipääsuks ressurssidele. Nimetatud sammud kätkevad endas ka väljakutset nende aluseks olevatele organisatoorsetele protsessidele (vt M 3.10 Usaldusväärse administraatori ja tema asetäitja valimine).

Dokumenteerimine

Kasutajakontode reguleeritud desaktiveerimine või kustutamine ning sellega seotud tähtajad tuleks dokumenteerida IT- koosluse turvasuunistes.

Kontrollküsimused:

- Kas kontrollitakse regulaarselt, et süsteemis ei oleks kasutamata administratiivseid kontosid ja kasutajakontosid?
- Kas kasutamata kasutajakontod desaktiveeritakse koheselt?
- Kas enne kasutajakontode kustutamist kontrollitakse, millistele objektidele on antud volitused ?
- Kas on olemas protseduurid andmete säilitamiseks ja/või edasi kasutamiseks pärast kasutajakontode kustutamist?
- Kas on olemas administratiivne asenduskonto?

M 2.372 IP-kõne kasutamise planeerimine

Algatamise eest vastutavad: IT-juht, infoturbeosakond:

Rakendamise eest vastutavad: IT-juht, administraator

IP-kõne turvalisel kasutamisel on põhiliseks eelduseks sobiv eelplaneerimine. IP-kõne kasutamise planeerimine võib toimuda mitme etapina *top-down* kavandi printsiibil. Lähtuvalt kogusüsteemi üldkontseptsioonist määratakse konkreetsed osakomponentide plaanid kindlaks spetsiifilistes alakontseptsioonides. Seejuures ei puuduta planeerimine ainult aspekte, mida tavaliselt seostatakse mõistega "turvalisus", vaid ka tavapärase kasutusega seotud aspekte, millega võivad kaasneda turvanõuded. Üldkontseptsioonis tuleks näiteks käsitleda alljärgnevaid tüüpilisi küsimusi:

- Kas IP-kõnedele tuleks üle minna osaliselt või täielikult? Kas IP-kõnet tuleks kasutada vaid suhtluseks PBX-seadmetega telefonijaamade vahel?
- Kas IP-kõnele või signaliseerimisinformatsioonile esitatakse kõrgendatud nõudeid käideldavuse, konfidentsiaalsuse ja tervikluse osas?
- Milliseid signaliseerimis- ja meediatranspordiprotokolle hakatakse kasutama?
- Kui paljudele kasutajatele tuleb IP-kõne teenust võimaldada?
- Kuidas peaks toimuma ühendamine avaliku telefonivõrguga? Kas IP–tehnoloogial põhinevad sideliinid on lubatud otse avalikust andmevõrgust?
- Kas on ette näha IP-kõne negatiivset mõju olemasolevale LAN-võrgu turvalisusele? Kas olemasolev LAN-võrk on IP-kõnede kasutamiseks küllaldaselt dimensioneeritud? Kas on vaja muuta võrguarhitektuuri?

IP-kõnede planeerimisel tuleb luua alljärgnevad alamkontseptsioonid:

- Krüpteerimise ulatus: Tuleb otsustada, mida krüpteerida. Näiteks võib võtta vastu otsuse, et kogu kommunikatsiooni LAN-võrgus ei krüpteerita, aga kõik väliskõned kaitstakse kolmandate isikute pealtkuulamise ja manipulatsiooni eest (vt M 2.374 IP-kõne krüpteerimise ulatus). Lisaks sellele tuleb otsustada, kas multimeedia- ja/või signaliseerimisprotokollid tuleks krüpteerida.
- Krüpteerimismehhanismid: Kui on otsustatud kommunikatsiooniliinid krüpteerida, tuleb ka otsustada, kuidas on võimalik kaitse integreerida. Krüpteerimine võib toimuda nii rakenduse tasemel, nagu näiteks H.235 või SPRTP (vt M 5.134 IP-kõne turvaline signaliseerimine ja M 5.135 Turvaline meediatransport SRTP abil), kui ka madalamates võrgukihtides, nagu näiteks SSL/TLS, IPSec või VPN) kaudu.
- Komponentide valik: Et oleks võimalik vastuvõetud otsuseid ellu viia, peavad kasutatavad seadmed võimaldama ka neid kasutada. Kui ei ole võimalik soetada vastavaid seadmeid, kuna näiteks ei ole võimalik täita kõiki nõudeid, tuleb planeerimist korrigeerida. Seeläbi tekkivad muudatused tuleb infoturbe osakonnaga kooskõlastada ja dokumenteerida.

- Valmisolek hädaolukorraks: Telefoniside olemasolu ei ole tähtsaks eelduseks mitte ainult äriprotsesside toimimisel. Telefoniside katkemisel puudub võimalus helistada hädaabinumbritele. Seepärast tuleb tarvitusele võtta teatud abinõud (vt M 6.100 IP-kõne (VOIP) hädaolukorraks valmisoleku plaani koostamine).
- Võrkude eraldamine: Teatud juhtudel võib olla mõttekas IP-võrk andmesidevõrgust loogiliselt või füüsiliselt eraldada (vt M 2.376 Andmeside ja IP-kõne (VOIP) võrgu eraldamine). Planeerimisfaasis tuleb otsustada, kas segmenteerimine on vajalik.
- IP-kõne teenused: Sageli võimaldavad IP-kõne komponendid lisateenuseid. Need võivad nõuda täiendavaid vahendustarkvara komponente või omavad teisi turvalisuse seisukohalt kriitilisi puudusi. Turvalisuse seisukohalt kriitiliste lisateenuste hulka kuulub näiteks kõnesse pealelülitumine, ruumi seire funktsioonid ja kõnede vaheldumine. Planeerimise käigus tuleb otsustada, milliseid teenuseid kasutatakse.
- Administratsioon ja konfiguratsioon: Aegsasti tuleb kindlaks määrata, kes hakkab tegelema IP-kõnede administreerimise ja konfigureerimisega. Selleks on vaja nimetada IP-kõnede eest vastutav administraator. Lisaks tuleb otsustada, kuidas peaks toimuma haldamine IP-kõne võrkude ja süsteemide haldamine (vt M 4.287 IP-kõne vahetarkvara turvaline administreerimine ja M 4.288 IP-kõne lõppseadmete turvaline administreerimine).

Üksikute IP-kõne komponentide sõnumite logimisel on suur tähtsus näiteks rikete diagnoosimisel ja kõrvaldamisel või rünnete avastamisel ja selgitamisel. Planeerimisfaasis tuleks otsustada, millist informatsiooni tuleks kindlasti logida ning kui kaua logifaile säilitatakse. Lisaks sellele tuleb kindlaks määrata, kas logiandmed tuleks salvestada lokaalselt süsteemil või tsentraalselt logiserveri võrgus. Kõik planeerimisfaasis vastuvõetud otsused tuleb dokumenteerida selliselt, et neid oleks hiljem võimalik taastada. Seejuures tuleb arvestada, et nimetatud informatsiooni peavad töötlema enamasti mitte selle autorid, vaid teised isikud. Seepärast tuleb tagada sobiv struktuur ja arusaadavus.

Täiendavad kontrollküsimused:

- Milline dokumentatsioon on olemas IP-kõne planeerimise kohta?

M 2.373 IP-kõne turvajuhendi väljatöötamine

Algatamise eest vastutavad: asutuse/ettevõtte juhatus, infoturbeosakond

Rakendamise eest vastutavad: IT-juht, infoturbeosakond

Telefoniteenuste käideldavusele esitatakse kõrgeid nõudeid. Sama oluline on aga ka nende konfidentsiaalsus. Seetõttu on eriti tähtis telekommunikatsiooniseadmete turvaline ja nõuetele vastav talitlus. Seda on võimalik tagada vaid juhul, kui tegutsemisviis on sätestatud olemasolevas ohutustehnilises juhendis. IP-kõnedele esitatavate tsentraalsete turvanõuete, samuti ka saavutatava turvataseme aluseks on üleorganisatsioonilised turvasuunised. Need peaksid olema formuleeritud spetsiaalses IP-kõnede turvasuunises, et konkretiseerida ja rakendada kõrgemal seisvaid ja üldisi turvasuuniseid. Seoses sellega tuleb kontrollida, kas lisaks üleorganisatsioonilistele turvasuunistele tuleb järgida ka teisi kõrgemal seisvaid eeskirju, nagu näiteks IT-suuniseid, paroolide kasutamise, IT-süsteemide, milles käitatakse IP-kõne komponente, või Interneti kasutamist reguleerivaid eeskirju. Kõik kasutajad ja grupid, kes osalevad IP-kõne komponentide planeerimises, soetamises ja kasutamises, peavad olema tuttavad IP-kõne turvasuunistega ning võtma need oma töö aluseks. Nii nagu kõikide suuniste puhul, tuleb nende sisu ja rakendamist kõrgemal seisva auditi käigus regulaarselt kontrollida. Turvasuunistes tuleks kõigepealt sõnastada üldised turvanõuded ning määrata IP-kõne kasutamise põhireeglid. Alljärgnevalt on loetletud aspektid, millele on kindlasti vaja pöörata tähelepanu.

Üldised IP-kõne kasutamise reeglid

Kõik kasutajad peaksid olema teadlikud potentsiaalsetest turvariskidest ja probleemidest IP-kõne kasutamisel, aga ka rakendatud turvameetmete võimaluste piiridest. Kuna IP-kõne vallas avastatakse üha uusi turvaauke, tuleb vastutatavatel infoturbega tegelevatel töötajatel ennast pidevalt uute riskide alal täiendada. Teatud juhtudel on vajalik töötajaid regulaarselt informeerida uutest avastatud riskidest, tõstes seeläbi nende teadlikkust. Turvasuuniste koostamisel on soovitatav formuleerida kõigepealt maksimumnõuded ja -eeskirjad süsteemi turvalisuse tagamiseks. Seejärel tuleks need kõigi asjaosalistega kooskõlastada ning kontrollida nende realiseeritavust. Ideaalse tulemuse saavutamiseks võetakse arvesse kõiki aspekte. Iga teises etapis kavandatud või vähendatud nõuetega eeskirja korral tuleks nende mitte arvesse võtmise põhjus dokumenteerida. Turvasuunistes peavad olema selgelt defineeritud alljärgnevad aspektid:

- Kas ja kus tohib IP-kõne komponente kasutada?
- Millistel tehnilistel tingimustel tohib IP-kõnet kasutada? Nende hulka kuulub eelkõige turvameetmete kindlaksmääramine, vajaliku turvariistvara ja -tarkvara valik ning installeerimine, samuti eeskirjad vastava IT-süsteemide turvaliseks konfigureerimiseks.
- Millist informatsiooni ei tohi üle IP-kõne edastada?
- Milliseid teenuseid ja funktsioone kasutatakse?

Töötajaid tuleb informeerida, millistel tingimustel tohib IP-kõnet kasutada väljaspool asutust, kuna seal võivad kehtida teised infoturbereeglid.

IP-kõne vahendustarkvara

IP-kõne vahendustarkvara käitamiseks tuleb reglementeerida vähemalt alljärgnevad aspektid:

- Tuleb sätestada seadmete soetamise tingimused, arvestades nõuete profiili (vt M 2.375 Asjakohane IP-kõne (VOIP) süsteemide valik).
- Tuleb sätestada administraatorite ja audiitorite töökorraldus. Selleks tuleks leida vastused alljärgnevatele küsimustele:
- Milliste kanalite kaudu tohivad administraatorid ja audiitorid omada juurdepääsu süsteemile (näiteks ainult lokaalselt konsooli kaudu, oma haldusvõrgu või krüpteeritud ühenduste kaudu)?
- Millised toimingud tuleb dokumenteerida? Millisel moel toimub dokumentatsiooni loomine ja korrashoid?
- Kas teatud muudatuste tegemisel kehtib nelja silma printsiip?
- Kas IT-süsteemide administraatori ja IP-kõne rakenduste eest vastutajate vastutusala on võimalik üksteisest lahutada?
- Vastutusalad tuleb kindlaks määrata ja reguleerida.
- Eeskirjad installeerimiseks ja konfigureerimiseks:
- Tegevusviis esmasel installeerimisel
- Vaikeseadete turvalisuse kontroll
- Rakendamine ning konfiguratsioon
- Eelnimetatud aspektid tuleb sätestada ja dokumenteerida.
- Tuleb juurutada kasutajate ja rollide haldus või laiendada olemasolevat. Selle hulka kuuluvad:
- Eeskirjad kasutajate ja rollide haldamiseks, volituste struktuurid (autentimise ja volitamise käik ja meetodid, volitused installeerimiseks, värskendamiseks, konfiguratsiooni muutmiseks jne.)
- Administraatorite rollikontseptsioon
- Kasutajate halduse kontseptsioon. Kasutajad tuleb sisse seada ja telefoninumbrid välja jagada. Kasutajatele võib võimaldada teatud privileege, nagu näiteks võimalust helistada tasulistele teenusnumbritele
- Turvaliseks talitluseks vajatakse alljärgnevaid regulatsioone:
- Dokumentatsiooni koostamiseks ja korrashoiuks, dokumenteerimise vormi ja ulatuse kindlaksmääramiseks, nt protseduuride juhised, kasutusjuhendid
- Milliseid teenuseid ja protokolle lubatakse või milliseid ei lubata
- Lubatud sideliinide osas, kuidas näiteks oleks võimalik vältida otseside loomist IP-kõne sisesüsteemidest avalikesse võrkudesse
- Tarkvarauuenduste läbiviimiseks
- Turvapoliitika eeskirjade sätestamiseks IT-süsteemide, milles IP-kõne vahendustarkvara kasutatakse.
- Eeskirjad turvalise talitluse tagamiseks peaksid sisaldama järgmist informatsiooni:
- Kuidas on võimalik tagada turvaline administreerimine (näiteks peaks juurdepääs administreerimiseks toimuma ainult turvaliste liinide kaudu)?
- Kuidas tuleks rakendada signaliseerimis- ja meediatranspordi protokolle?
- Milliseid tööriistu tuleks kasutada tööprotsessi ja hoolduse käigus?

- Kuidas peaks toimuma volituste andmine ning millistest protseduuridest tuleks tarkvara värskendamisel ja konfiguratsioonimuudatuste korral kinni pidada?
- Milliseid turvameetmeid tuleb rakendada operatsioonisüsteemis, milles kasutatakse vahendustarkvara?
- Logimise osas on vaja otsustada järgnevat:
- Millised sündmused tuleb logida?
- Kus logifaile säilitatakse?
- Kuidas ja kui pika aja tagant toimub logide analüüs?
- Andmevarunduse läbiviimiseks ja IP-kõne komponentide taastamiseks tuleb laiendada üleorganisatsioonilist andmevarunduskontseptsiooni.
- Tuleb reglementeerida käitumine süsteemi tõrgete, tehniliste vigade (kohalik tugi, kaughooldus) ja turvaintsidentide korral.

IP-kõne terminalid

Alljärgnevalt tutvustatakse IP-kõne terminalide kasutamise eeskirju, mis tuleks lisada turvaeeskirjadesse:

- Nõuete profiili alusel tuleks kehtestada seadmete soetamise eeskirjad
- Tuleb sätestada administraatorite ja audiitorite töökorraldus. Sobivaks näiteks on kasutatavate tarkvaratelefonide administratsiooni eraldamine IT-süsteemi administratsioonist.
- Installeerimise ja konfigureerimise nõuded tuleb sätestada turvajuhendis. Selleks tuleks leida vastused alljärgnevatele küsimustele:
- Kas tarkvaratelefoni konfiguratsioon on tarnimisel piisav või peab konfigureerimine olema võimalik kasutamise käigus?
- Kuidas muudetakse suure hulga terminalide korral kasutamise käigus konfiguratsiooni?
- Milliste kanalite kaudu tohivad administraatorid omada juurdepääsu terminalidele?
- Millist liiki teenuste konfigureerimist, nagu näiteks edastamised, tohivad kasutajad teostada?
- Eeskirjad on turvalise kasutamise tagamisel väga olulised. Siia kuuluvad järgmised eeskirjad:
- Administreerimise turvalisuse tagamine (näiteks juurdepääs vaid kaitstud sideliinide kaudu)
- Krüpteeritavate signaliseerimis- ja meediatranspordi protokollide kasutamine
- Tööriistad, mis on ette nähtud kasutamiseks tööprotsessis ja hooldustööde läbiviimisel, integreerimine olemasolevasse võrguhaldusesse
- Volitused ja protseduurid tarkvara värskendamisel ja konfiguratsioonimuudatuste läbiviimisel
- Nõuded meetmetele kasutaja äraolekul, nagu näiteks kõnede ümbersuunamine ja telefoni blokeerimine
- Turvalise talitluse tagamine operatsioonisüsteemile, milles kasutatakse tarkvaratelefoni

- Et tagada valmisolek hädaolukorraks, tuleb turvasuunistes sätestada reeglid alternatiivsete sidekanalite kasutuselevõtuks.

IP-kõne turvasuuniste täitmise vastutus on IT-osakonnal, muudatused ja kõrvalekalded on võimalikud vaid juhul, kui need on kooskõlastatud infoturbeosakonnaga.

Täiendavad kontrollküsimused:

- Kas IP-kõnede kasutamiseks ja talitluse tagamiseks on koostatud turvasuunised?
- Millal IP-kõne turvasuuniseid viimati uuendati?
- Kas IP-kõne turvasuuniste koostamisel võeti arvesse komponentide nagu terminalide, lüüside, lüüsivahu ja puhvrite erinevat kasutusotstarvet?

M 2.374 IP-kõne krüpteerimise ulatus

Algatamise eest vastutavad: IT-juht, infoturbeosakond:

Rakendamise eest vastutavad: IT-juht, infoturbeosakond

Juhul, kui häkkeril õnnestub sobivas kohas asutuse sisevõrgule ligi pääseda, on tal võimalik kogu võrguühendust kohtvõrgus salvestada. Kui IP-kõne kasutuskoormus ei ole krüpteeritud, on häkkeril võimalik igasugusele infole ligi pääseda. Näiteks võib ta signaliseerimisandmete alusel välja selgitada, kes, kui kaua ja kellega rääkis. Endastmõistetavalt võiks häkker analüüsida ka meediatranspordi protokolli kaudu edastatavat infot ning selle kaudu telefonikõnesid pealt kuulata. Seepärast tuleks mõelda IP-kõne kasutajaandmete krüpteerimisele. Krüpteerimist peavad võimaldama aga kõik osalevad PBX-süsteemid.

Kaitse organisatsiooni sees tegutsevate küberkurjategijate eest

Otsuse tegemisel, kas IP-kõne kaudu toimuv andmevahetus tuleks krüpteerida, on tihti kasulik käsitleda sise- ja väliskommunikatsiooni eraldi. IP-kõnede osas võib kohtvõrgu piirides kaaluda krüpteerimisest loobumist. Seejuures tuleb tagada, et kõnealusele infole ei oleks väljaspool organisatsiooni tegutseval häkkeril võimalik kaitseta võrguosa nagu näiteks traadita kohtvõrgu kaudu juurde pääseda.

Krüpteerimisest võib olla kasu sisekõnede kaitsmiseks organisatsiooni sees tegutsevate pahategijate eest. Selleks võiks kasutada IP-kõne terminale VPN (Virtual Private Network) lõpp-punktidena või krüpteeritud meediatranspordiprotokolle, nagu SRTP (Secure Realtime Transport Protocol). Kui kõik IP-kõne seadmed võimaldavad kasutada krüpteeritud signaliseerimisprotokolle, on soovitatav neid ka kasutada. Sellega välditakse muuhulgas ka paroolide pealtkuulamist ja näiteks SIP-registris teise kasutaja nimel volitamata sisselogimist.

Kaitse väljaspool asutust tegutsevate küberkurjategijate eest

Kui IP-kõne paketid väljuvad turvalisest LAN-võrgust, tuleb neid vastavaid meetmeid kasutades kaitsta. IP-kõne kaudu toimuva andevahetuse kaitseks tuleks välja valida üks või mitmed alljärgnevatest turvameetmetest:

- Turvaliste meediatranspordiprotokollide kasutamine nagu SRTP (Secure Realtime Transport Protocol).
- Signaliseerimisprotokolli krüpteerimine, näiteks TLS (Transport Layer Security) abil.
- Virtuaalne privaatvõrk: VPN-lüüside kasutamise kaudu saab krüpteeritult edastada infot üksteisest eemal asuvate LAN-võrkude vahel. Üksikuid seadmeid võib kasutada VPN-lõpp-punktidena. Selle eeliseks on veel asjaolu, et ka organisatsiooni sees tegutseval pahategijal ei ole infole juurdepääsu. Ilma krüpteeritavate signaliseerimis- ja meediatranspordiprotokollide otsese toetuseta saab sel moel kasutada logimisest mittesõltuvat krüpteerimist. Kui näiteks andmevahetuseks erinevate asukohtade vahel vajatakse mitmesugust IP-kõne vahendustarkvara (Middleware), tuleks ka need integreerida virtuaalsesse privaatvõrku, kui pole võimalik aktiveerida teisi krüpteerimismehhanisme.

Kui side näiteks erinevates asukohtades olevate vahendustarkvara komponentide vahel ei ole küllaldaselt kaitstud, on häkkeril võimalik teatud tingimustel pealt kuulata kõiki asukohtade vahel toimuvaid kõnesid. Kui vahendustarkvara kasutatakse IT-süsteemis, on reeglina võimalik probleemideta installeerida lisaks VPN tugi, mis ei sõltu IP-kõne logimisest.

- Raadiovõrgu krüpteerimine: Kaitseta organisatsioonisisest raadiovõrku on võimalik rünnata ka väljaspoolt selle asukohta. Kui IP-kõne vestluspartnerid on üksteisega ühenduses traadita kohtvõrgu kaudu, tuleb selle kaitseks kasutada kvalifitseeritud kaitset, nagu WPA2 (vaata ka moodulit B 4.6 Traadita kohtvõrgud). Kuna see krüpteering kaitseb vaid raadiovõrku, tuleb arvestada asjaoluga, et info edastamine ülejäänud LAN-võrgus toimub kaitseta.

Kui IP-kõne kaudu edastatav info ei välju LAN-võrgust teiste kanalite kaudu, kehtivad kvalifitseeritud krüpteerimisel samad tingimused nagu sisekommunikatsiooni korral, mille puhul võib teatud tingimustel krüpteerimisest loobuda. Kui kõne telefoniabonendiga peab toimuma avaliku telefonivõrgu kaudu, võib sidet IP-kõne terminali ja lüüsi vahel, mida kasutatakse IP-kõne võrgu ja avaliku võrgu vahel, teatud tingimustel VPNide või krüpteerivate signaliseerimis- ja meediatranspordiprotokollidega kaitsta. Kuna vaid väga vähesed telefonid on varustatud mehhanismidega ühendust vahendavate võrkude kaitseks ja nende rakendamine sõltub vastuvõtjast, ei ole krüpteerimine IP lüüsi ja vestluspartneri vahel enamasti reaalne. Kui krüpteeritud kommunikatsioon ei ole võimalik, näiteks organisatsioonivälistе äripartneritega, tuleb kasutajaid sellest informeerida ja selgitada neile ohtusid. Konfidentsiaalse sisuga informatsiooni ei tohiks puuduliku krüpteerimise korral telefoni teel vahetada. IP-kõne komponentide soetamisel tuleb jälgida, et need võimaldaksid krüpteerivate signaliseerimis- ja meediatranspordiprotokollide, nagu näiteks TLS ja SRTP kasutamist (vt M 2.375 Asjakohane IP-kõne (VOIP) süsteemide valik).

Kontrollküsimused:

- Kas IP-kõne komponentide vahel kasutatakse krüpteerivaid signaliseerimis- ja meediatranspordiprotokolle?
- Kas IP-kõne vahendustarkvara kommunikatsiooniks saab kasutada virtuaalset privaatvõrku?

M 2.375 Asjakohane IP-kõne (VOIP) süsteemide valik

Algatamise eest vastutavad: IT-juht, infoturbeosakond:

Rakendamise eest vastutavad: IT-juht, firma, kust seadmed ostetakse, administraator

PBX-seadmete tootjad pakuvad arvukaid telefoniteenuste lahendusi. Lisaks IP-kõne ning analoog- ja digitaaltelefoniteenuste seadmetele on võimalik soetada ka tooteid, mis sobivad mõlema arhitektuuriga. Näideteks on PBX-seadmed ühendust vahendavatele võrkudele, mis on varustatud IP ühenduse ja lüüsidega, mida saab lülitada IP-arhitektuuri ja avaliku, ühendust vahendava telefonivõrgu vahele. Vajalike toodete väljavalimisel on lisaks põhifunktsioonidele nagu signaliseerimis- ja meediatranspordiprotokollide tugifunktsioonide olemasolule vaja silmas pidada arvukaid ohutustehnilisi aspekte. Enne IP-kõne seadmete soetamist tuleb koostada nõuete nimekiri, mille alusel toimub turul saadaolevate toodete hindamine. Hindamise alusel võetakse vastu seadmete soetamise otsus, mis peab tagama soetatava toote nõuetele vastavuse praktilise töö käigus.

Üldised nõuded

Alljärgnevalt on loetletud mõned üldised nõuded, mida tuleks järgida IP-kõne terminalide ja vahendustarkvara soetamisel.

Üldkriteeriumid

- Kas soetada iseseisev IP-kõne seade (*appliance*) või standardsel arvutil töötav lahendus? Igal juhul peaks enamasti keeruline operatsioonisüsteem olema konfigureeritud nii, et oleks aktiveeritud ainult tõeliselt vajalikud funktsioonid, et toimuks piirangutega pääsuõiguste andmine ning süstemaatiline kitsaskohtade likvideerimine.
- Kas toode toetab kõiki vajalikke protokolle?
- Kas tootja või mõni sõltumatu ettevõte pakub tootekoolitusi?
- Kas on saadaval usaldusväärset informatsiooni tark- ja riistvara töökindluse kohta?
- Kas IP-kõne komponendid täidavad neile esitatavaid töövõime nõudeid?
- Kas toodet on hinnatud formaalsete meetodite, nagu näiteks *Common Criteria* alusel?
- Kas IP-kõne komponendid ühilduvad olemasolevate toodetega?
- Kas seadmed võimaldavad turvalist sisselogimist ja kasutajate haldust?
- Kas toote dokumentatsioon sisaldab täpset tehniliste ja administratiivsete detailide kirjeldust?
- Kas on võimalik sõlmida IP-kõne komponentide hooldusleping? Tihti on juurdepääs uuendus- ja tugifunktsioonidele tootja poolt võimalik vaid seoses kehtiva hooldusleping uga.
- Kas hooldusleping u raamides on võimalik kindlaks määrata ka maksimaalne reageerimisaeg probleemide kõrvaldamiseks?
- Kas tootja pakub tehnilise klienditeeninduse (*Hotline*) võimalust, mille abil on probleemid koheselt lahendatavad?
- Kas toodet on hõlbus installeerida, konfigureerida ja administreerida?

Logimine

Logimiseks pakutavad võimalused peaksid vastama vähemalt turvasuunistes sätestatud nõuetele. Erilist tähtsust omavad alljärgnevad punktid:

- Kas logimise detailsuse aste on konfigureeritav?
- Kas süsteem võimaldab logida kõiki vajalikke andmeid?
- Kas ligipääs logifailidele on kaitstud?
- Kas süsteem võimaldab tsentraalset logimist? Tsentraalne logimine kergendab logiandmete sihipärast analüüsimist.
- Kas logimist on võimalik teostada vastavuses andmekaitsenõuetega?

Tarkvara uuendused

- Kas tootele antakse regulaarselt välja värskendusi ja paiku? Kas turvapaiku on võimalik saada kohe pärast turvaaukude ilmnemist?
- Kas tarkvarauuenduste abil saab kasutusele võtta uuemaid signaliseerimis- ja meediatranspordiprotokolle, milles on võimalikud turvaaugud kõrvaldatud ja mis võimaldavad uute turvamehhanismide kasutamist?
- Kas värskendustesse on kaasatud ka IP-kõne komponentide madalamad kihid, nagu uuendused operatsioonisüsteemis või teenused, mis ei ole otseses seotud IP-kõne süsteemiga? Turvaaukude kõrvaldamiseks *Appliance* operatsioonisüsteemis või IT-süsteemis tuleks ka need komponendid uuendada.
- Kas uuendused ja paigad kindlustatakse selliselt, et uuenduste ülekandmisel on välistatud nende väljavahetamine manipuleeritud versioonide vastu?

Haldus

- Kas IP-kõne komponendid võimaldavad kasutada turvalisi haldusprotokolle?
- Kas IP-kõne komponente on võimalik konfigureerida selliselt, et kõik varem defineeritud turvaeesmärgid oleksid saavutatavad?
- Kas tähtsaid konfiguratsiooniparameetreid on võimalik kaitsta kasutajapoolse muutmise eest?
- Kas IP-kõne komponente on võimalik hallata tsentraalselt juhitava haldustarkvara kaudu? Kas haldusliides on kujundatud selliselt, et juhitakse tähelepanu vigastele, ebakindlatele või ebapüsivatele konfiguratsioonidele või blokeeritakse need?

Krüpteerimine

Selleks, et oleks võimalik IP-kõne seadmete kaudu krüpteeritult infot vahetada, peavad süsteemis osalevad seadmed olema varustatud vastavate funktsioonidega. Olenevalt kaitsevajadusest võib planeerimise käigus olla võetud vastu otsus loobuda organisatsioonisisese IP-kõne kaudu toimuva kommunikatsiooni krüpteerimisest. Sellele vaatamata tuleks ka sel juhul soetada IP-kõne komponendid, mis võimaldavad krüpteerimist või mida on võimalik vastava funktsiooniga täiendada. Arvestada tuleks järgmiste aspektidega:

- Kas IP-kõne komponendid võimaldavad krüpteerida meediatranspordi- ja signaliseerimisprotokolle või kas saab krüpteerimist hiljem rakendada?
- Kas IP-kõne komponente saab kasutada *VPN* -tunneli lõpp-punktidena?

Vahendustarkvara valik (*Middleware*)

Telefoniteenused on tihti äriprotsessi oluliseks osaks. Seetõttu esitatakse muuhulgas suuri nõudmisi ka selle käideldavusele. Soetamisel tuleb silmas pidada järgmisi kriteeriumeid:

- Kas IP-kõne vahendustarkvara on võimalik dubleerida?
- Kas tootja pakub kõrge käideldavusega lahendusi?
- Kas tuleb soetada üks või mitu tsentraalset seadet, mis pakuvad IP-kõne kõiki funktsioone või tuleb soetada mitu üksikut, teineteisest sõltumatut seadet? Üksikud, üksteisest sõltumatud seadmed on näiteks SIP-protokollid (signaliseerimisprotokollid), proksiserverid ja asukoha sidumise serverid (*Location Server)*. Süsteeme, mis võimaldavad kasutada kõiki IP-kõne funktsioone, on tihti lihtsam konfigureerida. Mitmeid jagatud süsteeme on seevastu kergem kalibreerida. Kuna mitmete seadmete administreerimine on tihti töömahukam, võib sellega tõenäoliselt kaasneda väär konfigureerimine.

Aktiivsete võrgukomponentide valik

Kui IP-kõnele üleminek nõuab uute võrguseadmete, näiteks kommutaatorite hankimist, peab ka nende puhul jälgima teatud nõudeid. Kui kasutatakse olemasolevat andmesidevõrku, peavad võrguseadmed eristama IP-kõne pakette ja neid eelisjärjekorras edastama. Kui kahe lokaalse võrgu vahel toimub telefoniside ebakindla andmevõrgu, näiteks Interneti kaudu, tuleb kehtestada täiendavad nõuded. Kui seni ei ole võetud krüpteerimiseks kasutusele mingeid meetmeid, tuleks näiteks ebakindla võrguga ühendatud lüüse kasutada VPN-terminalidena.

Täiendav kontrollküsimus:

- Kas IP-kõne komponentidele esitatavad nõuded on küllaldaselt spetsifitseeritud ja dokumenteeritud?

M 2.376 Andmeside ja IP-kõne (VOIP) võrgu eraldamine

Algatamise eest vastutavad: IT-juht, infoturbeosakond, tehnikaosakonna juhataja

Rakendamise eest vastutavad: IT-juht, administraator, tehnikaosakond

IP-kõne teenused võimaldavad helistada olemasolevate IP andmesidevõrkude kaudu. Samas võib skaleeritavuse, teenusekvaliteedi (QoS), administreeritavuse ja turvalisuse suurendamiseks eraldada andmesidevõrgud ka loogiliselt IP-kõne võrkudest. Vaja on kontrollida, kas andmeside- ja IP-kõne võrgu eraldamine üksteisest on vajalik. Eraldamine on otstarbekas juhul, kui IP-kõne ja andmesidevõrgule esitatakse erinevaid turvanõudeid.

Võrkude eraldamine virtuaalkohtvõrkude (VLAN) kaudu

Kohalike võrkude füüsiline segmenteerimine on võimalik aktiivsete võrgukomponentide või loogiline segmenteerimine vastavalt VLAN konfiguratsiooni, niisiis virtuaalkohtvõrkude (Virtual Local Area Networks) kaudu. Loogiline eraldamine teostatakse enamasti võrgu VLAN tehnoloogiat kasutades teisel tasandil VLAN kommutaatorites (vt M 2.277z Kommutaatori funktsionaalne kirjeldus). Virtuaalkohtvõrgud üksi ei paku siiski kaitset ründajate eest, kes oma IT-süsteemiga (personaalarvuti, sülearvuti või server) füüsiliselt virtuaalkohtvõrguga ühenduse loovad. Kuna võrgupistik, niisiis telefoni VLAN-port on kõigile vahetult juurdepääsetav, on ründajal võimalik rünnata otse virtuaalkohtvõrgus paiknevaid telefone, ühendades näiteks telefoni asemel VLAN võrguga oma personaalarvuti. Sel põhjusel tuleks lisaks loogilisele võrgust eraldamisele tarvitusele võtta lisaabinõud taoliste rünnete tõrjumiseks.

Võrkude füüsiline eraldamine

Kõrgendatud turvanõuete korral võib osutuda otstarbekaks kõnevõrgu täielik füüsiline eraldamine andmevõrgust. Andme- ja kõnevõrkude füüsiline eraldamine vähendab tunduvalt ründevõimalusi. Lisaks sellele on ühe võrgu väljalangemise korral, näiteks võrgu aktiivkomponentide väljalangemisel või kaabli purunemisel võimalik kasutada allesjäänud sidevõrku. Eraldatuse tõttu ei mõjuta andmesidevõrgu suur koormus kõnevõrgu koormust.

Lahutamisel tekkivad probleemid

Praktikas võib aga järjekindel IP-kõne võrgu eraldamine IP-andmesidevõrgust kaasa tuua mõningaid probleeme kusagil mujal:

- IP-kõne komponendid vajavad juurdepääsu kasutajate andmebaasidele, nagu LDAP kataloogid, mis tavaliselt on juba andmesidevõrgus olemas, kuid võrkude eraldamise tõttu tuleks need dubleerida.
- IP-kõne võrgu haldamine, milles kasutatakse täielikku domeeninime (DNS), nõuab reeglina ligipääsu andmesidevõrgule.
- IP-kõne komponentide haldus võib võrkude järjekindlal lahutamisel olla töömahukam, kuna näiteks IP-kõne komponentide tarkvara värskenduste laadimine ei ole enam võimalik andmesidevõrgu, näiteks SFTP kaudu, vaid tuleb installeerida kohapeal. Ka IP-kõne komponentide kaugkonfiguratsioon, näiteks turvakesta (SSH) või turvalise HTTP (S-HTTP) kaudu, eeldab ühendust andmesidevõrguga või eraldi IT-süsteeme konfigureerimiseks.

Neid probleeme võib lahendada ka vastavate andmeside- ja IP-kõne võrkude vaheliste lüüsidega. Paljude võrguteenuste jaoks on võimalik kasutada proksiserverit IP-kõne võrgus, mis edastab pöördused IP-kõne võrgust andmesidevõrku.

- Võrkude eraldamise korral võib osutuda problemaatiliseks ka multifunktsionaalsete seadmete kasutamine, näiteks IP-telefon koos integreeritud meilikliendiga või laialdaselt levinud tarkvaratelefonid (softphones). Sellised terminalid vajavad juurdepääsu nii IP-kõne võrgule kui ka andmesidevõrgule.

Esimeseks võimalikuks lahenduseks oleks nende seadmete kasutamine selleks loodud loogilises võrgus. Füüsiline eraldamine ei ole siin võimalik.

- Juhtmeühenduskulude vähendamiseks on paljudel riistvaralistel IP telefonidel (hardphones) integreeritud minikommutaator. Sellisel juhul ühendatakse telefon otse võrgupessa ning teine IT-süsteem, näiteks töökoha arvuti, ühendatakse telefoniga. Sellise järjestuse korral ei ole IP-kõne võrgu eraldamine andmesidevõrgust võimalik. Loogilise eraldamise korral peab korruse kommutaator suutma mõlemat ühe switch port 'iga (kommutaatori pordiga) ühendatud seadet eraldada. See on võimalik kasutades näiteks MACaadresse või IEEE 802.1 X autentimist.

Pordi kaitse

Kui kasutatakse tarkvaralisi IP-telefone või teisi IP-kõne terminale, mida kasutatakse ainult helistamiseks, tuleb silmas pidada, et võrguühendustest, millega need seadmed on ühendatud, on võimalik luua vaid ettenähtud IP-kõne ühendusi. Vastasel korral saaks ründaja ühendada mobiilse IT-süsteemi PBX-terminali võrgupesaga ning saada juurdepääsu talle mitte ettenähtud informatsioonile ja teenustele. Üheks näiteks on telefon, mis asub kohas, mis ei ole alalise järelevalve all, näiteks maa-aluses garaažis. Kaitse on võimalik vastavate aktiivkomponentide filtrireeglite abil. Vastavalt turvavajadustele võib kasutada ka lisameetmeid, näiteks IEEE 802.1X autentimist, et tagada turvaline kasutamine. Tuleb arvestada, et MAC aadresside dünaamiline või staatiline jaotamine (kommutaatori) pordi või VLAN pääsuloendi juurde ei taga piisavat turvalisust, kuna MAC aadresse on kerge võltsida.

Kontrollküsimus:

- Kas andmesidevõrk IP-kõne võrk on teineteisest füüsiliselt või loogiliselt eraldatud?

M 2.377 Turvaline IP-kõne komponentide kasutusest kõrvaldamine

Algatamise eest vastutavad: IT-juht, infoturbeosakond:

Elluviimise eest vastutavad: administraator

Kui IP-kõne komponente, näiteks terminale või vahendustarkvara on vaja kasutuselt kõrvaldada või asendada, tuleb seadmetelt kogu turvalisuse tagamise seisukohalt tähtis info kustutada. See ei kehti mitte ainult siis, kui seadmed antakse edasi tootjale, teenindusettevõttele, jäätmekäitlusettevõttele või muudele kolmandatele isikutele. Ka utiliseerimise, teisaldamise või teistele kasutajatele edasiandmise korral tuleb tarvitusele võtta vastavad meetmed. Lisaks lõplikule kasutuselt kõrvaldamisele puudutab see ka eeskätt parandus- ja hoolsustööde läbiviimist ning garantii korras toimuvat komponentide väljavahetamist. Paljudel juhtudel on vajalik koostöös tootjate, müüjate ja/või teenindusettevõtetega varakult välja selgitada, milliseid meetmed infoturbe seisukohalt tähtsa info kustutamiseks on lepingu- ja garantiitingimustega võimalik vastavusse viia. Tihti on võimalik koos kehtestada otstarbekohased protseduurid. Vastavalt seadmete kasutusotstarbele võivad need sisaldada järgmist infoturbe seisukohalt olulist informatsiooni:

- Nimekiri telefonikõnedest, kes kellele helistas
- Kõnede kellaaeg ja kestus
- Kasutajatunnused ja paroolid IP-kõne infrastruktuuri sisselogimiseks
- Kasutajate õigused ja privileegid
- Üksikute kasutajate meiliaadressid kõnepostide kasutamiseks
- Kõneposti tervitustekst
- Kasutajale jäetud teated
- IP-aadressid ja muu võrguinformatsioon võrgu ülesehituse kohta
- Logiandmed
- Sertifikaadid ja võtmed
- Konfiguratsioonifailid
- Personaalsed telefoniraamatud
- Asutuse telefoniraamatud kõigi töötajate telefonidega
- Paroolid erakõnede arveldamiseks
- Informatsioon kasutajatele pakutavate lisateenuste kohta, näiteks tähtaegade meeldetuletus
- Erandjuhtudel ka toimunud telefonikõnede täielik salvestus

Vastavalt nimetatud info turvavajadusele tuleb silmas pidada, et andmed kustutataks ehk muudetaks lugematuks enne, kui defektsed või vananenud seadmed kasutusest kõrvaldatakse või välja vahetatakse. Pärast andmete kustutamist tuleb üle kontrollida, kas kustutamine õnnestus. Seejuures kasutatavad protseduurid sõltuvad suuresti seadme liigist ja kasutusotstarbest. Tavaarvutite korral, mida kasutati IP-kõne komponentidena, tuleks kõvakettad sobiva tööriista abil nii kustutada, et failide taastamine ei oleks enam võimalik. Selleks võib käivitada arvuti väliselt buutimisseadelt ning kõvakettad suvaliste andmetega üle kirjutada. Seejuures on soovitatav ülekirjutamise protseduuri mitmeid kordi korrata. Eraldi seadmete korral sõltuvad protseduurid sellest, kas seadmesse on integreeritud kõvaketas või kas andmed on salvestatud säilmällu. Sageli on seadmetel tehaseseadete

taastamise võimalus, millega on võimalik kõik konfiguratsiooniseadistused tagasi viia väljastusstandarditele vastavatele väärtustele. Ka tehaseseadistuste taastamise korral tuleks üle kontrollida, kas andmed said ikka kustutatud või taastatud või kas äkki on veel mõned andmed või failid olemas. Lisaks seadmes olevale informatsioonile tuleb kontrollida, kas tundlikku informatsiooni on salvestatud varukoopiatele. Kui turvakoopiate säilitamine ei ole muudel põhjustel (nt arhiveerimine, seadusandlikud nõuded) vajalik, tuleb ka need pärast seadmete kasutuselt kõrvaldamist kustutada. Sageli on komponendid väljast nimedega kiirvalikuklahvidel, IP-aadresside, telefoninumbrite või muu tehnilise informatsiooniga markeeritud. Ka need markeeringud tuleb enne seadme jäätmekäitlusse andmist eemaldada.

Täiendavad kontrollküsimused:

- Kas konfiguratsiooni- ja logifailid kustutatakse turvaliselt või muudetakse enne seadmete jäätmekäitlusse andmist loetamatuks?
- Kas enne seadmete jäätmekäitlusse andmist eemaldatakse neilt markeeringud?

M 2.378z Süsteemiarendus

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: IT-juht, administraator, kasutajad

Selle turvameetme raames mõistetakse süsteemiarenduse all riistvara, tarkvara või keerulise, paljudest riistvara- ja tarkvarakomponentidest koosneva süsteemi loomist, muutmist või täiendamist. Kõikidel nimetatud juhtudel tuleb süsteemiarendus kooskõlastada eelnevalt IT-juhtkonnaga ja asjaga seotud olevate erialaosakondadega. Selleks tuleb defineerida esmane ülevaade vajalikest funktsioonidest ja nõuetest. Infoturbemeeskonda tuleb süsteemiarenduse plaanidest informeerida juba väga varajases staadiumis, mis võimaldab vajalike IT turvameetmetega arvestada juba kontseptsiooni loomise faasis. Lisaks süsteemi funktsionaalsusele tuleb igal juhul arvestada selle võimalike mõjudega äriprotsessidele ja organisatsiooni üldisele infoturbele. IT-süsteemi turvalisusele esitatavad nõuded tuleks välja selgitada ja kooskõlastada juba enne süsteemiarenduse algust. Turvameetmete tagantjärele juurutamine on seotud suuremate kulutustega ja pakub üldiselt vähem kaitset kui turvameetmed, mis on toote süsteemiarenduse või valikuprotsessi integreeritud juba algusest peale. Turvalisus peaks seetõttu olema IT-süsteemi või tootesse integreeritud komponent kogu selle elutsükli jooksul. Siinkohal nimetatud soovituste aluseks on „IT-alaste projektide planeerimine ja läbiviimine SLVs riiklikul tasandil" (V-mudel) ja osaliselt ka „Euroopa infotehnoloogiaturbe hindamiskriteeriumid" (ITSEC) ning standard „ Common Criteria for Information Technology Security Evalution" (CC).

Nõuete kataloogi koostamine

Nõuete väljatöötamisel tuleb lähtuda meetmest M 2.80 Tüüptarkvara nõuete kataloogi koostamine . Selles on lahti seletatud põhilised punktid, millega tuleb arvestada funktsionaalsete ja infoturbe seisukohalt oluliste nõuete kindlaksmääramisel.

Nõuete kataloog tuleb infoturbemeeskonnaga kooskõlastada. Juhul kui süsteemiarenduse käigus ilmnevad muutused nõuetes, peab ka infoturbemeeskond need heaks kiitma ja nõuete kataloogi tuleb uuendused sisse viia. Nõuete kataloog on aluseks toote vastuvõtmisele ja kinnitamisele.

Tegevusmudel

Süsteemiarendus peab toimuma kõikehõlmava, ühtse ja siduva tegevusmudeli järgi. Tegevusmudel peab hõlmama turvaspetsiifilisi rolle, tegevusi ja tulemusi, mille kaudu on võimalik kontrollida turvalisuse tagamiseks vajalike süsteemi funktsioonide sobivust ja rakendamist. Enne mudeli lõplikku juurutamist tuleb veenduda, et see sisaldab vähemalt järgmisi ITSECis/CCs määratletud faase:

- nõuete defineerimine,
- arhitektuuriline arendus,
- detailne arendus,
- realiseerimisfaas.

Infoturbe seisukohalt tähtsad tulemused nõuete defineerimise faasis

Nõuete defineerimise faasis tuleb vaatluse alla võtta vastava rakenduse infoturvet mõjutavad ohud, turvaaugud ja riskid, rakenduskeskkonna turvaaspektid,

välised spetsifikatsioonid ja projekti keskkond. Kaitsevajaduse kindlaksmääramise raames määratakse selle alusel kindlaks kaitsevajadus, mille põhjal formuleeritakse turvanõuded. Kontrollida tuleb turvanõuete sisu ja terviklust (vt M 2.80 Tüüptarkvara nõuete kataloogi koostamine).

Infoturbe seisukohalt tähtsad tulemused arhitektuuri arendusfaasis

Arhitektuuri arendusfaasis tuleb rakenduste sisekontroll, infoturbe põhifunktsioonid ning organisatsioonilised ja tehnilised turvameetmed spetsifitseerida erialasel tasandil. Tuleb kontrollida, kas turvanõuete kindlaksmääramine arhitektuuri arenduse spetsifikatsioonide kaudu vastab sisule ja on küllaldaselt detailne. Siinkohal on vajalik turvakomponentide selge ja loogiline eraldamine teistest komponentidest.

Infoturbe seisukohalt tähtsad tulemused detailse arenduse faasis

Detailse arenduse faasis tuleb turvaalaseid spetsifikatsioone täiustada sel määral, et need saaksid ilma edasist tõlgendamist vajamata võtta realiseerimise aluseks. Identifitseerida tuleb kõik moodulid, milles viiakse läbi kontrollifunktsioone, kus toimuvad turvakriitilised töötlus- ja kommunikatsiooniprotsessid ning juurdepääs tundlikele andmetele või millelt kantakse üle tundlikke andmeid. Kontrollida tuleb, kas erialase arenduse täiendamine detailse arenduse läbi toimub sisu kohaselt. Turvanõuete tagamiseks vajaliku sisekontrolli spetsifitseerimine peab toimuma programmiliideste (application program interfaces, API) defineerimise abil. Paremaks käsitlemiseks tuleks infoturbe rakendusliidesed (API) selgelt struktureerida ja ülejäänud moodulitest eraldada.

Infoturbe seisukohalt tähtsad tulemused realiseerimisfaasis

Realiseerimisfaasis peab toimuma spetsifitseeritud turvanõuete adekvaatne rakendamine vastavate infoturbe rakendusliideste abil. Tuleb kontrollida ja testida, kas selle spetsifikatsiooni, eriti turvaspetsifikatsiooni juurutamine on küllaldane.

Minimaalsed nõuded arenduskeskkonnale

Integreeritud arenduskeskkond (integrated development environment, IDE) on tarkvaraarenduse rakendusprogramm. Integreeritud arenduskeskkond lihtsustab tarkvaraarendust, kuna sinna on koondatud kõik põhilised süsteemiarenduse komponendid, näiteks kompilaator, silur ja redaktor. Kogu arenduse jooksul tuleb kasutada ühest ja siduvat teekide struktuuri. Nimede kasutamise tava tuleb defineerida ja rakendada seda nii programmi koodi kui ka moodulite nimetamisel. Selle eesmärk on tähtsa informatsiooni, näiteks arengustaadiumi ja -koha, dokumendi tüübi jne esiletõstmine vastava tähistuse abil.

Need on meetodid tööriistade ja rollide defineerimiseks ja rakendamiseks, mille abil on võimalikud järgmised tegevused:

- süsteemide (riist- ja tarkvara) ning nende komponentide ja omaduste kindlaksmääramine ja identifitseerimine;
- vajalike muutuste ja parenduste süstemaatilise ja kontrollitud töötlemise juhtimine;
- ettekavatsemata, kontrollimatute või juhtimata muudatuste ärahoidmine;
- kõigi vahe- ja lõpptulemuste arhiveerimine ja administreerimine;

- arenduste detsentraalne, st erinevates arengufaasides ühtse (turva-) standardi alusel läbiviimine;
- kõikide arendustööriistade ja arendusandmebaasi kasutajate selge ja ühetähenduslik identifitseerimine;
- kasutajate arendustööriistade juurdepääsu kontrollimine arendusandmebaasile olenevalt kasutaja rollist (teadmistarve);
- arendusandmete tervikluse tagamine;
- arendusandmete muutmise ja muudatusi läbiviinud isikute kindlakstegemine.

Kontrollitud ja testitud arendustulemusi peab olema võimalik fikseerida selliselt, et neid saaks arendustöö jätkamisel aluseks võtta. Eriti tähtis on, et tegevusmudeli defineeritud punktides saaks arenduse erinevatele arendusüksustele arendustöö jätkamiseks üle anda. Kasutatavad arendustööriistad peavad võimaldama kõikide teisendamiste või negatiivsete testitulemuste alusel vajalike muutuste säilitamist, läbiviimist ja kvaliteetset kaitset. Ka füüsiline keskkond, milles süsteemiarendus peab toimuma, tuleb varasema planeerimise käigus turvanõuete alusel kindlaks määrata. Nende hulka kuuluvad muu hulgas ka sisse- ja juurdepääsu kontrollimehhanismidele esitatavad nõuded.

Kvaliteedikontroll (QS)

Juba süsteemiarenduse alguses tuleb kavandada kvaliteedikontroll. Seejuures peavad sobivad meetmed tagama infoturbenõuetest kinnipidamise ja nende konstruktiivse ning analüütilise integreerimise arendusprotsessiga. Lisaks kontrollile, kas süsteem täidab spetsifikatsioonidele ja nõuete kataloogile vastavaid funktsioone, tuleb kontrollida ka süsteemi käitumist väär- või kuritarvitamise korral. Kindlaksmääratud ülevaatusaegadeks, vähemalt iga arengufaasi lõpuks, tuleb töötada välja ka kvaliteedikontrolli meetmed. Lisaks sellele võib vajaduse korral korraldada organisatsioonisiseseid ülevaatusi.

Nõuete defineerimise ja kavandamise faasis tuleb kavandada ja dokumenteerida testimisspetsifikatsioonid ja testimisjuhtumid, mis sobivad süsteemi kvaliteedi- ja turvanõuete täitmise kontrollimiseks. Realiseerimisfaasis ja vastuvõtmisel tuleb läbi viia vastavad testid. Testide läbiviimine tuleb dokumenteerida. Tuleb püüda jõuda nii kaugele, et testimistulemusi oleks võimalik automaatselt korrata ja võrrelda (regressioonitest). Baasandmeid on lubatud testimisandmetena põhimõtteliselt kasutada vaid anonüümsetena (vt M 2.82 Tüüptarkvara testimisplaani väljatöötamine ja M 2.83 Tüüptarkvara testimine .)

Süsteemi töösse rakendamine ja tarkvara hooldus

Süsteemi töösse rakendamine ja süsteemi hooldus peab olema reglementeeritud üheselt mõistetavate juhenditega.

Süsteemi töösse rakendamine

Tuleb tagada range arendus- ja tööprotsessi, eriti testimistulemuste ja reaalaja andmete töötlemise eraldamine. Tuleb luua selgelt ja arusaadavalt defineeritud arendatud süsteemide ja rakenduste kinnitamise meetod. Üleviimine testimiskeskkonnast töökeskkonda võib toimuda alles pärast kinnitamist. Ühtegi programmi osa, mis on mõeldud ainult testimiseks, ei kinnitata. Minimaalne eeldus kinnita-

miseks on vastuvõtmise täielik ja õnnestunud läbiviimine arvukate testimiste teel sihtkeskkonnas arendusprotsessi lõpul. Eriti tähtis on kinnitamise käigus kontrollida, kas IT-süsteemid ja IT-rakendused käituvad sihtkeskkonnas turvanõuete kohaselt. Tuleb garanteerida, et rakendataks vaid nõuetekohaselt kinnitatud programme või mooduleid (vt M 2.85 Tüüptarkvara kinnitamine):

- Arendustulemuste turvaliseks jaotamiseks peavad olema välja töötatud kindlad protseduurid (vt M 2.86 Tarkvara tervikluse tagamine).
- Väljajagatud rakenduste installeerimiseks ja konfigureerimiseks peavad olema kindlaks määratud ühtsed ja siduvad protseduurid (vt M 2.84 Tüüptarkvara installeerimisjuhendite otsustamine ja koostamine ja M 2.87 Tüüptarkvara installeerimine ja konfigureerimine).
- Arendajatel ei tohi mitte mingil ajal olla võimalik IT-süsteemide või rakenduste arendusprotsessi ajal neid volituseta ja kontrollimatult töösse rakendada või juba töös olevaid IT-süsteeme või rakendusi pärast vastuvõtmist või kinnitamist muuta (vt M 2.88 Tüüptarkvara litsentsi- ja versioonihaldus).
- Peab olema kindlaks määratud protseduur, mis näeb ette ülevõtmise olenevalt ajalistest ja lokaalsetest tingimustest.

Hooldus ja probleemide haldus

Välistada tuleb igasugune kasutuses oleva IT-süsteemi volitamata muutmine. Volitatud süsteemimuudatused peavad olema tõestatavad sobivate muutuste ja konfiguratsiooni haldamise protsesside abil. Muutuste ja konfiguratsioonihalduse raames tuleb defineerida ka kõikide süsteemi komponentide säilitustähtajad. Ka kasutuselt kõrvaldatud süsteemi komponendid, nagu programmi või mooduli versioonid, konfiguratsiooniandmed ja nende dokumentatsioon, peavad olema jälitatavad nende säilitustähtaja lõpuni. Tuleb välja töötada selgelt defineeritud protseduur ja ühemõtteliselt kindlaksmääratud kompetentsid vastutavale instantsile süsteemiga seotud probleemide kohta tagasiside andmiseks. Iga kindlaksmääratud puuduse põhjal või funktsionaalsuse laiendamiseks sisseviidud volitatud muudatus süsteemis peab toimuma valitud tegevusmudelist lähtudes ühtses arenduskeskkonnas, millele järgneb kontrollitud taasrakendamine tööprotsessi. Lisaks peab olemas olema selgelt ja arusaadavalt defineeritud avariiolukorras toimimise protseduur.

Lõppkasutaja tarkvara arendus

Sageli võimaldab standardtarkvara lõppkasutajatel endil oma programme arendada ja kasutada, et kergendada rutiinset tegevust (nt makroprogrammeerimise abil). Selliste isearenduslike programmide kontrollimatu rakendamine kujutab endast iseenesest mõistetavalt turvariski. Seetõttu tuleks organisatsioonis põhimõtteliselt otsustada, kas sellised omaarendused on lubatud või mitte ning kes ja kus selliseid arendusi teostada tohib (vt M 2.379z Tarkvaraarendus lõppkasutaja poolt). Ka omaarendused peavad enne töökeskkonnas rakendamist läbima testimis- ja kinnitamisprotseduurid. Samuti tuleb selgeks teha, kelle ülesanne on nende programmide hooldamine ja võimalike probleemide kõrvaldamine. Omaarenduslike programmide rakendamine tuleks sätestada turvasuunistes.

Kontrollküsimus:

- Kas organisatsioonil on olemas turvasuunised süsteemiarenduse läbiviimiseks?

M 2.379z Tarkvaraarendus lõppkasutaja poolt

Algatamise eest vastutavad: IT-juht
Rakendamise eest vastutavad: IT-juht, administraator, kasutajad

Paljud büroodes kasutatavad standardprogrammid võimaldavad kasutajal endal tarkvara arendada, näiteks eesmärgiga lihtsustada rutiinseid tegevusi.

Tüüpilised näited selle kohta on makroprogrammeerimine Microsoft Wordi või Accessi all. Kuigi töötajate loomingulisus ja pühendumine on tervitatavad, tuleb asutusel siiski võtta seisukoht, kuidas toimida makro- ja muu tarkvara lõppkasutajate arenduse korral. Arvesse tuleb võtta järgmist:

- üldjuhul ei ole makro- ja teiste programmide loojad õppinud programmeerijad;
- järgida tuleb asutuse turvajuhendeid;
- kuidas võiksid teised kasutajad loodud tarkvara rakendada (ja kes võtab sel juhul enda peale kasutajate juhendamise)?
- kuidas enamasti spontaanselt tekkinud programme hooldatakse ja dokumenteeritakse?

Kõigepealt tuleks igas asutuses langetada põhimõtteline otsus, kas selline tarkvaraarendus on soovitud või mitte. See tuleb kindlasti sätestada turvasuunistes.

Kui omaarenduslik tegevus ei ole lubatud, tuleb see funktsioon juba standardprogrammide installeerimisel desaktiveerida (kui see on võimalik). Kui omaarenduslik tegevus on lubatud, tuleks selle kohta luua vastavad kasutajatele mõeldud turvajuhised, mis sätestavad turvalisusele, dokumentatsioonile ja kvaliteedile esitatavad miinimumnõuded.

Sellises turvajuhendis peaks olema eelkõige sätestatud alljärgnevad aspektid:

- kehtivatest andmekaitse- ja infoturbe-eeskirjadest kinnipidamise nõue;
- nõuded kasutaja loodud tarkvara hoolikaks dokumenteerimiseks;
- omaarenduslikuks tegevuseks tohib kasutada vaid selleks lubatud tarkvarapakette (nt MS Word, MS Excel, või MS Access). Teiste rakenduste installeerimine või arenduskeskkondade kasutamine IT-osakonna loata ei ole lubatud.

Ka enda loodud tarkvarasse investeeritakse tööaega. Seetõttu tuleks jälgida, et see tarkvara oleks kättesaadav ka teistele töötajatele ning et seda pidevalt hooldataks. Lisaks peaks olema määratud kontaktisik, kelle poole oleks võimalik probleemide tekkimisel pöörduda. Isearendatud tarkvara värske versioon peaks olema kättesaadav kõigile kasutajatele. Seepärast on mõttekas saata kõik kaastöötajatele huvipakkuvad omaarendused edasi IT-osakonda. Seal otsustatakse, kas nende edasine levitamine on otstarbekohane ja kas seda on vajaduse korral võimalik kohandada ning pakkuda sellele kasutajatuge.

Kontrollküsimused:

- Kas on kindlaks määratud protseduur kasutaja arendatud tarkvaraga ümberkäimiseks?

- Kas on tagatud, et omaarendused on hästi dokumenteeritud?
- Kas on tagatud, et tarkvara värske versioon on kättesaadav kõigile kasutajatele?

M 2.380 Erandite kooskõlastamine

Algatamise eest vastutavad: infoturbeosakond, juht
Rakendamise eest vastutavad: infoturbeosakond, juht

Üksikutel juhtudel võib mõnest turvajuhendist kõrvalekaldumine osutuda otstarbekaks ja vajalikuks. Kuigi kõrvalekaldeid tuleb vältida, on kõrvalekaldumine teatud juhtudel siiski parem kui mõttetuks osutunud eeskirjadest jäigalt kinnipidamine. Kui erandid sagenevad, on see märk sellest, et olemasolev turvajuhend on aegunud. Seetõttu tuleb turvanõuded uuesti läbi vaadata ja uute olude järgi kohandada. Erandid tuleb igal juhul selleks volitatud isikutega kooskõlastada. Erandlikke lube tohib anda vaid harvadel juhtudel pärast põhjalikku kontrolli. Erandite kooskõlastamise korral tuleb kontrollida, ega need ei ohusta turvalisust. Selleks tuleb läbi viia riskide hindamine. Lõpuks tuleb koostada kirjalik põhjendus, millele kirjutab alla vastutav isik. Erandite kooskõlastamise protsessis peavad osalema nii vastutavad spetsialistid kui ka info ja rakenduste „omanikud" ning infoturbemeeskond. Erandeid tohib kooskõlastada vaid juhul, kui riski hinnatakse talutavaks. Erandite kooskõlastus tuleb välja anda tähtajaliselt.

Regulaarselt tuleb kontrollida (vähemalt iga 12 kuu tagant), kas erandite kooskõlastused on veel vajalikud ning kas kooskõlastused, mis teatud kindlas faasis osutusid vajalikuks, hiljem jälle tühistatakse. Erandite kooskõlastamiseks tuleb luua dokumenteeritud protsess. Dokumenteerida tuleb vähemalt alljärgnev:

- põhjendus, miks on vaja turvajuhistest kõrvale kalduda ja milliseid juhiseid see puudutab;
- erandi olemus ning selle mõjude ja asjassepuutuva valdkonna kirjeldus, kaasa arvatud riski hindamine;
- erandi rakendamise aeg;
- erandi taotleja ja kooskõlastaja;
- tähtajad.

Kõrvalekalletest tuleb informeerida kõiki asjassepuutuvaid töötajaid.

Kontrollküsimused:

- Kas erandite kooskõlastamiseks on välja töötatud kooskõlastamis- ja dokumenteerimisprotseduur?
- Kas erandite kooskõlastuste põhjendusi kontrollitakse regulaarselt?
- Kas on tagatud kõigi mittevajalike kooskõlastatud erandite tühistamine?
- Kas kõrvalekallete võimalikke tagajärgi analüüsitakse?

M 2.381 Traadita kohtvõrgu kasutamise strateegia väljatöötamine

Algatamise eest vastutavad: asutuse/ettevõtte juhatus, IT-juht, infoturbeosakond

Rakendamise eest vastutavad: IT-juht, infoturbeosakond

Enne traadita kohtvõrgu kasutuselevõtmist organisatsioonis tuleb kindlaks määrata organisatsiooni üldine strateegia traadita kohtvõrgu kasutamise osas. Tuleb otsustada, millised organisatsiooni üksused, millised rakendused ja millisel eesmärgil traadita kohtvõrku kasutama hakkavad ning milline informatsioonivahetus hakkab selle kaudu toimuma. Seejuures tuleks ka kindlaks määrata, millistesse ruumidesse traadita kohtvõrgud paigaldada (otstarbekas oleks see näiteks keskkondades, milles kasutajad liiguvad tihti teatud kindlate valdkondade piires) ja millistes valdkondades traadita kohtvõrku mitte mingil juhul ei tohiks olla (kuni aktiivse varjestuseni). Traadita kohtvõrgu komponente tohib kasutada näiteks järgmisteks otstarveteks:

- Organisatsiooni, selle osakonna või tootmisüksuse täielikuks katmiseks raadiovõrguga
- Mobiilsete komponentide kasutamiseks üksikutes ruumides, näiteks nõupidamisruumides
- Traadita kohtvõrgu pakkumiseks ärilistel eesmärkidel võõrastele (avalikud pääsupunktid - hotspots)

Raadiovõrgud võivad olla paigaldatud ühendatult või ühendamata teiste võrkudega, millest samuti sõltub olulisel määral ohu suurus ning sellega koos ka rakendamist vajavad turvameetmed. Olenevalt planeeritud kasutusotstarbest ja -keskkonnast võivad rakendamist vajavad turvameetmed olla väga erinevad. Sellega tuleks traadita kohtvõrgu kasutamiseks vajalike turvajuhiste ja reeglite formuleerimisel igal juhul arvestada. Otsus tuleks koos selle vastuvõtmise aluseks olevate põhjendustega dokumenteerida. Traadita võrgu ülesehitamisele peab eelnema põhjalik planeerimine, et saavutada professionaalseks kasutamiseks vajalik stabiilsus, ülekandekvaliteet ja turvalisus (vt M 2.383 Sobiva traadita kohtvõrgu standardi valik ja M 5.140 Traadita kohtvõrgu jaotussüsteemi ehitus).

Turvalise töö tagamiseks vajatakse suuri ressursse

Asutuse IT-alase töö eest vastutavatele isikutele ja infoturbeosakonnale peaks olema selge, et traadita kommunikatsioonisüsteemide, eriti traadita kohtvõrkude korral toimub paljude tehniliste aspektide kiire edasiarendamine ja muutmine. See tähendab IT-alase töö eest vastutavate isikute ja infoturbeosakonna jaoks ühelt poolt seda, et kohtvõrkude turvalises töös hoidmine nõuab rohkem ressursse, ning teiselt poolt seda, et infoturbealaste meetmete efektiivsust tuleb kontrollida ja muutustega kohandada lühemate vaheaegade järel kui teiste süsteemide puhul.

Traadita kohtvõrkude ja nendega ühenduses olevate IT-süsteemide turvaliseks kasutamiseks on vajalik kinni pidada alljärgnevatest põhimõtetest:

- Kasutatava traadita kommunikatsioonisüsteemide tehnoloogia tööpõhimõtted peavad olema täiesti arusaadavad selle funktsioneerimise eest vastutavatele isikutele.
- Kasutatava tehnika turvalisust tuleb regulaarselt hinnata. Samuti tuleb regulaarse kontrolli all hoida kasutatavate IT-süsteemide turvasätteid (nt pääsupunktid, sülearvutid, pihuarvutid).

- Traadita kohtvõrgu kasutamine peab olema reglementeeritud organisatsiooni turvapoliitikas, iga traadita kohtvõrgu kasutamise muudatus tuleb kooskõlastada organisatsiooni infoturbeosakonnaga.
- Selleks, et tagada edastatavate andmete usaldusväärne kaitse, tuleb välja töötada reeglid, mis määravad kindlaks adekvaatsete krüpteerimis- ja autentimismeetodite kasutamise, nende konfiguratsiooni ja võtmehalduse põhimõtted.
- Tuleb defineerida, milliseid traadita kohtvõrgu standardeid, nt IEEE 802.11g peavad kasutatavad seadmed toetama, et tagada üksikute komponentide koosmõju ning et turvamehhanismid tagaksid kogu süsteemi turvalisuse.

Traadita kohtvõrgu komponentide kasutamine

Paljudel lõpptarbijate IT-süsteemidel, näiteks süle- või pihuarvutitel on traadita kohtvõrgu funktsioonid, mis ei ole tehasest tarnimisel enamasti desaktiveeritud.

Tagada tuleb, et organisatsioonis ei toimuks kontrollimatut traadita kohtvõrgu kasutamist, vaid peab olema täpselt reguleeritud, kas neid traadita kohtvõrgu funktsioone tohib kasutada, ja kui, siis millistel raamtingimustel.

Kontrollküsimused:

- Kas traadita kohtvõrgu kasutamine on lubatud?
- Kas traadita kohtvõrgu kasutamiseks on olemas dokumenteeritud strateegia?
- Kas on kindlaks määratud, milliseid traadita kohtvõrgu standardeid kasutuses olevad traadita kohtvõrgu standardid kõige vähem peaksid toetama?

M 2.382 Traadita kohtvõrgu turvajuhendi väljatöötamine

Algatamise eest vastutavad: IT-juht, infoturbeosakond:

Rakendamise eest vastutavad: IT-juht, infoturbeosakond, administraator

Traadita kohtvõrgu komponentide kasutuselevõtuks asutustes ja ettevõtetes tuleb koostada sobivad turvasuunised. Kohtvõrku puudutavad turvasuunised peavad olema vastavuses üleorganisatsioonilise turvakontseptsiooni ja üldkehtivate turvasuunistega. Nende aktuaalsust tuleb regulaarselt kontrollida ning vajadusel uutele oludele vastavalt kohandada. Turvajuhised traadita kohtvõrgu kasutamiseks võib lisada olemasolevasse turvajuhendisse või koostada eraldi traadita kohtvõrgu turvajuhend. Traadita kohtvõrgu turvajuhend peaks muuhulgas sisaldama järgmisi punkte:

- Peaks olema kindlaks määratud, kellel on asutuses õigus traadita kohtvõrku installeerida, konfigureerida ja kasutada. Selleks on vaja kindlaks määrata ka terve rida põhitingimusi, näiteks:
- Missugust informatsiooni tohib edastada traadita kohtvõrgu komponentide kaudu?
- Kus tohib traadita kohtvõrku kasutada ning kuhu tohib paigutada pääsupunkte?
- Milliste teiste sisemiste ja välimiste võrkudega tohib traadita kohtvõrku siduda?
- Kõikidele traadita kohtvõrgu komponentidele tuleb kindlaks määrata turvameetmed ja määrata kindlaks turvaline standardkonfiguratsioon

Turvaintsidentide käsitlus

- Turvaprobleemide kahtluse korral tuleb informeerida turvalisuse eest vastutavat isikut, et ta saaks astuda edasised sammud (vt B 1.8 Turvaintsidentide käsitlus)

Traadita kohtvõrkude turvalisuse alane koolitus

- Traadita kohtvõrgu administraatoreid ja ka kasutajaid tuleb teavitada traadita kohtvõrkudega seonduvatest ohtudest ja vastavatest turvameetmetest või viia läbi vastav koolitus
- Traadita kohtvõrgu turvajuhendis kirjeldatud turvameetmete korrektset järgimist tuleks regulaarselt kontrollida

Klientidele mõeldud traadita kohtvõrgu kasutusjuhend

Et kasutajaid mitte detailidega üle koormata, oleks mõttekas koostada traadita kohtvõrgu kasutajatele eraldi kasutusjuhend. Sellises klientidele mõeldud kasutusjuhendis peaks olema lühidalt kirjeldatud traadita kohtvõrgu kasutamise eripärasid, nagu näiteks:

- Millistesse teistesse sisemistesse ja välimistesse võrkudesse tohib traadita kohtvõrgu klient pöörduda?

- Millistel tingimustel tohivad nad luua ühenduse sisemise või välimise traadita kohtvõrguga?
- Kas ja milliseid avalikke pääsupunkte tohib kasutada?
- *Ad hoc* peab olema välja lülitatud, et keegi teine ei saaks kliendiga otseühendust
- Mida tuleb ette võtta (kahtlustatava) traadita kohtvõrgu kliendi kompromiteerimise korral ja keda tuleb informeerida?

Tähtis on ka selgelt kirjeldada, kuidas tuleks ümber käia kliendipoolsete turvalahendustega. Nende hulka kuuluvad järgmised aspektid:

- Turvalisuse seisukohalt tähtsaid konfiguratsioone ei tohi muuta
- Viirusetõrjetarkvara peab olema pidevalt aktiveeritud
- Olemasolevat personaalset tulemüüri ei tohi välja lülitada (vt M 5.91 Interneti-PC personaalse tulemüüri installeerimine)
- Kõik ühiskasutusse antud kataloogid või teenused peavad olema desaktiveeritud või vähemalt kaitstud heade paroolidega
- Väliste traadita kohtvõrkude kasutamisel tohib kasutada vaid spetsiaalseid piiratud õigustega kasutajakontosid

Lisaks peaks traadita kohtvõrgu klientidele mõeldud kasutusjuhend sisaldama selget keeldu luua loata ühendust pääsupunktidega. Ülejäänud osas peaks juhend sisaldama klassifitseeritud informatsiooni näiteks konfidentsiaalse informatsiooni kohta, sisaldama andmeid selle kohta, milliseid andmeid traadita kohtvõrgu kaudu tohib edastada ja milliseid mitte. Kasutajaid tuleks traadita kohtvõrgust lähtuvatest ohtudest ning traadita kohtvõrgu turvasuuniste sisust ja mõjust informeerida.

Administraatoritele mõeldud traadita kohtvõrgu turvajuhend

Lisaks tuleks luua ka administraatoritele mõeldud traadita kohtvõrgu turvajuhend, mis võib olla aluseks ka administraatorite koolitusele. Selleks peaks olema kindlaks määratud, kes on vastutav erinevate traadita kohtvõrgu administreerimise eest, millised liidesed esinevad töös osalevate administraatorite vahel ning millal ja milline info peab liikuma vastutavate isikute vahel. Tingimata on tavaks, et aktiivkomponentide talitluse eest (jaotussüsteem ja pääsupunktid) on vastutav teine organisatsiooni üksus kui traadita kohtvõrgu klientide teenindamise või identsuse kontrollimise ja volituste haldamise eest. Administraatoritele mõeldud traadita kohtvõrgu turvajuhend peaks lisaks sisaldama traadita kohtvõrgu infrastruktuuri kasutuse kõige olulisemaid aspekte, näiteks järgenevat:

- Turvalise traadita kohtvõrgu konfiguratsiooni kindlaksmääramine ja turvalise standardkonfiguratsiooni defineerimine
- Traadita kohtvõrgu haldussüsteemi kasutamine
- Krüpteerimismeetodite valik ja teostus, kaasa arvatud võtmehaldus
- Regulaarne logifailide analüüs, vähemalt pääsupunktide logifailid
- Traadita kohtvõrgu mõõtmised: pääsupunktide ja klientide konfiguratsiooni ja võrgu leviala tuleks regulaarselt WLAN-testri ja võrgusnifferiga kontrollida. Samaaegselt tuleb otsida ka organisatsioonisiseseid volitamata kliente ja pääsupunkte;

- Asendussüsteemide kasutuselevõtt
- Meetmed traadita kohtvõrgu kompromiteerimise korral

Kui asutuses ei ole traadita kohtvõrke ametlikult paigaldatud, peaks infoturbeosakond vaatamata sellele regulaarselt skänneri abil otsima loata paigaldatud traadita kohtvõrgu komponente. Kõik traadita kohtvõrgu kasutajad, nii kliendid kui ka administraatorid, peaksid oma allkirjaga tõestama, et on lugenud traadita kohtvõrgu turvajuhendit ning et järgivad selles defineeritud juhiseid. Ilma kirjaliku tõenduseta ei tohi keegi traadita kohtvõrku kasutada. Allkirjastatud deklaratsioonid tuleb säilitada selleks sobivas kohas, näiteks isikutoimikus.

Täiendavad kontrollküsimused:

- Kas traadita kohtvõrgu kasutamiseks on olemas uuendatud turvajuhend?
- Kuidas kontrollitakse traadita kohtvõrgu turvajuhendi täitmist?
- Kas traadita kohtvõrgu kliendi käsutuses on üks eksemplar traadita kohtvõrgu turvajuhendist või infoleht, mis annab ülevaate tähtsaimatest turvamehhanismidest?
- Kas IT-alaste turvameetmete koolitustel tutvustatakse ka traadita kohtvõrgu kasutamise turvajuhendit?

M 2.383 Sobiva traadita kohtvõrgu standardi valik

Algatamise eest vastutavad: IT-juht, infoturbeosakond
Rakendamise eest vastutavad: IT-juht, infoturbeosakond, administraator

Traadita kohtvõrgu planeerimise raames tuleb kõigepealt kindlaks teha, kas asutuses on kasutusel süsteemid, mis töötavad 2,4 GHz või 5 GHz sagedusribas. Pärast olemasolevale olukorrale hinnangu andmist on võimalik otsustada, millist traadita kohtvõrgu standardit kasutama hakatakse. Traadita kohtvõrgu standardid IEEE 802.11, IEEE 802.11b ja IEEE 802.11g kasutavad 2,4 GHz sagedust, standardid IEEE 802.11a ja IEEE 802.11h 5 GHz sagedust. Õige sagedusriba valik aitab ära hoida teiste asutuses kasutuses olevate süsteemide põhjustatud traadita kohtvõrgu häireid. Turvamehhanisme kirjeldavad vaid standardid IEEE 802.11 ja IEEE 802.11i. Lisaks tehnilistele näitajatele tuleb ka üksikute traadita kohtvõrgu standardite olemasolevaid turvamehhanisme omavahel võrrelda. Autentimiseks ja krüpteerimiseks tuleks põhimõtteliselt kasutada vaid üldtunnustatud meetodeid.

Tuleb tagada piisava võtmepikkusega tunnustatud krüptoprotseduuride ning räsifunktsioonide kasutamine (vt M 2.164 Sobiva krüptoprotseduuri valimine). Turvamehhanismide WPA või WPA2 rakendamisel soovitatakse kasutada vastastikuse autentimisfunktsiooniga autentimisprotseduure. Sel juhul peab traadita kohtvõrgu klient end autentima pääsupunkti suhtes ja vastupidi. Sel juhul võib autentimiseks kasutada salajast teksti, niinimetatud eeljagatud võtit (Pre Shared Key) või EAP Framework RADIUS serveriga. Kõrgema kaitsevajaduse korral on soovitatav kasutada seadmete ja kasutajate autentimist, et traadita kohtvõrgule võivad juurdepääsu omada ainult asutusele tuntud (ning vastavalt turvajuhendile konfigureeritud) kliendid.

WEP ebaturvaline, WPA/WPA2 turvalisemad

Nii kasutab standard IEEE 802.11 ebaturvaliseks klassifitseeritud staatilise võtmega Wired Equivalent Privacy (WEP) protokolli. WEP kasutamise korral traadita kohtvõrkudes tuleb konfidentsiaalse informatsiooni edastamiseks kasutada lisaturvameetmeid. Tuleb otsustada vähemalt WiFi Alliance poolt arendatud turvamehhanismi Wi-Fi Protected Access (WPA) kasuks. Parema tulemuse traadita kohtvõrgu turvalisuse tagamiseks annab täiendav meede IEEE 802.11i või WPA2 näol. Turvalise andmevahetuse tagamiseks traadita kohtvõrgus defineeritakse muuhulgas ka Pre-Shared Key kasutamine koos ajutiste võtmete tervikluse protokolliga (Temporal Key Integrity TKIP) . IEEE 802.11i ise näeb tulevikule suunatud autentimismeetodina ette Counter Mode koos Cipher Block Chaining Message Authentication Code Protocol (CCMP) , mis lisab Counter Mode usaldusväärsust.

Samuti kasutab CCMP AES krüptoalgoritmi (Advanced Encryption Standard) informatsiooni krüpteerimiseks, vastupidiselt RC4-le WEP-is ja WPAs.

Erinevate standardite hoolikas võrdlus, eelkõige nende turvafunktsioone silmas pidades, on möödapääsmatu ning tuleb alati läbi viia. Alles pärast üksikute standardite põhjalikku hindamist võib järgneda traadita kohtvõrgu standardi valik. Otsustuskriteeriumid tuleb dokumenteerida selliselt, et need oleksid ka hiljem arusaadavad.

Kontrollküsimused:

- Millised protokollid ja standardid valiti traadita kohtvõrgu töölerakenda-

miseks?

- Kas otsustuskriteeriumid on dokumenteeritud?

M 2.384 Sobiva traadita kohtvõrgu krüpteerimisviisi valik

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: IT-juht, infoturbeosakond, administraator

Traadita kohtvõrgu turvalise kasutamise kindlustamiseks tuleb kommunikatsioon raadioliidese kaudu täielikult kindlustada. Ilma piisava krüpteerimiseta tekib oht, et volitamata isikud võivad traadita kohtvõrgu kaudu edastatavatele andmetele ligi pääseda. Lisaks sellele on mitteküllaldaselt kaitstud traadita kohtvõrk ründepunktiks sellega ühenduses olla võivale kohtvõrgule. Tuleb tagada ka andmete terviklus, et oleks võimalik kindlaks teha andmetega manipuleerimise juhud. Tähtis on ka traadita kohtvõrgu komponentide (vastastikune) autentimine.

Standardites IEEE 802.11 ja 802.11i on kirjeldatud erinevaid krüptograafilisi meetodeid, mida võib kasutada traadita kohtvõrgu turvalisuse tagamiseks. Nende hulgast tuleb kasutusala, kaitsevajadust ja asutuse suurust arvestades sobivad välja valida ning rakendada.

WEP-turvaprotokoll (Wired Equivalent Privacy)

WEP-protokoll on vanim ja kõige laialdasemalt levinud traadita kohtvõrgu krüpteerimisstandard, mida kirjeldab standard IEEE 802.11. WEP pakub vaid minimaalset kaitset, takistades juhuslikku pealtkuulamist või sisselogimist. WEPprotokolli peetakse tänapäeval iganenuks ja ebaturvaliseks, kuna on avastatud terve hulk turvaauke. Seega tuleb WEP-protokolli lugeda traadita kohtvõrgu turvalisuse tagamisel ebapiisavaks ning seda ei tohiks enam kasutada. Juhul kui WEP on ainuke krüpteerimismeetod, mida on võimalik kasutada, ning traadita kohtvõrgu komponentide kasutamine peab jätkuma, tuleks WEP siiski aktiveerida. Sel juhul tuleb kasutada maksimaalset võtmepikkust ning võtmeid regulaarselt käsitsi vahetada (vähemalt üks kord päevas). Selline otsus tuleb dokumenteerida ja kõigile traadita kohtvõrgu kasutajatele teatavaks teha. Sellist mitteküllaldaselt turvatud traadita kohtvõrku tohib äärmisel juhul kasutada vaid mittekriitilises valdkonnas, näiteks ainult internetiühenduseks. Sellisel juhul tuleb aga tagada, et ainult WEPprotokolliga turvatud raadiovõrgu kaudu ei edastataks konfidentsiaalseid andmeid ning need ei tohi olla kättesaadavad ka võrgukomponentide kaudu.

WPA, WPA2 ja IEEE 802.11i

IEEE 802.11i on uus traadita kohtvõrkude turvastandard, mis vastab osaliselt Wi-Fi Alliance poolt väljatöötatud Wi-Fi Protected Access 2 (WPA2) standardile. Vastandina WPAle, mis vastab IEEE 802.11i draft 3-le ning mis samuti anti välja Wi-Fi alliansi poolt, kasutavad WPA2 ja IEEE 802.11i AES- (Advanced Encryption Standard) krüptoalgoritmi. WPA ning WEP kasutavad edasi RC4 krüptoalgoritmi. Nii WPA kui ka WPA või IEEE 802.11i pakuvad valikuliselt rakendatava TKIPprotokolli (Temporary Key Integrity Protocol) abil dünaamilise võtmehalduse kaudu lisakaitset. WPA2 ja IEEE 802.11i puhul on andmete tervikluse tagamiseks AESstandardi rakendamismeetodina ja tervikluse tagamiseks lisaks ettenähtud CCMP meetodi kasutamine. Sõltuvalt võimalustest on soovitatav kogu traadita kohtvõrgu ulatuses kasutada WRA2-protokolli koos CCMP-meetodiga (vähemalt WPAd koos TKIPga), kuna neil on tugevamad algoritmid krüpteerimiseks ja tervikluse tagamiseks.

Vähemefektiivsemad meetodid ei ole vastavalt tehnika tasemele aktsepteeritavad.

Kasutajate autentimiseks võib kasutada eelsisestatud võtmeid (Pre Shared Keys – PSK). Neid kasutatakse esmaühenduse loomisel autentimiseks traadita kohtvõrgu komponentide suhtes. Eelsisestatud võtmete puhul tuleb arvestada, et need peavad olema oluliselt pikemad kui tavapärased kuuest kuni kaheksast märgist koosnevad võtmed, kuna sellest sõltub krüpteeringu turvalisus. See meetod on praktiline väiksemate traadita kohtvõrgu paigalduste puhul, suuremate võrkude korral tuleb kasutada EAP-meetodit vastavalt standardile IEEE 802.1X.

Alljärgnev tabel annab hea ülevaate erinevatest krüpteerimismehhanismidest:

	WEP	WPA	802.11i (WPA2)
Krüpteerimisalgoritm	RC4	RC4	AES
Võtmepikkus	40 või 104 bitti	128 bitti (64 bitti autentimisel)	128 bitti
Võti	staatiline	dünaamiline (PSK)	dünaamiline (PMK)
Initsialiseerimis-vektor	24 bitti	48 bitti	48 bitti
Andmete terviklus	CRS-32	MICHAEL	CCMP

TKIP ja CCMP

Ajutise võtmete tervikluse protokoll (TKIP) põhineb allapoole ühilduva lahendusena WEP-protokollil, kuid kõrvaldab selle suurimad nõrkused. TKIP-protokolli jaoks on standardis IEEE 802.11i WEPi mitteküllaldase tervikluskontrolli probleem lahendatud lisameetodi MICHAEL (parandatud tervikluse kontrolliks) kasutamisega. TKIP ja MICHAEL kasutamisse tuleb suhtuda kui ajutisse lahendusse. CCMPi all mõeldakse CTR režiimi (Counter Mode) koos CBC-MAC protokolliga (Cipher Block Chaining Message Authentication Code). Siin ei kasutata AES standardit otse klaarteksti, vaid sümmeetrilisest võtmest moodustatud lugeja krüpteerimiseks.

Tegelik krüpteerimistulemus tekib sel juhul klaarteksti ühe bloki XOR ühendusest AESiga krüpteeritud lugejaga. Lisaks sellele kasutatakse andmete tervikluse tagamiseks ahelrežiimi (Cipher Block Chaining – CBC). Võtmete haldamine ja jaotamine toimub taas eeldatavalt standardi IEEE 802.1X järgi. IEEE 802.11i-s on kasutatav võtmepikkus 128 bitti.

Laiendatav autentimisprotokoll (Extensible Authentication Protocol - EAP)

Autentimisel võib täiendava kaitsemeetodina kasutada laiendatavat autentimisprotokolli (EAP) vastavalt standardile IEEE 802.1X. EAP on detailselt kirjeldatud RFC 3748-s. Kasutaja registreerib end autentimisinstantsi, nt RADIUS-serveril, mis enne seansivõtme genereerimist kontrollib kasutaja pääsuõigust. EAP toetab tervet rida autentimismeetodeid, nii et on võimalik kasutada ja sertifikaate ja kahefaktorilist autentimist. Traadita kohtvõrgus kasutatavateks EAP meetoditeks võivad olla:

- EAP-TLS - EAP-TLS kasutamisel, defineeritud RFC 2716-s, viiakse X.509 sertifikaatide abil läbi mõlemapoolne autentimine. Selleks peab autenditav isik tõestama, et ta tunneb privaatset võtit, mis kuulub avaliku võtme juurde, mida tunneb tema suhtluspartner. Niisiis tuleb kindaks määrata meetodid,

mis on võimelised jaotama ja haldama vastavaid sertifikaate. Avaliku võtme infrastruktuuri (Public Key Infrastructure – PKI) sisseseadmine ja haldamine eeldab hoolikat planeerimist (vt M 2.232 Windows CA-struktuuri plaaneerimine). Võtmevahetus ise toimub TLSiga turvatud tunneli kaudu.

- EAP-TTLS - EAP-TTLS kasutamisel loobutakse vastupidiselt EAP-TLSile sellest, et traadita kohtvõrgu klient peab omama isiklikku sertifikaati. EAPTTLS rakendamisel vajab ainult server kehtivat sertifikaati. TLSiga turvatud tunneli kaudu saab klientide või kasutajate autentimiseks kasutada teisi, vahest ehk vähemefektiivseid meetodeid. EAP-TTLS on samuti nagu EAPTLS võtmeid genereeriv meetod, st sideseansi puhul genereeritakse iga kord uus seansivõti, mida kasutatakse tunneli turvamiseks TLSi abil.
- EAP-PEAP - EAP-PEAP on võtmeid genereeriv meetod ning nõuab sarnaselt EAP-TTLSile vaid autentimisserveril kehtivat X.509 sertifikaati. Vastandina EAP-TTLSile on kliendite autentimiseks turvatud tunnelis võimalik kasutada vaid teisi EAP meetodid, nagu näiteks EAP-MSCHAPv2 või EAPTLS.

Teisi EAP meetodeid on kirjeldatud standardis IEEE 802.1X.

WPA2 koos EAP-ga

Suuremate installatsioonide korral on üldiselt mõttekas rakendada kasutaja autentimiseks EAP-protokolli vastavalt standardile IEEE 802.1X. Uuemad traadita kohtvõrgu komponendid võimaldavad kasutada juba standardeid IEEE 802.11i ja sellega ka WPA2 turvaprotokolli. Uute traadita kohtvõrgu komponentide soetamisel tuleb eelnevalt kontrollida, kas need võimaldavad kasutada vastavaid EAP-meetodeid.

Võtmehaldus

Sideseansside või autentimise kaitseks kasutatavaid krüptovõtmeid tuleb regulaarselt vahetada (vt M 2.388 Asjakohane traadita kohtvõrgu võtmehaldus). Kõikide traadita kohtvõrgu komponentide puhul tuleb jälgida, et ühenduse loomisel teiste komponentidega ei aktsepteeriks need väiksema kaitsemõjuga krüpteerimismeetodeid, kui on välja valitud. Selliste komponentidega ei tohi luua ühendust.

Kontrollküsimused:

- Kas on välja valitud sobiv krüpteerimismeetod? Kas otsuse vastuvõtmine on dokumenteeritud?
- Kas kõik traadita kohtvõrgu komponendid toetavad valitud traadita kohtvõrgu standardit, nt IEEE 802.11i, et hoida ära ühildamatusest tingitud probleeme.

M 2.385 Sobivate traadita kohtvõrgu komponentide valik

Algatamise eest vastutavad: IT-juht, infoturbeosakond:
Rakendamise eest vastutavad: IT-juht, infoturbeosakond, administraator

Traadita kohtvõrgu seadmete väljavalimisel tuleb kõigepealt kindlaks teha, kas need vastavad traadita kohtvõrgu turvastrateegiale. Traadita kohtvõrgu komponente on olemas erinevates variantides ning need kuuluvad erinevatesse seadmeklassidesse. Komponentide erinevus ei seisne mitte ainult nende jõudluses, vaid ka turvamehhanismides ning kasutusmugavuses. Pealegi esitavad need kasutuskeskkonnas erinevaid tingimusi riist- ja tarkvarakomponentidele. Paljude erinevate traadita kohtvõrgu komponentide kasutamisel on arusaadav, et tekivad ühilduvusprobleemid. Olulised kriteeriumid traadita kohtvõrgu komponentide valimisel on niisiis turvalisus ja kokkusobivus.

Nõuete nimekiri

Kui asutuses võeti vastu otsus traadita kohtvõrgu paigaldamiseks, tuleb koostada nõuete nimekiri, millele toetudes saab hinnata turul pakutavaid tooteid. Hindamise alusel tuleks seejärel soetatavad tooted välja valida. Praktika näitab, et erinevate kasutusnõuete tõttu võib olla otstarbekas soetamiseks välja valida mitu seadmetüüpi. Seadmete mitmekesisust tuleks aga tugisüsteemide kasutamise lihtsustamiseks piirata. Üks tähtis kriteerium traadita kohtvõrgu komponentide soetamisel on ühilduvus juba olemasolevate seadmetega. Seadmete soetamisel tuleks tähelepanu pöörata ka andmete läbilaskevõimele ja ulatuskaugusele. Väliste antennidega on traadita kohtvõrgu komponentide ulatuskaugust võimalik suurendada. Seejuures tuleb tagada, et suurema ulatuskauguse tõttu ei ulatuks traadita kohtvõrk kohtadesse, kus seda ei ole vaja või ei tohi kasutata.

Pääsupunktide kriteeriumid

Pääsupunktide soetamisel tuleks muuhulgas kontrollida alljärgnevat:

- Mitu kanalit on kasutatavad?
- Kas SSID on muudetav?
- Kas SSID-beacon on desaktiveeritav?
- Milliste krüptograafiliste meetodeid võimaldab seade võimaldab seade kasutada (WEP, WPA, WPA2 ja teised)?
- Kas autentimisel saab kasutada nii avatud süsteemi (Open System) kui ka eelsisestatud võtmete meetodit (Shared Key Modus)?
- Millised EAP-meetodid vastavalt standardile IEEE 802.1X on kasutatavad?
- Kas seadme administreerimine on võimalik turvaliste kommunikatsioonikanalite kaudu, nt SSH või SSL, ning kas on võimalik desaktiveerida ebaturvalised protokollid, nt HTTP või Telnet?
- Kas on võimalik IP või MAC aadressipõhine filtreerimine?
- Kas on võimalik konfigureerida pääsuloendeid (ACL) ligipääsuks traadita
- Kas on võimalik konfigureerida pääsuloendeid (ACL) ligipääsuks traadita kohtvõrgu ja üle kohtvõrgu liideste ning ka konfiguratsiooniliidestele?
- Kas paketifilter on integreeritud?
- Kas ja millised muud pääsukontrolli mehhanismid on kasutatavad (filtreerimine erinevate kriteeriumide, nt portide, rakenduste, internetiaadresside (URL) jne alusel?
- Kas seade toetab tunnelprotokolle nagu PPTP või IPsec?

Tingimata tuleks testida, kas erinevate traadita kohtvõrgu komponentidel juurutatud samanimelised krüptograafilised meetodid ka korrektselt koos töötavad.

Pääsupunktide korrektne konfiguratsioon on üks oluline turvaaspekt. Mõnede pääsupunktide korral on võimalik konfiguratsioon otse traadita kohtvõrgu kaudu, mida tootjad reklaamivad kui mugavust. Kuna sellega kaasnevad aga ka turvaprobleemid, tuleks sellest loobuda. Kui aga selline funktsionaalsus on olemas, peaks see olema desaktiveeritav (ning kasutamisel põhimõtteliselt desaktiveeritud). Paljud pääsupunktid võimaldavad ühendada need seeriaviisilise või USB-liidese abil halduskonsooliga, muutes konfigureerimise mugavaks. Neid on võimalik administreerida HTTP või Telnet protokollide abil intraneti või Interneti kaudu. Selleks on vajalik tagada turvaline kaugpöördus, näiteks kommunikatsiooni turvamine turvasoklite kihi (SSL) või turvakesta (SSH) kaudu.

Internetipõhistesse kaugpöördustesse tuleks üldiselt suhtuda kriitiliselt. Administratiivne juurdepääs traadita kohtvõrgu komponentidele peaks olema võimalik vaid volitatud isikutele. Seetõttu tuleks uurida, kuidas see on kaitstud. Kui see toimub paroolide kaudu, peavad need olema valitud küllaltki keerukad (vt M 2.11 Paroolide kasutamise reeglid). Administratiivseks juurdepääsuks on parem kasutada efektiivseid autentimismeetodeid (vt M 4.133z Sobivate autentimismehhanismide valimine). Turvareeglite rakendamine pääsupunktide kaitseks on enamasti suuri ressursse nõudev tegevus. Selle hulka kuulub lisaks võtmete haldusele eelkõige erinevate parameetrite ja optsioonide konfigureerimine. Seetõttu on mõnedele pääsupunktidele loodud võimalused nende haldamiseks asutuses tsentraalse serveri kaudu. Need on siiamaani kahjuks veel firmapõhised lahendused, millega saab hallata vaid ühe tootja seadmeid. Kuna see võib seoses võrguühenduselementidega eeldada suuri ressursse, kuni võrgu haldaja on leidnud korrektse konfiguratsiooni, peaks olema võimalik need salvestada.

Online -abi ja traadita kohtvõrgu komponentide dokumentatsioon peaksid olema keeleliselt nii formuleeritud, et tehnilised kirjeldused oleksid tulevastele kasutajatele või administraatoritele arusaadavad.

Koostöövõime olemasoleva infrastruktuuriga

Soetamise käigus tuleks kontrollida traadita kohtvõrgu kõigi komponentide koostöövõimet olemasoleva infrastruktuuriga. Selle hulka kuulub näiteks:

- Traadita kohtvõrgus kasutatavat autentimismeetodit peavad toetama nii kliendid, pääsupunktid kui ka autentimisserver.
- Juhul kui traadita kohtvõrgus kasutatakse autentimist vastavalt standardile IEEE 802.1X, peavad pääsupunktid võimaldama EAP autentimist ja töötlema korrektselt IEEE 802.1X sisest informatsiooni.
- Tuleb kontrollida, kas autentimisserverit kasutades on võimalik loobuda eraldi andmebaasist kasutajate autentimiseks ja selle asemel teostada turvalisi autentimispäringuid tsentraalsesse kasutajate andmebaasi.

Suurema traadita kohtvõrgu installatsiooni soetamisel tuleb enne lõplikku soetamist viia läbi vastavad testimised. Kontrollkataloogi abil on võimalik hinnata tehniliste nõuete täitmist. Kontrollimise läbiviimine lihtsustab hilisemat traadita kohtvõrgu installeerimist ja vastuvõtmist.

Kontrollküsimused:

- Kas traadita kohtvõrgu komponentide valikul on küllaldaselt arvestatud turvaaspektidega?
- Kas kontrolliti ühilduvust juba olemasolevate traadita kohtvõrgu komponentidega?

M 2.386z Traadita kohtvõrgu migratsioonietappide hoolikas planeerimine

Algatamise eest vastutavad: IT-juht, infoturbeosakond
Elluviimise eest vastutavad: administraator

Traadita kohtvõrgu kiiresti muutuva tehnoloogia tõttu on praktikas vaid väga harva võimalik vältida olemasoleva installatsiooni edaspidist migratsiooni uute protokollide, tehnikate või toodete näol. Seejuures eristatakse reeglina kahte erinevat migratsioonitüüpi:

- Ülekandetehnoloogia migratsioon (nt üleminek IEEE 802.11g tehnoloogialt IEEE 802.11h tehnoloogiale)
- Traadita kohtvõrgu turvamehhanismide migratsioon (nt üleminek WEP meetodilt WPA-PSK meetodile või IEEE 802.11i koos IEEE 802.1X kasutamisega

Esimesel juhul tuleb läbida kogu traadita kohtvõrgu planeerimisprotsess, alates riskide hindamisest kuni sobivate turvamehhanismide valimiseni. Teisel juhul tuleb teatud juhtudel ajutiselt kasutada paralleelselt erinevaid turvasüsteeme ning viia läbi pääsupunktide, jaotussüsteemide (DS) ja traadita kohtvõrgu ülekandepunkti laiendatud konfigureerimine. Traadita kohtvõrgu komponentide või valdkondade kasutamist tuleb, kui need ei ole veel läbinud migratsioonifaasi, vajadusel piirata vastavate tehniliste ja organisatoorsete regulatsioonidega. Nii võib näiteks keelata komponentidelt, mis ei ole veel migratsiooni läbinud, juurdepääsu konfidentsiaalsetele andmetele või kindlustada veel migratsioonifaasi mitte läbinud traadita kohtvõrgu valdkonna eraldamine täiendava demilitariseeritud tsooni (DMZ) abil ülejäänud traadita kohtvõrgust ja LAN-võrgust. Võimaliku turvamehhanismide samaaegse kasutuse korral, näiteks WPA-PSK või WPA2-PSK ja WEP, tuleb täita alljärgnevaid juhtnööre:

- Turvamehhanismide samaaegne kasutusaeg peab olema nii lühike kui võimalik
- Juhul kui kasutatakse üheaegselt WEP meetodit ja eelsisestatud võtmeid (*Pre Shared Keys*), tuleb rangelt jälgida, et võtmeid vahetataks sageli (vähemalt kord päevas) ja kasutataks vaid keerukaid paroole (vt M 2.388 Asjakohane traadita kohtvõrgu võtmehaldus).
- Pääsupunktid peavad võimaldama mõlema meetodi samaaegset kasutamist migratsioonifaasis. Pääsupunktid, mis toetavad maksimaalselt WEP meetodit, tuleb võimalikult kiiresti asendada ja traadita kohtvõrgust eemaldada.
- Traadita kohtvõrgu kliendid, mis võimaldavad kasutada vaid WEP meetodit, (nt printer või pihuarvuti), tuleks sisse lülitada vaid juhul, kui neid on vaja. Need tuleks kiiremas korras asendada klientidega, mis võimaldavad kasutada WPA2.

- Traadita kohtvõrgu komponentide, nt printeri, konfigureerimine ei tohiks võimalusel toimuda raadiokanali, vaid seadme konsoolipordi kaudu.

Igal juhul tuleb üksikud migratsioonifaasid hoolikalt planeerida. Seejuures tuleks migratsiooni kasutada ka täiustunud traadita kohtvõrgu infrastruktuuri kindlustamiseks, millele peab järgnema traadita kohtvõrgu administraatorite ja kasutajate koolitus vastavalt uuele situatsioonile. Kui uute autentimismehhanismide juurutamise tõttu muutub traadita kohtvõrgu kasutajate registreerimisprotseduur, tuleb läbi viia ka kasutajate koolitus. Lisaks tuleks viia traadita kohtvõrgu kasutusjuhend vastavusse uute oludega.

Täiendavad kontrollküsimused:

- Kas on olemas kahe traadita kohtvõrgu tehnoloogia migratsiooniplaan? Kas selle kestvus on kindlaks määratud?
- Kas on tagatud, et vähem kaitstud komponentidel ei ole enam juurdepääsu konfidentsiaalsetele andmetele?

M 2.387z Kolmandate osapoolte kasutamine traadita kohtvõrgu paigaldamisel, konfigureerimisel ja nõustamisel

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: IT-juht, infoturbeosakond, administraator

Kui traadita kohtvõrgu installeerimine, konfigureerimine või haldamine tuleb tellida väljast, tuleb lisaks B 1.11 Väljasttellimine (Outsourcing) soovitatule pöörata tähelepanu ka alljärgnevalt kirjeldatud asjaoludele:

- Pidevalt tuleb kontrollida, kas traadita kohtvõrguga seotud installeerimistöid on võimalik teostada oma ressurssidega või kas seda on võimelised tegema oma asutuse töötajad. Selleks on vaja läbi viia teostatavus- ja tasuvusanalüüs.
- Turvastrateegia ja -suunised peaksid looma asutuse oma töötajad, mitte kolmandad isikud. Sellega hoitakse ära olukord, et asutuses ei tegele enam keegi põhjalikult traadita kohtvõrgu turvaaspektidega, mille tulemusena võivad vajalikud turvaaspektid ununeda. Nõustamine ja abi kolmandate isikute poolt on vajalik juhul, kui selleks puuduvad sisemised ressursid.
- Traadita kohtvõrgu installeerimise väljasttellimisel tuleb koostada detailne nõuete nimekiri. Selles on vaja täpselt defineerida minimaalsed nõuded kõigile traadita kohtvõrgu komponentidele ja kõigile traadita kohtvõrguga seotud võrguosadele, jne. Nõuete nimekiri peaks olema lepinguliseks aluseks väljasttellimisel ning hiljem kontrollimise aluseks töö vastuvõtmisel.
- Töö teostajale tuleb tutvustada traadita kohtvõrgu töölerakendamise turvastrateegiat ja turvasuuniseid. Tööde teostajalt tuleb lepingu tingimustele vastavalt nõuda nende täitmist ja elluviimist. Lepingus fikseeritud tööde teostamist tuleb regulaarselt kontrollida, et varakult ennetada potentsiaalseid probleeme. Turvastrateegia ja -suunised peaksid moodustama nõuete nimekirja kindla koostisosa.
- Töö teostaja peaks omama laialdasi ja aastatepikkusi kogemusi traadita kohtvõrkude installeerimise ja nende turvameetmete alal. Töö teostaja peab esitama vastavad tõendid ning neid tuleb vähemalt pisteliselt kontrollida.
- Töö teostaja peab olema lepinguliselt kohustatud mitte edastama informatsiooni traadita kohtvõrgu konfiguratsiooni ja komponentide, samuti parooli-de, võtmete ja pääsutunnuste ja -mehhanismide kohta volitamata isikutele. Töö teostaja peaks olema kohustatud mitte salvestama vahemällu ka töö teostamise käigus ülejäänud võrgust saadud informatsiooni ja andmeid või neid volitamata isikutele edasi andma.
- Enne traadita kohtvõrgu installeerimist peab töö teostaja läbi viima vastavad testid. Seejuures tuleb kõiki planeeritud turvamehhanisme põhjalikult testida. Selles faasis on eriti ohustatud asutusesisene arvutivõrk (LAN), kui see on traadita kohtvõrguga ühendatud ning seetõttu tuleks sellele luua vastav kaitse.
- Traadita kohtvõrgu installeerimisel peaks tööde teostaja jälgima, et ta ei jätaks võrku tagauksi. Töö teostaja peab kõik seadistused ja konfiguratsiooniandmed täpselt dokumenteerima ning tööde lõppedes andma tellijale üle täieliku dokumentatsiooni.
- Pärast installeerimistööde lõppemist peab toimuma võrgu vastuvõtmine vastavalt kokkulepitud tööde ja teenuste nimekirjale. Lisaks võivad nõuete nimekirjas toodud pärast töö üleandmist koostatud dokumendid olla kontrollimise

aluseks, kuna selles võivad olla määratletud ka näiteks vastuvõtutingimused.

- Töö vastuvõtmine peaks toimuma sõltumatute ekspertide kaasabil, et oleks võimalik lasta ka tehnilised üksikasjad üle kontrollida.
- Juhul kui on soetatud juhtmeta ründetuvastussüsteem (IDS), tuleb vastavad varem defineeritud juhtumid ka läbi mängida. Sel juhul on soovitatav viia läbi traadita kohtvõrgu proovikasutamine. Seejuures tuleks ka kontrollida, kas ka traadita kohtvõrgu sensorid hõlmavad kogu kontrollitavat ala. Lisaks sellele tuleks simuleerida erinevaid avariiolukordi.
- Vastuvõtmise käigus tuleb dokumentatsiooni erilise hoolikusega kontrollida selle täiuslikkuse ja võimalike ebakõlade suhtes.
- Kui väljastpoolt tellitud töö teostaja hakkab traadita kohtvõrku ka pärast selle installeerimist hooldama, peab ta olema lepinguliselt kohustatud seejuures omandatud informatsiooni, nagu näiteks paroole, konfidentsiaalsed andmeid, konfiguratsiooniandmeid jne mitte edasi andma volitamata isikutele. Samuti tuleks koos tööde teostajaga koostada hädaolukorraks valmisoleku plaan. Selles peaks olema täpselt defineeritud kõigi võimalike traadita kohtvõrgu kasutamisel tekkivate probleemide raskusaste, reageerimisaeg, vastavad tööetapid ning avariist teavitatavad isikud

Täiendavad kontrollküsimused:

- Kas töö teostajale on tutvustatud traadita kohtvõrgu töölerakendamise turvastrateegiat ja turvasuuniseid?
- Kas koos tööde teostajaga on koostatud hädaolukorraks valmisoleku plaan traadita kohtvõrgu töös esinevate võimalike probleemide kõrvaldamiseks?

M 2.388 Asjakohane traadita kohtvõrgu võtmehaldus

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Elluviimise eest vastutavad: administraator

Krüptograafiliste turvamehhanismide kasutamise eelduseks on sobilike võtmete konfidentsiaalne, terviklik ja autentne loomine, jagamine ja installeerimine (vt M 2.46 Krüpteerimise õige korraldus). WEP või WPA-PSK kasutamisel sõltub traadita kohtvõrgu turvalisus olulisel määral kasutatavate traadita kohtvõrgu võtmete sobilikust valikust ja saladuses hoidmisest. Seepärast tuleb võtmete haldamiseks valida õige meetod, mis sobib kokku olemasolevate krüptomehhanismidega. Seejuures tuleb eelkõige vahet teha staatilise (manuaalse) ja dünaamilise võtmehalduse vahel.

WEP

WEP kasutab ainult ühte staatilist võtit, mis tähendab, et kogu traadita kohtvõrgu kõikides komponentides kogu võrgu ulatuses peab olema sisestatud sama WEP-võti. Peale selle ei näe WEP ette dünaamilist võtmehaldust, mistõttu tuleb võtmeid hallata käsitsi. Kuna WEP-võtmed võivad lühikese aja jooksul kaotada oma usaldusväärsuse, ei tohiks WEP-i enam kasutada. Kui see peaks mingil põhjusel siiski kasutust leidma, tuleb võtmeid regulaarselt vahetada (vähemalt kord päevas).

WPA/ WPA2 koos TKIP või CCMPga

WPA kasutab TKIP protokolli, mis võimaldab kasutada dünaamilisi krüptograafilisi võtmeid erinevalt WEPist, mis võimaldab kasutada vaid staatilisi võtmeid. Lisaks defineerib IEEE 802.11i tervikluse kontrolliks ja edastatavate andmete krüpteerimiseks krüpteerimimeetodina CCMPd. TKIP ja CCMP on sümmeetrilised meetodid, mis tähendab, et kõik kommunikatsioonipartnerid peavad omama ühisvõtit. Seda võtit nimetatakse *Pairwise Master Key* (PMK). *Pairwise Master Key* (PMK) jõudmine süsteemis osalevatele traadita kohtvõrgu komponentidele on võimalik kahel erineval moel:

- Staatilised võtmed: PMKd on pääsupunktidel ja klientidel võimalik konfigureerida käsitsi (analoogselt WEP-ile) staatilise võtmena, mille nimeks on *Pre Shared Key* (PSK). Enamasti on võimalik ühiselt kasutatavat salavõtit kindlaks määrata ka paroolide abil. Nende paroolide ümberarvutamine PMK-ks toimub räsifunktsioonide kaudu. Kui selline PSK on liiga lihtne (mõeldud on võtme pikkust ja märkide juhuslikkust), on see vastuvõtlik niinimetatud sõnaraamatu rünnakutele (*dictionary attack*). Seetõttu peaksid need paroolid olema keerulised ja vähemalt 20-kohalised. Alates võrgu teatud suurusest on võtmete käsitsi uuendamine seotud suurte probleemidega.PSK kasutamine koos WPA või WPA2-ga on võimalik. Kui kasutatakse WPA-PSK-d või WPA2-PSK-d, on võtmete vahetus kommunikatsiooni kaitseks või autentimiseks soovitav iga kolme kuni kuue kuu tagant.
- - Dünaamilised võtmed: Suuremat turvalisust pakub dünaamiline võtmehaldus- ja –jaotamismehhanism, mille käigus toimub regulaarne ja eriti pärast traadita kohtvõrgu kliendi edukat autentimist pääsupunktis uue võtme (PMK) loomine. Siin kasutab IEEE 802.11i võtmehalduseks ja –jaotamiseks teist standardit, nimelt standardit IEEE 802.1X. Nimetatud

standard on loodud pordil põhinevaks võrgupääsukontrolliks traadiga võrkudes. IEEE 802.11 1X põhimõte seisneb selles, et võrgupordi sisselülitamine toimub alles siis, kui kasutaja on end võrgu suhtes õnnestunult autentinud. Autentimine toimub niisiis teises kihis. Et see üldse funktsioneeriks, spetsifitseerib IEEE 802.1X kliendi, võrguelemendi ja autentimissüsteemi vahele liidese loomise. Nimetatud liides põhineb EAP-protokollil (*Extensible Authentication Protocol*) ning selle protokolli kohandamisel ülekandmiseks teisele kihile LAN-is (EAP-na LAN-i kaudu, nimetatud EAPOL). Käsikäes sellega toimub võtmehalduse- ja -kaitse funktsiooni kindlaksmääramine.

Kõikide traadita kohtvõrgu komponentide võtmeinfot tuleb regulaarselt, vähemalt kord kvartalis uuendada. Suuremate installatsioonide puhul peaks töömahu vähendamiseks traadita kohtvõrgu tsentraalne haldussüsteem sisaldama selleks sobivat funktsiooni. Kõikide traadita kohtvõrgu komponentide võtmete vahetamist tuleb hoolikalt testida juba planeerimisfaasis, et võimalikud probleemid varakult avastada.

Täiendavad kontrollküsimused:

- Kas kõikide traadita kohtvõrgu komponentide võtmete vahetus on testitud?
- Kas võtmete vahetus on ajaliselt planeeritud?

M 2.389z Avalike pääsupunktide turvaline kasutus

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Elluviimise eest vastutavad: kasutajad

Avalike pääsupunktide näol on tegemist ruumiliselt piiratud raadiovõrguga, mis võib piirduda ühe ruumi, halli või tootmisruumiga. Enamasti on avalikud pääsupunktid paigaldatud kasutamiseks võõrastele. Nende põhieesmärgiks on pakkuda traadita internetiühendust. Sellised avalikud pääsupunktid paiknevad tavaliselt hotellides, lennujaamades, messihallides, raudteejaamades ja konverentsikeskustes. Avalikke pääsupunkte tuleb alati vaadelda kui ebaturvalisi pääsupunkte, esiteks selle tõttu, et nende turvalisus ei ole väljastpoolt kergesti määratav, ning teiseks seetõttu, et enamus neist pakuvad teenuseid Shared Networks kujul. Seetõttu võib üldjuhul igalt lõppseadmelt olla võimalik pääseda ligi kõikidele teistele lõppseadmetele. Kuna avalike pääsupunktide kasutamisest tulenevaid ohte ei ole üldjuhul võimalik täpselt hinnata, tuleb nende kasutamine traadita kohtvõrgu turvasuunistega täielikult keelata. Sel juhul tuleb aga rakendada ka tehnilisi meetmeid, et traadita kohtvõrgu klient ei omaks juurdepääsu sellisele avalikule pääsupunktile. Avalike pääsupunktide operaatoritel on võimalik rakendada mitmesuguseid meetmeid nende poolt pakutavate raadioliinide ja teiste teenuste turvalisuse tagamiseks (vt M 4.293 Avalike pääsupunktide turvaline käitamine), kuid kasutajatega koostööd tegemata ei ole see saavutatav. Siia alla kuuluvad muuhulgas järgmised meetmed:

- Avaliku pääsupunkti turvalisuse ja operaatori usaldusväärsuse hindamiseks peaksid kasutajad uurima, milliseid turvameetmeid on avalike pääsupunktide kaitsmiseks kasutatud.
- Enne kasutamist tuleb tutvuda hinnakirjaga ja arveldamise meetoditega. Kasutaja vaatevinklist on oluline teada, milliseid isikuandmeid tuleb edastada ning kuidas nendega ümber käiakse. Lisaks sellele peaksid kasutajad jälgima, et avalikus pääsupunktis ei oleks võimalik salvestada või kuritarvitada nende autentimisandmeid. Autentimine peaks põhimõtteliselt toimuma krüpteeritult, s.t. autentimiseks tuleb kasutada pretensioni ja vastusega protokolli krüpteeritud kanali kaudu (Challenge-Response protokollid).
- Iga avaliku pääsupunkti kasutaja peaks teadma oma pääsupunkti turvalisusele esitatavaid nõudeid ning nende põhjal otsustama, kas ja/või millistel tingimistel on tema jaoks pääsupunkti kasutamine aktsepteeritav.

Krüpteerimise kasutamine

- Hiljemalt siis, kui on vaja üle kanda finantstegevust puudutavaid andmeid, isikuandmeid või teisi konfidentsiaalseid andmeid, näiteks krediitkaardinumbreidd, PIN-koode, paroole või e-maile, tuleb tagada, et kõik kliendi turvameetmed, eelkõige krüpteerimine, oleks aktiveeritud. Näitena võiks tuua e-mailide turvalise edastamise HTTPS-veebiliidese või selleks ettenähtud turvalise internetiprotokolli (Secure POP, IMAPS, SMTP) kaudu.
- Kui operaator tagab raadiokanali krüpteerimise, võiks põhimõtteliselt loobuda krüpteerimisest rakenduste tasemel. Lisameetmena on krüpteerimist aga siiski soovitatav kasutada, kuna see on enda kontrolli all. Mitte mingil juhul ei tohi võõrastes võrkudes edastada krüpteerimata paroole.

- Organisatsioonisisese võrguga ühendusse astumiseks tuleks traadita kohtvõrgu kliendil põhimõtteliselt rajada krüpteeritud ühendus asutuse usaldusväärse avaliku pääsupunkti kaudu.
- Kui viibitakse avaliku pääsupunkti levialas, ei soovitata seda aga kasutada, traadita kohtvõrgu liides tuleks välja lülitada, et vältida tahtmatut sisselogimist.

Kas sertifikaat on korrektne?

- Kui avaliku pääsupunkti operaator pakub autentimiseks sertifikaate, peaksid kasutajad nende korrektsust kontrollima. Kuigi see on tülikas, tuleks kontrollida selliseid andmeid nagu fingerprint , kehtivusaeg, omanik, sertifikaadi väljastaja õigsus.

Klientide kaitse

- Kõikidel mobiilsetel klientidel, mille kaudu on võimalik erinevatesse traadita kohtvõrkudesse sisse logida, tuleb kasutada ka teisi lokaalseid turvameetmeid, näiteks pääsuõiguse kontrolli, kasutajate autentimist, viirusetõrjet, personaalset tulemüüri, kitsendustega pääsuõiguste andmist failidele ja ressurssidele operatsioonisüsteemi tasandil, lokaalset krüpteerimist jne. Ülejäänud traadita kohtvõrgu kliendi turvameetmed on kirjeldatud M 4.297 Traadita kohtvõrgu komponentide turvaline kasutamine .
- Avalike pääsupunktide kasutamise jaoks on soovitatav luua lisaks turvalise põhikonfiguratsiooniga ja piiratud õigustega spetsiaalsed kasutajakontod. Mitte mingil juhul ei tohi administraatoriõigustega kasutaja oma kliendilt logida välistesse võrkudesse.

Täiendav kontrollküsimus:

- Kas kasutajatele tutvustatakse eeskirju ja turvameetmeid, mida tuleb järgida avalike pääsupunktide kasutamisel.

M 2.390 Traadita kohtvõrgu komponentide kasutusest kõrvaldamine

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Elluviimise eest vastutavad: administraator

Traadita kohtvõrgu komponentide kasutuselt kõrvaldamisel tuleb kogu konfidentsiaalne informatsioon kustutada. Kindlasti tuleb eemaldada või kehtetuks muuta kogu autentimisinformatsioon juurdepääsuks traadita kohtvõrgule ja teistele kättesaadavatele ressurssidele, mis on salvestatud turvainfrastruktuuris ja teistes süsteemides. See tähendab, et näiteks krüptograafilised võtmed tuleb kindlasti kustutada ja digitaalsete signatuuride sertifikaadid tühistada.

Traadita kohtvõrgu klientide kasutuselt kõrvaldamine

Traadita kohtvõrgu klientidena võib kasutust leida terve hulk erinevaid seadmeid. Nende hulka kuuluvad muuhulgas:

- Sülearvutid
- Pihuarvutid, nutitelefonid ja muud traadita kohtvõrgus kasutatavad seadmed
- Traadita kohtvõrgus kasutatavad telefonid, printerid, kaamerad

Nende lõppseadmete jaoks on traadita kohtvõrgu ühenduse funktsioon tavaliselt üks mitmesugustest erinevatest funktsioonidest. Selliste lõppseadmete kasutuselt kõrvaldamise korral tuleb jälgida, kas need sisaldavad turvakriitilist informatsiooni, mis tuleb kustutada, teisele seadmele üle kanda või arhiveerida, näiteks:

- Lõppseadme kasutajainfo
- Sertifikaadid või nende juurde kuuluvad privaatsed võtmed (kasutajale või seadmele)
- Traadita kohtvõrgu paroolid
- Autentimismeetodite võtmed, näiteks WPA-PSK-võtmed
- PIM-andmed, niisiis kontaktinformatsioon, kalendrikirjed, jne

Olenevalt seadme liigist ja salvestuste sisust tuleb tundliku informatsiooni hävitamiseks, kustutamiseks ja taaskasutamiseks kasutada sobilikke meetodeid. Näiteks sertifikaadid tuleb tühistamiseks kanda vastavasse sertifikaaditühistusnimistusse (CRL). Kui traadita kohtvõrgu klient varastatakse, tuleb järgida kogu eelnevalt loetletud informatsiooni ning tuleb hoolitseda selle eest, et seadmesse salvestatud informatsiooni ei saaks enam kasutada juurdepääsuks vastava asutuse traadita kohtvõrgule.

Pääsupunktide kasutuselt kõrvaldamine

Pääsupunktide tööst kõrvaldamisel tuleb põhimõtteliselt jälgida samu põhimõtteid nagu traadita kohtvõrgu klientide puhul. Vähemalt alljärgnevalt nimetatud turvakriitiline informatsioon tuleb kustutada, üle kanda või arhiveerida:

- WPA või WPA2 eelsisestatud võtmed (*Pre Shared Keys*); RADIUS-võtmed (RADIUS *Shared Secrets*)

- IPSec-võtmed (PSK-d või sertifikaadi privaatvõtmed
- Kasutajaandmed (eriti integreeritud traadita kohtvõrgu kasutajahalduse puhul)
- Konfiguratsiooni informatsioon, näiteks RADIUS-serverite IP-aadressid ja nimed, pääsupunkti enda nimi, IP-aadress, mestiident (SSID)

Olenevalt seadme liigist ja salvestuste sisust tuleb tundliku informatsiooni hävitamiseks, kustutamiseks ja taaskasutamiseks kasutada sobilikke meetodeid. Vastavad meetodid tuleb õigeaegselt välja valida ja testida. Tihti sisaldavad pääsupunktid veel teisigi andmeid (näiteks konfiguratsiooniandmed), mis on salvestatud säilmällu või on väljastpoolt pealkirjastatud (näiteks arvuti nimi, SSID, IP-aadress ja muu tehniline informatsioon). Nimetatud informatsioon tuleks võimaluse korral enne seadme edasiandmist eemaldada, sest ründaja saab ka sellisest infost vihjeid võimalikuks ründeks. Selleks et ükski tegevus ei ununeks, on ülaltoodud informatsiooni alusel soovitatav koostada nimekiri tegevustest, mis viiakse läbi süsteemi kasutuselt kõrvaldamiseks.

Täiendav kontrollküsimus:

- Kas on kindlaks määratud sobilikud meetodid traadita kohtvõrgu turvakriitilise informatsiooni hävitamiseks, kustutamiseks ja taaskasutamiseks?

M 2.391 Tuleohutuse eest vastutava isiku varajane informeerimine

Algatamise eest vastutavad: tehnikaosakonna juhataja, tuleohutuse eest vastutav töötaja

Elluviimise eest vastutavad: tuleohutuse eest vastutav töötaja, tehnikaosakond

Kõikide toru- ja kaablitrasside ehitustööde korral, mis on mingil moel seotud seinte läbiviikudega või liikumiseks vajalike koridoride ja avariiväljapääsudega, tuleb informeerida tuleohutuse eest vastutavat isikut. Tuleohutuse eest vastutava isiku informeerimine peab toimuma aegsasti enne tööde alustamist, et tuleohutuse eest vastutaval isikul oleks piisavalt aega arvestada kõikide tuleohutust ennetavate aspektidega kavandavate tööde planeerimis- ja realiseerimisfaasis. Tuleohutuse eest vastutavale isikule tuleb ka tööde teostamise faasis anda õigeaegse informeerimise kaudu võimalus kontrollida tööde teostamise vastavust eeskirjadele enne ligipääsu sulgemist , näiteks ripplae paigaldamist. Tuleohutuse eest vastutava isiku kaasamine tuleb reglementeerida üleorganisatsiooniliste juhenditega ning näidata ehitustööde planeerimis- ja vastuvõtmisdokumentatsioonis (vt M 1.6 Tuletõrje-eeskirjade täitmine).

Täiendavad kontrollküsimused:

- Kas tuleohutuse eest vastutavat isikut on informeeritud tema õigustest ja kohustustest seoses kaablite paigaldamisel läbiviidavate töödega?
- Kas on olemas kirjalikult koostatud tegutsemisjuhis tuleohutuse eest vastutava isiku kaasamiseks kaablite paigaldustöödesse?

M 2.392 Virtualiseerimisserverite ja virtuaalsete IT-süsteemide modelleerimine

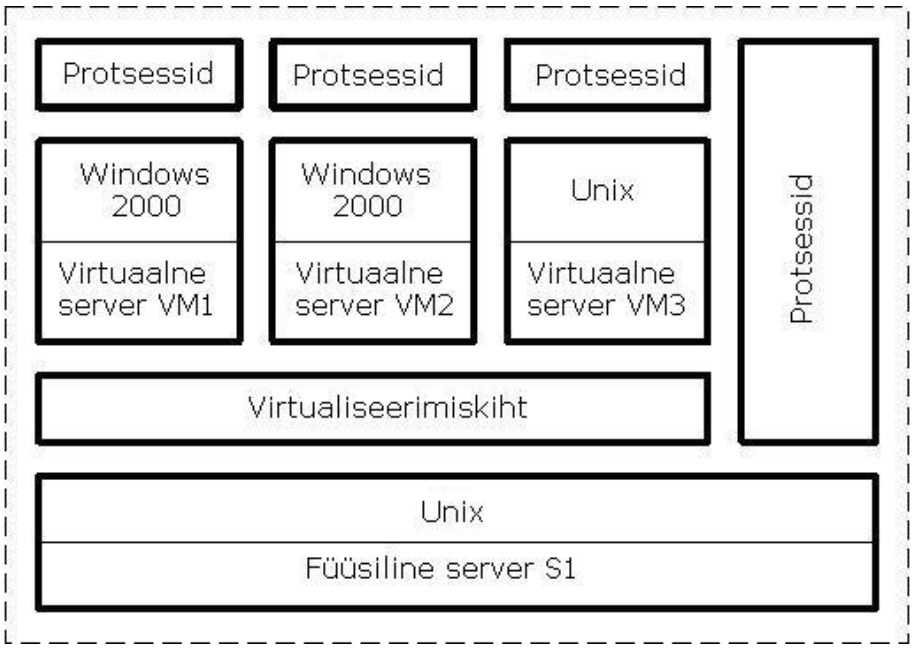
Algatamise eest vastutavad: infoturbespetsialist, IT-juht
Rakendamise eest vastutavad: administraator, IT-juht

Saavutamaks IT-ettevõttes ettenähtud üldist turvalisust, tuleb kõiki virtualiseerimisservereid ja virtuaalseid IT-süsteeme turvalisuskontseptsiooni osas süstemaatiliselt jälgida. IT etalonturbe osas tähendab see eelkõige, et kõik virtuaalsed IT-süsteemid tuleb kaasata struktuurianalüüsi ja modelleerimisse. Modelleerimise all mõistetakse IT etalonturbe puhul moodulite olemasolevatele sihtobjektidele (IT-süsteemid, rakendused, ruumid jne) allutamist. Põhimõtteliselt toimub virtuaalsete IT-süsteemide modelleerimine samade reeglite järgi nagu iseseisvate füüsiliste süsteemide puhul. See tähendab, et järgida tuleb IT etalonturbe peatükis 2.2 esitatud juhiseid. IT etalonturbe moodulite allutamine lähtub esmajoones IT-süsteemi funktsioonist (server, klient jne), kasutatavast operatsioonisüsteemist (Unix, Windows jne) ja sellel käitatavatest rakendustest (andmebaas, veebiserver jne). Turvakontseptsiooni hooldamise hõlbustamiseks ja keerukuse vähendamiseks tuleb eriti hoolikalt kontrollida, mil määral on võimalik virtuaalseid IT-süsteeme rühmitada.

Põhimõtteliselt saab ühte rühma viia ka erinevatel füüsilistel arvutitel asuvaid virtuaalseid IT-süsteeme. Seda tuleb aga igal konkreetsel juhul kontrollida. Rühmitamisjuhised leiate IT etalonturbe alt. Kui virtualiseerimiskihi all rakendatakse täisväärtuslikku ja iseseisvat alusoperatsioonisüsteemi, tuleb see sõltumatult virtuaalsetest IT-süsteemidest modelleerimisse kaasata. Ka sel juhul tuleb kontrollida rühmitamise võimalikkust.

Näidisstsenaarium
Näitena vaatleme füüsilist serverit S1, millel käitatakse virtualiseerimistarkvara abil kolme virtuaalserverit VM1, VM2 ja VM3. Alusoperatsioonisüsteemina kasutatakse füüsilisel serveril S1 ühte Unixi versiooni. Virtualiseerimiskiht on antud näites üks Unixi all töötav tarkvarakomponent, st tegemist on hostipõhise serveri virtualiseerimisega (tüüp 2). Virtualiseerimisserverile VM3 on installitud Unix. Rakendused võivad töötada nii kolmel virtuaalserveril kui ka (virtualiseerimiskihti vältides) otse serveri S1 alusoperatsioonisüsteemil.

Järgnevalt on esitatud selle näidiskonfiguratsiooni skeem:



Märkus: Täisväärtuslik alusoperatsioonisüsteem ei ole kõigi virtualiseerimislahenduste puhul virtualiseerimiskihi all kasutatav.

Juhul kui VM1 ja VM2 rühmitamise eeldused on täidetud, näeks modelleerimine eelpool kirjeldatud näidisstsenaariumi puhul välja järgmiselt (väljavõte):

Moodul	Sihtobjekt
B 3.101 Server	S1
B 3.101 Server	VM3
B 3.101 Server	VM1st ja VM2st koosnev grupp
B 3.102 Server Unixi all	S1
B 3.102 Server Unixi all	VM3
B 3.108 Windows Server 2003	VM1st ja VM2st koosnev grupp

Tabel: Moodulite jaotamine sihtobjektide vahel

Kontrollküsimused:

- Kas kõik virtualiseerimisserverid on õigesti modelleeritud ja turvakontseptsioonis süstemaatiliselt arvesse võetud ?
- Kas kõik virtuaalsed IT-süsteemid on õigesti modelleeritud ja turvakontseptsioonis süstemaatiliselt arvesse võetud?

M 2.393 Infovahetuse reguleerimine

Algatamise eest vastutavad: organisatsiooni juht, IT-juht, infoturbeosakond
Rakendamise eest vastutavad: vastutav spetsialist, töötajad

Informatsioon võib esineda erineval kujul. Enamasti käsitletakse IT etalonturbe valdkonnas paberkandjal või elektroonilisel kujul olevat informatsiooni.

Põhimõtteliselt tuleb kogu informatsiooni sobival viisil kaitsta, alustades mõtete ja ideedega, millele lisandub kirjutatud ja trükitud informatsioon, ning lõpetades elektrooniliste sõnumite, kõne-, pildi- või videosalvestistega. Kui kahe või enama suhtluspartneri vahel toimub infovahetus, tuleb selle kaitseks võtta vaatluse alla mitmeid erinevaid aspekte. Igat liiki informatsiooni vahetusel tuleb kõigepealt selgeks teha järgmised asjaolud:

- Kui suur on selle kaitsevajadus (vt M 2.217 Teabe, rakenduste ja süsteemide hoolikas liigitamine ja käitlus)?
- Kellega tohib informatsiooni vahetada (vt M 2.42 Võimalike suhtluspartnerite määramine)?
- Kuidas seejuures informatsiooni kaitsta?

Infovahetus peaks toimuma selgete ja arusaadavate reeglite alusel, mis hõlmavad kõikvõimalikke infovahetusviise, nii suulist infovahetust kui ka andmevahetust andmekandjate, e-posti, faksi, (mobiil)telefoni või interneti kaudu. Põhimõtteliselt tuleb tagada, et informatsioon ei satuks valedesse kätesse, et seda ei näeks ega kuuleks valed isikud ning et seda ei saaks märkamatult muuta.

Kõik töötajad peavad olema teadlikud, et nad vastutavad siseinfo kaitsmise eest. Näiteks ei tohiks paberkandjal ideekavandeid jätta nõupidamisruumidesse, projekte ei tohiks arutada rongis ega restoranis, helistajale ei tohiks jagada kontrollimatult siseinfot. Kaitset vajavat infot ei tohi jätta väljatrükituna järelevalveta printeritesse või faksiseadmetesse või kuskile mujale laokile. Nõupidamis-, koolitus- ja konverentsiruumide seina- ja valged tahvlid tuleb pärast iga koosoleku lõppemist puhastada, pabertahvlite kasutatud lehed tuleb samuti eemaldada. Töötajate tähelepanu tuleks pidevalt juhtida taolistele asjaoludele, kasutades selleks näiteks sobivaid selgitusi ja näitlikustamist intranetis või majalehes. Regulaarselt tuleks kontrollida, kas kommunikatsioonipartnerid on volitatud vastavat informatsiooni vastu võtma. Näiteks võib olla muutunud isikute organisatsiooniline kuuluvus, posti- või meiliaadress või faksinumber ning nii võib edastatud informatsioon sattuda valedesse kätesse. Esmakontakti korral tuleks isiku identiteeti täiendavalt kontrollida, kuna visiitkaarte võib välja anda suvalisele nimele. Seetõttu on soovitatav kontrollida uute äripartnerite tausta, võttes kontakti asutuste või ettevõtetega, kus nad töötavad, või soovituste kaudu.

Elektroonilise andmevahetuse kaitsmise viise on üksikasjaliselt kirjeldatud moodulites B 5.2 Andmekandjatel toimuv andmevahetus ja B 5.3 Rühmatarkvara .

Kontrollküsimused:

- Kas on tutvustatud informatsioonivahetuse käigus järgitavaid reegleid?
- Kas kõiki kaastöötajaid on infovahetusega kaasnevatest ohtudest küllaldaselt informeeritud?

M 2.394 Elektriseadmete kontrollimine

Algatamise eest vastutavad: tehnikaosakonna juhataja

Elluviimise eest vastutavad: tehnikaosakond

Pärast paigaldamist ja sellele järgneval perioodil tuleb elektrotehnilisi installatsioone regulaarsete vaheaegade järel kontrollida. Eesti standard EVS-HD 60364-6:2007 (Madalpingelised elektripaigaldised. Osa 6: Kontrolltoimingud). Kontrollija vaatab installatsioonid ja nende teostuse kohapeal üle ning teostab proovimõõtmised. Seejuures kontrollitakse järgnevat:

- Kas kõik elektriseadmed on installeeritud vastavalt tootja eeskirjadele?
- Kas tuletõkked on korrektselt paigaldatud?
- Kas juhtmete valik, arvestades voolukoormust, kaitseseadmete valikut ja seadistust, on õige ja tehtud vastavalt planeeringule?
- Kas elektriskeemid on täielikud ja korrektsed?
- Kas on paigaldatud hoiatussildid?
- Kas kõik juhtmed on ühendatud nõuetele vastavalt?
- Kas kõik maandusjuhtmed on paigaldatud?

Lisaks sellele hõlmab esmakontroll kogu seadme isolatsioonitakistuse mõõtmist ja selle automaatse väljalülitumise kontrolli ning tõestust. Esmakontrolli tulemuseks on elektrotehniliste seadmete töökindluse ja efektiivsuse kindlaksmääramine. Ka pärast seda tuleb lasta erialaspetsialistil elektriseadmete töökindlust regulaarselt kontrollida. Esmatähtsaks eesmärgiks on õnnetuste vältimine ja lisaks selle saavutamiseks tehtavale tuleb ka kontrollida ja dokumenteerida, milline on seadme kasutamisel tehtavate muudatuste mõju (tingitud näiteks tarbijate arvu olulisest suurenemisest). Kontrollimise protokollid, milles on kajastatud kontrolli ja mõõtmiste tulemused, tuleb arhiveerida.

Täiendavad kontrollküsimused:

- Kas on olemas kõik kontrollprotokollid, milles on kajastatud ülevaatuste ja mõõtmiste tulemused ning seadmete juures kindlakstehtud muutused?

M 2.395 IT-kaabeldusele esitatavate nõuete analüüs

Algatamise eest vastutavad: planeerija, IT-juht, tehnikaosakonna juhataja
Rakendamise eest vastutavad: planeerija, IT-juht, tehnikaosakonna juhataja

Analüüsides nõudeid, mis mõjutavad IT-juhtmestiku töökindlat, vajadustele vastavat ja ökonoomset teostust„ tuleb tähelepanu pöörata mitmesugustele probleemidele. Esmatähtsaks küsimuseks on enamasti vajalik andmeedastusmaht. Nimetatud küsimust analüüsides võetakse kõigepealt vaatluse alla lühemaks ajaks planeeritud seadmekasutus institutsioonis töötavate kasutajate poolt ning sellest tulenev IT-kasutuse pikemaajaline areng. Seejuures tuleb arvestada kahe arenguga:

- Ühest küljest muutub sagedusriba üha odavamaks. Selle tulemusena hakkavad kolmandate isikute poolt pakutavad või neilt tellitavad teenused esitama IT-juhtmestiku mahutatavusele üha kõrgemaid nõudeid. Tüüpilistele IT-teenustele nagu e-mail ja veeb (WWW) lisanduvad nüüd IT-võrguteenuste hulka ka heli ja pildi edastamine ning digitaaltelevisioon. Seetõttu tuleb IT-juhtmestiku kvaliteedi valikul arvestada suureneva vajadusega sagedusriba osas.
- Teisest küljest muutub IT-võrk üha uute rakenduste kandjaks. Kõik rakendused, mis võivad kasutada IT-maailma protokolle ja standardeid, hakkavad neid tõenäoliselt ka kasutama. See tähendab, et tulevikus ei ole IT-võrk ja sellega koos ka IT-juhtmestik mitte ainult kommunikatsiooni vahendajaks arvutite vahel. Ka telefonikommunikatsioone ja rakendusi, mis siiamaani kasutavad vaid oma rakendusspetsiifilist võrgutehnikat, arendatakse edasi ning hakkavad kasutama ühtset IT-tehnikat. Nende kujutletavate arengute tagajärjeks on, et ühenduste arv tuleb vastavalt planeerida ning et IT-juhtmestiku kavandamisel ei tohiks ühtki hooneosa plaanist välja jätta. Lisaks sellele tuleb hoonesisene juhtmestik paigaldada paindlikult ja selliselt, et seda oleks võimalik laiendada, sest muutustega ruumide ja ruumiosade kasutamisel kaasnevad kohe ka muutused võrguühendusele esitatavates nõuetes.

Vaatamata tehnika ühtlustamisele on mõningatel juhtudel vajalik planeerida teatud rakenduste jaoks erinevad ja eraldi kaablid. Eriti just kõrge kaitsevajadusega kasutusvaldkondades, nagu alarmtehnika või masinate ja seadmete juhtimine, on selliste rakenduste jaoks eraldi kaablite ja edastustehnika kasutamine sobilik või isegi vajalik. Kui kasutusvaldkonnad on erineva kaitsevajadusega ning nende kaitset pole võimalik teisiti teostada (nt virtuaalsed privaatvõrgud – VPN), tuleks need üldjuhul eraldada.

Käideldavus
Käideldavuse tagamiseks on kõigepealt vajalik kaablitrasside hoolikas planeerimine ja rajamine. Kui kasutajate nõuded on nii suured, et ka laiaulatuslikemate juhtumite korral peavad ühendused ja hoone võrguinfrastruktuur kasutatavad olema, tuleks rajada selleks varutrassid (vt M 6.103z Primaarkaabelduse liiasus ja M 6.104z Hoone kaabelduse liiasus).

Terviklus

Et tagada edastatavate andmete terviklus, on kõige tähtsamaks nõudeks varjestamine väliste mõjude eest. See tähendab eelkõige, et IT-juhtmestik tuleb paigaldada elektrotehnilisest juhtmestikust eraldi. Lisaks tuleb kindlaks teha, millised kaablitüübid on sobilikud kasutamiseks konkreetsetel juhtudel (vt M 5.3 Sidetehniliselt sobivad kaablitüübid).

Konfidentsiaalsus

Kui üheks oluliseks aspektiks on edastatavate andmete konfidentsiaalsus ehk kaabli võime tagada kaitse pealtkuulamise vastu, siis on esimeseks valikuks valguskaablid (fiber-optic cabel). Need nõuavad potentsiaalsetelt pealtkuulajatelt pealtkuulamiseks palju rohkem tehnilisi ressursse kui vaskjuhtmetel põhinevad lahendused. Veelgi tähtsam on jaoturite ja ühenduspesade kaitse, et takistada tavapäraste IT-seadmete ühendamist lokaalsesse võrku pealtkuulamise eesmärgil. See kehtib loomulikult ka valguskaablite kohta. Paljudel juhtudel on edastatavate andmete konfidentsiaalsuse ja tervikluse tagamiseks võimalik kasutada alternatiivina või täiendavalt krüptograafilisi meetodeid, kui seda võimaldavad ka võrku ühendatud lõppseadmed ja ülekandeprotokollid. Seevastu käideldavuse tagamisel aitavad krüptograafilised meetodid kaasa vaid erandjuhtudel.

Muud nõuded

Tuleb jälgida, et IT-juhtmestiku kaudu saaks toimuda või toimuks ka aktiivkomponentide, näiteks IP-telefonide või traadita kohtvõrgu pääsupunktide varustamine energiaga. Seal, kus on vaja planeerida selliste seadmete ühendamine, on kohustus kasutada vaskkaableid, kuna vooluga varustamine on võimalik üksnes vaskkaablite kaudu.

Kontrollküsimused:

- Kas IT-juhtmestiku planeerimisel arvestati ka tulevikus lisanduvate kasutajate seisukohtadega?
- Kas on olemas IT-juhtmestiku kaitsevajaduse dokumenteeritud analüüs?

M 2.396z IT-kaabelduse dokumenteerimise ja märgistuse nõuded

Algatamise eest vastutavad: IT-juht
Rakendamise eest vastutab: IT-juht

Kui on plaanis IT-juhtmestikku uuendada või moderniseerida, tuleb tellijal ja tööde teostajal (võrgu planeerija, tarnijad ja paigaldajad) kokku leppida, kuidas tuleks koostada IT-juhtmestiku dokumentatsioon. Tellija peab tagama, et tal oleksid süsteemi töölerakendamisel olemas nii juhtmestiku sisemine kui ka välimine dokumentatsioon. Sisemine dokumentatsioon hõlmab kõiki ülestähendusi, mis puudutavad IT-juhtmestiku paigaldust ja ekspluatatsiooni. Sisemine dokumentatsioon peab olema nii põhjalikult koostatud ja korras hoitud, et see võimaldaks juhtmestikku võimalikult hästi kasutada ning tulevikus edasi arendada. Väline dokumentatsioon hõlmab ühenduste märgistust, mis võimaldab juhtmestikku kasutada. Sabotaaži ja teiste pahatahtlike rünnete ärahoidmiseks on vajalik, et juhtmestiku väljastpoolt nähtav dokumentatsioon (nt võrgupesade ja kaablilõppude märgistus) peaks nii vähe kui võimalik silma paistma.

Potentsiaalsele ründajale tuleb anda nii vähe vihjed kui vähegi võimalik, samal ajal peavad IT-personalile nähtavad olema märgistused, mis on vajalikud nõuetele vastavate ja tõestatavate hädaparandus- ja võrgutööde läbiviimiseks.

Kui on planeeritud keskmise ja suure mahuga kaablite paigaldamine, tuleb dokumenteerimiseks kindlasti kasutada sobilikku tarkvara. Seetõttu tuleb juba planeerimisfaasis kindlaks määrata failiformaatide standardid ja sellega koos kasutatav tarkvaraprogramm ja -versioon. Nii on võimalik tagada, et tööde teostaja esitab dokumentatsiooni vormis, mida tööde tellija saab vahetult edasi kasutada. Samuti peaks kindlaks määrama eeskirjad, kuidas nimetada faile ning nendes sisalduvaid elemente ja struktuure. Faili versioon peaks võimaluse korral olema äratuntav juba nime järgi, näiteks seeläbi, et iga faili nimi algab kuupäevaga kujul AAAAKKPP.

Ka nimede ja märgistuste kasutamiseks dokumentides tuleb kehtestada kindlad reeglid. Näiteks tuleb kokku leppida, kuidas tähistatakse paigaldatud vaskkaablite erinevaid klasse joonistel (näide: L 123-cu6a = juhe 123, vask, CAT 6a). Tihti tekib probleeme seoses ruumide numereerimisega: arhitekt paneb need tavaliselt planeerimisfaasis paika. Neid ruumide numbreid kasutatakse ka IT-juhtmestiku planeerimisel ja paigaldamisel. Kui kasutaja seab pärast hoone vastuvõtmist sisse teise süsteemi ruumide tähistamiseks ja nimetamiseks, võib see tekitada segadust, kahjustada süsteemi tööd või tuua kaasa teisi turvaprobleeme. Näiteks võib juhtuda, et ruuminumbrite ebaõige seostamise tõttu võidakse luua kaabliühendused valede ruumidega ning seega valede IT süsteemide vahel.

Esimeseks sammuks IT-juhtmestiku dokumenteerimisel on planeerimis- ja paigaldusdokumentatsiooni loomine. Eeskätt tuleb dokumenteerida võrgu jaoks kavandatud topograafia. Seejuures märgitakse hoone- ja ruumide plaanile kõigepealt kavandatud kaablite ja trasside kulgemisteed ning ühenduspesade asetus.

Seejärel peab paigaldaja esitama kaablite ühendustööde teostamiseks vajalikud dokumendid. IT-juhtmestiku dokumentatsioon koosneb järgmistest osadest:

- Trasside kulg ja kasutamine hooneosas
- Trasside kulg, juhtmete paigaldus ja ühenduspesade asetus korruste kaupa

- Ruumide plaanid kõigi IT-juhtmestikuga tehnikaruumide jaoks koos kappide paigalduse ja võimalike toitepunktidega võõraste võrkude jaoks
- Kappide plaanid koos kappide paigalduse ja paikade plaanidega
- Tellimusele vastava teostuse vastavusdeklaratsioonid
- Tarneinfo, mõõtmisprotokollid ja vastuvõtmisel teostatud kontrollimised

Nimetatud dokumentatsioon on tellija poolt ehituse vastuvõtmise aluseks ja selle oluliseks osaks. Võrgu hilisemaks kasutamiseks on otstarbekas koostada eraldi dokumendid olemasoleva võrgu seisukorra kirjeldamiseks ja edasiseks kirjeldamiseks.

Otsene seostamine ehituse planeerimise ja tüüpiliste programmidega ning ehituse planeerimisega seotud andmeformaatidega (CAD) on otstarbekad pigem paigaldusetapis. Töö käigus on tihti otstarbekas dokumentatsioonis panna rõhku IT-võrgu loogilisele ja IT-spetsiifilistele struktuuridele ning ehituslikud aspektid tahaplaanile jätta. Selleks otstarbeks sobivad rohkem “IT-lähedased” tarkvaravahendid.

Tavaliselt oskavad töötajad selliseid programme paremini kasutada kui CAD-tarkvara.

Kontrollküsimus:

- Kas kõik osapooled on dokumendivahetuse formaadis kokku leppinud?

M 2.397 Printerite, koopiamasinate ja multifunktsionaalsete seadmete kasutamise planeerimine

Algatamise eest vastutavad: IT-juht, infoturbeosakond
Rakendamise eest vastutavad: IT-juht, administraator

Printerite, koopiamasinate ja multifunktsionaalsete seadmete turvalise kasutuse põhiliseks eelduseks on eelnevalt läbiviidud põhjalik planeerimine. Printerite kasutamist võib planeerida mitmes etapis top-down meetodil: Kogu süsteemi üldplaanist lähtudes fikseeritakse osakomponentide jaoks tehtavad konkreetsed plaanid spetsiifilistes osakontseptsioonides. Seejuures ei puuduta planeerimine mitte ainult neid aspekte, mida klassikalistel juhtudel seostatakse mõistega “turvalisus”, vaid ka normaalseid kasutuslikke aspekte, millega võivad kaasneda nõuded turvavaldkonnale.

Üldkontseptsioonis tuleks käsitleda näiteks järgmisi põhipunkte:

- Kõigepealt tuleb kokku leppida, kuhu printerid ja koopiamasinad paigaldada ja kes neid ruume või seadmeid tohivad kasutada (vt M 1.32 Printerite ja koopiamasinate turvaline paigutus).
- Järgmisena peab kehtestama võrguprinterite kasutamise reeglid, niisiis kellele millised kasutusõigused millistele printeritele ning milliste ülesannete täitmiseks antakse.
- Printereid ja koopiamasinaid tuleb kaitsta rünnete eest.
- Füüsiliste manipulatsioonide vastu tuleks rakendada vastavaid meetmeid.

Näiteks kui hooldusjuurdepääsudele paigaldada lukud, pitserid või ligipääsuklapid, võib see raskendada muudatuste tegemist volitamata isikute poolt või vähemalt aidata tehtud muudatusi märgata.

- Rünnete tegemist võrkude kaudu tuleb raskendada. Siia kuulub näiteks volitamata juurdepääs liidestele kaugadministreerimiseks LAN süsteemi kaudu (vt M 4.301 Juurdepääsu piiramine printeritele, koopiamasinatele ja multifunktsionaalsetele seadmetele).
- Kaitsta tuleb ka elektroonilist informatsiooni nii printerile edastamisel kui ka selle edasisel töötlemisel. Näiteks tuleks mõelda kõikide printerite ja koopamasinate kõvaketastele (vahest ka ainult ajutiselt) salvestatavate dokumentide krüpteerimisele. Printerite, koopiamasinate ja teiste sarnaste seadmete kasutamise planeerimisel peaks arvestama järgmiste osakontseptsioonidega:

Üldised aspektid:

- Ostmine ja üürimine: Mõningatel juhtudel võib olla otstarbekas printereid või koopiamasinaid mitte osta, vaid üürida. Kui seadmeid üüritakse, tuleb tagada, et salvestusseadmesse salvestatud dokumendid kindlalt kustutataks, et järgmine klient, kes seadme üürile võtab, ei saaks neid taastada. Sellega seoses tuleb eelnevalt kontrollida, kas salvestisi on võimalik usaldusväärselt kustutada, ilma et neile tekitataks füüsilisi kahjustusi.

- Lokaalsed või võrguprinterid: Tuleb otsustada, kus võtta kasutusele lokaalsed printerid, mida hakkavad kasutama vaid üksikud IT-süsteemid või kus võtta kasutusele võrguprinterid, mida on võimalik kasutada paljudel kasutajatel. Mõnikord on eelised ka kompromisslahendusel: Kasutajad, kes peavad tihti välja trükkima konfidentsiaalseid andmeid, hakkavad nende väljatrükkimiseks kasutama lokaalset printerit. Ülejäänud kasutajate käsutusse antakse võimsamad tsentraalsed printerid ning kompromisslahenduse korral saavad neid väiksema kaitsevajadusega info väljatrükkimiseks kasutada ka eelnevalt mainitud kasutajad.
- Printserverid: Võrguprintereid võib juhtida otse töökohaarvutilt või ühe (või mitme) printserveri kaudu. Printserver võtab printimistellimused IT-süsteemidelt vastu ning edastab need soovitud printerile. Lisaks tsentraalsele administreerimis- ja logimissüsteemile on printereid võimalik efektiivsemalt kaitsta rünnete eest, kui ainult printserverid tohivad omada võrguprinteritele juurdepääsu. Otsustada tuleb sobiva lahenduse kasuks.
- Kasutuseeskirjad: Et printerite, koopiamasinate, skannerite ja multifunktsionaalsete seadmete kasutamine asutustes ja ettevõtetes oleks turvaline ja efektiivne, tuleb koostada turvasuunised, mille aluseks on olemasolevad turvaeesmärgid ning mis arvestavad ka kavandatud kasutusmudelile esitatavaid nõudeid. Need spetsiifilised turvasuunised tuleb asutuse üldise turvakontseptsiooniga vastavusse viia.
- Sellele toetudes tuleb korraldada nimetatud seadmete turvaline kasutamine ning selleks on vaja välja töötada turvasuunised (vt M 2.398 Printerite, koopiamasinate ja multifunktsionaalsete seadmete kasutusjuhised). Tuleb jälgida, et printeritele, multifunktsionaalsetele ja sarnastele seadmetele laieneks turvakontroll ning et ka nende seadmete kasutamisel kontrollitaks regulaarselt turvasuuniste täitmist.
- Privileegide jagamine: Tuleb otsustada, kas ühe printeri teatud funktsioone tuleks lubada kasutada vaid valitud kasutajatel. Näiteks võib tuua kulukamad funktsioonid, näiteks värvilised väljatrükid või paberdokumendid erilistel paberiformaatidel. Vastavad kasutajaõigused võivad printeri haldamist ja vigade otsimist raskendada.
- Kulumaterjalide varude täiendamine: Printeritele ja koopiamasinatele tuleb regulaarselt kulumaterjali, näiteks toonerit ja paberit juurde muretseda. Tuleb kehtestada eeskirjad, kes selle eest vastutavad ning millistest protseduuridest seejuures tuleb kinni pidada (vt M 2.2 Ressursside haldamine ja M 2.52 Faksimaterjalide varude jälgimine ja täiendamine).
- Eeskirjad juurdepääsuks dokumentidele: Tuleb tarvitusele võtta meetmed, mis raskendavad juurdepääsu võõrastele dokumentidele.
- Turvakriitiline informatsioon: Kui võrguprintereid kasutatakse tihti turvakriitilise informatsiooni väljatrükkimiseks, tuleb tagada, et väljatrükitud materjalidele omaksid juurdepääsu vaid selleks volitatud isikud. Selleks võib näiteks kasutada võrguprintereid ja koopiamasinaid, mille kasutamisel peavad kasutajad end iga väljatrüki teostamiseks seadme juures autentima (vt M 4.299z Autentimine printerite, koopiamasinate ja multifunktsionaalsete seadmete kasutamisel). Alternatiivina võiks printeri kasutusõiguse anda ka vaid vähestele usaldusväärsetele isikutele, kes jagavad väljatrükitud materjalid isikutele, kellele need on mõeldud.
- Muud piirangud: Tuleb selgeks teha, kas ja millised piirangud printerite ka-

sutamisel peaks kehtima. Näiteks ei ole normaaljuhul otstarbekas, et töötajad, kes sisenevad võrku väljastpoolt, võivad eemalasetsevatest printeritest väljatrükke teha, kuna nad ei saa kohe väljatrükitud materjali kätte. Ka ajale, mille jooksul tavaliselt väljatrükkimist ei toimu, võib rakendada vastavad piirangud.

- Võrguprinterite kaitse: Juurdepääsu võrguprinteritele tuleb piirata (vt M 4.301 Juurdepääsu piiramine printeritele, koopiamasinatele ja multifunktsionaalsetele seadmetele).
- Administreerimine: Selleks, et volitamata isikud ei saaks printeri seadistust muuta, tuleb võrguprinterite kaitseks rakendada vastavaid meetmeid.
- Füüsiline kaitse: Tuleks kaaluda meetmete rakendamist otseselt seadmega manipuleerimise ärahoidmiseks.
- Võrguspetsiifiline kaitse: Võrgukomponentide kasutamisel tuleb rakendada kaitsemehhanisme võrgust tehtavate rünnete vastu. Kui võrguprinteritele ja võrgu infrastruktuurile tehnilise juurdepääsu kontrolliks on võimalik kasutada standardit IEEE 802 1X või sellega sarnaseid meetodeid, tuleks neid ka rakendada. See kaitseb võrguga ilma volituseta ühendatud IT-süsteemide eest. Lisaks sellele ei tohiks printserveritel olla võimalik ühendust luua teiste IT-süsteemidega peale eelseadistatud serverite.
- Käideldavus: Tuleb rakendada meetmeid printserveri või üksikute seadmete väljalangemise ärahoidmiseks. Vastavate hooldusleping utega on võimalik tehniliste defektide ilmnemisel seadmete avariiseisundis olemise aega vähendada (vt M 6.105 Printerite, koopiamasinate ja multifunktsionaalsete seadmete hädaolukorraks valmisoleku plaan).
- Krüpteerimine: Meetmes M 4.300z Printerite, koopiamasinate ja multifunktsionaalsete seadmete infoturve on võetud vaatluse alla ka probleemid, mis mängivad tähtsat osa planeerimisel.
- Kõvaketta krüpteerimine: Paljud printerid ja koopiamasinad on varustatud integreeritud salvestitega, millele on salvestatud informatsioon. Kui seade võimaldab krüpteerimise kasutamist, tuleks seda ka kasutada.
- Kommunikatsiooni krüpteerimine: Tuleks kaaluda töökohaarvuti ja printserveri ning printserveri ja printerite vahelise kommunikatsiooni krüpteerimist.

Kõik planeerimisfaasis vastuvõetud otsused tuleb nii dokumenteerida, et neid oleks hiljem võimalik taastada. Seejuures tuleb tagada sobiv struktureeritus ja arusaadavus.

Kontrollküsimused:

- Kas printerite ja koopiamasinate turvaline kasutamine on siduvalt kindlaks määratud?
- Milline dokumentatsioon on olemas printerite ja koopiamasinate kasutuselevõtu planeerimise kohta?

M 2.398 Printerite, koopiamasinate ja multifunktsionaalsete seadmete kasutusjuhised

Algatamise eest vastutavad: IT-juht, infoturbeosakond
Rakendamise eest vastutavad: administraator, infoturbeosakond, kasutajad

Printerite, koopiamasinate ja multifunktsionaalsete seadmete turvalist kasutamist ei ole võimalik saavutada vaid tehniliste meetmetega. Lisaks nendele tuleb kindlasti välja töötada eeskirjad administraatoritele ja kasutajatele. Administraatoritele mõeldud eeskirjas peaks olema kirjeldatud kõik printerite, koopiamasinate ja multifunktsionaalsete seadmete kaitseks rakendatavad turvameetmed. See dokument on mõeldud kvalifitseeritud personalile. Kasutajatele mõeldud eeskirjad printerite, koopiamasinate ja multifunktsionaalsete seadmete turvaliseks kasutamiseks tuleks koondada ülevaatlikku infolehte. See infoleht tuleks üles panna kõikidesse kohtadesse, kus nimetatud seadmed asuvad.

Tähelepanu tuleb pöörata järgmistele aspektidele:

- Juurdepääs kopeerimis- ja printimisruumidele: Võimaluse korral tuleks piirata juurdepääsu ruumidele, milles asuvad printerid ja koopiamasinad (vt M 1.32 Printerite ja koopiamasinate turvaline paigutus). Soovitav on juurdepääsuõigus anda näiteks ühe osakonna töötajatele või ühel korrusel töötavatele kasutajatele. Kasutajaid tuleb informeerida juurdepääsupiirangutest ja sellest, kellele juurdepääsuõigus on antud.
- Äraviimata dokumentide käitlemine: Sageli jäetakse väljaprinditud dokumendid ära viimata või valesti väljaprinditud dokumendid hävitamata. Kõik kasutajad peavad olema informeeritud, et nad peavad oma väljatrükitud dokumendid lähemal ajal ära viima. Dokumendid, mida pole võimalik ühegi kasutajaga seostada, tuleks kokku korjata ja parem kohe paberihundis hävitada.
- Tundlike dokumentide käitlemine: Kõrge konfidentsiaalsusastmega informatsiooni ei tohiks kõigile juurdepääsetava printeriga välja trükkida ja/või koopiamasinaga paljundada. Ametlikult salajas hoitavaid dokumente (saladokumente) tuleb kaitsta vastavalt kehtivatele eeskirjadele ja juhenditele.
- Autentimine seadme juures: Kui autentimine peab toimuma vahetult printeri, koopiamasina või multifunktsionaalse seadme juures (vt M 4.299z Autentimine printerite, koopiamasinate ja multifunktsionaalsete seadmete kasutamisel), tuleb kasutajaid selle meetodi osas instrueerida.
- Väljatrükkide jaotamine: Kui võrguprinteritega prinditakse tihti turvakriitilist informatsiooni, tuleks kaaluda otsuse vastuvõtmist, et lasta väljatrükke välja jagada usaldusväärsetel isikutel. See abinõu on alternatiiv seadme juures autentimisele ning selle eeliseks on, et juurdepääsu vastavatele printeritele vajavad vaid need isikud.
- Standardprinteri väljavalimine: Kui kasutajate käsutuses on mitu printerit, võivad nad oma kliendil peaaegu kõikide rakenduste jaoks standardprinteri välja valida. See funktsioon on kasutajale mugav, sest võimaldab ilma lisasisestusteta nende poolt eelistataval printeril väljatrükke teha. Lisaandmete sisestamisel saab printimist teise seadmesse suunata. Standardprinteriks tuleb valida üks loogiline (virtuaalne) seade, näiteks prindieelvaate-programm või PDF-generaator. See pakub teatud kaitset selle eest, et informatsiooni ei

saa märkamatult välja printida, näiteks kogemata rakenduse printimisnupule vajutades. Digitaalsete koopiamasinate eeliseks on, et üks kord sisseskaneeritud dokumenti saab ükskõik kui tihti välja printida. Selleks, et volitamata isikud ei omaks informatsioonile juurdepääsu, tuleb selleks kasutatav ajutine salvesti pärast kasutamist kustutada. Paljude koopiamasinate juures saavad kasutajad seda ainult manuaalselt, seepärast tuleb vastavad nõuanded ja juhised seadmetele paigaldada. Kõik kasutajad peaksid tutvuma printerite ja koopiamasinate turvalist kasutamist käsitleva infolehega. Seepärast peaks infoleht olema üles pandud igasse kopeerimis- ja printimisruumi.

Kontrollküsimused:

- Kas on olemas administraatoritele mõeldud eeskirjad printerite, koopiamasinate ja teiste sarnaste seadmete haldamiseks?
- Kas kõik kasutajad on tutvunud printerite ja koopiamasinate turvalist kasutamist käsitleva infolehega?

M 2.399w Printerite, koopiamasinate ja multifunktsionaalsete seadmete soetamise ning väljavalimise kriteeriumid

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: firma, kust seadmed ostetakse, administraator

Uute printerite, koopiamasinate või multifunktsionaalsete seadmete soetamisel on võimalik need eelnevalt nii välja valida, et nende hilisema kasutuse käigus on võimalik saavutada kõrge turvatase vaid väheste personalile ja organisatoorsele tööle tehtavate lisakulutustega. Paljud printerid ja koopiamasinad on modulaarse ülesehitusega. Põhiseadmele saab lisada uusi funktsioone. Siia kuuluvad näiteks ka sellised täiendavad turvamehhanismid nagu autentimine PINide või kiipkaartide abil. Seepärast tuleb enne printerite, koopiamasinate ja teiste sarnaste seadmete soetamist lisaks üldistele nõuetele kindlaks määrata ka turvanõuded. Nõuded ja nende põhjal tehtud otsused tuleb dokumenteerida.

Järgnevalt on loendatud mõned põhimõttelised nõuded, mida tuleb printerite soetamisel arvesse võtta:

Põhilised funktsionaalsed nõuded

- Kas tuleb muretseda võrku ühendatavad seadmed?
- Kas seadme võimsus vastab kasutajate hulgale?
- Millist tüüpi ja millise printimismeetodiga printerid tuleb muretseda?
- Kas seadmele on hiljem võimalik lisada täiendavaid funktsioone? Paljusid seadmeid on hiljem võimalik täiendada vastavate lisafunktsioonide ja -tarvikutega, näidetena võiks nimetada võrku ühendamise võimalust, kahepoolset printimist, lisasahtleid paberi jaoks ja autentimisvõimalust.

Üldine turvalisus

- Kas süsteem võimaldab kasutada turvalisi administreerimisprotokolle? Selleks, et seadmeid saaks tsentraalselt administreerida, peavad võrku ühendatavad seadmed võimaldama administreerimiseks turvalisi protokolle, brauseri põhise konfiguratsiooni korral näiteks SST/TLS.
- Kas informatsiooni on võimalik salvestada krüpteerituna? Selleks, et takistada pärast kõvaketta (volitamata) väljamonteerimist juurdepääsu andmetele, paigutavad mõned seadmed informatsiooni kõvakettale krüpteeritult.
- Kas on ette nähtud võimalus autentimiseks vahetult seadme juures (nt parooli või PIN- koodi sisestades või kiipkaarti kasutades) või saab selle funktsiooni hiljem lisada? Paljude seadmete puhul on autentimine ette nähtud, mõnede puhul on see siiski ette nähtud vaid administreerimiseks, et kaitsta konfiguratsiooni rünnete eest. Siiski on olemas ka seadmeid, mille puhul on võimalik turvata kõiki kasutusjuhte, nii et informatsioon prinditakse välja alles siis, kui kasutaja on end seadme juures autentinud. Nimetatud funktsiooni abil on võimalik ära hoida, et ühele võrguprinterile edastatud või koopiamasinasse skaneeritud informatsiooni saaksid välja printida selleks volitamata isikud. Sama funktsiooni on võimalik kasutada ka kulude kontrollimiseks.
- Kas on olemas aaskinnitused või teised võimalused seadmete füüsiliseks kaitsmiseks varguse eest?
- Kas riistvaraga manipuleerimist saab korpuselukkude paigaldamise või sarnaste meetmete rakendamise teel raskendada? Tihti juhtub näiteks, et printeritest või koopiamasinatest varastatakse salvestusmoodulid.

Andmete turvaline kustutamine

- Kas kasutajad saavad salvestisse salvestatud materjali peale igat kopeerimist kustutada? Paljudesse seadmetesse on salvestid, enamasti kõvaketastena, sisse ehitatud. Kui andmed salvestatakse sinna krüpteerimata, saavad volitamata isikud neid teatud tingimustel lugeda. Lisaks sellele eksisteerib oht, et ründajad lasevad seadmesse salvestatud materjali uuesti välja trükkida. Seetõttu on mõnedel seadmetel funktsioonid, mis võimaldavad salvestisse salvestatud informatsiooni kustutada. Seadistused tuleks teha selliselt, et kustutamine toimub pärast igat koopiate tegemist automaatselt.
- Kas on võimalik kogu kõvaketast kustutada? Andmete hilisemaks kõrvaldamiseks peaks olema võimalik kogu kõvaketas ülekirjutamise teel kustutada. Kogu kõvaketta kustutamine peaks olema võimalik ainult vastava kustutamiskäsu alusel, mille on andnud selleks volitatud isik.
- Kas kustutatav informatsioon kuvatakse seadme ekraanil? Nii viimasena salvestatud andmete kustutamine kui ka kogu kõvaketta kustutamine ülekirjutamise teel peaksid olema seadme ekraanil kuvatud.

Võrgutehniline turvalisus

- Kas seade on varustatud võrgutehniliste kaitsemehhanismidega, nagu näiteks IP- ja pordifiltriga?
- Kas seade peab võimaldama traadita kohtvõrgu või Bluetooth -i kasutamist või piisab kaabliühendusest? Raadiosidetehnika kasutamine on seotud suuremate turvariskidega kui kaabelühendus. Seetõttu peab raadiopõhiste lahenduste korral enamasti rakendama täiendavaid turvameetmeid.
- Kas seade võimaldab krüpteerida printeri kommunikatsiooni? Et kõrvalised isikud ei saaks väljaprinditavat informatsiooni selle edastamise ajal võrgu kaudu lugeda, tuleks kasutada võrguprotokolle, mis võimaldavad informatsiooni krüpteerida. Üheks näiteks oleks interneti prindiprotokoll (Internet Printing Protokoll -IPP) koos turvasoklite kihiga (Secure Sockets Layer - SSL)
- Kas seadet saab integreerida olemasolevasse IEEE 802.1X keskkonda? IEEE 802. 1X võimaldab lõppseadmete autentimist võrgus. See kaitseb selle eest, et IT süsteeme saaks lubamatult LANi abil kasutada.

Hooldatavus

- Kas tootja pakub regulaarseid uuendusi ja kiire käideldavusega turvapaiku?

Eriti tähtis on, et tootja reageeriks võimalikult kiiresti turvalisusega seotud puudustele, millest talle on teatatud?

- Kas toote hooldamiseks on võimalik sõlmida hooldusleping uid? Sageli on juurdepääs tootja uuendustele ja tugiteenustele võimalik üksnes kehtiva hooldusleping u olemasolul.

- Kas hooldusleping on sobiv ainult juhul, kui garanteeritud reageerimis- ja taaskäivitamisajad vastavad seadme käideldavusele esitatavatele nõuetele.
- Kas turustaja või tootja pakub tehnilist klienditeenindust (Hotline), mis on võimeline pakkuma kohest abi probleemide lahendamisel? Eelnevalt nimetatud aspekt peaks olema hooldusleping koostisosaosa. Lepingu sõlmimisel tuleb jälgida, et hotline 'i või tugiteenuse töötajad räägiksid ka keelt, mida räägivad isikud, kes hakkavad neile helistama.

Kulud

- Kui suured on seadmete soetamiskulud?
- Kui suured on eeldatavad jooksvad kulud, kaasa arvatud kulud hooldusele, ekspluatatsioonile ja kasutajatoele? Nimetatud kulutustega tuleks juba seadmete soetamisel arvestada? Hooldust ja kasutajatuge sisaldavate lepingute sisu tuleks kontrollida näiteks reageerimisaegade, hotline -teenuse ning personali kvalifikatsiooni osas.

Kontrollküsimused:

- Kas defineeritakse printerite, koopiamasinate ja multifunktsionaalsete seadmete soetamisele esitatavad nõuded?
- Kas nõuded dokumenteeritakse?
- Kas printerite, koopiamasinate ja multifunktsionaalsete seadmete soetamisel võetakse valikukriteeriumidena arvesse ka turvaaspekte?

M 2.400 Printerite, koopiamasinate ja multifunktsionaalsete seadmete turvaline kasutuselt kõrvaldamine

Algatamise eest vastutavad: IT-juht, infoturbeosakond
Rakendamise eest vastutab: administraator

Kui printerid, koopiamasinad, multifunktsionaalsed seadmed või nimetatud seadmete üksikud komponendid tuleb kasutusest kõrvaldada või välja vahetada, tuleb kogu turvalisuse tagamise seisukohalt oluline informatsioon seadmetest kustutada. See kehtib eelkõige juhul, kui komponendid eraldatakse seadmest ja antakse edasi kolmandatele isikutele. Sellekohasteks näideteks on seadme müümine, tagastamine peale liisinguaja lõppemist, väljavahetamine tootja poolt ja parandustööde teostamine teenindusfirmas. Aga isegi juhul, kui seadmeid kasutatakse asutusesiseselt edasi või need hävitatakse, tuleb kogu kaitset vajav informatsioon seadmest kustutada.

Olenevalt kasutusotstarbest ja seadme tüübist võivad seadmesse olla salvestatud näiteks järgmised turvalisuse seisukohalt olulised andmed:

- "Vahemällu salvestatud" informatsioon: Digitaalsetesse koopiamasinatesse skaneeritakse enne väljaprintimist tavaliselt kogu dokument. Ka printerite puhul salvestatakse dokument kõigepealt vahemällu. Vahemällu salvestamiseks on seadmetesse sisse ehitatud komponendid, enamasti kõvaketaste näol. Teatud tingimustel saab vahepeal kustutatud dokumente taastada. Mõnedel seadmetel on olemas spetsiaalne funktsioon salvestatud informatsiooni kustutamiseks.
- Konfiguratsiooniseaded: Eriti võrku ühendatavate seadmete puhul annavad sellised konfiguratsiooniseaded nagu IP-aadressid teatud tingimustel informatsiooni võrgustruktuuri kohta. Seetõttu tuleks konfiguratsiooniseaded kustutada või taastada tarneolekus olnud algseaded. Paljudel seadmetel on selleks vastavad funktsioonid olemas.
- Paroolid: Paljude seadmete puhul on ette nähtud parooli- või turvamärgipõhine (token 'i põhine) autentimine, mõnede puhul siiski ainult administreerimiseks. Kuid on ka seadmeid, mille puhul aktiveeritakse autentimine igakordsel seadme kasutamisel. Kõik paroolid tuleks taastada sellistena, nagu need olid seadme tarneolekus.
- Sertifikaadid: Mõned seadmed pakuvad võimalust sertifikaadipõhise autentimise kasutamiseks, näiteks IEEE 802. 1X kasutades. Kõik sertifikaadid tuleks taastada sellistena, nagu need olid seadme tarneolekus.
- Muu jääkinformatsioon: Teatud tingimustel võib kulumaterjalide, näiteks tooneritrumlite abil, väljaprinditud dokumente taastada. Suurema turvavajaduse korral tuleb pärast riskide hindamist otsustada, kas kasutatud kulumaterjalid tuleb hävitada.

Enne seadmete kasutuselt kõrvaldamist või edasiandmist kolmandatele isikutele tuleb sisesalvesti kustutada. Juhul kui kõvaketast saab välja monteerida, soovitatakse see eraldi kustutada. Pärast salvesti kustutamist tuleb üle kontrollida, kas kustutamine õnnestus. Seejuures kasutatavad protseduurid sõltuvad suuresti seadme liigist ja kasutusotstarbest. Juhul kui seadmesse on salvestatud eriti turvakriitiline informatsioon ning kui ei suudeta piisava kindlusega tagada, et and-

med on tõesti kustutatud, võib osutuda vajalikuks salvesti füüsiliselt purustada või kasutuskõlbmatuks muuta.

Kontrollküsimused:

- Kas konfiguratsiooniandmed ja paroolid kustutatakse enne seadme kasutusest kõrvaldamist turvaliselt?
- Kas kontrollitakse, et salvestile salvestatud informatsioon on tõepoolest kustutatud?
- Kas kulumaterjalide, nagu tooneritrumlite abil on võimalik jääkinformatsiooni kätte saada?

M 2.401 Mobiilsete andmekandjate ja seadmete kasutamine

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: administraator, kasutajad

Olenevalt seadme tehnilisest ülesehitusest saab mobiilsete andmekandjate abil vahetada suurel hulgal suuremahulisi andmefaile. Mobiilsete andmekandjate mudelitest oli mõne aasta eest veel täiesti võimalik ülevaadet omada. Tavaliselt kasutati andmevahetuseks väljavahetatavaid andmekandjaid nagu disketid või CDd. Vahepeal on mobiilsete andmekandjate sortimenti täiendatud suure hulga mudelitega, nii et esmapilgul on raske aru saada, et tegemist on andmekandjaga.

Näiteks on olemas käekellad või muusika mahamängimise seadmed, millesse on integreeritud andmesalvesti. Nende integreeritud andmesalvestite suurus algab tavaliselt mõnesajast megabaidist ning võib ulatuda kuni mitme gigabaidini. Seetõttu tuleks vahetatavate andmekandjate ja mobiilsete seadmetega ümberkäimisel tähelepanu pöörata mõningatele põhiprobleemidele.

Tuleb välja selgitada järgmised aspektid:

- Milliseid mobiilseid andmekandjaid tuleb institutsioonis kasutada (vt M 2.9 Aktsepteerimata riist- ja tarkvara kasutuse keeld)?
- Milliseid tegelikult kasutatakse ja kes neid kasutab (nt varaloendite põhjal, mida on kirjeldatud M 2.2 Ressursside haldamine)?
- Milliseid andmeid tohib mobiilsetele andmekandjatele salvestada ja milliseid mitte (vt M 2.217 Teabe, rakenduste ja süsteemide hoolikas liigitamine ja käitlus)?
- Kuidas kaitstakse mobiilsetele andmekandjatele salvestatud andmeid volitamata juurdepääsu, manipuleerimise ja kaotsimineku eest?
- Milliste asutuseväliste isikutega tohib andmekandjaid vahetada ning milliseid turvaeeskirju tuleb seejuures täita (vt B 5.2 Andmekandjatel toimuv andmevahetus)?
- Kuidas takistatakse mobiilsete andmekandjate kasutamist informatsiooni volitamata edasiandmiseks?
- Kuidas hoitakse ära kahjurvara levitamine mobiilsete andmekandjate kaudu?

Lisaks eeltoodule tuleks otsustada, kas töötajad tohivad oma isiklikke mobiilseid andmekandjaid ja teisi seadmeid institutsioonisiseselt kasutada. Samuti tuleb otsustada, kas institutsioonivälise isikute poolt kaasa toodud mobiilseid andmekandjaid ja teisi seadmeid tohib kasuatada institutsioonisiseselt näiteks andmevahetuseks. Mida rohkem piiranguid sisaldavad turvaeeskirjad mobiilsete andmekandjate ja teiste seadmetega ümberkäimiseks, seda suuremad on piirangud ka igapäevatöös. Seetõttu tuleks kõiki turvaeeskirju koostades mõelda, kas nende rangusaste on sobiv.

Arengute jälgimine

Andmekandjate hulk ja variantide mitmekesisus suurenevad tulevikus veelgi. Andmekandjad muutuvad üha enam “nähtamatuks”, kuna need integreeritakse teistesse seadmetesse. Regulaarselt tuleks kontrollida, kas mobiilsete andmekandjate ja seadmetega ümberkäimiseks kehtestatud turvaeeskirjad on ikka veel

aktuaalsed, alustades sellest, kas need hõlmavad veel antud momendil kasutatavate andmekandjate kõiki variante.

Krüpteerimine

Mobiilseid andmekandjaid on sõidus olles kerge kaotada ning neid võidakse ka varastada. Seetõttu tuleks mobiilsetele andmekandjatele salvestatud konfidentsiaalne info krüpteerida. Selleks oleks kõige parem kasutada tooteid, mille abil on võimalik kõikide mobiilsele andmekandjale salvestatavate andmete automaatne krüpteerimine (vt M 4.29z Kaasaskantavatele IT-süsteemidele mõeldud krüpteerimistoote kasutamine).

Buutimistõkked

Kõik IT-süsteemid tuleks varustada buutimistõkkega, mis takistab selliste väliste andmekandjate käivitamist nagu disketid, CD-ROMid või USB-pulgad, nii et nende abil ei oleks võimalik kontrollimatult tarkvara installeerida või konfiguratsiooni muuta (vt M 4.4 Eemaldatavate andmekandjate draivipilude ja väliste andmekandjate nõuetele vastav kasutamine). Iga konkreetse institutsiooni jaoks tuleks dokumenteerida sobilikud protseduurid ning koostada nende põhjal töötajate jaoks turvasuunised. Mobiilsetest andmekandjatest tulenevate riskide sobilikul viisil vähendamiseks on otstarbekas rakendada erinevaid tehnilisi meetmeid (vt M 4.200z USB-salvestuskandjatega ümberkäimine ja M 4.232z Mälulaienduskaartide turvaline kasutamine), kuid ainult sellest ei piisa. Antud küsimuses tuleb tingimata tõsta töötajate teadlikkust.

Kontrollküsimused:

- Kas on olemas mobiilsete andmekandjatega ümberkäimist reguleerivad turvasuunised?
- Kas kõiki töötajaid on informeeritud mobiilsete andmekandjate kasutamist käsitlevatest turvaeeskirjadest?

M 2.402z Paroolide uuendamine

Algatamise eest vastutavad: IT-juht, infoturbeosakond
Rakendamise eest vastutavad: IT-juht, infoturbeosakond

Kui kasutajad peavad end paroolide abil autentima, võib ette tulla paroolide unustamist. Ühest küljest tuleb kasutajaid sellises situatsioonis kiiresti aidata, et nad saaksid edasi töötada. Teisest küljest tuleb takistada, et volitamata isikud saaksid ebapiisava volituste kontrolli tõttu juurdepääsu IT-süsteemidele (vt G 5.42 Inimestega manipuleerimine (Social Engineering)). Seetõttu peab iga institutsioon valima paroolide uuendamiseks endale sobivad meetodid. Seejuures on oluline, et paroolide uuendamiseks kehtestataks paindlikud eeskirjad. Protseduuride jäik defineerimine ei ole kaasaegses mobiilses töökeskkonnas enamasti otstarbekohane.

Ühelt poolt peaks tegutsemisviis vastama konkreetse parooli kaitsevajadusele, teiselt poolt tuleb arvestada kasutajate juurdepääsunõuetega. Milline protseduur konkreetsel juhul sobib, sõltub paljudest faktoritest, näiteks institutsiooni suurusest, töötajate arvust, töötajate geograafilisest jaotusest (kas nad on alati kohapeal kättesaadavad, kas nad viibivad tihti klientide juures, kuidas nendega kontakti saab jne) ja loomulikult parooliga kaitstud informatsiooni ja äriprotsesside turvavajadustest (juurdepääs üksnes lokaalsele IT-süsteemile, LANile, sisevõrkudele väljastpoolt, internetipostkastile jne).

Nõuanne: tavaline autentimismeetod, mille puhul kasutatakse kasutajanime ja parooli, sobib reeglina normaalse kaitsevajaduse korral. Kõrgema kaitsevajaduse puhul tuleks kasutada efektiivsemaid autentimismeetodeid, näiteks kombineerides omavahel kiipkaardi, USB-volitustõendi ja ühekordse parooli kasutamist.

Alljärgnevalt käsitletakse mõningaid parooliuuendusvariantide eeliseid ja puudusi, mille hulgast on võimalik konkreetse kasutusjuhtumi jaoks sobivad meetodid välja valida:

- Kirjalikult posti või faksi teel – nimetatud juhul kasutatakse parooli uuendamiseks formulari, millele kasutaja peab kirjutama oma nime ja formulari allkirjastama. Seejärel tuleb täidetud formular saata posti või faksi teel kasutajatoele. Tegemist on põhjaliku meetodiga, eriti juhul, kui formularid arhiveeritakse. Meetodi puudus on aga asjaolu, et olevalt institutsiooni suurusest kulub veidi aega, enne kui formular (majasisese) postiga kasutajatoeni jõuab. Et volitamata isik ei saaks õigustatud kasutaja nimel lasta parooli uuendada, peaks selle variandi korral olema võimalik allkirju võrrelda. Sel juhul peab kasutajatoe töötaja formularil olevat allkirja võrdlema eelnevalt deponeeritud allkirjaga. Vastuse uue parooliga võiks kasutajatoe töötaja saata samuti posti või faksi teel. Faksi kasutamisel ei saa üldiselt siiski garanteerida, et parool jõuab ainult kasutajani. Kui vastus saadetakse posti teel, tuleks kasutada kinni pitseeritud ümbrikku. Meetodi puudus on postiga teel saatmiseks kuluv aeg.
- Telefoni teel ilma lisainformatsiooni nõudmiseta. Kõige lihtsam variant on paroolide uuendamine telefoni teel. Seejuures on kasutaja turvaline verifitseerimine kulukas. Kasutajatugi peab olema võimeline kasutajat hääle järgi identifitseerima. Nimetatud lahendus sobib kasutamiseks institutsioonides, mis ei ole väga suured ning mille töötajad suudavad üksteist telefonitsi hääle järgi ära tunda. Telefoninumbri kontrollimine on samuti ebapiisav. See võib olla näiteks võltsitud. Ründaja võib ka töötaja äraolekut kasutades helistada tema büroost kasutajatoele. Just see meetod, st paroolide uuendamine

üksnes telefonikõne alusel, seisab isegi social engineering-tüüpi rünnakute keskpunktis. Kui vähegi võimalik, tuleks sellest variandist loobuda.

- Telefoni teel koos lisaküsimuste esitamisega. Et parooli vahetamist telefoni teel lihtsustada, võib kasutajatugi esitada ka küsimusi täiendava informatsiooni saamiseks, mis on eelnevalt deponeeritud. Tegemist võib olla näiteks töötaja sünnipäeva või isikliku numbriga (need on muidugi tunnused, mida on lihtne teada saada). Need võivad olla märksõnad, mida kasutajal on küll kerge meelde jätta, kuid mida on raske ära arvata. Selleks on soovitatav deponeerida mitte ainult üks mõiste, vaid mitu mõistet, ning iga mõiste jaoks deponeerida ka sobiv küsimus. Näiteks võiks kasutajatoel olla koos õige vastusega deponeeritud küsimus „Mis oli kodulooma nimi, kes Teil oli, kui olite 10-aastane?”. Võimaluse korral tuleks vältida selliste eelnevalt formuleeritud küsimuste kasutamist, nagu „Kuidas on Teie isa eesnimi?”, kuna selliste küsimuste vastuseid on lihtne välja uurida.
- Identiteedi kontrollimine juba salvestatud informatsiooni abil. Telefoni teel küsimuste esitamisel võib identiteedi kontrollimiseks kasutada ka muud, juba kasutajaks registreerimisel salvestatud informatsiooni. See võiks olla näiteks töötaja kood, sünnikuupäev või midagi sarnast. Seejuures on puuduseks asjaolu, et enamik sellisest tavaliselt eelnevalt salvestatud informatsioonist on paljudes kohtades teada ning enamasti on seda ka võimalik internetist kiiresti üles leida.
- Isiklik kohale ilmumine. Nimetatud juhul peab kasutaja ise teatud kindla isiku juurde minema ja laskma seal parooli vahetada. Olenevalt institutsiooni suurusest võib see isik olla ülemus, teatud valdkonna eest vastutav spetsialist või kasutajatoe töötaja. Kõnealusel isikul peaks igal juhul olema õigus anda (uuesti) juurdepääsuõigusi ning nende andmist taotleda ja läbi viia.
- Usaldusväärse isiku volitamine. Selle variandi puhul võiks teha signeeritud e-kirja saatmise kasutajatoele ülesandeks näiteks kolleegile, kes palub e-kirjas parooli uuendada. Krüptograafilise signatuuri abil saab kontrollida, kes taotluse esitas. Kui töötaja ei ole sellist ülesannet saanud, saaks ründe toimumist tagantjärele tõestada. Uue parooli võiks krüpteeritud e-kirja teel edastada volitatud isikule, kes teatab parooli vastavale kasutajale. Lisaks tuleks parooli kasutajat parooli uuendamisest informeerida, et saaks võimalikku rünnet avastada. Selle meetodi puudused seisnevad asjaoludes, et rünnet on võimalik kindlaks teha alles tagantjärele ja et uuendatud parooli saaks teada kolmas isik.

Ühekordsete paroolide andmine

Üldiselt peaks kasutajatugi paroole uuendades väljastama ainult ühekordselt väljastatavaid paroole, nii et kasutajad peavad vahetult pärast paroolide õnnestunud registreerimist muutma need ümber ainult neile endile teadaolevateks paroolideks. Seejuures peaks kasutajatugi jälgima, et parooli uuendamiseks ei kasutataks ühte ühtset parooli, sest kuuldus sellest leviks kiiresti. Lisaks sellele peaks parooli märgiline koostis olema nii keerukas, et seda ei oleks kerge ära arvata. Samuti peaks kasutajatugi täpsustama, kas parooli uuendamine on tõesti vajalik.

Uue parooli teada andmine

Uue parooli teatamiseks töötajale võib samuti kasutada mitmeid mooduseid, näiteks:

- kasutajatugi teatab töötajale uue parooli teisel eelnevalt määratud viisil, näiteks majasisese posti teel või eelnevalt registreeritud telefoninumbrile tagasi helistades (mitte juhul, kui sellelt numbrilt tuli taotlus parooli uuendamiseks);
- parooli võib saata ülemusele, sekretariaati või mõnda teise usaldusväärsesse kohta, kus töötajat tuntakse ja teda sellest informeeritakse;
- parool saadetakse eelnevalt registreeritud aadressile (füüsilisele või e-posti aadressile);
- parool toimetatakse kohale kulleriga, kes kontrollib vastuvõtja isikutunnistust.

Kasutajatoe töötajate koolitus

Tähtis on ka, et kasutajatoe töötajad saaksid piisavas mahus volituste haldamise alast koolitust. Nad peaksid tundma nii tüüpilisi näitlemismeetodeid (social engineering), et selgitada välja volitamata juurdepääs informatsioonile või IT-süsteemile, kui ka olema õppinud probleemsete juhtumite käsitlemist ja paindlike lahenduste leidmist. Kogemus näitab, et jäika tegutsemisviisi on kergem ära petta, eriti juhul, kui ründajale on see tuttav, võrreldes sellega, kui töötajad loominguliselt tegutsevad. Kui näiteks on vastu võetud otsus, et parooli uuendamisel tuleb alati ülemust informeerida ja teda ei ole võimalik kätte saada, on parem otsida sobiv esindaja kui oodata liiga kaua. Juhtudeks, kui konkreetse parooli kaitsevajadus on liiga kõrge ja kasutajatoe töötaja ei taha turvaliste võimaluste puudumise tõttu vastutust võtta, peab olemas olema eskalatsioonistrateegia.

Töötajate informeerimine

Kõik kasutajad peaksid olema teadlikud sellest, mida nad peavad ette võtma, kui nad on parooli unustanud. Lisaks sellele peaksid kõik kasutajad võtma tõsiselt juhtumeid, kui nad registreerimisel avastavad, et nad ei tea korrektset parooli. Peale lihtsa unustamise võib see olla märk sellest, et ründaja on saanud volitamata juurdepääsu informatsioonile. Kahtluse korral tuleks sellest teavitada infoturbeosakonda (vt M 6.60 Turvaintsidentide käsitlusprotseduurid ja teavitamiskanalid).

Kontrollküsimused:

- Kuidas informeeritakse vastutavat instantsi blokeeritud paroolist?
- Kuidas uus parool edastatakse?

M 2.403 Kataloogiteenuste kasutuselevõtu planeerimine

Algatamise eest vastutavad: IT-juht, infoturbejuht

Rakendamise eest vastutavad: IT-juht, administraator

Kataloogiteenuse kontseptsiooni loomisel tehtud vigu on pärast paigaldamist väga raske kõrvaldada. Seetõttu tuleb kataloogiteenuste kasutamist hoolikalt planeerida. Kataloogiteenuse planeerimise ja kontseptsiooni loomise faasis defineeritakse teenuse kasutusotsarve ja rakendusvaldkonnad ning määratletakse kasutamiseks vajalikud turvapoliitikad. Kui kataloogiteenuse kasutusnõuded on kindlaks määratud, tuleb selle teenuse kasutuselevõtmiseks välja valida sobivad komponendid (vt M 2.406 Kataloogiteenuste kasutamiseks sobivate komponentide valik). Enne kataloogiteenuse juurutamist tuleb otsustada, kuidas seda kasutama hakatakse. Kasutusotstarbest sõltuvad muuhulgas kataloogiteenuse struktuurile esitatavad nõuded. Vajalike planeerimistööde liiki ja mahtu mõjutavad oluliselt ka kataloogiteenusesse salvestatavad andmed. Sõltuvalt kataloogiteenuse keerukusest võib kataloogiteenuse kontseptsiooni planeerimine kesta mitu kuud ja isegi üle aasta. Planeeritud kasutusstsenaariumist sõltub kehtestatav turvapoliitika. Kataloogiteenuse kasutusvõimaluste näited:

- Telefoninumbrite, postiaadresside jms aadressiraamat
- Sidumine meilisüsteemidega
- Digitaalsed sertifikaadid, PKI (*Public Key* infrastruktuurid)
- IT-süsteemide ja rakenduste ülevõrguline konfiguratsiooniinfo
- Ühtne, tsentraalne, asukohast sõltumatu kasutajate haldamine
- Inimeste ja protsesside autentimine võrgus asuvatesse IT-süsteemidesse sisselogimisel

Nimetatud näited on vaid valik kataloogiteenuse võimalikest kasutusviisidest ning need võivad varieeruda tüübi, suuruse ja lahenduse osas. Võimalike kasutusostarvete kombinatsioonid pole mitte ainult võimalikud, vaid kujutavad endast ka kataloogiteenuste eeliseid. Samal ajal suurendab see kataloogiteenuse keerukust, mis toob endaga kaasa kohustuse vastavat kasutusala hoolikamalt planeerida.

Ligipääs Internetist

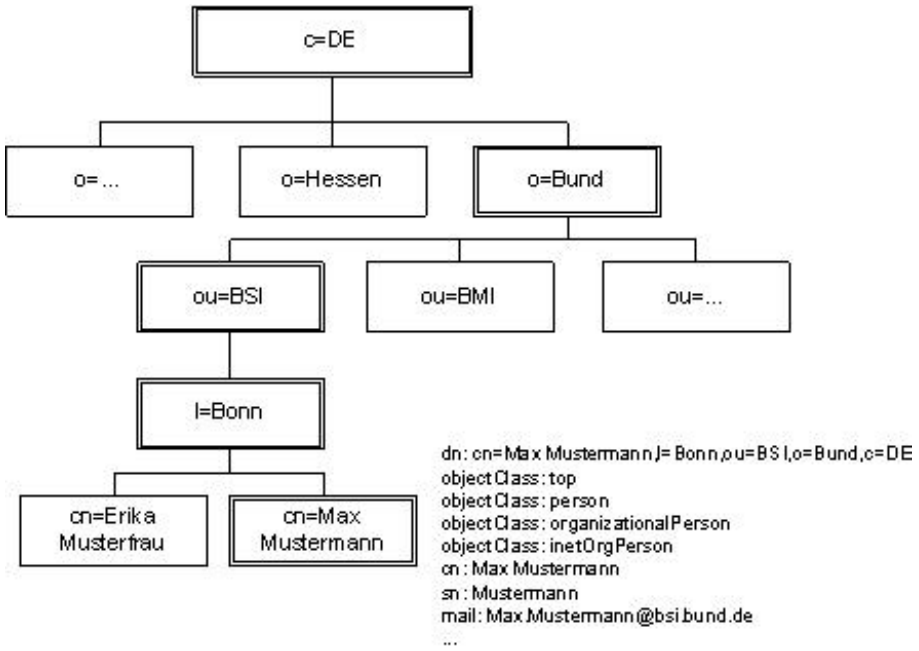
Edasised küsimused tekivad planeerimisel pärast seda, kui on kindlaks määratud, kas kataloogiteenus või selle osad peaksid olema ligipääsetavad ka väljaspool organisatsiooni sisevõrku.

- Kuidas turvatakse kataloogiteenuse väliseid juurdepääse?
- Kuidas turvata juurdepääsu kataloogiteenuse andmetele?
- Milliseid autentimismehhanisme läheb tarvis?
- Millistele andmetele võib väljast anonüümselt ligi pääseda?
- Millistele andmetele tohib ligi pääseda pärast edukalt läbitud autentimist?
- Millised krüptograafilised meetodid on vajalikud, et tagada edastatavate andmete konfidentsiaalsus ja terviklus?

Puustruktuuri kavandamine

Kataloogiteenusele esitatavad nõuded tuleb analüüsida ja seejärel dokumenteerida. Lisaks kataloogiteenuse kasutusotstarbe kindlaksmääramisele tuleb

välja töötada objektiklassidest ja atribuuditüüpidest koosnev mudel, mis vastab ettenähtud kasutusotstarvete nõuetele. Puustruktuuri kavandamiseks *Directory Information Tree* 's (DIT-s) tuleb esmalt valida kõrgeim element, juurelement (ingl *root*). Üldjoontes saab kõik edasised objektid paigutada selle juure alla. Organisatsiooni töötajate või võrgu kasutajate kataloogi jaoks on mõistlikum luua struktuur, mis lähtub osakondadest. Tavapärane objektiklass selliste organisatsiooniüksuste loomiseks on "organizationalUnit". Seejärel tuleks üksikud isikud või kasutajad taasluua kataloogipuu objektidena. Selle jaoks on olemas mitmed skeemid, mis on paigaldatud juba koos kataloogiteenusega või mida saab lisada ning mis pakuvad sõltuvalt vajalikust info detailsusest erinevaid klasse. Lihtsaim objektiklass on „ *person* ", mis on esmajoones mõeldud ainult isiku nime, telefoninumbri ja parooli info jaoks. Paroole ei tohi atribuudi "userPasswordälla mitte kunagi salvestada krüpteerimata kujul. Siia tasub salvestada ainult *hash* -väärtus. Veelgi parem oleks vältida nii paroolide kui ka *hash* -väärtuste salvestamist kataloogiteenuse üldloetavasse alasse, vaid salvestada need hoopis alasse, mis on eranditult ette nähtud autentimiseks. Sellest tuletades saab kasutada valikut "organizationalPerson", mis oskab kajastada erinevaid aadresse ja (telefoni-)numbreid, samuti osakonda kuuluvust, kirjeldamaks isikute seoseid vastava organisatsiooniga. Sellest omakorda tuletatud, samanimelisest skeemist pärinev klass "inetorgPerson" võimaldab kasutada lisaatribuute alates täiendavatest telefoninumbritest, aadressidest ja meiliaadressidest kuni auto numbrimärkideni. Seda klassi on võimalik kasutada inimeste kirjeldamiseks väljaspool seoseid, mis kajastavad inimesi oma organisatsiooni alluvussuhetes, näiteks internetiteenuste kasutamise kirjeldamiseks.



Joonis: puustruktuuri näide

Skeemi täiendamine

Skeemidel, mis on tavaliselt kataloogiteenustega kaasas, on juba umbes tuhat objektiklassi ja atribuuti. Sellest kogumist tuleb valida kataloogiteenuse kasutamiseks vajalikud elemendid, lähtudes eelnevalt läbiviidud vajaduste analüüsist. Üldjuhul piisab ka eeldefineeritud klassidest. Praktikas võib olla vajalik kasutada olemasolevat atribuuti mõnes teises kontekstis ja anda talle selleks teine tähendus, ilma selle nime muutmata. Seda võimalust tuleks kasutada ainult siis, kui on tagatud, et äravahetamine ja objekti väärkasutus on välistatud. Kui olemasolevad objektiklassid ja atribuuditüübid on planeeritava kasutusotstarbe jaoks ebapiisavad, saab olemasolevat skeemi täiendada. Seejuures tuleb jälgida, et igal skeemiobjektil oleks objekti ID (OID), mille alusel oleks võimalik seda selgelt tuvastada. OID-nimeruume haldab *Internet Assigned Numbers Authority* (IANA) ning need seotakse jäädavalt selle omanikuga. Seega tuleks alati vältida võõra omaniku olemasoleva skeemi muutmist. Oma skeemiobjektide loomiseks saab aadressilt www.iana.org taotleda isikliku nimeruumi. Väljastatud OID-alusnumbri alla tohib luua isiklikke harusid. Kui kataloogiteenus on peamiselt ette nähtud IT-ressursside haldamiseks, tuleks puustruktuuri ülesehitamisel pöörata piisavalt tähelepanu sellele, et struktuur saaks kohandatud vastavalt administratiivsetele oludele. Organisatsiooni struktuuri ei tohiks puustruktuuris liiga detailselt imiteerida, kuna see võib tekitada probleeme kataloogiteenuse administreerimisel. Puustruktuur ei tohiks olla liialt ühetasandiline, kataloogipuu osasid peaks saama tükeldada erinevateks partitsioonideks ja jaotada neid selle põhjal võrgus erinevatele serveritele. Lisaks on selle puhul eeliseks, et kataloogiteenuse serverite vahel asetleidev replikeerimine ei mõjuta kogu puud (vt M 2.409 Kataloogiteenuse partitsioonide loomise ja replikeerimise planeerimine). Kui kataloogiteenuseid kasutatakse mitmel erineval otstarbel, tuleks kataloogi andmeid võimalusel hoida vastavalt andmete turbevajadusele kataloogiteenuse serveri eraldatud alades. Erineva turbevajadusega alad kergendavad muuhulgas andmete varundamist ja juurdepääsukaitse korrektset konfigureerimist. Lisaks sellele ei tohiks otsese internetiühendusega varustatud kataloogiteenuse serveris hoida andmeid, millele ei tohi väljast ligi pääseda. Kataloogiteenuse planeerimise raames tuleb arvestada järgnevate aspektidega:

- Milline on kasutusotstarve, millised on ülesanded ja millist infot peab kataloogiteenus sisaldama?
- Milline peaks olema liigitus asukohtade, organisatsioonide, organisatsiooni allüksuste ja muudesse objektide lõikes?
- Milliseid objektiklasse on vaja ja millised peavad olema nende kohustuslikud või vabalt valitavad atribuudid?
- Milliseid infole ligipääsuks vajaminevaid pääsuõigusi tuleks kasutajatele võimaldada kataloogiteenuse erinevate liideste kaudu?
- Millised on planeeritud meetmed, et kaitsta tõhusalt kataloogiteenuse andmeid volitamata andmekogumise eest, nt LDAP-pakettide allkirjastamine?

Üldjuhul tuleb planeeritud kataloogiteenuse struktuur alati täielikult dokumenteerida. See aitab tagada stabiilsust, järjepidevat ühesugust administreerimist ja sellega ka süsteemi turvalisust. Eriti täpselt tuleb fikseerida:

- Milliseid objektiklasse kasutatakse millisel moel ja milliseid atribuute kasutatakse millise sisu jaoks?
- Milliseid skeemitäiendusi tehakse ja mis põhjusel?

Iga kataloogiteenuse objekti puhul peab olema dokumenteeritud:

- Nimi ja asukoht kataloogiteenuse puus näiteks “AsukohtTartu”, isa-objekt: OU “BSI”,
- Millena seda objekti rakendatakse, näiteks võrguprinterina,
- Millised administratiivsed pääsuõigused tuleb määrata objektile ja selle atribuutidele, (nt täielikult hallatud “Admin1” poolt) ja
- Kuidas konfigureerida kataloogiteenuse õiguste pärimist, nt kas õiguste pärimise blokeerimise või filtreerimise abil.

Isikuandmetega ümberkäimine kataloogiteenuses

Isikuandmeid sisaldava kataloogiteenuse planeerimisse tuleks kaasata ka asutuse andmekaitsega tegev osapool, et arvestada võimalikult varakult ka selliste andmekaitseaspektidega, mis käsitlevad informatsiooni kasutamist isikliku määramise õiguse vaatepunktist. Protsessi tuleks õigeaegselt kaasata ka töötajate esindus. Täpselt nagu teistele kataloogiteenuste andmetele, kehtib ka isikuandmetele nõue, et kataloogiteenuse sissekannete konfidentsiaalsust ja terviklust on tarvis kaitsta ja samas tuleb tagada ka nende käideldavus ja aktuaalsus. Lisaks üldistele meetmetele tuleb kataloogiteenuste kasutamisel arvestada järgnevaga:

- Isikuandmetega seotud sissekanded peaksid kataloogiteenuses piirduma konkreetse kasutusotstarbe jaoks vajaliku infoga. Asutusesisese kataloogiteenuse puhul võivad selleks olla meiliaadressid, telefoninumbrid, faksinumbrid või avalikud võtmed. Kui see pole ülesannete täitmiseks ilmtingimata vajalik, ei tohiks asutusevälise võrguga ühendatud kataloogiteenuses hoida näiteks infot, mis kajastab isikute tööülesandeid, tööaegu ja tööasukohti. Rämpsposti vältimiseks tuleks hoolikalt läbi mõelda, kas ja millisel kujul tuleks kataloogiteenuses kajastada meiliaadresse.
- Üldiselt tuleb alati tagada, et juurdepääs infole, mis sisaldab isikuid kajastavaid sissekandeid, peaks olema piiratud vastavalt tööülesannete täitmiseks vajaminevale määrale.
- Kui kataloogiteenust soovitakse kasutada personali kajastava infosüsteemi baasina, tuleb planeerimisse kaasata töötajate esindus.
- Kui kataloogiteenust või selle osi võimaldatakse kasutada ka väljaspool asutuse intranetti, näiteks teiste asutuste või äripartnerite andmetega varustamiseks, tuleb arvestada üldkehtivate andmekaitsemäärustega.

Kataloogiteenuse administreerimise planeerimine ja rakendatava administratiivse mudeli planeerimine on tähtsad ülesanded (vt M 2.407 Kataloogiteenuste administreerimise planeerimine). Personali planeerimise osas tuleb välja selgitada, kui palju töötajaid on vaja kataloogiteenuse ülesehitamiseks ja tööshoidmiseks ning milline peab olema nende töötajate väljaõpe. Kui vajamineva väljaõppega töötajaid on vähe, tuleb õigeaegselt võtta kasutusele vajalikud koolitusmeetmed (vt M 3.62 Kataloogiteenuste administreerimise koolitus).

Täiendavad kontrollküsimused:

- Kas kataloogiteenuse kasutuselevõttu planeeriti hoolikalt?
- Kas kõikide planeeritud objektide puhul on kindlaks määratud nende täpne kontekst kataloogipuus?
- Kas planeerimisse on kaasatud kõik puudutatud osapooled? Kas kataloogiteenuse planeerimisse kaasati muuhulgas ka andmekaitsespetsialist?
- Kas kataloogiteenuse jaoks on välja töötatud sobiv volituste kontseptsioon?
- Kas planeeritava kataloogiteenuse struktuur on dokumenteeritud?
- Kas on planeeritud rakendada meetmeid, mis suudaksid tõhusalt takistada kataloogiteenuste andmete volitamata kogumist?
- Kas kataloogiteenusesse salvestatud isikuandmete kasutamine on reguleeritud?

M 2.404 Kataloogiteenuse turvakontseptsiooni koostamine

Algatamise eest vastutavad: IT-juht, infoturbejuht

Rakendamise eest vastutavad: IT-turvalisuse eest vastutav töötaja

Kataloogiteenuse jaoks tuleb koostada turvakontseptsioon. Sellega määratakse, milliseid teenuseid, komponente jne peab kasutama ja milliseid tohib kasutada. Järgnev nimekiri annab kokkuvõtliku ülevaate erinevatest valdkondadest, mida vastav kontseptsioon peaks reguleerima. Antud nimekirja tuleb kohandada ja täiendada vastavalt konkreetsetele kasutusvaldkondadele. Vastavad spetsiaalsed turbealased ettekirjutused peavad olema kooskõlas asutuse üldise turvakontseptsiooniga.

Üldinfo:

- Kuidas tuleks kataloogiteenuse servereid füüsiliselt kaitsta?
- Milliseid kataloogiteenuse komponente tohib kasutada?
- Milliseid tööriistu tuleks kasutada administreerimisel?
- Kuidas toimub kataloogiteenuse puu struktureerimine ja partitsioonidesse jaotamine?
- Millises ulatuses millisel ajahetkel tohib teha skeemimuudatusi?
- Milliseid objektiklasse tohib kasutada erinevate võimalike atribuudikogumitega?
- Millised erinevat tüüpi replikeerimised peaksid aset leidma?
- Millised arvutid on kataloogiteenuse serveriks ja millised arvutid peaksid sisaldama replikatsiooni?
- Millised arvutid on juurdomeenid ja vajavad seetõttu spetsiaalset kaitset?

Volituste jagamine:

- Millised on erinevatele kasutajatele jagatavad õigused?
- Millised volitused antakse erinevatele administraatoritele?
- Milliseid autentimismeetodeid tuleks kasutada?
- Kuidas toimub õiguste pärimine puustruktuuri raames?

Haldamine:

- Millised on loodavad administraatorirollid?
- Kes ja millal tohib skeemi muuta?
- Milliseid administreerimisülesandeid tohib või peab delegeerima?

Andmeside:

- Milline andmeside peab toimuma turvatult?
- Milliste mehhanismidega tagatakse andmete käideldavus, konfidentsiaalsus ja terviklus?

Sertifikaadi autentsus:

- Milliseid parameetreid tuleks kasutada sertifitseerimisüksuste jaoks?
- Kellel lubatakse sertifitseerimisüksuse seadistusi muuta?
- Millised objektid tuleb varustada sertifikaatidega?

- Milliseid sertifikaate tuleb kasutada SSL-ühenduste jaoks?

Kasutatava operatsioonisüsteemi failisüsteem:

- Millised süsteemifailidega seotud volitused peaksid olema erinevatel administraatoritel ja kasutajatel?
- Kas krüpteerimist tuleks kasutada failisüsteemi tasandil?

LDAP:

- Millised kasutajad tohivad millistel tingimustel kataloogiteenusele ligi pääseda LDAP vahendusel?
- Kas anonüümset sisselogimist tuleks võimaldada või mitte?
- Millised võrgurakendused tohivad kataloogiteenust kasutada LDAP vahendusel?
- Kas LDAP-side peaks üldjuhul aset leidma SSLi kaudu?
- Kas kasutajate paroole tohib edastada loetava teksti kujul?

Kataloogiteenuse klient-juurdepääsud:

- Milliseid autentimisprotseduure tuleks kasutada või lubada?
- Millisele kataloogipuule tohib ligi pääseda võrgust?
- Millistele ressurssidele võimaldatakse erinevatel kasutajatel ligi pääseda võrgu kaudu?

Atribuutide krüpteerimine

- Kas atribuute tuleks krüpteerida või mitte?

Kaugpääs süsteemiseireks ja administreerimiseks:

- Kas kaughoolduseks tohib kasutada tarkvaratööriista?
- Kes tohib selliseid tarkvaratööriistu kasutada?
- Kuidas konfigureeritakse selleks otstarbeks HTTPS protokoll?

Kirjeldatud punktid tuleb detailsemalt välja töötada kataloogiteenuste turvapoliitikas (vt M 2.405 Kataloogiteenuse turvapoliitika koostamine).
Täiendavad kontrollküsimused:

- Kas kataloogiteenuste jaoks on koostatud turvakontseptsioon?
- Kas vastav turvakontseptsioon on kooskõlas kogu asutust hõlmava turvakontseptsiooniga?

M 2.405 Kataloogiteenuse turvapoliitika koostamine

Algatamise eest vastutavad: IT-juht, infoturbejuht

Rakendamise eest vastutavad: IT-juht, administraator

Kataloogiteenuse kasutuselevõtu planeerimise järgmiseks organisatoorseks ülesandeks on turvakontseptsioonist (vt M 2.404 Kataloogiteenuse turvakontseptsiooni koostamine) lähtuva kataloogiteenuse turvapoliitika väljatöötamine. Turvapoliitika määrab, millised konkreetsed turvanõuded peavad kataloogiteenuse süsteemis kehtima ja kuidas tuleb neid paigaldamisel ja käitamisel rakendada. Kataloogiteenuse turvapoliitika peaks reguleerima kõiki kataloogiteenuse turvalisust puudutavaid teemasid. Käesoleva, komponentidest lähtuva teemaloetelu saab seada järgnevasse ajalisse järjestusse:

1. Kataloogiteenuse puustruktuuri defineerimine

Esimese sammuna tuleb määrata kataloogiteenuse puu loogiline struktuur, jaotumine organisatsiooniks (mis vastab juurelemendile ja seega puu kõrgeimale elemendile) ja organisatsiooniüksusteks (*Organizatio-nal Units*, lühend OU) samuti tuleb määrata kindlaks serverite ja hallatavate võrguressursside jaotumine (vt M 2.403 Kataloogiteenuste kasutuselevõtu planeerimine). Seejärel tuleb määrata kataloogiteenuses hoitavate objektide ning nende atribuutide liik ja kogus. Vajadusel tuleb selleks muuta kataloogiteenuse skeemi. Lisaks tuleks siinkohal määrata kataloogiandmete jaotamine partitsioonidesse ja replikatsioonide tegemine (vt M 2.409 Kataloogiteenuse partitsioonide loomise ja replikeerimise planeerimine).

2. Vastutusalade reguleerimine

Kataloogiteenust peaksid käitama ainult koolitatud võrguadministraatorid. Avariiolukorraks valmisoleku planeerimise raames tuleb tagada sobivate asendajate olemasolu. Üldjuhul tuleks kataloogiteenuse käitamiseks luua rollipõhise administreerimise kontseptsioon. Kataloogiteenuse turvaparameetreid tohivad muuta ainult volitatud administraatorid. Kataloogi üksikute kasutajate vastutusalad on toodud tekstis allpool.

3. Nime andmise põhimõtete määramine

Kataloogipuu haldamise kergendamiseks tuleb määrata nime andmise põhimõtted, et serverite, rakenduste, printerite, kasutajate, kasutajagruppide ja muude kataloogiteenuse objektide jaoks kasutataks nimesid, mis on kõigile üheselt mõistetavad.

4. Kasutajakontode reeglite määramine

Enne kasutajakontode sisseseadmist tuleb määrata piirangud, mis kehtivad kas kõikidele või ainult teatud kontodele. Eriti puudutab see paroolide kasutamist ja süsteemi reageerimist sisselogimiskatsetel esinevatele vigadele. Lisaks tuleks reguleerida sisselogimisskriptide koostamist.

5. Kasutajagruppide sisseseadmine

Halduse lihtsustamiseks tuleks samade nõuete alla kuuluvad kasutajaobjektid koondada ühtsetesse kasutajagruppidesse. Kasutajate õigused ning kataloogiobjektide ja ka muude eeldefineeritud funktsioonidega seotud pääsuõigused määratakse sellisel juhul juba gruppidele, mitte enam üksikutele kasutajaobjektidele. Kasutajaobjektide õigused ja volitused määrab kasutajagrupp, mille alla nad kuuluvad. Näiteks kõik ühe osakonna töötajad on võimalik koondada ühte kasutaja-

gruppi. Kasutajavolitusi tuleks jagada kasutajatele ükshaaval ainult siis, kui see on erandkorras vältimatu.

6. Logimisnõuete määramine

Siin tuleb määrata, millised kataloogiteenuse poolt loodavad sündmused vajavad logimist ja millise sündmuste kombinatsiooni korral tuleb teavitada administraatoreid. Lisaks tuleb otsustada, kui kaua tuleks sündmusi kajastavaid andmeid säilitada.

7. Andmesalvestuse reeglid

Tuleb kindlaks määrata kasutajaandmete salvestamise koht ja meetod, kuidas neid andmeid kaitstakse (vt M 2.138 Struktureeritud andmetalletus). Andmeid ei tohiks salvestada üksikute klientide lokaalsetele kõvaketastele. Andmete salvestamise küsimus tuleb selgitada üksikute partitsioonide tasandil. Andmeid tuleb liigitada vastavalt nende kaitsevajadusele, vastavalt peab ka kataloogi partitsioneerimine toimuma usaldusväärsete ja kaitstud *host* 'idele. Eriti tuleb seejuures arvestada ülimalt konfidentsiaalsete andmetega.

8. Projektikaustade sisseseadmine

Kasutajat ja projekti puudutavate andmete (objektide) kindla eraldamise tagamiseks tuleks määrata sobiv kataloogistruktuur, mis toetab objektide eraldi hoidmist.

9. Pääsuõiguste määramine

Kataloogiteenuste objektide jaoks tuleb kindlaks määrata, milliseid atribuute töö jaoks lubada ja millised pääsuõigused tuleks neile määrata.

10. Klient-server võrgu administraatorite ja kasutajate vastutusalad

Lisaks võrguhaldusülesannetele tuleb kataloogisüsteemi puhul kindlaks määrata üksikute administraatorite vastutusalad. Erinevad vastutusalad võivad olla näiteks:

- kataloogiteenuse puu või üksikute partitsioonide haldamine
- skeemidefinitsiooni haldamine,
- sertifitseerimisüksuse ja võtme-objektide haldamine,
- üksikute serverite või klientide logifailide analüüsimine,
- pääsuõiguste andmine ja
- paroolide deponeerimine ja vahetamine ning andmete varundamine.

Ka kasutajad peavad klient-juurdepääsuga kataloogiteenuse kasutamisel teatud vastutuse enda kanda võtma, eriti kui neile antakse õigused administratiivsete funktsioonide täitmiseks. Tavaliselt piirdub see siiski ainult endale määratud kataloogiteenuse paroolide vastutustundliku hoidmisega.

11. Koolitus

Lõpuks tuleb kindlaks määrata, milliseid kasutajaid on tarvis erinevate teemade vallas koolitada. Alles pärast piisavat koolitust hakata kataloogiteenust igapäevaselt kasutama. Eriti põhjalikult tuleb kataloogiteenuse haldamise ja turvalisuse osas koolitada administraatoreid.

Loodud turvapoliitika tuleb dokumenteerida ja edastada vajalikus mahus kataloogiteenuse kasutajatele. Kataloogiteenuste turvapoliitika koostamisel tuleb jälgida, et see oleks kooskõlas asutuse olemasolevate turvapoliitikatega, ei läheks nendega vastuollu (sisuline ühtsus) ja ei satuks konflikti olemasolevate seadustega. Tavaliselt kohandatakse või täiendatakse kataloogiteenuse turvapoliitika abil vastavalt vajadusele olemasolevaid regulatsioone, nt komponentidele esitatavaid

täiendavaid nõudeid. Sealjuures tuleb sõltuvalt olukorrast võtta vastu uued, kataloogiteenuse funktsioone puudutavad reeglid. Üldjuhul peab kataloogiteenuse planeerimine lähtuma turvapoliitikatest, mõjutades samal ajal ka ise vastavaid turvapoliitikaid (feedback -protsess).

Täiendavad kontrollküsimused:

- Kas turvapoliitikad käsitlevad kõiki kataloogiteenuse jaoks planeeritud olulisi kasutusvaldkondi?
- Kas kõiki kasutajaid on informeeritud kataloogiteenusele kehtivate turvapoliitikate kohta?

M 2.406 Kataloogiteenuste kasutamiseks sobivate komponentide valik

Algatamise eest vastutavad: IT-juht, infoturbejuht

Rakendamise eest vastutavad: IT-juht

Kataloogiteenuse planeerimise ja kontseptsiooni loomise faasis defineeriti teenuse kasutusotsarve ja rakendusvaldkonnad ning määratleti kasutamiseks vajalikud turvapoliitikad. Kui kataloogiteenuse kasutusnõuded on kindlaks määratud, tuleb selle teenuse kasutuselevõtmiseks välja valida sobivad komponendid. Eriti kehtib see ostetava tarkvara kohta. Nõuetele peavad loomulikult vastama ka vajaminev riistvara koos operatsioonisüsteemiga ja võrgu infrastruktuur.

Kataloogiteenuse tarkvara valimine

Kataloogiteenuste tarkvara toodavad paljud erinevad firmad ja see on saadaval erinevate platvormide jaoks. On olemas nii tasulisi tooteid kui ka tasuta variante. Praktiliselt kõik tuntud kataloogiteenused põhinevad tänapäeval LDAP-standardil.

Alljärgnevas nimekirjas on toodud mõned näited, see ei sisalda tootehinnanguid ja pole täielik:

- Novell-võrkudes rakendatav eDirectory, endine NDS
- Fedora Directory Server, mida toetab Red Hat
- OpenLDAP (avatud lähtekoodiga tarkvara erinevatele operatsioonisüsteemidele)
- Apple Open Directory, mida rakendatakse Mac OS X serverites
- IBM Tivoli Directory Server
- Sun Java System Directory Server
- Network Information Service (NIS) Unixi võrkudes (ei põhine LDAP protokollil)

Kataloogiteenused võivad olla juba operatsioonisüsteemi integreeritud, näiteks Active Directory on liidetud Windows Server tarkvarasse, aga võib olla saadaval ka eraldiseisvate tarkvarakomponentidena erinevate operatsioonisüsteemide nagu OpenLDAP, või Java-platvormile nagu nt Sun Java System Directory Server.

Liideste ühilduvus

Kataloogiteenuse tarkvara soetamisel on oluliseks kriteeriumiks asjaolu, et tarkvara peab ühilduma rakendustega, mida hakatakse kataloogiteenuses vastavalt planeerimisfaasis langetatud otsustele kasutama. Siinkohal tuleb eriti hoolikalt vaadelda neid liideseid, mida kataloogiteenus peaks hakkama pakkuma. Üldjuhul järgivad praktiliselt kõik saadaolevad kataloogiteenused standardit LDAPv3.

LDAP-standardile on siiski võimalik teha ka tootepõhised täiendusi. Muudatused võivad kõne alla tulla nii funktsioonides kui ka konkreetsetes turvaomadustes.

LDAP täiendamisvajaduse korral tuleb kontrollida, kas kataloogiteenuse tarkvara pakub ka neid. Lisaks võivad soetamisel olla valikukriteeriumiteks täiendavad liidesed, kui need on kataloogiteenuse efektiivse kasutamise seisukohalt olulised.

Kataloogiteenuste sellised liidesed on näiteks Extended Markup Language (XML), Directory Services Markup Language (DSML) ja Simple Object Access Protocol (SOAP) samuti tasulised Active Directory Service Interfaces (ADSI) ja

Novell Directory Access Protocol (NDAP). Kataloogiteenuse käideldavuse tagamiseks tuleb tuvastada nõuded, mida esitavad kataloogiteenusele rakendused ja nende kasutajad.

Iga nõude puhul tuleb tagada, et kataloogiteenus suudaks vastavate päringute töötlemisega toime tulla. Kui kliendil läheb tarvis lisakomponente, tuleb soetamise protsessi kaasata ka need valikukriteeriumid.

Turvanõuete täitmine

Kataloogiteenuse planeerimise ja kontseptsiooni loomise raames sõnastati kasutusotstarbest lähtuvad nõuded teenuse turvalisusele.

Seega tuleks kataloogiteenuse realiseerimiseks vajalike tarkvarakomponentide valimisel püstitada vähemalt järgnevad küsimused:

- Kas vaatluse all oleva tootega saab kõiki administratiivseid ülesandeid delegeerida või jaotada selliselt, et need vastaksid seatud nõuetele ja vajadusel ka tuleviks läbiviidavatele planeerimistele? Kas üksikute administraatorigruppidega seotud õigusi saab seadistada sellise täpsusega, et nende puhul saaks piirduda ainult tööks vajalike pääsuõiguste jagamisega? Kas kataloogiteenusega seotud administratiivsete protseduuride konfidentsiaalsust ja terviklust saab piisavalt kaitsta?
- Kas kataloogiteenuse kasutajate autentimiseks on olemas piisavalt tugevad mehhanismid, mis vastavad asutuse nõuetele?
- Kas asukohtade ja kasutajate vahel toimuvates andmeedastustes on tagatud andmete konfidentsiaalsuse säilimine?
- Kas kataloogiteenuse komponendid pakuvad piisavat tuge olukorras, kus autentimiseks, krüpteerimiseks, digitaalallkirjade jaoks või PKI kasutuse raames läheb tarvis elektroonilisi sertifikaate?
- Kas kataloogiteenuse multi-master replikeerimine on vajaduse tekkimisel võimalik? Kas kataloogiteenuse tarkvara toetab multi-master replikeerimist kõikidel nõutud tasanditel? Erinevalt master-slave installatsioonist on multi-master replikeerimisel mitu master -serverit, mis võtavad vastu ja töötlevad rakenduste või nende kasutajate päringuid. Selleks pöördutakse alati päringu esitaja suhtes kõige lähima master -serveri poole. Multi-master tööreżiimi on soovitatav kasutada eeskätt selliste kataloogiteenuse struktuuride puhul, mis asuvad üksteisest ruumiliselt kaugel. Kõikidel juhtudel tuleb tagada, et master -serverite vahel toimuks regulaarne replikeerimine, sest kõik master' id peavad sisaldama kataloogiteenuse täielikku andmekogumit. Seetõttu on multi-master tööreżiimi halduskulud suuremad.

Koolitus ja edasine tugi

Kataloogiteenuse turvalise paigaldamise, konfigureerimise ja käitamise tagamine nõuab administratiivpersonalilt piisavat kompetentsi. Seega tuleb kataloogiteenuse tarkvaratoodete valimisel jälgida, kas tootja või mõni sõltumatu teenuseosutaja pakub nende jaoks sobivaid koolitusi. Kui kataloogiteenuse töö käigus esineb keerukamaid probleeme, võib osutuda vajalikuks kasutada tootja või kolmanda osapoole laialdasemat tugiteenust.

Seega tuleks kataloogiteenuse komponentide soetamisel mõelda sobivate tugilepingute või teenusetasemelepete (SLAde) sõlmimisele. Vajalikud koolitused ja tugiteenused tuleb kaasata kataloogiteenuse üldkulude arvutustesse.

Tarkvaratööriistad

Kataloogiteenuste administreerimiseks ja andmete haldamiseks pakutakse tavaliselt mitmeid erinevaid tarkvaratööriistu. Kataloogiteenuse valimisel tuleks seega kindlaks määrata, kas on olemas ka sobivad tarkvaratööriistad, mis toetaksid vastava kataloogiteenuse administreerimist. Lisaks tuleks uurida, kas võimalikud tarkvaratööriistad suudavad täita neile esitatud nõudeid.

- Kas tarkvaratööriistad toetavad piisavas ulatuses kataloogiteenuse ja selle andmete haldamist? Kas administreerimist toetatakse paigaldamisel, konfigureerimisel ja käitamisel piisavas mahus vastavalt kataloogiteenuse keerukusele, et vältida vigu ja eksimusi?
- Juhul kui otsustatakse vastavad tarkvaratööriistad kasutusele võtta, kas sellistel tingimustel on võimalik muuta administreerimiseks ja seireks rakendatavaid juurdepääsud ja liidesed piisavalt turvaliseks?

Skaleeritavus

Kataloogiteenuse käideldavuse tagamisel on oluline ka selle aluseks oleva andmebaasi jõudlus.

- Kas kataloogiteenus on piisavalt skaleeritav?
- Kas kataloogiteenuse struktuurid ja selle võimalike sissekannete hulk on sellised, et need suudaksid täita ka võimalikke tulevikus esilekerkivaid vajadusi?

Riistvara

Kui kataloogiteenuse jaoks ettenähtud riistvara või sellel töötav operatsioonisüsteem on juba olemas või mingil muul põhjusel eelnevalt kindlaks määratud, piirab see tavaliselt sobiva tarkvara valikut ja sellega tuleb arvestada. Teisalt, kui kataloogiteenus integreeritakse heterogeense riistvara- ja tarkvarasüsteemide maastiku hulka, peab kataloogiteenuse tarkvara seda toetama. Juhul kui loodava kataloogiteenuse tarbeks tuleb soetada uus riistvara ja/või operatsioonisüsteem, tuleb arvestada, et need täidaks jõudlusele ja salvestusmahule seatud nõudmisi, kuna sellest sõltub võime tagada kataloogiteenuse käideldavust ja andmete terviklust (vt M 2.317 Serveri soetamise kriteeriumid)

Võrgud

Sama kehtib ka võrgu infrastruktuuri puhul. Kui on plaan kasutada olemasolevaid võrke koos etteantud ribalaiustega, tuleb valida sellised kataloogiteenuse komponendid, et kataloogiteenusele esitatavate päringute korral toimuks võrgukoormuse jaotamine selliselt, et see ei seaks ohtu teenuse käideldavust. Uue võrgu planeerimisel või olemasoleva täiendamisel tuleb tagada sellised sideühendused, et need vastaksid analüüsi põhjal eeldatavale kataloogiteenusega seotud võrguliiklusele.

Kontrollküsimused:

- Kas on olemas kriteeriumite kataloog, milles alusel valitakse ja soetatakse kataloogiteenuseks vajalikke komponente?
- Kas Active Directory komponentide turvanõuded sõnastati lähtuvalt nende kasutusotstarbest?

M 2.407 Kataloogiteenuste administreerimise planeerimine

Algatamise eest vastutavad: IT-juht, infoturbejuht

Rakendamise eest vastutavad: IT-juht, administraator

Kataloogiteenuse haldamine nõuab hoolikat planeerimist. Selle käigus tuleks jälgida, et administratiivseid ülesandeid ja vastavaid administraatorite kontosid oleks võimalik teineteisest piisavalt lahutada. Enamikel juhtudel peaks kataloogiteenuse haldamine ja kataloogis sisalduvate andmete haldamine olema teineteisest lahutatud, nt seeläbi, et luuakse erinevad administratiivsed rollid nagu teenuste haldamine ja andmete haldamine, mis seotakse omakorda erinevate vastutusaladega.

Teenuseadministraatorid

Teenuseadministraatorid peaksid hoolitsema kogu kataloogiteenuse käigushoidmise, kogu kataloogi hõlmavate seadistuste, tarkvara paigaldamise ja hooldamise, samuti kataloogiteenuse serveritele operatsioonisüsteemi paigaldamise eest.

Andmeadministraatorid

Andmeadministraatorid peaksid jällegi vastutama selliste andmete haldamise eest, mis on salvestatud kataloogiteenusesse ja seega kataloogiteenuse serveritele. Neil ei tohiks olla võimalust kataloogiteenust seadistada ega ka seda kättesaadavaks teha. Lisaks ei tohiks andmeadministraatorid vastutada kõikide kataloogiteenuse andmete eest. Tavaliselt haldavad nad kataloogiteenusest ainult teatud objektide hulka. Sel põhjusel tuleks konkreetse administraatorikonto haldusvõimalusi piirata ja lubada tal tegelda ainult teatud kindlate kataloogiteenuse osadega, milleks tuleb kataloogiteenusesse objektide kohta salvestatud pääsuloendites (*Access Control List* 'ides) teha vastavad seadistused. Osa infot, mis on vajalik kataloogiteenuse haldamiseks või konfigureerimiseks, juhivad kataloogiteenuses olevad objektid automaatselt ise. Vaatamata sellele, et vastav info nagu nt usaldussuhted, skeemid või replikeerimisreeglid on kataloogiteenuses salvestatud kujul olemas, peaksid teenuseadministraatorid seda infot siiski ka haldama. Sel põhjusel lubatakse teenuseadministraatoritel täita ka andmeadministraatorite ülesandeid, kuid mitte vastupidi.

Rollipõhine administreerimine ja delegeerimine

Lisaks sellele võib kataloogiteenuse jaoks planeerida ka ulatusliku administratiivse mudeli kasutuselevõtmist. Rollipõhise administreerimise juurutamine ja administreerimisülesannete delegeerimise võimalus mõjutavad kataloogiteenuse turvalisust ja vajavad seetõttu erilist tähelepanu. Turbega seotud administreerimisülesannete mõistlik, ülevaatlik ja läbivalt ühtmoodi kujundamine tagab muuhulgas ka süsteemi parema läbipaistvuse ja tõstab selle efektiivsust. Kataloogiteenuse administreerimise planeerimise raames tuleb igas institutsioonis vastata järgnevatele küsimustele:

- Milliseid administraatorigruppe vajatakse?
- Millist administratiivset mudelit tuleks rakendada? Tsentraalne või detsentraalne haldus?
- Millised administratiivsed rollid peaksid eksisteerima puustruktuuris?
- Kas administratiivseid ülesandeid peaks saama delegeerida? Kellele?

- Millistele objektidele tohivad kataloogiteenuse erinevate liideste kaudu ligi pääseda erinevad administraatorid?

Kataloogiteenuse administreerimise planeerimisel tuleks arvestada järgnevate turbeaspektidega:

Selged volitusstruktuurid

- Delegeerimiseks määratakse pääsuõigused kataloogiteenuse objektidele ja nende atribuutidele. Puustruktuuri osaks olevate objektide haldamiseks kasutatakse siinjuures tavaliselt pärimismehhanismi. Delegeerimise ja õiguste pärimise puhul tuleks vältida keerukaid lahendusi. Keeruliste lahenduste kohta võib kiiresti kaduda ülevaade, nende haldamisvõime võib kahaneda miinimumini ning see omakorda võib viia väärkonfiguratsioonidest tulenevate turvalünkade tekkimiseni.
- Tavaliselt on standardina kataloogiteenuse esmasel paigaldamisel süsteemi poolt sisse seatud üldadministraator, kellel on täielik juurdepääs kõikidele kataloogiteenuse objektidele. Selline lahendus tuleks esmakordse paigaldamise käigus ära muuta. Pääsuõiguste jagamine peaks toimuma eelnevalt kehtestatud administratiivse mudeli alusel.
- Administratiivsete rollide delegeerimise rakendamisel tuleks administraatoritele jagada ainult sellised õigused, mis on vajalikud delegeeritud administratiivsete ülesannete täitmiseks.
- Eriti hoolikalt tuleks seetõttu oma laiaulatuslike volituste pärast kaitsta administratiivset juurdepääsu kataloogiteenuse esimesse, st kõrgeimasse tasandisse. Kõrge kaitsevajaduse korral tuleks seevastu kaaluda lahendust, mis võimaldaks vastavat juurdepääsu kasutada ainult kas nelja silma põhimõtte või jagatud parooli alusel.
- Skeemimuudatused on ülimalt kriitilise tähtsusega operatsioonid ja kui üldse, tohivad neid teha ainult volitatud administraatorid pärast seda, kui vajalikud tööd on hoolikat ette planeeritud. Muudatused tuleb täpselt dokumenteerida.
- Juhul kui kataloogiteenuse alla integreeritakse oma sertifitseerimisüksus (*Certification Authority* , CA), tuleb selle tööd ja administreerimist planeerida vastavalt eelnevalt kehtestatud turvapoliitika nõuetele.
- Administratiivsed tegevused tuleb delegeerida selliselt, et ülesannete kattumine oleks võimalikult välistatud. Vastasel korral võivad kaks administraatorit teha vastuolulisi muudatusi, mis võivad põhjustada konflikte replikeerimises. Mittekattuvate volitustega administreerimismudeliga saab vähendada replikeerimiskonfliktide ohtu. Võimalike või juba esinenud replikeerimiskonfliktide puhul tuleks regulaarselt ja ka pärast olulisi muudatusi väärtused käsitsi üle kontrollida.

Dokumentatsioon

- Administratiivse delegeerimise mudel ja sellest tulenev õiguste andmine tuleb dokumenteerida.

- Suurte kataloogiteenuste puhul tasuks kaaluda tarkvaratööriista toega haldamist. Praktiliselt kõikide kataloogiteenuste jaoks on olemas erinevad tasulised ja tasuta tarkvaratööriistad. Tarkvaratööriistade rakendamisel tuleb neid turvaliselt konfigureerida ja käitada.

Täiendavad kontrollküsimused:

- Kas kataloogiteenuse enda ja selle andmete haldamisega seotud administratiivsed ülesanded on teineteisest rangelt lahutatud?
- Kas on sisse seatud rollipõhine administreerimine ja võimalus üksikute administreerimisülesannete delegeerimiseks? Kas administratiivse delegeerimise mudel on vaba kõikvõimalikest kattumistest?
- Kas kõik administratiivsed valdkonnad ja volitused on piisavalt dokumenteeritud?

M 2.408z Kataloogiteenuste üleviimise planeerimine

Algatamise eest vastutavad: IT-juht, infoturbejuht

Rakendamise eest vastutavad: IT-juht, administraator

Sageli ei tegeleta sugugi mitte täiesti uue kataloogiteenuse ülesehitamisega, kuna asutuse võrgus võib juba olemas olla mitu üksikut kataloogiteenust, mis võivad olla häälestatud ainult teatud rakenduste või protseduuride täitmiseks või mille teenused on saadaval ainult kusagil alamvõrgus. Viimane on eriti tõenäoline siis, kui organisatsiooni endised autonoomsed osad on liitumise käigus koondatud ühisesse võrku. Kataloogiteenuse üleviimine võib olla põhjendatud serverimaastiku ümberseadmisega uuele riistvarale, uuele operatsioonisüsteemile või olemasoleva operatsioonisüsteemi vahetamisega uuema versiooni vastu.

Kataloogiteenuste üleviimine nõuab kõikidel juhtudel hoolikat planeerimist, kuna ümberkorralduste tõttu võivad tekkida turvaaugud.

- Tagada tuleb andmete tervikluse säilimine. Puudutatud kataloogiteenuste andmetes ei tohi üleviimise tagajärjel tekkida soovimatuid muudatusi. Kui planeeritakse üleviimist, tuleb üle viia täielikult kõik kataloogiteenuse objektid.
- Tagada tuleb andmete konfidentsiaalsuse säilimine. Üleviimise käigus ja ka pärast selle lõppemist tuleb tagada, et andmetele ei oleks võimalik volitamata ligi pääseda.
- Lõpetuseks on oluline, et käideldavus oleks vajalikus mahus tagatud ka kataloogiteenuste üleviimise ajal kuni kataloogiteenus lülitub pärast edukat üleviimist tagasi tavarežiimi.

Erinevate üleviimisteede eelised ja puudused

Kataloogiteenuse üleviimiseks on olemas erinevad meetodid, mis erinevad üksteisest suuresti just täiendavate riistvara puudutavate nõudmiste osas:

1. Kataloogiteenuse värskendamine: selle ümberseadmisprotseduuri käigus paigaldatakse olemasolevatesse arvutitesse kataloogiteenuse värskendus (Update). Täiendav riistavara pole vajalik. Puuduseks on asjaolu, et asjassepuutuvat arvutit ei saa ümberseadmise ajal kasutada.
2. Täielik uuesti installeerimine: üleviimine leiab aset kataloogiteenuse infrastruktuuri paralleelse ülesehitamisega. Pärast installeerimist ja konfigureerimist võetakse uus kataloogiteenus igapäevasesse kasutusse. See ei mõjuta olemasolevat süsteemi ning üleviimise ajal on võimalik seda edasi kasutada. Selle variandi puuduseks on suur vajadus täiendava riistvara järele.
3. Jupikaupa üleviimine: See variant on võimalik, kui kataloogiteenus on jaotatud hierarhilisteks osastruktuurideks (partitsioonideks). Üleviidava partitsiooni jaoks luuakse esmalt paralleelne struktuur, mida hakatakse kasutama pärast edukat ülesehitamist.

Sel moel vabanenud riistvara saab kasutada järgmise osastruktuuri paralleelseks ülesehitamiseks. Üldist soovitust kataloogiteenuse üleviimismeetodi valimiseks ei saa siinkohal anda, kuna sobiv meetod sõltub olulisel määral konkreetsetest oludest ja tuleb valida lähtuvalt asutuse vajadustest.

Värskendamine ja restruktureerimine

Üleviimist on võimalik läbi viia ka kahes faasis. Esmalt võetakse olemasolevad kataloogiteenuse struktuurid üks ühele üle. Tegelikult on tegu ainult tarkvara või operatsioonisüsteemi värskendamisega vastavates kataloogiteenuse serverites. Selle meetodi probleemiks on mitmete puudujääkide säilimine ja asjaolu, et kataloogiteenus vajab turvalisuse põhjustel jätkuvalt konfigureerimist. Teises faasis toimub kataloogiteenuse restruktureerimine. Selle protseduuri puhul on enamasti tegu täiesti uue süsteemi ülesehitamisega. Eeliseks on võimalus asendada vanad ja raskesti administreeritavad struktuurid uutega. Lisaks saab kataloogiteenuses vajalikul moel kajastada ka organisatsioonis toimunud muudatusi. Sellele vaatamata tuleb siinkohal arvestada, et uue struktuuri planeerimine ja teostamine on tihti seotud suure ajakuluga.

Üleviimise kontseptsioon

Kataloogiteenuse üleviimisprotseduuri keerukuse tõttu tuleb eelnevalt luua vastav üleviimise kontseptsioon. Selle käigus tuleks ennekõike arvestada järgmiste punktidega:

- Kas kataloogiteenust on tarvis üleviimise raames käitada heterogeenses struktuuris korraga erinevate tarkvaraversioonide või operatsioonisüsteemidega Sellisel juhul tuleks kindlaks määrata, kas vastavat segarežiimi rakendatakse ainult kindlaksmääratud ülemineku ajal või püsivalt. Segarežiimi puhul tuleb jälgida, et üksikud komponendid oleksid omavahel ühilduvad, et tagada süsteemi käideldavus. Lisaks on oluline, et turvamehhanismid oleksid piisavalt tugevad kataloogiteenuse kasutajate autentimiseks, kataloogis olevate andmete konfidentsiaalsuse ja tervikluse tagamiseks, andmepäringute turbe tagamiseks ning vastaksid kataloogiteenusele esitatud nõuetele.
- Kas üleviimise käigus on tarvis teha muudatusi ka kliendi poolel? Sõltuvalt kataloogiteenuse üleviimise mahust saab muuta nt klient-kataloogiteenus suunal rakendatavat autentimisprotokolli. Kataloogiteenuse uute turvaomaduste kasutamiseks võib klientide üleviimine olla lausa vajalik.

Partitsioonide loomine ja replikeerimine

- Kas kataloogiteenuses on tarvis muuta partitsioonide loomise ja replikeerimise põhimõtteid? Selliste sügavatoimeliste muudatuste jaoks on oluline restruktureerimisprotsessi nõuetekohane planeerimine, eelkõige just siis, kui eesmärgiks on kataloogiteenuse jõudluse suurendamine.

Üleviimise planeerimine ja dokumenteerimine

Üleviimise üksikud etapid tuleb planeerida võimalikult detailselt, eesmärgiks seatud üleviimise protsess tuleb dokumenteerida ning kõikidele osapooltele tuleb tagada juurdepääs dokumentatsioonile. Üleviimisprotsessist ülevaate loomiseks võib esile tuua järgmised kohustuslikud etapid:

Tööde ajakava koostamine

- Üleviimise kohta tuleb koostada tööde ajakava, mida peab olema võimalik ka reaalselt täita. Üleviimise planeerimise käigus tuleb arvestada vajadusega, et tööde ajakava võib olla tarvis jooksvalt kooskõlastada.
- Üleviimise plaan peab määratlema kataloogiteenuse serveri ülemineku strateegia.

Üleviimise järjekord

- Kindlaks tuleb määrata kataloogiteenuse serverite üleviimise järjekord. Seejuures tuleb eriti hoolikalt arvestada serveriga, mis on kataloogiteenuse hierarhia juureks (root).
- Kui üleviimisega samal ajal peab toimuma klientarvuti üleviimine, tuleb ka selleks välja töötada õige järjekord. Kui klientide üleviimine toimub enne kataloogiteenust osutavate serverite üleviimist, tuleb pärast kataloogiteenuse üleviimist tavaliselt klienti veel kord konfigureerida. Vastupidise töödejärjekorra puhul tuleb jälgida kliendi ühilduvust kataloogiteenusega, et tagada selle käideldavus ja välistada turvaaukude tekkimine.

Volituste üleviimine

- Kui kasutajate ja kasutajagruppide haldamine baseerub üleviidaval kataloogiteenusel, tuleb arvestada sellega, et üleviimine võib mõjutada pääsuõiguseid. Kui üleviimise käigus muudetakse kasutajakontode autentimisatribuute nagu nt kasutajanime, tuleb tagada, et lubatud juurdepääse oleks võimalik edasi kasutada. Teisest küljest tuleb jällegi tagada, et ressurssidele ei pääseks enam ligi vanade autentimisatribuutidega.

Usaldussuhted

- Üleviimise ajal tuleb jälgida, et kataloogiteenuse erinevate osade vahel vajaminevaid usaldussuhteid loodaks õigesti. Tuleb planeerida, millises üleviimise faasis erinevad usaldussuhted kehtima peaksid.

Tarkvaratööriistade kasutamine

- Üleviimisprotsessi raames rakendatakse tavaliselt erinevaid üleviimistööriistu.

Enne üleviimist tuleb seega planeerida, kuidas rakendada võimalikke tarkvaratööriistu. Tuleb kindlaks määrata, milliseid tööriistu erinevates üleviimise etappides kasutatakse.

- Kui üleviimine nõuab laiaulatuslike volituste andmist, et tarkvaratööriistad pääseksid ligi vajalikule infole, tuleb arvestada, et selle tagajärjel võivad tekkida turvaaugud. Pärast seda, kui neid laiaulatuslikke volitusi enam ei vajata, tuleb need viivitamata tühistada. Samuti on soovitav nende volitustega loodud juurdepääsusid sobival moel jälgida.

- Tuleb kindlaks määrata üleviimise läbiviimise eest vastutavad isikud ja anda neile selleks piisavad volitused, mis on reeglina küllaltki laiaulatuslikud. Vastavatel juhtudel tuleb seetõttu jälgida, et üleviimisega hakkaksid tegelema ainult usaldusväärsed isikud. Muuhulgas tuleks üleviimise kontseptsioonis määratleda, milliste tööülesannete täitmisel tuleb ilmtingimata järgida nelja silma põhimõtet.

Testimisfaasi planeerimine

- Kõikidel juhtudel tuleks kataloogiteenuse üleviimise jaoks planeerida ka põhjalikud analüüsimis- ja testimisfaasid. Testid tuleks läbi viia isoleeritud testimisvõrgus.

Enne üleviimise algust tuleks kataloogiteenuse andmetest teha täielik varukoopia.

- Tuleb koostada avariiplaan, mis võimaldaks kataloogiteenust taastada üleviimisele eelnenud seisundis, et üleviimise võimaliku ebaõnnestumise korral saaks võimalikult kiiresti taastada töökorras süsteemi.

Lõpetav eesmärgi ja hetkeolukorra võrdlemine

- Pärast üleviimise lõpetamist on soovitav võrrelda kõikide turvaseadistuste puhul neile püstitatud eesmärke ja saavutatud hetkeolukorda ning eriti on soovitav analüüsida kataloogiteenusele ja seal hoitavatele andmetele määratud pääsuõiguste turvaseadistusi.

Meta-kataloogiteenus üleviimise asemel

Kui kataloogiteenuse üleviimise planeerimisel selgub, et vastav üleviimine oleks liiga aeganõudev või poleks teostatav ette antud aja jooksul, võib kaaluda nn meta-kataloogiteenuse rakendamist. Meta-kataloogiteenus loob kokkuvõtte teiste, juba olemasolevate kataloogiteenuste andmetest. See võimaldab mitut erinevat kataloogiteenust omavahel sünkroniseerida.

Realiseerimiseks on erinevaid võimalusi:

- Meta-kataloog toimib infoedastajana, pakkudes kõiki katalooge ühendatult nagu oleks tegu ainult ühe kataloogiga. Seetõttu nimetatakse seda ka virtuaalseks kataloogiks. Meta-kataloogiteenus pakub ühtset vaadet mitme ühendatud kataloogiteenuse infole, teenused ise saavad aga jätkuvalt oma isiklikke skeeme ja nimeruume kasutada. Siinkohal tuleb arvestada sellega, et vastav meta-kataloog sõltub ühendatud kataloogide pidevast olemasolust ning nende vahel tuleb luua sideühendused, mis suudaksid toime tulla suure hulga päringute ja neile antavate vastustega.

- Meta-kataloogiteenus, mis töötab keskse infosalvestina, võtab ühendatud kataloogiteenustest valitud info üle oma enda kataloogi. Luuakse metaobjektid, mis sisaldavad süsteemi aluseks olevate kataloogiteenuste kogutud atribuute.
- Jätkuva sünkroniseerimise võimaldamiseks on meta-kataloogiteenuse objektid seotud algkataloogidega. Jälgida tuleb, et see sünkroniseerimine toimuks kas sündmustepõhiselt või piisavalt suure sünkroniseerimissagedusega, mis suudaks tagada, et meta-kataloogiteenuse andmed oleksid võimalikult värsked.

Eelnevalt toodud aspektide loetelu tuleb käsitleda juhtnöörina sarnaste ja täiendavate küsimuste koostamisel, mida on tarvis esitada üleviimise kontseptsiooni väljatöötamise raames. Tuleb silmas pidada, et üleviimise plaani tuleb alati kohandada vastavalt konkreetsele situatsioonile, et kohapeal tekkivate nõudmistega oleks piisavalt arvestatud.

Kontrollküsimused:

- Kas üleviimiste jaoks on välja töötatud vastav kontseptsioon?
- Kas kataloogiteenuses tehtud skeemimuudatused dokumenteeriti?
- Kas pärast üleviimist tühistati kõik üleviimiseks vajalikud laiaulatuslikud volitused?

M 2.409 Kataloogiteenuse partitsioonide loomise ja replikeerimise planeerimine

Algatamise eest vastutavad: IT-juht, infoturbejuht

Rakendamise eest vastutavad: IT-juht, administraator

Skaleeritav kataloogiteenus võimaldab tükeldada kataloogiteenuse andmebaasi osasid partitsioonideks ja jaotada neid erinevatele kataloogiteenuse serveritele. See lühendab päringule kuluvat keskmist aega, kuna päringud ei tööta enam ilmtingimata läbi kogu olemasolevat kataloogipuud, vaid piirduvad konkreetse partitsiooniga. Lisaks suurendab see töökindlust, kuna ühe konkreetse serveri võimaliku tõrke korral on mõjutatud ainult sellel asuv partitsioon, aga mitte kogu kataloogiteenuse andmebaas. Lisaks võimaldab partitsioneerimine jaotada andmeid eelneva klassifikatsiooni alusel sobivalt turvaliseks muudetud serveritele. Partitsioneerimise planeerimisel tuleb arvestada kataloogiteenuse poolt defineeritud partitsioneerimisreeglitega. Partitsioonid võivad omakorda sisaldada alampartitsioone, mille loomisel tuleb samuti lähtuda kindlaksmääratud reeglitest. Lisaks kataloogipuu partitsioneerimise mehhanismile pakuvad kataloogiteenused võimalust kataloogipuu osasid teiste kataloogiteenuse serverite peale replikeerida. Kataloogiteenuste terminoloogia kohaselt nimetatakse replikeeritud osasid replikatsioonideks või reproduktsioonideks. Replikeerimise planeerimisel tuleb analüüsida eeldatavat võrguliiklust, et teha kindlaks nõuded sideühenduste ribalaiusele või kohandada replikatsioonide topoloogiat lähtudes etteantud võrguparameetritest.

Partitsioonide loomine

Partitsioonide planeerimisel tuleks arvestada järgnevate punktidega:

- Kaitsevajadus: Kataloogis sisalduv info tuleks jaotada erinevatesse klassidesse lähtuvalt selle kaitsevajadusest. Lähtuvalt klassidest tuleks objektid laiali jagada neile sobiva turbeastmega serveritele. Siinkohal tuleb eriti jälgida, et objektid, mis sisaldavad tundlikku infot, näiteks krüptograafilised võtmed, jagataks piisavalt turvaliste serverite alla.
- Kataloogiteenuse nõutav käideldavus: koormuse paremaks jaotamiseks peab kataloogiteenuse serveritel olema kataloogi andmetest piisavalt palju replikatsioone.
- Administreerimisülesannete jaotamine: selleks et administreerimisülesannetega seotud töörollide eraldamine langeks kokku andmete eraldamise põhimõttega, peaksid administreerimisülesanded olema ära jagatud üksikute partitsioonide lõikes.
- Kataloogiteenuse reeglid partitsioonide loomise kohta : kataloogiteenuse partitsioonide loomise reeglid tuleb kindlaks määrata ja nendest tuleb kinni pidada.

Oluliseimad reeglid on järgmised:

- Iga partitsioon algab hierarhiliselt üksiku konteinerobjektiga.
- Partitsiooni peab moodustama kataloogiteenuse puuga seotud alampuu (sub-tree).
- Erinevad partitsioonid ei tohi kattuda.
- Partitsiooni nimi peab olema partitsiooni juurobjekti FQDN (Fully Qualified Distinguished Name).

Replikeerimine
Replikatsioonide planeerimisel tuleb arvestada järgnevate punktidega:

- Kataloogiteenuse käideldavuse ja töökindluse nõuete põhjal on tarvis tuletada nõuded tehtavate replikatsioonide arvule.
- Koormusjaotuse planeerimise aluseks on süsteemilt nõutav jõudlus.
- Tuleb otsustada, kas filtrite defineerimisega replikatsioonide jaoks on võimalik saavutada suuremat turvalisust.

Mainitud võit turvalisuses tuleneb peamiselt võimalusest hoida andmeid teineteisest lahutatult, lähtudes eelnevalt läbiviidud andmete liigitamisest eri klassidesse. Sellega saab realiseerida põhimõtte, et iga kataloogiteenuse server sisaldab ainult neid andmeid, mida ta „vajab“ (st neid, mida vajavad teenusele päringu edastavad kasutajad või rakendused). Replikeerimise halvasti läbimõeldud konfiguratsiooni tulemusel võib süsteemi jõudlus väheneda. Kui otsitavad andmeid teatud kataloogiteenuse serveris ei leidu või pole seal nähtavad, kuna vastavad filtrireeglid ei luba neid kuvada, jätkub otsimise protsess taustal (kui see on lubatud). Seega võib filtreerimisreeglite vale konfigureerimine mõjuda süsteemi jõudlusele negatiivselt. Tuleb arvestada partitsioone või replikatsioone sisaldavate serverite täpsete kontekstidega. Liiga ühetasandilise struktuuri puhul tekib suur sisemine replikeerimisvajadus. Lisaks põhjustavad üksikud, hetkel ligipääsmatud serverid vastavate olekuteadete ilmumist ka kõikides teistes kõnealuse replikeerimisega seotud kataloogiteenuse serverites.
Täiendavad kontrollküsimused:

- Kas partitsioonide loomisel arvestati kataloogiteenuse käideldavuse ja kaitsevajadusega?
- Kas olemasolev ribalaius on replikatsioonide õigeaegseks tegemiseks piisav?

M 2.410 Kataloogiteenuse korrakohane kasutuselt kõrvaldamine

Algatamise eest vastutavad: IT-juht, infoturbejuht

Rakendamise eest vastutavad: administraator

Kataloogiteenuse kasutamisest kõrvaldamisel, nt asendades selle uuema versiooni ja uuema riistvaraga, tuleb arvestada järgnevalt toodud punktidega. Kataloogiteenuse kasutusest kõrvaldamine vajab hoolikat planeerimist ja vastutustundlikku teostamist, et näiteks volitatud kasutajad saaksid jätkuvalt sisse logida ja võrgus olevatele ressurssidele oleks tagatud vajalik juurdepääs, kuid samal peab saama ebavajalikuks muutunud andmeid ja volitusi ka turvaliselt kustutada või püsivalt tühistada. Enne kasutuselt kõrvaldamist tuleb kontrollida, kas kataloogiteenusest on tehtud varukoopia, mille abil saab võrgus esineda võivate probleemide korral kataloogiteenuse taastada. See puudutab ka krüpteeritud andmeid, mille puhul on tegu tähtsa infoga, mis moodustab kataloogiteenusest teatud kindla osa, kuid on salvestatud teistesse asutuse võrgus paiknevatesse arvutitesse. Kui kataloogiteenus hõlmab sertifitseerimisüksust, võib kasutusest kõrvaldamine mõjutada krüptograafilisi võtmeid ja sertifikaate. Sellistel juhtudel tuleb kontrollida, kas võtmematerjalist tuleks teha eraldi varukoopia. Neil juhtudel, kus kasutuselt kõrvaldatav kataloogiteenus sisaldab infot, mida teatud protseduurid või rakendused jätkuvalt vajavad, tuleb tagada, et vajaminev info oleks piisaval määral kättesaadav teistest allikatest.

Andmekandjate kustutamine/ utiliseerimine

Kõikide puudutatud arvutite andmekandjad tuleb enne taaskasutusse võtmist turvalisel moel kustutada (vt M 2.167 Andmete kustutamine või hävitamine). Ka riistvara utiliseerimise puhul tuleb tagada, et see vastaks kõikidele turvanõuetele (vt M 2.13 Tundlike ressursside jäljetu hävitamine *)*.

Partitsioonide kustutamine kataloogiteenusest

Juhtudel, kus kataloogiteenus on osadeks jaotatud ülesehitusega, sisaldavad üksikud kataloogiteenuse serverid sageli kogu kataloogiteenuse ühes partitsioonis saadaolevast nimeruumist ainult teatud kindlat osa. Ülejäänud kataloogiteenuse osad on kasutuselt kõrvaldatava osaga loonud omad viited. Kataloogiteenuse ühe partitsiooni kasutuselt kõrvaldamise korral tuleb jälgida, et kataloogiteenuse hierarhias ei asuks kustutatava partitsiooni alluvuses ühtki teist partitsiooni. Need kaotaksid oma nimeruumis oleva seose kataloogiteenuses kõrgemalasetsevate osadega ja muutuksid seega täiesti kasutuskõlbmatuks. Kui selline partitsioon või vastav kataloogiteenuse server eemaldatakse tervest kataloogiteenusest, tuleb kõik eemaldatud osale suunatud viited kataloogiteenuse teistes komponentides kas kohandada või kustutada. Muuhulgas on sellest puudutatud järgnevad valdkonnad:

- viited objektidele ja nende atribuutidele,
- usaldussuhted,
- indeksid (kataloogid),
- kasutajate haldamine,
- süsteemiseire (*monitoring*).

Siinkohal tuleb arvestada, et mainitud viiteid võivad sisaldada ka väliste organisatsioonide kataloogiteenused. Seega tuleb kasutuselt kõrvaldamise planeerimise

raames tagada, et vajalikud muudatused viidaks sisse ka valdkonnaga seotud välistes organisatsioonides.

Kui kasutusest kõrvaldataval partitsioonil oli kataloogiteenuses tähtis roll, näiteks globaalse indeksi Master või omanik, tuleb see roll esmalt mõnele teisele kataloogiteenuse osale üle kanda, kuna vastasel korral pole kataloogiteenuse funktsioneerimine enam tagatud.

Täiendavad kontrollküsimused:

- Kas kataloogiteenuse kasutusest kõrvaldamisest informeeritakse ka asutuseväliseid kasutajaid?
- Kas kataloogiteenuse üksikute partitsioonide kasutuselt kõrvaldamisel jälgitakse, et see ei mõjutaks negatiivselt teisi partitsioone?
- Kas kasutuses olnud andmekandjatelt kustutatakse kõik andmed turvaliselt?

M 2.411 Active Directory teenuse- ja andmehalduse lahutamine

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: administraator

Windows Server operatsioonisüsteemide administratiivsed ülesanded saab üldjoontes jagada kahe erineva vastutusalaga rollide vahel, milleks on „Teenuste haldamine“ ja „Andmete haldamine“.

Teenuste haldamine

Teenuste haldamise all mõistetakse Active Directory kui teenuse enda hooldamist. Teenuseadministraatorid haldavad domeenikontrollereid, nt paigaldavad operatsioonisüsteemidele värskendusi, konfigureerivad Active Directory 't, tehes nt kogu kataloogi hõlmavaid seadistusi, mis puudutavad usaldussuhteid või replikeerimise arhitektuuri.

Andmete haldamine

Andmete haldamine Active Directory 's või Active Directory tervikstruktuuri kuuluvatel arvutitel peab toimuma andmeadministraatorite poolt. Seejuures ei tohi andmeadministraatorid muuta Active-Directory teenust ennast, näiteks teha muudatusi kataloogiteenuse replikatsioonis. Pääsuloendite (Access Control List 'ide, ACL-ide) abil tuleks üksikute alamvaldkondade kaupa kehtestada volitustele võimalikult suured piirangud. Kuna teenuseadministraatorid vajavad teenuste haldamiseks ulatuslikke volitusi, peaksid nad saama teostada ka andmehaldusega seotud administratiivseid tegevusi. Vastupidist võimalust tuleks aga takistada, st andmeadministraatorid ei tohiks saada võimalust Active Directory konfiguratsiooni muuta. Administratiivsete kontode kuritarvitamise vältimiseks tuleb ülamainitud rollidega seotud kasutajakontosid sobival moel kaitsta. Selleks vajalikud Active Directory konfiguratsioonid leiate meetmest M 4.318 Active Directory turvaliste haldusmeetodite rakendamine .

Täiendavad kontrollküsimused:

- Kas teenuste ja andmete haldamiseks vajalikud administratiivsed kasutajad on teineteisest lahutatud?
- Kas administratiivsed kontod on piisaval määral kuritarvitamise eest kaitstud?

M 2.412 Autentimise kaitse Active Directory kasutamisel

Algatamise eest vastutavad: IT-juht
Rakendamise eest vastutavad: administraator

Active Directory toimib võrgus tsentraalse komponendina. Võrgusiseselt usaldusväärse side tagamiseks vastavate sidepartnerite vahel tuleb võrguressursside kasutamisel tagada, et autentimine ja volitamine leiaks aset piisavalt turvaliselt. Säilitamaks Active-Directory autentimise raames võimalikult kõrget kaitset, tuleks LAN-manager -autentimine desaktiveerida ja domeenikontrollerite vaheline Server-Message-Block -andmeside (SMB-andmeside) samuti nagu ka domeenikontrolleri ja domeenis olevate arvutite vaheline andmeside varustada digitaalsete allkirjadega. Lisaks tuleks desaktiveerida ligipääsuvõimalused, mis ühilduvad Windows Server 2008-le eelnenud versioonidega, samuti piirata anonüümset juurdepääsu domeenikontrolleritele.

LAN Manager autentimine

Kõrge turvalisuse saab saavutada ainult siis, kui kõik domeenikontrollerid, süsteemi kuuluvad serverid ja tööjaamad toetavad autentimisprotokolli NTLMv2 (NT LAN Manager Version 2). NTLMv2 on saadaval standardina (vt M 5.123 Võrgusuhtluse kaitse Windowsis). Varasemate Windowsi versioonide vanemad autentimisprotokollid pakuvad vähem kaitset. Näiteks salvestatakse LAN Manager autentimisprotokollis (LM) kontoparoolid ebaturvalisse LM-hash-formaati. NTLM-hash on LM-hash-formaadist krüptograafiliselt tugevam.

SMB-allkirjastamine

SMB-protokoll on aluseks Microsofti faili- ja printimiskinnituste jaoks, samuti mitme muu võrguoperatsiooni, nt Windowsi kaughalduse jaoks. Takistamaks nt Manin-the-Middle -ründeid (vt G 5.143 Man-in-the-Middle tüüpi rünne), mille käigus muudetakse SMB-pakette nende edastamise käigus, toetab SMB-protokoll SMBpakettide digitaalset allkirjastamist.

Anonüümsed juurdepääsud

Võimalikult suure turvalisuse tagamiseks tuleks anonüümsed juurdepääsud domeenikontrolleritele ja Active-Directory -andmetele rangelt ära keelata. Nimetatud sammud võivad varasemate Windowsi klient- ja server-operatsioonisüsteemide kasutamisel põhjustada tõrkeid võrgu töös, kuna need ei toeta üldse ülalmainitud kaitsemeetmeid või toetavad nende kasutamist ainult osaliselt. Seega pole käideldavuse tagamisel alati võimalik ebaturvalist LAN-Manager-autentimist desaktiveerida, SMB-andmesidet digitaalselt allkirjastada ega ka domeenikontrollerite anonüümseid juurdepääse keelata. Sellistel juhtudel tuleks jõuda selgusele, kas oma tööks anonüümset juurdepääsu vajavad teenused ja programmid kaaluvad üles võimalikud turvakaalutlused või mitte. Langetatud otsused tuleb dokumenteerida koos jääkriskidega ja IT-juhi poolt allkirjastada. Kui serverikeskkonnas käitatakse erinevaid Windowsi operatsioonisüsteeme, tuleb meetmes M 4.314 Domeenide ja domeenikontrollerite turvaliste poliitikaseadistuste loomine

kirjeldatud turvasoovitusi kohandada selliselt, et need oleks kooskõlas ka varasemate Windowsi versioonidega.

Kontrollküsimused:

- Kas serverikeskkond võimaldab järjepidevalt rakendada NTLMv2?
- Kas LAN-Manager autentimine desaktiveeriti ja SMB-andmeside varustatakse digitaalsete allkirjadega?
- Kas Windows Server 2008-le eelnenud versioonidega ühilduv juurdepääs desaktiveeriti?
- Kas anonüümsed juurdepääsud domeenikontrolleritele on tõkestatud?

M 2.413 DNSi turvaline kasutamine Active Directory 's

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: administraator

Active-Directory installatsioon koosneb tavaliselt mitmetest, kataloogi erinevaid partitsioone käitavatest serveritest. Juurdepääsu kergendamiseks nii klientide jaoks kui ka serverite vahel, nt replikeerimisel, kasutab *Active Directory* DNSi (*Domain Name System*), mis abistab seda *Active Directory* serverite otsimisel. Seega on DNS-teenus *Active Directory* aluseks.

Active Directory 'ga integreeritud DNS-tsoonid

Active Directory tervikluse ja käideldavuse tagamiseks tuleb hoolt kanda, et volitamata süsteemid ei saaks võrgus DNSi kliendipäringuid kõrvale juhtida. Windowsi keskkonnas peaks DNSi andmete kaitset suurendama seeläbi, et domeenikontrolleritel tuleks *Active Directory* 'sse integreerida DNSi tsoonid. Selleks salvestatakse tsoonipõhised DNSi andmed *Active Directory* konteinerisse nimega "MicrosoftDNS". *Active Directory* 'sse integreeritud DNS-tsoonide konfiguratsiooniandmed salvestatakse Windowsi registrisse. Konfiguratsiooniandmetele tuleks juurdepääs võimaldada ainult administratiivülesandeid täitvate kontode jaoks. Järgnevalt selgitatakse eranditult *Active Directory* 'sse integreeritud DNS-tsoone ja seega Windowsi serveri spetsiifilisi omadusi *Active Directory* turvaliseks käitamiseks. Antud teemast väljuvaid, üldisi DNSi kaitsmise meetodeid siin ei kirjeldata. DNS-infrastruktuuri kaitseks on tarvis kaitsta DNSi servereid, samuti DNSi serveritel asuvaid andmeid ja tagada kliendi päringutele antavate DNS-vastuste terviklus. Selle rakendamist kirjeldatakse alljärgnevalt.

DNS-Cache kaitse

Tagamaks domeenikontrollerile vahemällu salvestatud DNS-andmete terviklust, tuleb aktiveerida DNSi serveriprotsessi valik „Vahemälu kaitsmine kahjustuste eest". See peab tagama, et vahemälusse oleks võimalik lisada eranditult vaid volitatud DNS-sissekandeid.

DNS-juurdepääsu piiramine filtrikomponentidega

Domeenikontrollerite DNS-teenuse juurdepääsu tuleks piirata nii palju kui võimalik. Seda on võimalik saavutada näiteks sellega, et piiratakse kahe võrgusegmendi turvalüüside vahel asetleidvat DNS-teenust (UDP-port 53). DNS-teenus peab seejuures olema kättesaadav järgnevate komponentide jaoks:

- DNS-klientide ja vastava DNS-serveri vahel,
- tsooniülekandeid teostavate DNS-serverite vahel,
- DNS-serverite vahel, mis delegeerivad kliendipäringuid vastavatele tsoonidele, ja vastavate tsoonide eest vastutavate DNS-serverite jaoks,
- kliendipäringuid edasi juhtivate DNS-serverite ja hierarhias kõrgemalasetsevate DNS-serverite vahel.

Võrgukoormuse seire

Lisaks tuleks jälgida DNS-päringuid puudutavat võrguaktiivsust, kuna ebatavaliselt suur DNS-päringute esinemine võib viidata *Denial-of-Service* -ründele (DoS-ründele), mis on suunatud DNS-serveri ja seega võib-olla ka domeenikontrolleri vastu. Sellisel juhul tuleks ründaja võimalikult ruttu tuvastada ja rakendada sobivaid vastumeetmeid (vt M 6.106 Kataloogiteenuse hädaolukorraks valmisoleku plaani koostamine).

IPsec DNS-serveri ja DNS-kliendi vahel

IPsec (*Internet Protocol Security*) andmeturbe standardi abil on võimalik võrgus tagada IP-andmeliikluse konfidentsiaalsust, autentsust ja terviklust. IPsec-ühenduse loomisel autendivad klient ja server üksteist vastastikku, et kontrollida DNS-kliendi andmete autentsust. DNS-andmete terviklust saab edastamisel tagada IPsec'i abil, kasutades kas autentimispäist ehk AH-d (*Authentication Header*) või sõnumi kapselturvet ehk ESP-d (*Encapsulating Se-curity Payload*). Erinevalt Ipsec'i *Authentication Header* 'ist krüpteeritakse ESP kasutamisel andmeside veel ka täiendavalt. ESP puhul on tagatud ka DNS-andmete konfidentsiaalsus. Seega tuleks kasutada ESP-d. IPSec'i kasutamine suurendab andmehulka. Seega tuleks enne IPsec'i kasutamist veenduda, et olemasolevate ressursside hulk oleks piisav, et aktiveeritud krüpteerimise või allkirjastamise puhul oleks võrgus tagatud ka piisav andmete läbilaskevõime.

Salvestatud DNS-andmete tõhus kaitse

Serveritel hoitavate DNS-andmete kaitsmisel tuleks arvestada järgnevate punktidega:

Turvalised dünaamilised värskendused

- Windows Server operatsioonisüsteemidega tuleb kaasa ka DNS-server. Selle rakendamisel tuleb seda konfigureerida selliselt, et töödeldaks ainult *Active-Directory* -tervikstruktuuri poolt volitatud klientide registreerimispöördumisi. Kui seda ei kasutata, tuleb see desaktiveerida.
- Kui kasutatakse mõne teise tootja DNS-serverit, tuleb jälgida, et see toetaks DNS-andmete turvalist dünaamilist värskendamist ja oleks vastavalt konfigureeritud.

DNS-andmete pääsuloendid

- Kasutajate juurdepääs DNS-andmetele vastavas *Active-Directory* -konteineris "MicrosoftDNS" peaks olema ACLide toel sisse seatud selliselt, et täieliku juurdepääsu domeeni andmetele saaksid ainult administraatorid, domeeniadministraatorid, organisatsiooni administraatorid ja DNS-administraatorid.

Usaldusväärne administreerimine

- DNS-serverite ja seega ka DNS-andmete administreerimine on turbe seisukohast sama kriitiline nagu *Active Directory* konfigureerimine. Seega tuleb administraatorite volituste jagamisel tegutseda sama põhimõtte alusel nagu teenuste administreerimiseks vajalike administraatorikontode volituste andmisel (vt M 2.411 Active Directory teenuse- ja andmehalduse lahutamine).

Sekundaarsete DNS-tsoonide vältimine

- Sekundaarsete DNS-tsoonide infot ei salvestata domeenikontrollerile mitte *Active Directory* 'sse, vaid tekstipõhisesse tsoonifaili. Võimalusel tuleks kasutada jaotatud DNS-struktuuri, mille puhul haldab iga DNS-server ainult ühte tsooni ja suunab vastavad teistelt serveritelt tulevad kliendipäringud edasi nende eest vastutavale DNS-serverile. Kui sekundaarseid DNS-tsoone ei

saa sel moel näiteks suurema andmemahu tõttu vältida, tuleb tsoonifaili volitamata juurdepääsude eest kaitsta NTFS-volituste abil. Sekundaarsetele domeeniandmetele tohiksid omada täielikku juurdepääsu ainult üldadministraatorid, domeeniadministraatorid, organisatsiooniadministraatorid ja DNS-administraatorid.

Täiendav info

Täiendavat infot DNS-serverite konfigureerimise kohta leiate internetis dokumentidest „Best Practice Active Directory Design for Managing Windows Networks “ ja „ Best Practice Active Directory Deploy-ment for Managing Windows Networks “, mis asuvad Microsofti TechNetis (http://technet.microsoft.com).

Täiendavad kontrollküsimused:

- Kas volitamata süsteemide poolt esitatud DNS-kliendipäringute vältimiseks kasutatakse integreeritud DNS-tsoone või DNS-andmete turvalist dünaamilist värskendamist?
- Kas juurdepääs DNS-serveri konfiguratsiooniandmetele on piiratud, võimaldades seda ainult administratiivsetele kontodele?
- Kas DNS-Cache kaitseks on DNS-serveritel kasutusele võetud spetsiaalsed kaitsemeetmed?
- Kas DNS-teenuse juurdepääsu piiramiseks rakendatakse turvalüüsis filtrikomponenti?
- Kas DNS-päringuid puudutavat võrguliiklust jälgitakse?
- Kas DNS-serveri ja kliendi vahelises sides on tagatud selle konfidentsiaalsus, käideldavus ja terviklus? Kas IPSec'i kasutamisel DNS-kommunikatsiooni kaitsmiseks arvestatakse sellega, et võrgus oleks tagatud piisav andmete läbilaskevõime?
- Kas Active Directory 's on juurdepääs DNS-andmetele pääsuloendite (ACL-ide) abil piiratud, võimaldades seda ainult administraatoritele?
- Kas sekundaarseid DNS-tsoone välditakse?

M 2.414 Domeenikontrollerite kaitse arvutiviiruste eest

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: administraator

Piisava arvutiviiruste ja muude kahjulike programmide vastase kaitse tagamiseks tuleb ellu viia põhjalik arvutiviiruste vastase kaitse kontseptsioon. Vastavat protseduuri kirjeldatakse moodulis B 1.6 Viirusetõrje kontseptsioon . Arvutiviiruste vastase kaitse kontseptsioonis tuleks arvestada ka asutuse domeenikontrolleritega.

Selleks, et viirusetõrjetarkvara kasutamine domeenikontrolleril ei mõjuks igapäevastele tööprotsessidele negatiivselt, tuleb domeenikontrollerite puhul arvestada mõningate eripäradega. Käesolevas meetmes kajastatavad juhised on üldised juhised. Sõltuvalt olukorrast tuleb lisaks arvestada ka vastava viirusetõrjetarkvara tootjajuhistega.

Sobiva viirusetõrjetarkvara valimine

Viirusetõrjetarkvara valimisel tuleb jälgida, et seda oleks kindlasti võimalik kasutada ka domeenikontrolleril. Valiku tegemisel on määravaks, et viirusetõrjetarkvara kasutaks operatsioonisüsteemi tootja poolt ettenähtud programmeerimisliideseid (Application Programming Interface, API). Vale programmeerimisliidese kasutamisel võib viirusetõrjetarkvara pöördus muuta kontrollitavate failide metaandmeid. Sel juhul on võimalik, et operatsioonisüsteemi FRS (File Replication Service) annab korralduse organisatsioonis oletatavasti muudetud faili replikeerimiseks. Sellised ebavajalikud replikeerimised võivad vähendada süsteemi jõudlust ja seetõttu tuleks neid vältida. Täiendavat infot ühildumisvõimeliste viirusetõrjetarkavarde kohta leiate Microsoft-Knowledge-Base artiklist, mille ID nr on 815263. Enne lõplikku kasutuselevõtmist tootmiskeskkonnas tuleks viirusetõrjetarkvara nõuetekohast funktsioneerimist testida testimiskeskkonnas. Sealjuures peaks testimiskeskkond olema tootmiskeskkonnale võimalikult sarnane, et tuvastada mõju domeenikontrolleri üldjõudlusele.

Domeenikontrollerite piiratud kasutamine

Kahjuliku tarkvara sissetungimise vältimiseks tuleks domeenikontrolleritel eranditult kasutada operatsioonisüsteemi pakutavaid Active-Directory funktsioone ja võimalusel vältida muude teenuste pakkumist. Eriti oluline on, et domeenikontrollerit ei kasutataks tavapärase töökohana. Seega ei tohiks domeenikontrollerisse lokaalselt sisseloginud kasutajale võimaldada Internetis surfamist, emailide vastuvõtmist ega ka juurdepääsu välistele andmekandjatele nagu nt USBandmekandjatele või DVD-ROMidele. Samuti ei tohiks domeenikontrollerit kasutada serverina, mis annab kaustasid ühiskasutusse. Kui domeenikontrolleritel tehakse andmed võrgus kättesaadavaks andmete ühiskasutusse andmise abil, kontrollib viirusetõrjetarkvara iga pöörduse puhul, kas neis andmetes leidub kahjulikku tarkvara ning see võib domeenikontrolleritel põhjustada probleeme jõudlusega. Seega tuleks andmete ühiskasutusse andmine domeenikontrolleritel desaktiveerida.

Domeenikontrollerite kriitilised andmed

Üldjuhul peaks viirusetõrjetarkvara kõiki failidele tehtud pöördusi taustal läbipaistvalt kontrollima. Windows-Server-operatsioonisüsteemis leidub aga ka selliseid andmeid, nt kataloogiteenuse andmebaas, logiandmed, andmete replikeerimisteenuse andmebaas, mille puhul võib viirusetõrjetarkvara juurdepääs mõjuda

domeenikontrolleri tööle pärssivalt. Vältimaks failide asjatut tõkestamist viirusetõrjetarkvara poolt ja tagamaks domeenikontrolleri probleemivaba töö, tuleks seega arvestada järgnevate punktidega.

Juurdepääs Active Directory andmebaasile ja logifailidele ESE (Extensible Storage Engine) kaudu

Kataloogiteenuse andmebaas ja logifailid avatakse Active Directory poolt eksklusiivseks failijuurdepääsuks ESE abil. Seega pääseb ESE ligi ainult neile failidele, mida viirusetõrjetarkvara ei blokeeri. Samal ajal saab ka viirusetõrjetarkvara ligi ainult neile failidele, mida omakorda ESE ei blokeeri. Niihästi andmebaasi failid kui ka logifailid kasutavad Active-Directory -siseseid kontrollsummasid, mis muutuvad viirusetõrjetarkvara mõjul kehtetuks ja tekitavad andmebaasides ebakõlasid. Ebaühtlane andmebaas võib põhjustada Active Directory avarii. Seega tuleb regulaarsest viirusekontrollist välja jätta järgnevad failid:

- Active-Directory peamine andmebaas
- Active-Directory tehingute logifailid
- Active-Directory töökaust

ESE kaudu toimuv juurdepääs andmete replikeerimisteenuse (FRS-i) andmebaasile ja logifailidele Nagu juba kirjeldatud, võib viirusetõrjetarkvara oskamatul kasutamisel tekkida olukord, kus viirusetõrjetarkvara poolt andmebaasi- või logifailidele tehtavate pöördustega võivad hakata konkureerima replikeerimisteenuse pöördused. Samuti võib nende failide sisemise kontrollsumma muutumine põhjustada Active Directory töö katkemise.

Seega tuleks regulaarsest viirusekontrollist välja jätta järgnevad failid:

- Failid andmete replikeerimisteenuse töökaustas.
- Andmete replikeerimisteenuse andmebaasi kajastavad logifailid.
- Staging -kaust (Cache uute ja muudetud, replikeerimist vajavate failide jaoks) ja andmete replikeerimisteenuse püsireplikatsioon (koopia Distributed-File-System 'i tüvest ja selle alla kuuluvatest otseteedest).
- Andmete replikeerimisteenuse eelinstalleerimiskaust.

Kui kasutatakse andmete replikeerimise teenust, et replikeerida Windowsi volitusi, mille otsetee siht asub Windows Server operatsioonisüsteemil, tuleb kontrollist välja jätta ka selle SYSVOL kausta failid.

Andmete replikeerimine andmete replikeerimisteenusega (File Replication Service, FRS)

Windows-Server operatsioonisüsteemid kasutavad failide replikeerimisteenust sisselogimisskriptide ja SYSVOL kausta süsteemipoliitikate replikeerimiseks erinevate domeenikontrollerite vahel. Kui viirusetõrjetarkvara muudab mõne faili metaandmeid (turvainfot või ajatemplit), replikeerib FRS vastava faili domeenikontrollerite vahel uuesti. See põhjustab SYSVOL failide sagedasemat replikeerimist ja tekitab sellega:

- võrgu ribalaiuse intensiivsemat kasutamist,

- suuremat ressursikulu domeenikontrolleritel ja
- suure koguse failide tekkimist Staging -kaustas.

Üleliigse replikeerimise vältimiseks tuleks arvestada järgnevate punktidega:

- Tuleb valida viirusetõrjetarkvara, mis ei muuda SYSVOL-failide metaandmeid.
- Kui selline valik pole võimalik, tuleb SYSVOL-kataloog ja selle alamkataloogid viirusetõrjetarkvara automaatsest kontrollist välja jätta. Siinjuures suureneb aga viiruseprobleemide oht, kuna erinevalt ülamainitud failidest, jäävad antud juhul viirusetõrjetarkvara kontrolli alt välja ka käitusfailid, nt sisselogimisskriptid. Seetõttu tuleks juhuks, kui viirusetõrjetarkvara enam SYSVOL-katalooge ei kaitse, kasutada domeenikontrolleritel ja administraatorite tööjaamades eranditult ainult digitaalsete allkirjadega varustatud sisselogimisskripte.

Microsofti operatsioonisüsteemide värskendusfunktsioon (Update)

Windows-Server operatsioonisüsteemi värskendusfunktsiooni (Microsoft Update, Windows Update või Automatic Update) puhul võib viirusetõrjetarkvara eksklusiivne pääsuõigus failidele põhjustada probleeme. Vastavate probleemide vältimiseks tuleks regulaarsest viirusekontrollist välja jätta järgnevad failid:

- Värskendusfunktsioonidega seotud andmebaasifailid, nt kaustas %windir%\SoftwareDistribution\Datastore fail “Datastore.edb”
- Kasuta %windir%\SoftwareDistribution\Datastore\Logs salvestatud tehingute logifailid

Kontrollküsimused:

- Kas arvutiviirustevastase kaitse kontseptsioonis arvestatakse domeenikontrolleritega?
- Kas rakendatava viirusetõrjetarkvara tootja on kinnitanud selle sobivust domeenikontrolleritel kasutamiseks?
- Kas viirusetõrjetarkvara testiti enne kasutuselevõttu piisaval määral testimiskeskkonnas?
- Kas domeenikontrolleri IT-süsteemil välistatakse muude teenuste pakkumine?
- Kas kaustade ühiskasutusse andmine on domeenikontrolleritel desaktiveeritud?
- Kas viirusetõrjetarkvara kontrollib taustal kõiki failidele tehtavaid pöördusi?
- Kas kataloogiteenuse andmebaas, logifailid ning failide replikeerimisteenuse failid ja kaustad on viirusekontrollist välja jäetud?
- Kas on tagatud, et viirusetõrjetarkvara ei muuda SYSVOL-failide metaandmeid ja et SYSVOL-kaust on piisaval määral viiruste eest kaitstud?
- Kas andmebaasifailid ja tehingute logifailid, millel on seos värskendusfunktsioonidega, on regulaarsest viirusekontrollist välja jäetud?

M 2.415 VPN vajaduste analüüs

Algatamise eest vastutavad: IT-juht, infoturbejuht

Rakendamise eest vastutavad: IT-turvaspetsialist, administraator

Enne VPN-ühenduse ülesehitamist üksikute IT-süsteemide, asutuse erinevate asukohtade vahel või ka klientidega, tuleks teostada vajaduste analüüs. Vajaduste analüüsi eesmärgiks peaks olema esmalt selgitada, millised on konkreetsel juhul kõne alla tulevad kasutusvaldkonnad ning teisalt, millised on kasutusvaldkondadest tulenevad nõudmised riist- ja tarkvarakomponentidele. Kasutusvaldkondade väljamõtlemine ja läbimängimine võimaldab leida VPN-arhitektuurile või VPN-komponentidele vajalikke erinõudeid.

Olulised nõuded

Vajaduste analüüsimise raames tuleb muuhulgas arvestada järgnevate punktidega:

- Äriprotsesside määratlemine: Esmalt tuleb selgeks teha, milliste äriprotsesside jaoks soovitakse virtuaalset privaatvõrku (VPNi) kasutada ja millist infot selle kaudu edastada. Tulemuste põhjal tuleb välja töötada vajalikud nõuded ja need oma ettevõtte või ametiasutuse jaoks tähtsuse järjekorda seada. Lisaks äriprotsessidele tuleb arvestada ka rakendustega, mis vastavaid protsesse toetavad. Seejuures tuleb ka välja selgitada, millised asjassepuutuvad rakendused on ajalises mõttes kriitilised või nõuavad suurt ribalaiust.
- Rakenduseesmärkide määratlemine: VPNidel on mitmeid erinevaid kasutustsotstarbeid, nt kaughoolduse teostamine, üksikute töötajate või tervete asukohtade ühendamine. Seega tuleb selgeks teha, millistele eesmärkidel seda rakendatakse ja milliseid VPN-tüüpe selleks kasutada (nt Site-to-Site -, End-to-End - või End-to-Site -VPNe).
- Kasutajate määratlemine: Tuleb kindlaks märata, millistel kasutajatel (nt töötajatel väljaspool kontorit, töölähetuses viibivatel töötajatel, harukontori töötajatel) on õigus oma töös VPNi kasutada, millised peavad olema nende volitused ja vajalikud eelteadmised. Seejuures tuleks ka kindlaks määrata, kuidas neid turvaliselt identifitseerida ja autentida.
- Vastutusalade reguleerimine: Ka VPN-komponentide hooldamise ja haldamisega peab tegelema personal, kes on oma ülesannete kõrgusel. VPNi vajaduste analüüsi raames tuleb seega kindlaks määrata, kes on vastutav VPNide administreerimise ja käitamise eest ja seda mõlemal VPNi poolel. Lisaks tuleb selgitada, kelle poole pöörduda VPNi avarii või turvaintsidentide esinemise puhul. See kõik eeldab vastavate teadmistega spetsialistide olemasolu.
- Konfidentsiaalsus ja terviklus: Sõltuvalt konfidentsiaalsusest ja terviklusest tulenevast kaitsevajadusest esitatakse VPNile sageli erinõudeid, mille täitmiseks on üldjuhul vaja rakendada täiendavaid turvameetmeid. Sageli on siinkohal olemas hierarhias kõrgemalasetsevad reeglid või suunised, millega tuleb VPNi komponentide soetamisel ja käitamisel arvestada. Konfidentsiaalsusest ja/või terviklusest tuleneva kõrge turbevajadusega infot edastamiseks on soovitav kasutada Common Criteria alusel sertifitseeritud VPNi komponente (vt M 2.66 Sertifikaatidega arvestamine IT soetamisel). Sertifitseeritud VPN-komponentide näiteks on SINA-tootepere (turvaline InterNetwork-arhitektuur). Lisaks ainult VPN-ühenduse loomiseks mõeldud krüp-

tolüüsile (SINA-Box 'ile) pakub SINA-tootepere ka integreeritud krüptofunktsioonidega (SINA-Client 'iga) lõppsüsteeme, samuti haldussüsteemi.

- Käideldavus: Eriti just asukoha võrku ühendamisel soovitakse sageli, et VPNi kaudu saaks igal hetkel kiiresti infot vahetada. Kui asjassepuutuvate rakenduste käideldavusega seotud turbevajadused on kõrged, tuleks vajaduste analüüsis sellega arvestada. Käideldavusele esitatud kõrgendatud nõudeid ei saa VPNides alati tagada tehniliste turvameetmete rakendamisega, kuna VPNid ehitatakse sageli üles võrkude kaudu, mis pole oma kontrolli all ja pole seega mõjutatavad.
- Võrkude piiramine: VPNide abil saab erinevaid võrkusid koondada turvalise ühenduse abil üheks loogiliseks võrguks. Sõltuvalt konfiguratsioonist saavad seeläbi kõik ühte võrku kuuluvad IT-süsteemid ligi pääseda teiste võrkude kõikidele IT-süsteemidele või ainult teatud IT-süsteemidele. VPNi vajaduste analüüsi raames tuleks otsustada, millistest asukohtadest tohib vastava VPNi kaudu erinevatele võrkudele ja IT-süsteemidele ligi pääseda.
- Kasutatavate rakenduste ja protokollide valik: VPNi kaudu saab erinevat infot saata ja vastu võtta. Näiteks saab edastada e-maile, kopeerida andmeid või luua juurdepääsu veebiserverile. Lisaks nendele klassikalistele teenustele saab töötada ka nt terminaliserveril või VoIP kaudu helistada. Seega tuleks määrata, milliseid rakendusi tohib VPNi kaudu kasutada ja milliseid mitte. Otsustada ei tule mitte ainult seda, milliseid rakendusi kasutada, vaid ka seda, milliste protokollidega vastavat infot edastada. Näiteks saab määrata, et võrgukasutus peab toimuma NFSi asemel ainult SMB kaudu.
- Ribalaius ja viivitus: VPN võimaldab pöörduda eemalasuvas võrgus olevate rakenduste poole. Kuna VPN-ühendused luuakse sageli WANi kaudu, tuleb ajakriitiliste rakenduste puhul arvestada spetsiaalsete eeldustega, eriti kasutatava ribalaiuse ja edastusel esinevate viivituste osas. See puudutab näiteks juurdepääsu terminaliserverile või helistamist VoIP kaudu. VPNi vajaduste analüüsi käigus tuleks arvestada vajaliku ribalaiusega, lubatud viivitusega, samuti võrgu muude kvaliteedinäitajatega.
- Geograafilised piirangud VPN võimaldab ringiliikuvatel töötajatel ennast suvalisest asukohast asutuse LANi sisse valida. Kui seda aga ei soovita, tuleb kindlaks määrata, millistest asukohtadest tohib LANile ligi pääseda. Seda saab ka tehniliste lahendustega toetada. Näiteks võib lubada ainult ühe või väheste teenusepakkujate IP-aadresside vahemikke. Sissevalimisega ühenduse puhul saab nt filtreerida suunakoodide alusel. Siiski tuleks arvestada, et need tehnilised pääsupiirangud pole täiesti usaldusväärsed. Lisaks tuleb ka kasutajate jaoks välja töötada asjakohased organisatsioonilised nõuded.

Need punktid ei pea automaatselt kehtima kogu asutuse jaoks, neid saab rakendada ka vastavalt üksikutele asukohtadele või kasutuseesmärkidele. Eriti just mitme asukoha ühendamisel ei saa mitte igale asukohale määrata sama prioriteeti. Väikestele edasimüüjate büroodele esitatakse tavaliselt käideldavuse osas teistsugused nõuded kui ettevõtte keskusele. Samuti on End-to-End-VPN 'idele esitatavad nõuded teistsugused kui Site-to-Site-VPN 'ide omad. Lahendusena saab erinevaid rakenduseesmärke liigitada lähtuvalt nende nõuetest ribalaiusele, käideldavusele, konfidentsiaalsusele, terviklusele ja teenuse kvaliteedile (Quality of Service või lühidalt QoS). Vajaduste analüüsi tulemused tuleb dokumenteerida ja kooskõlastada tehnilise personaliga. Valdkonnaga kaasnevad nõudeid ja infoturbesuunistes sõnastatud turbe-eesmärke tuleb käsitleda VPN-kontseptsiooni

loomise (vt M 2.416 VPNi kasutamise planeerimine ja M 2.417 VPNi tehnilise teostuse planeerimine) ja realiseerimise koostisosadena.

Täiendavad kontrollküsimused:

- Kas on kindlaks määratud, milliste äriprotseduuride ja rakenduste jaoks tohib erinevaid VPNe kasutada ja millist infot tohib nende kaudu edastada?
- Kas on kindlaks määratud, millised kasutajad tohivad erinevaid VPNe kasutada, millised peavad olema nende volitused ja eelteadmised?
- Kas iga VPNi kasutamise kohta on kindlaks määratud sobivad identifitseerimis- ja autentimisprotseduurid?
- Kas VPNide käitamise ja kasutamisega seotud vastutusalad ja teavitamisprotseduurid on kindlaks määratud?
- Kas iga VPNi puhul on kindlaks määratud, millistest asukohtadest tohib erinevatele võrkudele ligi pääseda?
- Kas valdkonnaga kaasnevate nõuetega ja institutsiooni turvaeesmärkidega on arvestatud?

M 2.416 VPNi kasutamise planeerimine

Algatamise eest vastutavad: IT-juht, infoturbejuht

Rakendamise eest vastutavad: IT-turvaspetsialist, administraator

Kuna VPNi sisseseadmine on keerukas ülesanne, eeldab see struktureeritud lähenemist. Seega peaks VPNi kasutuselevõtmisele eelnema hoolikas planeerimine. Käesolev samm järgneb vahetult vajaduste analüüsile (vt M 2.415 VPN vajaduste analüüs) ja peaks tuginema sealt saadud teadmistele.

Organisatoorne külg

Järgnevalt on toodud erinevad olulisemad küsimused, millele tuleks leida organisatoorse kontseptsiooni koostamise raames vastused leida. Sõltuvalt konkreetsest olukorrast tekib loomulikult ka vajadus täiendavate, oludega kohandatud reeglite järele.

- Määratleda tuleks vastava VPNiga seotud vastutusalad (installeerimine, haldamine, kontroll, seire).
- Sõltuvalt organisatoorsest struktuurist tuleb olemasolevate rollide vastutusalasid laiendada või luua uusi rolle (vt M 2.1 IT kasutajate vastutuse ja reeglite kehtestamine).

Volituste kontseptsioon

- Tuleb kindlaks määrata, kuidas ja kelle poolt viiakse läbi kasutajakontode ja juurdepääsuõiguste haldamine ja administreerimine (volituste kontseptsioon). Näiteks ekstraneti kaudu ühendatud tarnija peab omama teistsuguseid pääsuõigusi kui ühendatud harukontor.
- VPN-juurdepääsu kasutamise jaoks on soovitatav luua erinevad kasutajagrupid, kellel on erinevad volitused. Üksikute kasutajate kuuluvust mõnda gruppi tuleks reguleerida vastava nõuete profiili abil, mis määrab, millised eeldused peavad olema gruppi kuulumiseks täidetud. Võimalikud eeldused on kasutusotstarve (nt kaugtöö, töötamine väljaspool asutust, hooldustööd), tõestatud teadmiste olemasolu (nt koolitustel osalemine) ja ülemuste nõusolek. Kaugjuurdepääsu kasutamise reguleerimise üle tuleb otsustada asutusesiseselt. Sageli on juba sarnased eeskirjad olemas, näiteks Interneti juurdepääsude kasutuseeskirjad, mida on tarvis ainult sobival moel kohandada.
- Kasutajatele antud sisse- ja juurdepääsuõigused tuleb dokumenteerida ja muudatuste korral dokumentatsiooni vastavalt täiendada.

Kasutuskohtadele seatavad nõudmised

- Konkreetselt teadaolevate eemalasuvate töökohtade (kaugtöö) puhul tuleb kindlaks määrata, millistele nõuetele peab kaugtöökoht vastama (nt milline peab olema töökoha turvalisus ja seal kasutatav tehniline varustus), et lubada sealt VPN-ühendusi asutuse LANi. Kontseptsioon võib kehtestada esialgse, vajadusel ka perioodiliselt korduva ruumide ja sealse tehnika kontrolli ning reguleerida, kuidas ja kes seda kontrolli peaksid läbi viima.
- VPN-kliendi töökohad pole sageli LANi käitaja kontrolli all ja on seetõttu suure ohupotentsiaaliga. Võrreldes statsionaarsete klientidega kaasnevad mobiilsete klientide puhul täiendavad ohud. Mitte iga koht, kus on olemas

tehnilised eeldused VPN-ühenduse loomiseks, ei ole selleks sobiv. Seetõttu tuleb kehtestada reeglid, millistest asukohtadest tohib siht-LANiga VPN-ühendusi luua. Sõltuvalt planeeritud kasutusvaldkonnast võib olla palju mõttekam koostada nn must nimekiri eriti ebasobivate asukohtade kohta. Nende hulka võivad kuuluda näiteks hotellide fuajeed, hotellide ärikeskused või ühiskondlikud transpordivahendid.

Muudatuste haldus

- VPN-juurdepääsu turvaprobleemid võivad endaga kaasa tuua kogu LANi kompromiteerimise. VPNi administreerimise jaoks tuleks seega määrata protseduurid, mis kirjeldavad, kuidas viia VPNi konfiguratsiooni sisse muudatusi (näide: muutmisloa taotlemine, planeeritava konfiguratsiooni kontrollimine, muutmine, sisseviidud muudatuste kontrollimine).

Asutusesisene või asutuseväline teostus

- Kontseptsiooni täiendavaks oluliseks punktiks on põhimõtteline küsimus, kas vajalik VPN tuleks realiseerida ise või peaks kasutama asutusevälist lahendust. Paljudel teenusepakkujatel on ette näidata suurepärased oskused ja põhjalikud kogemused VPNide planeerimise, juurutamise ja käitamise osas. Samas ei ole alati kasulik terve VPNi käitamist enda käest ära anda. VPNi asutusevälise käitaja puhul tuleb arvestada nõuetega moodulis B 1.11 Väljasttellimine (Outsourcing) .
- Tuleb välja selgitada VPNi kaitsevajadus. Kaitsevajadus tuletatakse edastatava info ja ühendatud IT-komponentide kaitsevajadusest. Selles kontekstis tuleb muuhulgas ka tuvastada, millised on tagajärjed, kui süsteemi käideldavus lakkab olemast, ja millised on lubatavad tööseisakud.
- Tuleb defineerida VPNi turvamehhanismidele esitatavad nõuded (nt seoses autentimise ja tervikluse tagamisega). Siinjuures tuleb selgeks teha, kas tugeva krüptograafia kasutamine kõikides asjassepuutuvates asukohtades on seadusega lubatud.

Asutusevälised

- Kui asutusevälistel tarnijatel või klientidel on ühendus VPNiga, tuleb määratleda erinevad turvatsoonid. Turvatsoonidest tohib lubada ainult selliseid pöörduseid, mis on tõepoolest kasutaja jaoks vajalikud.

Turvapoliitika järgimise kohustus

- Kuritarvitamise ennetamiseks tuleb VPNi turvapoliitikas määratleda VPNi kasutajate õigused ja kohustused. Kasutajaid tuleb kohustada turvareeglitest kinni pidama.
- Kuna LANi kaugjuurdepääsu puhul tekivad spetsiifilised turvariskid, mis tulenevad tavaliselt VPN-kliendi ebaturvalisest keskkonnast, peaks iga VPNi kasutaja läbima asjakohase koolituse. Vastava koolituse raames tuleks kasutajaid ühelt poolt teavitada konkreetsetest VPNiga seotud ohtudest ja teiselt poolt õpetada neile tehniliste seadmete ja tarkvaraga ümberkäimist. Autentimis- *Token* 'ite kasutamisel tuleb kasutajatele õpetada nende nõuetekohast rakendamist. Samuti tuleb kasutatavate toodete osas põhjalikult

koolitada administraatoreid ja selgitada neile VPNi turvariske ja turvameetmeid.

- Administraatoritel ei pea olema mitte ainult piisavalt aega VPNi käitamiseks, vaid ka selleks, et otsida infot avastatud VPNi turvaaukude kohta, et luua VPNi tööks vajalik infoturbe tagamise meetmekontseptsioon ja ka selleks, et viia ennast kurssi uute komponentidega.

VPNi kasutamise planeerimise plaan tuleb esitada juhtkonnale kinnitamiseks. Kõik otsused tuleb kontrollitavalt dokumenteerida.

Täiendavad kontrollküsimused:

- Kas VPNi käitamise eest vastutavad isikud on määratud?
- Kas on kindlaks määratud, kuidas ja kelle poolt viiakse läbi VPNi tööks vajalike kasutajakontode haldamine ja administreerimine?
- Kas iga VPNi puhul on teada selle turbevajadus, mis puudutab selle konfidentsiaalsust, terviklust ja käideldavust?
- Kas kõik VPNi kasutajad on saanud VPNi kasutamise osas piisava koolituse ja on kohustatud turvapoliitikat järgima?
- Kas on kindlaks määratud, millised juurdepääsuvõimalused antakse asutusevälistele VPNi kasutajatele?
- Kas antud pääsuõigused dokumenteeritakse ja kas neid kohandatakse muudatuste korral?
- Kas on kindlaks määratud, millistele nõuetele peavad vastama VPN- juurdepääse kasutavad töökohad?
- Kas on sisse seatud VPNi muudatuste haldus?

M 2.417 VPNi tehnilise teostuse planeerimine

Algatamise eest vastutavad: IT-juht, infoturbejuht

Rakendamise eest vastutavad: IT-turvaspetsialist, administraator

Lisaks organisatoorset tööd ja personali puudutavatele planeerimistöödele, mida käsitletakse meetmes M 2.416 VPNi kasutamise planeerimine , nõuab VPNi sisseseadmine ka otsuseid mitmete tehniliste aspektide osas. Need otsused tuleb ilmtingimata langetada enne VPNi soetamist ning need on aluseks selle hilisemal realiseerimisel. Ühilduvusprobleemide vältimiseks tuleb tehnilise planeerimistöö käigus väga hoolikalt arvestada olemasolevate tehniliste raamtingimustega. Järgnevalt on toodud erinevad olulisemad küsimused, millele tuleks tehnilise kontseptsiooni koostamise raames vastused leida. Sõltuvalt konkreetsest olukorrast tekib loomulikult ka vajadus täiendavate, oludega kohandatud reeglite järele.

Tehniline varustus

- Kirjeldus, kuidas peaks välja nägema VPNi tehniline teostus erinevate riist- ja tarkvarakomponentide näol. Komponente kirjeldatakse ainult nende funktsiooni alusel. Sellele järgneva olemasolevate süsteemikomponentide ja saadaoleva tootevaliku analüüsi põhjal saab kontseptsiooni üksikuid elemente hakata siduma reaalsete seadmete ja tarkvaratoodetega (vt M 2.419 Sobivate VPN-toodete valimine).
- Kirjeldada tuleb kõiki potentsiaalseid VPN-lõpp-punkte, mis võimaldavad LANi sissevalimist, ja selleks otstarbeks kasutatavaid juurdepääsuprotokolle.
- Antud turvakontseptsiooni raames tuleb kindlaks määrata kõik VPNi juurdepääsupunktid, mis loovad ühendusi kohtvõrguga ning lisaks tuleb kirjeldada, kuidas need juurdepääsupunktid ühendatakse LANiga (vt B 3.301 Turvalüüs (tulemüür)). Turvakontseptsioon peab analüüsima, lähtudes olemasolevast võrgustruktuurist, millised alamvõrgud on VPN-juurdepääsu kasutamisel ligipääsetavad. Tuleks kaaluda eraldiseisvate juurdepääsuvõrkude (Access Network 'ide) loomist, kust tootmisvõrku edasiliikumine saab toimuda ainult kontrollitult (läbi marsruuterite, paketifiltrite või sisemise tulemüüri). Juurdepääsuvõrkude sisseseadmine eeldab täiendava riist- ja tarkvara soetamist ja hooldamist (vt M 5.77 Alamvõrkude rajamine).
- Dokumenteerida tuleb kõik teenused ja protokollid, mida VPN-juurdepääsu kaudu lubatakse, samuti ressursid, millele VPN-juurdepääsu kaudu ligi pääseb. Valik sõltub kasutatavatest rakendustest. Ajaliselt kriitilise andmeside jaoks läheb võib-olla tarvis QoS'i (Quality of Service), MPLS'i (Multi Protocol Label Switching) või eraldi liine.

Krüpteerimisprotseduur

Andmete kaitsmiseks tuleb määratleda sobivad krüpteerimisprotseduurid. Olulised on siin muuhulgas järgnevad:

- Tunneldus - Sideühendust saab krüpteerida madalamal protokollitasandil (näiteks nn tunneldamise abil, M 5.76 Sobivate tunneldusprotokollide kasutamine VPN-süsteemis). Selleks tuleb välja valida sobiv protseduur. Ka tavalistes VPNides on selle kasutamine standardina sees, kuid nende arv ja kasutusvõimlused on väga erinevad.

- TLS/SSL-protokoll- Krüpteerimiseks võib kasutada ka TLS/SSLi, juhul kui madalal protokollitasandil ei ole mingil põhjusel krüpteerimist võimalik kasutada. See kehtib eriti juurdepääsudele, mis suunatakse veebiserverisse või meiliserverile, mis toetavad standardina TLS/SSLiga turvatud kommunikatsiooni (vt M 5.66 TLS-i/SSL-i kasutamine).
- Krüpteerimine võrguühenduselementidega - Lisaks side kaitsmisele tarkvaralahendustega võib kaaluda ka krüpteerivate võrguühenduselementide (ruuterite, modemite) kasutamist. Need on eriti kasulikud statsionaarseks kasutamiseks ja mitme arvuti ühendamiseks, kuna krüpteerimine toimub läbipaistavalt ja lõppsüsteeme see ei koorma. Arvestada tuleb sellega, et võrguühenduselemendid vajavad hoolikat konfigureerimist ja hooldamist. Ka otseste, nt analoogtelefonivõrkude või ISDNi kaudu sissevalimismeetodite puhul on andmete kaitsmiseks vajalik rakendada krüpteerimist.
- Meetmes M 3.65 Sissejuhatus VPNi põhimõistetesse tutvustatakse erinevaid VPNide liike. Vajaduste alusel tuleb otsustada, milline VPNi tüüp tuleks kasutusse võtta.
- Tuleb otsustada, kas ühendus peaks toimuma eriotstarbeliste Carrier -liinide kaudu. Antud otsus mõjutab oluliselt vajaminevaid kulutusi.
- Stabiilse käitamise ja pideva tõhustamise tagamiseks tuleks kasutada sobivaid seiresüsteeme. Seiresüsteemides saadud info võimaldab VPNi töö peenhäälestamist (vt M 4.321 VPNi turvaline käitamine).

VPNi tehnilise teostuse planeerimise plaan tuleb esitada juhtkonnale kinnitamiseks.

Täiendavad kontrollküsimused:

- Kas VPNi tehniline teostus on dokumenteeritud?
- Kas on kindlaks määratud, milliseid krüpteerimismeetodeid tuleks VPNi jaoks kasutada?
- Kas on kindlaks määratud, kuidas peavad kasutajad ennast VPNis autentima?
- Kas on kindlaks määratud, millised on Carrier -võrgule esitatavad nõuded?
- Kas VPN-lõpp-punktid ja lubatud juurdepääsuprotokollid on määratletud?
- Kas teenused, protokollid ja ressursid, mis on vastava VPNi kaudu lubatud, on määratletud?
- Kas on kindlaks määratud, millised alamvõrgud on VPNi kaudu ligipääsetavad?
- Kas on kindlaks määratud, kuidas toimub VPNi seire?

M 2.418 VPNi kasutamise turvapoliitika koostamine

Algatamise eest vastutavad: IT-juht, infoturbejuht

Rakendamise eest vastutavad: IT-juht, IT-turvaspetsialist, administraator

VPN-komponentide kasutamiseks ametiasutustes ja ettevõtetes tuleb koostada sobiv turvapoliitika. Vastav VPNi eripärasid kajastav turvapoliitika peab olema kooskõlas asutuse üldise turvakontseptsiooniga ja üldiste turvapoliitikatega. Neid tuleb regulaarselt kontrollida, kas need on veel jätkuvalt päevakohased ning neid vajadusel kohandada. VPNi puudutavaid spetsiifilisi nõudeid võib kas olemasolevates poliitikates täiendada või võtta kokku eraldi poliitikasse. VPNi turvapliitika peaks muuhulgas kajastama järgmiseid punkte:

- Turvapoliitika peaks kirjeldama, kes tohib asutuses VPN-komponente installeerida, konfigureerida ja kasutada.
- Millist infot tohib VPNide kaudu edastada?
- Millistes asukohtades tohib VPN-komponente kasutada?
- Millistele muudele sise- või välisvõrkudele või IT-süsteemidele tohib VPNi kaudu ligi pääseda?
- Kõikide VPN-komponentide jaoks tuleks määratleda turvameetmed ja standardne konfiguratsioon.

Intsidentide käsitlemine

- Kõikidele VPNi kasutajatele tuleb selgeks teha, et turvaprobleemide kahtluse korral tuleb sellest informeerida turvalisuse eest vastutavat isikut, et ta saaks hakata probleemiga tegelema (vt B 1.8 Turvaintsidentide käsitlus).

VPN-turbealane treening

- Administraatoreid, aga ka VPN-komponentide kasutajaid tuleb koolitada või informeerida VPN-ohtudest ja kohustuslikest turvameetmetest. VPNi turvapoliitikas kirjeldatud turvameetmete järgimist tuleks regulaarselt kontrollida.

VPNi kasutajapoliitika

Vältimaks kasutajate koormamist liigsete detailidega on mõistlik koostada eraldiseisev VPNi kasutajapoliitika, nt infolehe kujul. Sellises kasutusjuhises tuleks kirjeldada VPNi kasutamise eripärasid, muuhulgas näiteks:

- milliste muude asutusesiseste ja -väliste võrkudega või IT-süsteemidega tohib VPN-klienti ühendada,
- millistel raamtingimustel on lubatud oma asutuse või mõnda välisesse VPNi sisse logida,
- mida tuleb teha VPN-kliendi (oletatava) kompromiteerimise puhul, esmajoones, kelle poole üldse tuleb pöörduda.

Kasutajate tähelepanu tuleb juhtida sellele, et VPNe tohib luua ainult sobivates asukohtades ja asutuse poolt kasutusloa saanud IT-komponentidega. Sõltuvalt kasutusotstarbest võivad ebasobivad kasutuskohad olla näiteks hotellide fuajeed, hotellide ärikeskused või ühistransport, ka võõradministreeritud IT-süsteemid ei pruugi selleks sobida (vt M 4.251 Töötamine võõraste IT-süsteemidega). Oluline on täpselt kirjeldada, kuidas tuleks ümber käia kliendipoolsete turvalahendusega. Näiteks:

- Ühtegi turvalisust puudutavat konfiguratsiooni ei tohi muuta,
- Paroole ei tohi salvestada kliendile, välja arvatud selleks kinnitatud paroolisalvestamistööriistadega (vt M 4.306 Paroolisalvestusvahenditega ümberkäimine),
- Alati peab olema aktiveeritud mõni viirusetõrjetarkvara,
- Olemasolevat *Personal Firewall* 'i ei tohi välja lülitada (vt M 5.91 Interneti-PC personaalse tulemüüri installeerimine),
- Kasutajad ei tohi muuta VPN-kliendi konfiguratsiooni; seda tohivad teha ainult selleks ametisse nimetatud administraatorid ja
- Kõik kataloogide või teenuste kasutusselubamised peavad olema desaktiveeritud või vähemalt korralike paroolidega kaitstud.

Lisaks peaks kasutajapoliitika sisaldama infot selle kohta, milliseid andmeid tohib VPNis kasutada ja edastada ja milliseid mitte. Esmajoones kuulub selle alla tundliku info nagu nt konfidentsiaalsete dokumentidega ümberkäimine. Kasutajatele tuleb selgitada VPNiga kaasnevaid ohtusid, samuti VPN-poliitikate sisu ja mõju.

VPNi administreerimispoliitika

Lisaks tuleks ka administreerimiseks koostada VPNi spetsiifikaga arvestav poliitika, mida oleks muuhulgas võimalik kasutada ka administraatorite koolitamise baasmaterjalina. Selleks tuleks kindlaks määrata, kes vastutab erinevate VPN-komponentide administreerimise eest, milliste liidestega on omavahel ühendatud käitamisprotsessis osalevad administraatorid ning millal ja millist infot tuleb vastutavate isikute vahel vahetada. Seega on üsna tavaline, et serveripoolsete komponentide käitamise eest on vastutav hoopis teine organisatsiooni allüksus kui VPN-kliendi või identiteedi ja volituste halduse eest. Administraatoritele suunatud VPNi poliitika peaks hõlmama VPN-infrastruktuuri käitamiseks olulisi põhiaspekte, näiteks:

- Turvalise VPN-konfiguratsiooni kehtestamine ja turvaliste standardkonfiguratsioonide defineerimine
- Kõikide VPN-komponentide turvaline haldamine
- Krüptograafiliste protseduuride valimine ja juurutamine koos võtmehaldusega
- Logifailide regulaarne kontrollimine, vähemalt serveritel
- Asendussüsteemide kasutussevõtmine

- Meetmed VPNi kompromiteerimise korral

Kõik VPNi kasutajad, nii tavakasutajad kui ka administraatorid, peavad allkirjaga kinnitama, et nad on VPNi poliitika läbi lugenud ja järgivad seal määratletud juhiseid. Ilma niisuguse kirjaliku kinnituseta ei tohiks mitte keegi VPNi kasutada. Allkirjastatud kinnitusi tuleks hoida sobivas kohas, näiteks personalitoimikus.

Täiendavad kontrollküsimused:

- Kas on olemas päevakohane VPN-turvapoliitika?
- Kas iga VPN-kasutaja on saanud vastavast VPNi poliitikast koopia või infolehe selle kohta, millised on tähtsamad turvamehhanismid?
- Kas VPNi kasutamisega seotud turvapoliitikat selgitati kasutajatele turvameetmete koolituse raames?

M 2.419 Sobivate VPN-toodete valimine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond

Rakendamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, infoturbejuht

Ettevõtetel ja ametiasutustel on võrkudele mitmeid erinevaid nõudeid, näiteks erinevate asukohtade ühendamine ja mobiilsete töötajate või kaugtöötajate ühendamine sisevõrguga. Vastavalt on erinevad ka asutuste vajadused, millega tuleb VPN-toodete valimisel arvestada. Samuti tuleb rakendada meetmete M 3.65 Sissejuhatus VPNi põhimõistetesse ja M 2.416 VPNi kasutamise planeerimine väljatöötatud tulemusi. VPN-tooted erinevad üksteisest oma jõudluse, pakutavate turvamehhanismide, kasutusmugavuse ja majanduslikkuse poolest. Lisaks seavad erinevad tooted ka erinevaid tingimusi kasutuskeskkonna riist- ja tarkvarakomponentidele. Enne VPN-toote soetamist tuleks koostada müügilolevate toodete hindamiseks nimekiri. Võrdluse alusel saab langetada põhjendatud ostuotsuse.

Väljast tellimine

Kui VPN tellitakse teenusepakkuja käest, ei ole tavaliselt võimalik teenusepakkuja tootevalimisprotsessi mõjutada. VPN-teenusepakkujate valimise juhised leiate meetmest M 2.420 Trusted VPN teenusepakkuja valimine . VPN koosneb tavaliselt mitme riist- ja tarkvarakomponendi kombinatsioonist. Esmalt võib laias laastus tõmmata eristava joone LANiga ja kliendiga seotud komponentide vahele. Soetatavad komponendid sõltuvad väljavalitud VPN-süsteemiarhitektuurist. Suurtes asutustes käitatakse sageli erinevate kasutusotstarvete jaoks samaaegselt ka mitut VPN-ühendust. Selleks on tavaliselt tarvis spetsiaalseid IT-süsteeme (riistvara koos tarkvaraga), mis on loodud konkreetselt VPN-serverina kasutamiseks.

Eraldiseisvad seadmed (*Appliances*)

Paljud erinevad tootjad pakuvad VPN-komponente eraldiseisvate seadmetena. Seejuures on tegu eelkonfigureeritud seadmetega, mis on loodud ja konfigureeritud konkreetseks kasutusotstarbeks (siin: VPN-lõpp-punkti tarbeks). Võrreldes tsentraalse VPN-komponendi ülesehitamisega standardsete IT-komponentide baasil, mis tuleb veel (kas omal jõul või teenusepakkuja poolt) konfigureerida, on eraldiseisvate seadmete konfigureerimine sageli lihtsam. Sellele eelisele vastandub aga jällegi tõsiasi, et niisugused konfiguratsioonid on vähem paindlikumad ning pakuvad vähem võimalusi erinõuete täitmiseks.

Nõuded tootele

VPN-toodete valimisel tuleb jälgida, et nende puhul oleks täidetud järgnevad turvalisusega seotud põhifunktsioonid:

- Identifitseerimine, autentimine ja volitamine: Siin käivad süsteemide identifitseerimine ja autentimine üksteise alla, nii suunal süsteem kasutaja suhtes kui ka suunal kasutaja süsteemi suhtes. Tootega peab olema võimalik sisse seada erinevaid kasutajatunnuseid koos erinevate õigusteprofiilidega. Toode peaks sisaldama piisavalt tugevaid ja tunnustatuid autentimisprotseduure. Kaugpöördused peavad olema kaitstud piisavalt tugevate autentimismehhanismidega. Lisaks peab olema võimalik VPN-komponentidel taasluua määratletud pääsuõigusi.
- Teenuste kvaliteet (*Quality of Service* , QoS): Võrguüleminekute kontekstis tuleb teenuste kvaliteedi mõiste all käsitleda sellise kommunikatsiooni seiret ja juhtimist, mis võib toimuda läbi turvalüüsi. Sobiv toode peab täitma VPN-kontseptsioonis väljatöötatud vajadusi ja võimaldama kehtestada tööks kriitilise tähtsusega rakendustele prioriteete.

- Andmeedastuste turvalisus: Andmeedastuse turvalisuse kindlustamiseks rakendatakse funktsioone, mis tagavad andmete turvalisuse ja tervikluse. Lisaks tuleb tagada sidepartnerite autentsus. Seejuures on oluline, et toode pakuks turvalisi krüptograafilisi mehhanisme, mis vastaksid kaasaja tehnilistele nõuetele (vt M 2.164 Sobiva krüptoprotseduuri valimine). VPNi planeerimisel ja realiseerimisel tuleb lisaks arvestada VPN-lõpp-punktide integreerimisega turvalüüsi alla.
- Võtmehaldus: Võtmehaldus nõuab sobivate funktsioonide olemasolu, mis võimaldaksid hallata ja jaotada krüptograafiliste mehhanismide sajalasi ja avalikke võtmeid ning vajadusel neid ka ise luua. Valitud tooted peaksid seejuures olema võimalikult paindlikud ja võimaldama sujuvalt integreerida erinevaid tehnikaid.

Järgnev nimekiri annab ülevaate võimalike hindamiskriteeriumite kohta, kuid see ei mitte mingil juhul täielik ning kindlasti on seda nimekirja võimalik täiendada. Lisaks siinloetletud kriteeriumitele tuleb välja töötada täiendavad spetsiifilised nõuded, mis tulenevad konkreetsetest kasutusvaldkondadest (vt M 2.415 VPN vajaduste analüüs).

1 Üldised kriteeriumid

1.1 Jõudlus ja skaleeritavus

- Kas toode suudab täita jõudlusele seatud nõudeid?
- Kas toode pakub koormuse jaotamise funktsioone?
- Kas tooted suudavad edastatud infot tihendada (ingl *compress*) ja hõrendada?
- Kas toodet on võimalik tulevikus kasvavate vajaduste korral laiendada (kas sellel on nt moodulitel põhinev ülesehitus, uute VPN-serverite ühendamisvõimalus, ühine kasutajahaldus kõikide VPN-juurdepääsude jaoks?)

1.2 Hooldamine

- Kas toodet on lihtne hooldada?
- Kas tootja väljastab tarkvarale regulaarselt värskendusi?
- Kas tootele pakutakse hoolduslepingut?
- Kas hoolduslepingutes on võimalik kindlaks määrata maksimaalne aeg, mis tohib kuluda probleemi kõrvaldamisele?
- Kas tootja pakub koos tootega ka kompetentset klienditeenindust (kõnekeskus, infoliin), mis oleks võimeline probleemide korral ka kohe abi pakkuma?
-

1.3 Usaldusväärsus/rikkekindlus

- Kas tegu on usaldusväärse tootega?
- Kas tootja pakub kõrge käideldavusega lahendusi?
- Kas toodet on võimalik rakendada pidevkasutuses?

1.4 Kasutajasõbralikkus

- Kas toote installeerimine, konfigureerimine ja kasutamine on lihtne? Kas toode vastab kehtivatele ergonoomiaalastele eeskirjadele?
- Kas VPN-klient on loodud selliselt, et sellega tuleb toime ka kogemusteta kasutaja, ilma et sellega kaasneksid kõrgendatud turvariskid (kas on olemas kontekstipõhine abi, *online* -dokumentatsioon, detailsed veateated)?
- Kas VPN-kliendi kasutamist on võimalik konfigureerida selliselt, et süsteem ei koormaks kasutajaid liigsete tehniliste detailidega? Kas sellele vaatamata säilib siiski ka kõrge turbeaste?

2. Funktsioon

2.1 Installeerimine ja kasutuselevõtt

- Kas VPN-klienttarkvara installeerimist on võimalik eelseadistavate konfigureerimisparameetritega automatiseerida?
- Kas VPN-klienttarkvara installeerimisega saaksid hakkama ka väheste sellealaste kogemustega töötajad?
- Kas olulisemaid konfiguratsiooniparameetreid on võimalik kaitsta kasutaja poolt tehtavate muudatuste vastu?
- Kas toode ühildub enamlevinud riist- ja tarkvaraga (operatsioonisüsteemid, sissepistetavad kaardid, draiverid)?
- Kas vaadeldav VPN ühildub enamlevinud süsteemihaldussüsteemidega?

2.2 Käitumine rikete korral

- Kas VPN-juurdepääsu turvalisus on tagatud ka kriitilise vea esinemise korral?
- Kas süsteemi käitumist kriitilise vea korral on võimalik seadistada?
- Kas on võimalik nt seadistada, et kriitilise vea ilmnemise puhul toimub automaatselt taaskäivitus või administraatorit teavitatakse olukorrast?

2.3 Haldamine

- Kas tootega kaasasolev dokumentatsioon sisaldab detailset infot kõikide tehniliste näitajate ja haldamisega seotud andmete kohta?
- Kas tootel on haldamiseks olemas graafiline kasutajaliides? Kas haldamisliides on koostatud nii, et süsteem viitab konfiguratsioonis esinevatele vigadele, konfiguratsiooni ebaturvalisusele või selle kõrvalekalletele või takistab nende rakendamist?
- Kas lisaks graafilisele haldusliidesele pakutakse ka käsuviibal põhinevat liidest?
- Kas administratiivsed funktsioonid on kaitstud sobiva juurdepääsukontrolliga?

2.4 Logimine

- Kas toode pakub sobivaid funktsioone logimiseks?
- Kas saab seadistada, kui detailselt peaks logimine toimuma ja milliseid sündmusi tuleks logis kajastada? Kas logisse salvestatakse kõik olulised andmed?
- Kas logimist on võimalik seadistada selliselt, et andmete kogumine toimuks erinevate kategooriate põhjal (nt lähtuvalt ühendusest, kasutajatest, protokollidest, teenustest)?
- Kas logiandmed on varustatud pääsuõiguste kaitsega?
- Kas logiandmeid saab lisaks lokaalsele salvestamisele salvestada veel ka eemalolevatele arvutitele (kas tootel on tsentraalne protokoll)
- Kas kaugsalvestuse tarbeks pakutakse levinud andmeedastusvõimalusi, mis toetaks logimist ka võõraste süsteemide kaudu (nt *syslog*)?
- Kas logiandmeid saab edastada kaitstult?
- Kas tootel on olemas kergestikasutatavad funktsioonid, mis võimaldavad logiandmeid analüüsida?
- Kas toote logimismehhanism suudab teha koostööd kasutatava süsteemihaldussüsteemiga, eriti edastusformaati ja edastusprotokolli osas?
- Kas toode võimaldab teatud sündmuste esinemisel teavitada administraatorit või rakendada automaatselt ka teatud kaitsemeetmeid? Näiteks kui mõne kasutajakonto alt on toimunud järjestikku mitu ebaõnnestunud autentimiskatset, on sageli mõistlik vastav kasutajakonto sulgeda.
- Kas logimist saab kohandada vastavalt institutsiooni vajadustele ja institutsioonis kehtivatele erinõuetele?

2.5 Side ja andmeedastus

- Kas VPN-toode toetab LANi poolel kõiki olulisi võrgutehnoloogiaid (nt Ethernet'i, ATM'i)?
- Kas VPN-toode toetab WANi poolel kõiki planeeritud juurdepääsutehnoloogiaid (nt ISDN'i, mobiiltelefoni, analoogtelefoniliine, X25't)?
- Kas VPN-klientide arv, kes saavad ennast toote puhul samaaegselt VPN-serverisse sisse valida on piisav?
- Kas VPN-toode toetab levinud, kaugpöördust võimaldavaid sidevõrkudes töötavaid protokolle (nt PPP'd, SLIP'i)?
- Kas VPN-toode toetab levinud, kaugpöördust võimaldavaid teenuseprotokolle (nt TCP/IP'd)?
- Kas internetipõhise juurdepääsu kasutamisel toetatakse levinumaid tunneliprotokolle (nt PPTP'd, L2F'i, IPSec'i, SSL'i)?
- Kas VPN-toode pakub sõltuvalt kasutatavast tehnoloogiast täiendavaid, tehnoloogiast sõltuvaid mehhanisme (nt kanalite kokkuühendamist ISDN'is, VPN-kliendile tagasihelistamist VPN-serveri poolt)?

2.6 Turvalisus: side, autentimine ja juurdepääs

- Kas toode pakub sobivaid funktsioone turvaliseks andmeedastuseks?
- Kas side turvaliseks muutmisel kasutatakse standardseid mehhanisme?
- Kas kõik kasutatavad krüptograafilised meetodid on sisse seatud ja kas need vastavad kaasaja tehnilistele nõuetele?

- Kas toote arhitektuur võimaldab ka hiljem uusi turvamehhanisme juurde installeerida?
- Kas toode pakub sobivaid funktsioone kasutajate autentimiseks enne seda, kui neile antakse juurdepääs lokaalsetele ressurssidele?
- Kas erinevaid autentimismehhanisme on võimalik üksteisega ühendada?
- Kas süsteemiarhitektuuri ülesehitus võimaldab uusi autentimismehhanisme ka hiljem juurde integreerida?
- Kas VPN võimaldab kasutada ühte või mitut levinud välist autentimisteenust nagu nt SecureID, TACACS+, RADIUS?
- Kas on võimalik lisada täiendavaid väliseid autentimisteenuseid?

Kui kõik soetatavale tootele esitatavad nõuded on dokumenteeritud, tuleb hakata analüüsima müügilolevaid tooteid, et välja selgitada, milline toode suudab neid nõudeid kõige paremini täita. On küllaltki ootuspärane, et kõik tooted ei ole võimelised kõiki nõudeid korraga või võrdselt hästi täitma. Seega tuleks kaaluda, millised konkreetsed nõuded on asutuse jaoks kõige olulisemad. Samamoodi võib teha ka toodete lõikes pingerea, tuues välja, kui suures mahus suudab vastav toode teatud nõuet täita. Läbiviidud tootehindamise alusel saab langetada põhjendatud ostuotsuse. Enne installeerimist tuleb kontrollida, kas valitud tooted tõepoolest täidavad vajalikke nõudeid piisavalt ja ühilduvad nõutud tehnoloogiatega. VPN-seadmete valimine on VPNi sujuva töö tagamisel üheks määravaks asjaoluks. Seega tuleb enne otsustamist hoolikalt mõelda, kuna hilisemate muudatustega kaasnevad sageli ka suured kulutused või väheneb turvalisus.

M 2.420 Trusted VPN teenusepakkuja valimine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond
Rakendamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, infoturbejuht

VPNi iseseisev käitamine nõuab vastutavalt administraatorilt põhjalikke erialaseid teadmisi. Lisaks spetsiaalsetele VPN-seadistustele tuleb arvestada täiendavate krüptograafiliste aspektidega ja optimeerida avalike võrkudega ühendamist.

Kui kõikide seadistuste hulgast tehakse parim valik, on võimalik kaitsta andmete konfidentsiaalsust ja terviklust ning hoida ära käideldavuse mõjutamist.

Avariid avalikes võrkudes, mille külge on VPN-lüüs ühendatud, võivad aga jätkuvalt katkestada andmevooge VPNiga ühendatavate asukohtade vahel. Selliste, iseseisvalt administreeritavate „Secure-VPNide“ alternatiiviks on „Trusted-VPNid“.

Trusted-VPNi korral antakse info turvalise edastamise ülesanne asutusevälisele teenusepakkujale. Lepingute abil saab teenusepakkujat kohustada kaitsma edastatava info konfidentsiaalsust, terviklust ja käideldavust. Selle asemel, et kasutada avalikke võrke, näiteks Internetti, edastatakse Trusted-VPNide korral infot läbi teenusepakkuja eraldi liinide (Carrier -võrkude). Kuna Carrier -võrk allub teenusepakkuja enda kontrollile, suudab ta kuni teatud määrani tagada seal edastatava info turvalisuse. Teenuse tellija vaatepunktist annab teenusepakkuja tema käsutusse seadmed, mis liidetakse tellija juures ühendamist vajavate LANide külge.

Kuna teenusepakkuja jätab sageli andmed krüpteerimata ja kogu haldamine jääb välise teenusepakkuja hoolde, tuleks Trusted-VPNe kasutada ainult vähese kaitsevajadusega andmete edastamiseks ilma täiendavate kliendipoolsete turvamehhanismideta. Isegi sellise kasutusotstarbe puhul tasub andmeid siiski kliendi poolel täiendavalt krüpteerida. Kõrgema turbevajaduse korral tuleb andmed krüpteerida enne nende edastamist. Trusted-VPNi oluliseks puuduseks on sõltuvus teenusepakkujast. Teenusepakkuja vahetamine on sageli väga töö- ja ajamahukas. Trusted-VPNide suureks eeliseks on asjaolu, et sobivad teenusepakkujad on sageli esindatud mitmes riigis korraga. Eriti just rahvusvahelises keskkonnas on asutusel keeruline tagada igas asukohas isikliku VPNi tööks vajaliku kvalifitseeritud personali ja protsesside olemasolu. Trusted-VPNteenusepakkuja valimisel, samuti sellele järgneval lepinguläbirääkimistel tuleks arvestada infoga, mis on toodud meetmetes M 2.252 Väljasttellitava teenuse sobiva tarnija valimine
M 2.253 Välise teenusepakkujaga sõlmitava lepingu koostamine .

Trusted-VPNi käitamisel tuleb arvestada ka järgnevate punktidega:

- Service Level Agreement - Suurema kulutuse tõttu ei ole majanduslikult mõistlik valida teenusetasemeleppe sõlmimiseks partnerit, kes pakub maksimaalset kvaliteeti. Olulisem on juba eelnevalt otsustada, mida täpselt ja millise kvaliteediga teenust tarvis läheb. Vastavad punktid tuleb teenusetasemelepingutes (SLAdes) kokku leppida ja dokumenteerida. Teenusetasemelepingutes on toodud pakutava teenuse mõõdetavat kirjeldus, kaasa arvatud eeldatava kvaliteedi ja rakendavate mõõtmisvõimaluste kirjeldus. Lisaks tuleb teenusepakkujaga kokku leppida, milline on tagajärg teenusetasemelepingu rikkumisel ja kuidas peaks toimuma asjakohane aruandlus.

- Globaalne ühendus - Sageli kasutatakse VPNe mitte ainult asukohtade ühendamiseks, vaid ka mobiilsete töötajate ühendamiseks LANiga. Kui mobiilsete töötajate ühendamine peaks toimuma Trusted-VPNi kaudu, peab teenusepakkuja tagama sissevalimispunktide olemasolu, et töötajad saaksid nendega ühendust mõne alltoodud lahenduse abil.
- Andmeühendus avalike võrkude kaudu - Siinpuhul luuakse andmeühendus avaliku võrgu kaudu, nt läbi Interneti. Kuna avalike võrkude kaudu toimuvat andmeühenduste edastamiskvaliteeti ei saa mõjutada, võib selles protsessis esineda tõrkeid. Näiteks nõuavad terminaliserver-rakendused tihti suurt ribalaiust, mis pole kõikjal kättesaadav.
- Sissevalimisega ühendused - Sissevalimisega ühenduste puhul saavad mobiilsed töötajad ennast vahetult telefoniühenduse, nt mobiilsidevõrgu kaudu sisse valida teenusepakkuja pääsupunkti. Antud lahendus võib tekitada palju probleeme sageli välismaal viibivate mobiilsete töötajate puhul, kui telefoniühendust on tarvis luua üle pika vahemaa. Seega tuleks selle lahenduse valimisel jälgida, et teenusepakkuja võimaldaks kasutada ka erinevaid sissevalimispunkte.
- Ala katmine - Sageli kasutatakse VPNe mitme asukoha omavaheliseks ühendamiseks. Erinevalt mobiilsetest kaastöötajatest on erinevate asukohtade vahel loodavate ühenduste puhul käsutada palju suurem ribalaius, et tagada suuremaid andmemahtusid sisaldava info edastamist. Kolmanda osapoole kaudu toimuvate sissevalimistega ühenduste asemel ühendatakse asukohad Trusted-VPNidega tavaliselt püsiühenduse abil. Välismaal asuvate allüksuste ühendamine on eriti oluline just ülemaailmselt tegutsevate ettevõtete jaoks. Seega tuleb selgitada, kas teenusepakkuja on suuteline ja kas ta tohib tellijat sobivate ühendustega varustada.
- Tariifistruktuurid - Lisaks tehnilistele nõuetele on olulised ka finantsalased raamtingimused. Erinevate ribalaiuste jaoks väljatöötatud teenusepakettide kõrval saab sageli juurde osta täiendavaid tugiteenuseid või garantiisid, näiteks kõrge käideldavuse garantiid.
- Seire (aruanded) - Reeglina tagavad teenusepakkujad kliendile käideldavuse, konfidentsiaalsuse ja tervikluse puhul teatud kvaliteedi. Teenusetasemelepingus kindlaksmääratud nõuete täitmise jälgimise aluseks on suure jõudlusega seiresüsteem. Kliendil peab olema võimalus kindlaksmääratud nõuete täitmist vastavalt kontrollida.
- Tõrgete kõrvaldamine - Klient peab teadma, kelle poole tuleb tõrgete puhul pöörduda. Tõrked võivad tähendada näiteks andmeedastusprobleeme teenusepakkuja võrgus ja rikkis lüüse, mis loovad ühendusi LANi ja teenusepakkuja võrgu vahel.

Kõik kokkulepitud teenused tuleb võimalikult täpselt ja üheselt mõistetavalt kirjalikult fikseerida. Trusted-VPNide turvalisust tuleb regulaarselt kontrollida, et võrgu konfidentsiaalsus oleks pidevalt tagatud. Selleks peavad teenuse tellijal olema vajalikud volitused. Sõltumatu kolmanda osapoole kontrolli tulemused tuleks edastada teenusetarnijale. Kõikidele asutustele, kes peavad tellija juures kontrolle sooritama (nt järelvalveametitele), tuleb võimaldada ka VPN-teenusetarnija kontrollimist, (nt anda vajalikud sisenemisõigused ja volitused andmete kontrollimiseks).

Kontrollküsimused:

- Kas kõik lepped Trusted-VPNi teenusetarnijaga on kirjalikult fikseeritud?

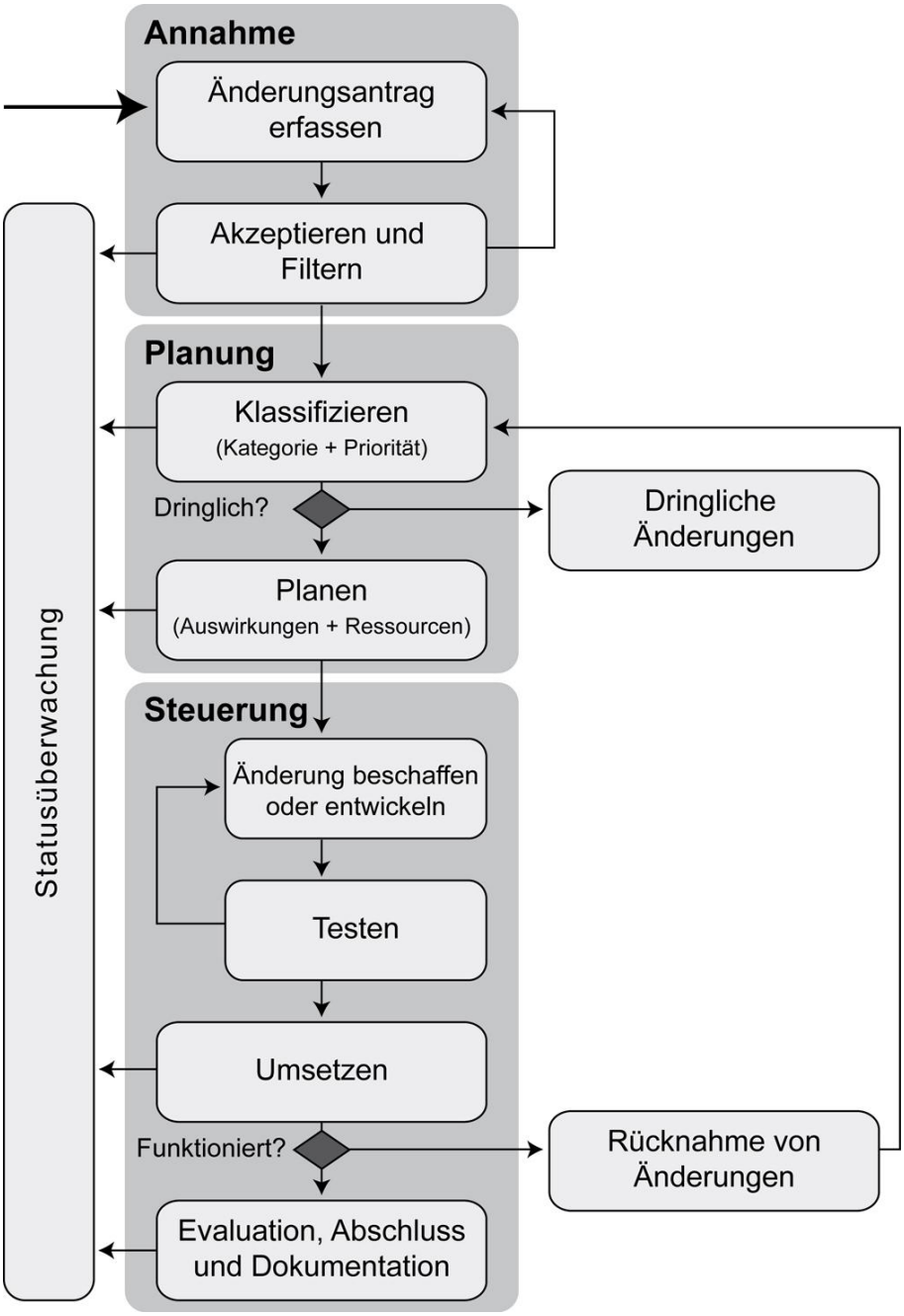
- Kas Trusted-VPNide turvalisust kontrollitakse regulaarselt?

M 2.421 Turvapaikade ja muudatuste halduse planeerimine

Algatamise eest vastutavad: IT turvaspetsialist, IT-juht
Rakendamise eest vastutavad: muudatuste haldur

Iga asutus peaks paikade ja muudatuste haldamiseks sisse seadma selgelt defineeritud protsessi ja reguleerima erinevate ülesannetega seotud vastutusalasid (vt M 2.423 Vastutusalade kindlaksmääramine turvapaikade ja muudatuste halduseks). Kõiki riist- ja tarkvaras tehtavaid muudatusi tuleks suunata ning kontrollida paikade ja muudatuste haldamise protsessi kaudu. Kõikide muudatuste tuvastamiseks ja hindamiseks peaks kõik paikade ja muudatuste haldusprotsessi hallatavad IT-süsteemid kuuluma muudatuste halduri kontrolli alla. Muudatusi süsteemide konfiguratsioonis ja olekus peaks saama teha ainult muudatuste halduse kaudu.

ITILi alusel saab paikade ja muudatuste halduse protsessi kirjeldada järgmise skeemi abil:



Joonis. Paikade ja muudatuste haldusprotsessi ülevaade

Annahme – vastuvõtt; Änderusngsantrag erfassen – muudatustaotluse esitamine; Akzeptieren und Filtern – kinnitamine ja filtreerimine; Planung – planeerimine; Statusüberwachung – oleku jälgimine; Klassifizieren (Kategorie + Priorität) – liigitamine klassidesse (kategooria + prioriteet); Dringlich? – kiireloomuline?; Dringliche Änderungen – kiireloomulised muudatused; Steuerung – juhtimine; Änderung

beschaffen oder entwickeln – muudatuse hankimine või väljaarendamine; Testen – testimine; Umsetzen – ellurakendamine; Funktioniert? – kas toimib?; Rücknahme von Änderungen – muudatuste tühistamine; Evaluation, Abschluss und Dokumentation – hindamine, lõpetamine ja dokumentatsiooni koostamine

Koordineerimine
Pärast seda, kui muudatustaotlus (request for change, RfC) on (nagu kirjeldatud meetmes M 2.422 Muudatustaotluste käsitlemine) esitatud ja kinnitatud, tuleb see esmalt kategoriseerida ja anda sellele prioriteet ning alles seejärel algab teostamise planeerimine ja koordineerimine.

Lõpetuseks tuleks enne paiga või muudatuse paigaldamist arvestada veel ka järgmiste punktidega:

- Paikade ja muudatuste hankimine või väljatöötamine. Paljud tootjad pakuvad võimalust saada infot uue müügile tulnud riist- või tarkvara või avastatud vigade ja nende kõrvaldamise kohta regulaarselt meili teel. Täiendid ja paigad pannakse tavaliselt allalaadimiseks valmis internetiserveritele. Teatud osa niisugustest allikatest on juurdepääsetavad ainult kehtiva registreerimise või tugilepingu sõlmimise korral. Sageli võimaldab paigaldatud tarkvara või operatsioonisüsteem kasutajal laadida võimalikke tarkvaramuudatusi otse vastava rakenduse või süsteemi vahendusel. Mõned tootjad pakuvad klientidele erirakendusi, et tooteid paremini hallata ja värskendada. Lisaks kasvab järjest ka selliste rakenduste hulk, mis otsivad tootja juurest interneti kaudu uuendusi päris iseseisvalt, kui kasutaja ja turvaseadistused seda muidugi lubavad ja informeerivad kasutajat nende olemasolust. Turvalisuse vaatepunktist on muudatuste automaatne paigaldamine problemaatiline. Seega tuleks hoolikalt järele mõelda, kas selliseid mehhanisme kasutada või mitte. Täiendav võimaluseks tarkvaramuudatuste hankimisel on ise vastav tarkvara välja töötada, mis hangib vajalikke muudatusi siis, kui tekivad turvaaugud või kui mõned muud nõuded tekitavad vajaduse selle järele. Kuid see nõuab lisaks erialastele teadmistele ka vajalike liideste olemasolu.
- Testimine. Pärast muudatuse paigaldamist tuleb kontrollida, kas süsteemid toimivad. Seejuures peaks vastav osakond tegema võimaluse korral iga muudatuse jaoks valiku selle tüüpilistest kasutusotstarvetest ja nendest lähtuvalt vastavad muudatused läbi testima. Tulemused tuleb dokumenteerida ja võrrelda oodatud tulemustega, et tuvastada võimalikke vigu. Lisaks tuleb uurida kõiki testi ajal loodavaid logifaile, et selgitada, kas sissekannetes leidub infot, mis võiks viidata tõrgetele.
- Integreerimine tarkvara jagamisse, integreerimise testimine. Sageli tuleb tootja pakutavate täiendite spetsiaalseid paketi- või failiformaate enne kohandada, et neid saaks kasutada automaatses tarkvara jaotamise süsteemis. See kehtib eriti siis, kui installeerimise ajal tuleb käivitada veel teisi aktiivseid komponente, näiteks kestaskripte. Muudatusi tuleb eelnevalt testsüsteemil kontrollida, kas need on piisavalt tõhusad, alles seejärel võib hakata muudatusi laiali jagama.

Rakendamine

Muudatusi peavad hakkama ellu viima muudatuste haldusega määratud töötajad. Seda protseduuri jälgib muudatuste haldur. Juhul kui muudatusi pole võimalik piisavas mahus testida, võib mõnikord osutuda mõistlikuks paigaldada need esmalt mõnele väikesele kasutajagrupile. Seejärel peaks toimuma tulemuste hindamine ja alles siis rakendatakse muudatusi ka teistel süsteemidel. Kui seda pole olude sunnil võimalik või mõistlik teha, nt kui sarnaseid muudatusi on juba sageli ilma probleemideta sisse viidud või kui omavahel sobimatud tarkavaraolekud ei võimalda muudatusi valikuliselt jaotada, võib läbi viia ka muudatuste täieliku jaotamise.

Hindamine

Sisseviidud muudatusi tuleb paigaldamise järel hinnata. Seejärel hindab tulemust kas muudatuste haldur või muutenõukogu (change advisory board, CAB), lähtudes järgmistest aspektidest:

- Kas muudatus või paik saavutas loodetud eesmärgi?
- Kas muudatuse tellija ja kasutaja on tulemusega rahul?
- Kas esines kõrvalmõjusid (tõrkeid rakendustes, mida muudatus ei puudutanud)?
- Kas planeeritud kuludest, töömahust ja ajakavast peeti kinni?

Kui muudatus oli edukas, võib muudatustaotluse või muudatuste andmekogumi sulgeda. Muudatuse ebaõnnestumise korral tuleb otsustada, kas teostatud muudatusi tuleks kohandada. Mõningatel juhtudel võib olla soovitatav muudatused tühistada ja töötada välja uus või muudetud muudatusnõue.

Ebaõnnestunud muudatuste puhul võib olla lisaks mõistlik uurida ebaõnnestumise põhjuseid ja sellest lähtuvalt IT-süsteeme või protsesse kohandada. Nii saab edaspidi sarnaseid probleeme vältida. Olenevalt muudatuste liigist ja mahust võib olla mõistlik hinnata muudatusi vahetult pärast nende paigaldamist. Teisest küljest võib olla samuti mõistlik sellega mõni päev või nädal oodata, kuni muudatuste võimalikud mõjud on ennast piisavalt ilmutanud ja on selge, kas eesmärk saavutati või mitte. Teostatud muudatused on alles siis edukalt lõpule viidud, kui neile on antud positiivne hinnang ja muudatused on dokumenteeritud. Vältimaks selle nõude unustamist, peaks muudatuste haldur laskma seda endale automaatse meeldetuletusega meelde tuletada.

Muudatuste tühistamine

Riist- või tarkvaramuudatuste tühistamise vajadus selgub otse hindamisprotsessi käigus. Kui muudatustega ei saavutatud soovitud tulemust või kui olukord muutus koguni halvemaks, tuleks muudatused tühistada, eeldusel, et see on tehniliselt võimalik ja majanduslikult vastuvõetav. Sageli on kasutatud paikade ja muudatuste haldustarkvaral selleks olemas ka vajalik tehniline tugi. Kui seda siiski ei ole, tuleb tehtud paigad ja muudatused tühistada käsitsi.

Lõpetamine ja dokumenteerimine

Kõik muudatustaotlused, riist- ja tarkvaramuudatused, testid ja nende tulemused tuleks dokumenteerida andmebaasi, olenemata sellest, kas need olid edukad või mitte (vt M 2.34 IT-süsteemi muutuste dokumenteerimine). Muudatuste paigaldamisel esinenud vigadest ja nende kõrvaldamisest saadud teadmised tuleks asutuses samuti tuleviku tarbeks dokumenteerida.

Riistvara

Paljudes asutustes on sisse seatud rutiinsed protsessid, mille käigus varustatakse

operatsioonisüsteeme ja rakendusi tarkvaravärskendustega kaitseks turvaaukude ja kahjuliku tarkvara vastu. Samasugust protseduuri on tegelikult tarvis ka riistvara jaoks, kuid kui riistvara töötab nõuetekohaselt, unustatakse see sageli ära. Paljudes IT-seadmetes kasutatakse kompaktseid operatsioonisüsteeme, mis on sageli kohandatud vastava riistvara jaoks. Siia alla kuuluvad näiteks marsruuterid, kommutaatorid, võrguprinterid ja mobiiltelefonid. Seetõttu on tarvis tagada, et ka need seadmed oleksid kaasatud muudatuste haldamisse ja et ka neid varustataks turvalisuse tagamiseks oluliste tarkvaravärskendustega.

Kontrollküsimused:

- Kas paikade ja muudatuste haldamise jaoks on defineeritud eraldi protsess?
- Kas paikade ja muudatuste haldur suunab ja kontrollib kõiki riistvarasse ja tarkvarasse sisseviidavaid muudatusi?

M 2.422 Muudatustaotluste käsitlemine

Algatamise eest vastutavad: infoturbejuht, IT-juht

Rakendamise eest vastutavad: muudatuste haldur

Paikade ja muudatuste taotlused tuleb sisse anda ja läbi töötada kindlaksmääratud protseduuri alusel.

Muudatustaotluste esitamine ja haldamine

Esmalt tuleb kõiki muudatustaotlusi (request for changes, RfC) hallata. Kogu vajaliku info kokkukogumiseks on soovitatav koostada taotluse esitaja jaoks blankett (vt muudatusnõude näidist IT etalonturbe abimaterjalide alt). Vastav taotlus on muu hulgas vajalik ka muudatuste kooskõlastamiseks (vt M 2.427 Muudatustaotluste kooskõlastamine). Kui olemasoleva probleemi lahendamiseks on esitatud muutmise taotlus, tuleks koos sellega dokumenteerida viide probleemile, milleks on tavaliselt andmebaasis kajastuva probleemi registreerimisnumber. Mitte igat muudatustaotlust ei käsitleta paikade ja muudatuste protsessis tavapärase muudatusena. Osasid rutiinseid muudatusi, mida on selgelt kirjeldatud, mis viiakse läbi standardiseeritult, kuid kajastavad siiski muudatust, saab käsitleda ka teenindustaotlusena. Teenindustaotlus oleks näiteks parooli taastamine ja nt paikade ja muudatuste halduse kontekstis muudatus teenuse sisselogimisteates (tekstis, millega teenus ühenduse loomisel endast võrguliidese kaudu märku annab).

Muudatustaotluste filtreerimine ja kinnitamine

Kui muudatustaotlus on laekunud, kontrollib seda muudatuste haldur (change manager). Kontrolli käigus tuleks tuvastada teostamatud, ebavajalikud või topelt esitatud muudatustaotlused. Sellised taotlused tuleb koos põhjendusega tagasi lükata. Taotluse esitajad saavad seeläbi võimaluse muudatustaotluse üle järele mõelda ja selle ümber sõnastada. Kui muudatustaotlus on kinnitatud, võetakse info muudatuste andmekogumisse, et muudatus ellu viia.

Andmekogu võib asuda tarkvaratööriistas, paberil või isekoostatud andmebaasis. Edasise protseduuri käigus lisatakse muudatuste andmekogumile veel järgnev info:

- Tuvastatud prioriteet ja kategooria
- Mõjude hindamine ja info vajalike ressursside kohta
- Muudatuste halduri või muutekogu (change advisory board, CAB) hinnang
- Autoriseerimise kuupäev ja kellaaeg
- Muudatuse teostamise plaanitud kuupäev
- Muudatuse sisseviimise värske kuupäev ja kellaaeg
- Hindamise kuupäev
- Testitulemused ja esinenud probleemid
- Ettepaneku või taotluse võimaliku tagasilükkamise põhjus
- Protseduuriskeem ja hindamisandmed

Muudatustaotlus liigitamine (prioriteet ja kategooria)

Kui muudatustaotlus on vastu võetud, tuleb sellele anda prioriteet ja kategooria:

- Prioriteet kirjeldab muudatuse olulisust ning sõltub pakilisusest ja võimalikest mõjudest. Kui tegu on teadaoleva vea korrektuuriga, mis on juba varem paikade ja muudatuste halduse raames liigitatud, võidakse prioriteet olenevalt oludest ka juba kohe üle kanda. Sealjuures peaks muudatuste haldur muudatuse prioriteeti veel kord kontrollima ja vajaduse korral korrigeerima. Sama kehtib turvapaikade ja värskenduste puhul, mida taotleb infoturve. Lõpliku prioriteedi määrab siiski muudatuste haldur, võttes arvesse teisi töösolevaid muudatustaotlusi.
- Muudatuste haldur määrab kategooria, tuginedes oodatavatele mõjudele ja vajaminevatele ressurssidele.

Prioriteetidest ja kategooriatest koosnev liigitus määrab muudatustaotluse edasise töötlemise ja kirjeldab seeläbi planeeritava muudatuse tähendust. Muudatustele määrab prioriteedid muudatuste haldur ning prioriteedid on jagatud erinevatesse astmetesse, kusjuures turvaosakonnale peaks olema antud vetoõigus liiga madala või valesti antud prioriteedi tühistamiseks.

Muudatuste haldur tohib näiteks määrata järgmisi prioriteediastmeid:

- Kõrgeim prioriteet: kõrgeima prioriteediga muudatustaotlus puudutab näiteks probleemi, mis põhjustab sihtgrupile IT-teenuste kasutamises tõsiseid takistusi. See prioriteet määratakse ka kiirelt vajaminevatele IT-muudatustele (nt turvalünga sulgemisele kaitseks internetis liikuva ussviiruse eest). Selle prioriteediga muudatusi nimetatakse ka tungivateks muudatusteks (urgent changes). Need muudatused erinevad kõrge ja tavalise prioriteediga muudatustest selle poolest, et nende puhul peavad vajaminevad ressursid olema kohe kättesaadavad. Samuti võib osutuda vajalikuks CAB või infoturbe haldussüsteemi meeskonna kiireloomuline koosolek. Kui muudatustele määratakse see prioriteet, võivad kõik varasemad plaanid arvestada kas viivituse või esialgu lausa peatumisega.
- Kõrge prioriteet: see prioriteet kätkeb endas nt tõsisest veast tulenevat muudatust või muudatust, mis on seotud muude kiireloomuliste tegevustega. See muudatus muutub peamiseks arutlusteemaks järgmisel CAB koosolekul, kus on tarvis määrata ressursside kasutamine seoses selle testimise ja sisseviimisega.
- Tavaline prioriteet: see muudatus ei ole väga pakiline ega avalda olulist mõju, kuid sellele vaatamata ei tohi seda siiski ka edasi lükata. CAB-s saab see muudatus ressursside jaotamisel tavalise prioriteedi.
- Madal prioriteet: madala prioriteediga muudatus tuleks sisse viia, kuid sellega võib oodata kuni soodsa hetke saabumiseni (nt järgneva versiooni paigaldamiseni või plaanipärase hoolduseni).

Üldjuhul määrab kategooriad muudatuste haldur, kuid ka siin peaks turvahaldusel olema vetoõigus liiga madala kategooria määramise vastu. Kategooriad peavad andma hinnangu, kuidas muudatus mõjub ja kuidas koormab muudatuse sisseviimise protsess asutuse tööd.

Näiteks saab määrata järgmised kategooriad:

- Vähesed tagajärjed: selle kategooria muudatus nõuab vähe aega ja vaeva. Muudatuste haldur saab selle muudatuse kinnitada ja ei pea seda esitama kinnitamiseks CAB-le.
- Märkimisväärsed tagajärjed: sellesse kategooriasse kuuluvad muudatused, mille töökulu on suur ja mis avaldavad märkimisväärset mõju IT-teenuste kasutamisele. CAB arutab sellised muudatused läbi, et määratleda vajalik tööde maht ja vähendada riske. Koosoleku ettevalmistamiseks saadetakse esmalt vajalik dokumentatsioon CAB liikmetele, vajaduse korral ka mõningatele IT-spetsialistidele ja arendajatele.
- Kaugeleulatuvad tagajärjed: sellesse kategooriasse kuuluv muudatus on väga suure töömahuga. Sellise muudatuse jaoks vajab muudatuste haldur esmalt turvaosakonna meeskonna volitust. Seejärel tuleb muudatus esitada CAB-le hindamiseks ja edasiseks planeerimiseks.

Paikade ja muudatuste haldamise protsessis osalevad töötajad planeerivad kõikide vastuvõetud muudatuste teostamise. Vajaduse korral toimub see koostöös CAB-ga. Paikade ja muudatuste haldamise protsessis on siinkohal oluline arvestada asjakohaste tehnika- ja personaliressurssidega ning hinnata mõju, mida muudatuste elluviimine võib igapäevatööle avaldada.

Arvestada tuleb vähemalt järgmiste aspektidega:

- Asjassepuutuvate IT-süsteemide käideldavus
- Asjassepuutuvate IT-teenuste usaldusväärsus ja taastatavus
- Asjassepuutuvate IT-teenuste hädaolukorra halduse planeerimine
- Tõrkeplaanid, st avariiplaanid reageerimiseks muudatustest tulenevatele ebasoovitavatele tagajärgedele
- Andmevarundusprotseduurid
- Muudatuste võimalik mõju teistele IT-teenustele (kõrvalmõjud)
- Vajalikud tehnika- ja personaliressursid ja nende kulud
- Vajalikud volitused
- Finantside kooskõlastused, kui täiendi paigaldamine on kulukas või kui tuleb kasutusele võtta toote uuem versioon (upgrade)
- Tehnilised kooskõlastused, kui on tarvis soetada täiendavaid IT-süsteeme
- Ärialased kooskõlastused, kui uuendamine mõjutab nt tarnijat
- Vajalike IT-spetsialistide arv ja kättesaadavus
- Muudatuse soovitud sisseviimise aeg
- IT-teenuste kasutamisest tulenevad tagajärjed ja sellest tekkivad muudatused teenusetasemelepingutes
- Võimalikud konfliktid seoses teiste muudatustega

Kontrollküsimused:

- Kas paiku ja muudatusi kajastavate taotluste esitamiseks ja läbivaatamiseks on olemas kindlaksmääratud meetod?

- Kas kõik muudatustaotlused (RfC-d) kogutakse kokku ja dokumenteeritakse?
- Kas muudatuste haldur kontrollib kogutud muudatustaotlusi?
- Kas iga muudatustaotlus saab prioriteedi ja kategooria?
- Kas vastavate prioriteetide jaoks eraldatakse vajalikud ressursid?

M 2.423 Vastutusalade kindlaksmääramine turvapaikade ja muudatuste halduseks

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT-juht
Rakendamise eest vastutavad: IT-juht

Paikade ja muudatuste haldussüsteemi ülesehitamisel tuleb määrata mitmeid vastutusalasid. Sealjuures tuleb tagada, et iga ülesande ja organisatsiooni valdkonna jaoks oleks täpselt määratletud, millised on konkreetsete töötajate vastutusalad paikade ja muudatuste haldamise protsessis ja kuidas toimub koostöö koordineerimine erinevate valdkondade vahel. Paljudel juhtudel on tavaline, et asutuse erinevate valdkondade töötajatel on muudatuste sisseviimisel ka erinevad vastutusalad. Nii võib nt üks valdkond vastutada peamiste operatsioonisüsteemide hooldamise eest ja teine valdkond operatsioonisüsteemile installeeritud teenuste (nt meiliserverite, erirakenduste jms) eest. Selle tagajärjel võib tekkida olukord, kus kogu süsteemi paikade eest vastutavad erinevad valdkonnad. Sellistel juhtudel on eriti oluline, et vastutusalad oleksid määratletud võimalikult täpselt. Selliselt jaotatud vastutusalad peaksid kajastuma ka volituste kontseptsioonis, paikade ja muudatuste jaotamise tööriistade konfiguratsioonis ja IT-süsteemis.

Muudatused peavad ilmtingimata toimuma koordineeritult. Ükski töötaja ei tohi teha muudatusi seda eelnevalt muudatuste halduriga kooskõlastamata. Ka kõik IT käitusega seotud töötajad peavad oluliste muudatuste puhul alati muudatuste halduriga nõu pidama. See tagab, et üksikud muudatused ei hakka üksteist takistama ega vii süsteemi täielikku avariiolukorda.

Muudatuste haldur (change manager)

Muudatuste koordineerimise ja hindamise keskne roll on muudatuste halduril. Selleks tuleb asutuses nimetada isik, kes tagab paikade ja muudatuste tõhusa haldamise. Muudatuste haldur filtreerib, võtab vastu ja liigitab kõik muudatustaotlused. Lisaks vastutab ta vajalike volituste ja ka muudatuste planeerimise, koordineerimise ja elluviimise eest.

Muutenõukogu (change advisory board, CAB)

Vähemalt keskmise suurusega asutuses või keerukate IT-infrastruktuuride olemasolu korral peaks muudatuste haldurit toetama muutenõukogu. Praktikas on osutunud mõistlikuks võtta lisaks paikade ja muudatuste ülesannete tehnilise teotamisega tegelevatele isikutele CAB liikmeks ka üks isik asutuse igast erialavaldkonnast. CAB kutsutakse regulaarselt kokku, et muudatusi hinnata ja aidata muudatuste halduril neid analüüsida, prioriteetide järjekorda seada ja kinnitada. Tavaliselt esitatakse CAB-le ainult tõsisemate muudatustega seonduv info. Seetõttu võib CAB kooslus ka erineda. Kõik CAB liikmed võiksid kokku saada näiteks iga kolme kuu järel, et arutada kriitilisi muudatustaotlusi. Vähekriitiliste, regulaarsete muudatuste jaoks võivad kokkulepped toimuda vahetult muudatuste halduri ja vastutava administraatori või testimismeeskonna vahel. Selleks, et CAB saaks oma ülesandeid nõuetekohaselt näita, peavad tema liikmed suutma hinnata muudatuste tähendust ja mõju, seda nii ärieesmärkide ja -protsesside seisukohalt kui ka tehnilisest vaatepunktist.

Kontrollküsimused:

- Kas igas organisatsiooni valdkonnas on paikade ja muudatuste haldamise

jaoks määratud vastutavad töötajad?

- Kas paikade ja muudatuste halduses määratud vastutusalad kajastuvad ka volituste kontseptsioonis?
- Kas muudatuste haldur on määratud?
- Kas kõik paikade ja muudatuste haldamise protsessiga tegelevad isikud on kursis paikade ja muudatuste haldamise, infoturbe ja krüptograafiliste protseduuridega seotud mõistetega?

M 2.424 Paikade ja muudatuste haldamise tööriistade turvapoliitika

Algatamise eest vastutavad: infoturbejuht, IT-juht

Rakendamise eest vastutavad: IT turvaspetsialist, muudatuste haldur

Paikade ja muudatuste haldamise tööriist on kesksel kohal paikade ja muudatuste haldamise protsessi elluviimises ning asutuse turvalise ja nõuetekohase töö tagamiseks vajaliku tarkvara jaotamises. Paikade ja muudatuste haldamine peab toimuma vastuvõetava organisatoorse ja tehnilise töömahuga. Seejuures tuleb muu hulgas arvestada äriprotsesside ja sellega seoses ka andmete ja süsteemide turbevajadusega. Seega tuleks paikade ja muudatuste haldamise jaoks koostada eraldi turvapoliitika. See peab olema kooskõlas asutuse turvakontseptsiooni ja sellest tuletatud turvapoliitikatega. Erinevad aspektid, mille jaoks tuleb vastavas turvapoliitikas sõnastada eeskirjad, on järgmised:

Planeerimist puudutavad nõuded

- Tarkvaratööriista serverirakenduse skaalale paigutamise tarbeks tuleb juba eelnevalt sõnastada nõuded dubleerimise ja koormuse jaotamise kohta, samuti tehnilise liiasuse kasutamise kohta.
- Tagamaks turvalist võrguühendust asutuseväliste allikatega, kust hangitakse paiku või muudatusi, nt tootjatega, tuleb määratleda asjakohased reeglid. Näiteks saab kliendi ja kasutatava tarkvara tootja vahelist otseühendust vastavate turvalüüsireeglite abil ümber suunata proksidele.
- Paikade ja muudatuste tervikluse ja autentsuse usaldusväärseks kontrollimiseks tuleb kindlaks määrata sobivad kontseptsioonid ja komponendid.
- Formuleerida tuleb nõuded, mis sätestavad, et paikade ja muudatuste halduse tööriista käitamise, hädaolukorra ja taaskäivitamise tarbeks peab alati olema saadaval vajalik dokumentatsioon. Nõuete alla kuulub muu hulgas ka punkt, et vastavat dokumentatsiooni tuleb hoida värskena. Lisaks tuleb määratleda koht, kus tuleks dokumentatsiooni hoida, ja kui mitmes eksemplaris peab dokumentatsioon olemas olema.

Administreerimisalased nõuded

- Paikade ja muudatuste haldusega tegelevate töötajate jaoks, samuti paikade ja muudatuste halduse tarkvara hallatavate teenuste jaoks on vaja, et koostataks volituste kontseptsioon.
- Administraatorite jaoks tuleb kindlaks määrata, kuidas volitusi anda, milliseid volitusi nad saavad ja milliseid nad ise tohivad anda.

Installeerimisalased nõuded

Paikade ja muudatuste haldustööriistade konfiguratsioonid peavad olema turvalised. Vastavad konkreetsed seadistused sõltuvad oluliselt asutuses kasutatavatest rakendustest ja IT-süsteemidest. Üldistavaid juhiseid leiate selle kohta meetmest M 4.237 IT-süsteemi turvaline aluskonfiguratsioon .

- Tuleb kindlaks määrata, kuidas seadistada paikade ja muudatuste haldustööriista jaoks olulisi IT-ressursse, näiteks paikade ja muudatuste jaotamistarkvara komponente ja operatsioonisüsteemide komponente, arvestades seejuures piisavalt turbeaspektidega.

- Paikade ja muudatuste halduse tööriist tuleb sobival moel LANis eraldada. Uusi muudatusi ja paiku ei tohiks testida tootmisvõrgus, vaid eraldi testimisvõrgus.

Turvalise käitamise nõuded

- Paikade ja muudatuste haldustööriista tööks tuleb määratleda eeskirjad ja protseduurid, näiteks, kes tohib seda kasutada ja kus tohib muudatusi teha.
- Paiku ja muudatusi hangitakse sageli interneti kaudu. Ühendused avalike või väheusaldusväärsete võrkudega peavad olema alati turvalüüsidega kaitstud.
- Paikade ja muudatuste haldustööriist ise tuleb integreerida paikade ja muudatuste haldamise protsessi. Seoses sellega tuleb määrata, kuidas käsitleda paikade ja muudatuste haldustööriistas endas tehtavaid riist- ja tarkvaramuudatusi.

Logimis- ja seirenõuded

Kindlaks tuleb määrata paikade ja muudatuste haldustööriista puhul tekkivate andmete seire, logimine ja logiandmete analüüsimine.

Andmete varundamine

Kindlaks tuleb määrata sobiv andmevarundusmeetod. Andmete varundamisel tuleks regulaarselt varundada vähemalt järgmisi komponente:

- Paikade ja muudatuste halduse jaoks vajaminevate tööriistade konfiguratsioonid ja seadistused
- IT-süsteemide hetkel kehtivaid konfiguratsioone sisaldavad andmebaasid
- Isetõlgitud tarkvara puhul täpsed kompileerimisseadistused
- Installeeritud paigad ja muudatused
- IT-süsteemide viimased taastepunktid
- Võimalikud olemasolevad vanemad versioonid, nt kuna tarkvara uusimat versiooni pole veel piisavalt testitud või seda ei saa kõikidel süsteemidel kasutada
- Tarkvarapakettide kontrollsummade ülevaade, mis tuleks igaks juhuks salvestada ainult ainukirjutusega WORM-andmekandjale (write once read many)
- Lisaks tuleb paikade ja muudatuste haldamise protseduur integreerida asutuse andmevarunduspoliitikasse (vt M 6.32 Regulaarne andmevarundus).

Tõrked ja ootamatuste ennetamine

Ootamatuste ennetamiseks tuleb arvestada paikade ja muudatuste halduse hallatavate rakenduste ja IT-süsteemide avariiplaanidega. Sõltuvalt paikade ja muudatuste haldustööriistale esitatud käideldavusnõuetest tuleks kaaluda, kas paikade ja muudatuste haldustööriista jaoks tuleks koostada eraldi avariiplaan, et olla valmis paikade ja muudatuste paigaldamise ajal või hiljem esineda võivateks ebasoodsateks mõjudeks.

Kontrollküsimused:

- Kas paikade ja muudatuste haldustööriista jaoks on koostatud turvapoliitika?
- Kas turvapoliitikas on arvestatud kõikide paikade ja muudatuste haldustööriista kasutamiseks oluliste aspektidega?

M 2.425 Asjakohane turvapaikade ja muudatuste haldusinstrumentide valik

Algatamise eest vastutavad: infoturbejuht, IT-juht, muudatuste haldur

Rakendamise eest vastutavad: muudatuste haldur, IT-juht

Paikade ja muudatuste haldamise protsessi saab lihtsustada erinevate toodete või tootekombinatsioonidega. Tööriista kasutamiseks paikade ja muudatuste protsessis võib olla mitmeid põhjuseid. Sageli on määrava tähtsusega heterogeensed IT-infrastruktuurid ja ressursside tõhusam kasutamine.

Enne paikade ja muudatuste haldamisprotsessi jaoks tööriista soetamist tuleks tuvastada nõuded ja raamtingimused, et leida asutuse jaoks sobiv lahendus. Toote hindamisprotseduur on alati sarnane ja lähtub asutuses kehtivast paikade strateegiast olenemata sellest, kas paikade ja muudatuste haldusel läheb tarvis tööriista operatsioonisüsteemi, tootja erineva tootevaliku või suure heterogeense IT-koosluse jaoks.

Järgneb valik olulisemaid omadusi, millega tuleb toote valimisel arvestada ja mis on tarkvaratööriistale esitatavate nõuete sõnastamise aluseks.

- Platvormide tugi – selle mõiste all on olulised esmajoones kaks aspekti. Ühest küljest vaadeldakse seda, milliseid platvorme paikade ja muudatuste protsessi puhul toetatakse, teisest küljest aga, millistel platvormidel on tarkvaratööriist suuteline töötama. Täpsemalt tuleks vaadelda eriti just esimest aspekti, kuna näiteks server-klient-valdkonnas toetab suurem osa tööriistade tootjatest muudatuste sisseviimist Microsofti toodetesse. Siiski ei tähenda see kohe, et kaetud oleks kogu asutuses olev tootevalik alates töökoha ja serveri operatsioonisüsteemist kuni üksikute toodeteni.
- Paikade analüüs – osad tootjad keskenduvad jaotusprotsessiga seotud suure hulga värskenduste käitlemisele ja nende kiirele jaotamisele, samuti tarneolekust teavitamisele. Osad edastavad jällegi rohkem infot paikade ja nende põhjuste kohta, osalt koos asjassepuutuvate failide nimekirja, kitsaskohtade täpse kirjelduse ja tooteomaste testaruannetega. Riist- ja tarkvaramuudatuste sisemiseks liigitamiseks võib detailne info pakkuda asendamatut abi just kiiret jaotamist vajavate turvapaikade puhul.
- Paikade verifitseerimine – suurem osa tootjatest annavad koos paikade ja muudatustega kaasa kontrollsummasid, sõrmejälgi või allkirju, et kinnitada nende ehtsust ja terviklust, kuid ainult vähesed tööriistad oskavad neid tõendeid ka reaalselt kontrollida. Sel põhjusel esineb oht, et soovimatu tarkvara jaotatakse asutuse peale massiliselt laiali, põhjustades seeläbi tõsiseid probleeme. Turvalisuse põhjustel ei tohiks seega kasutada muudatustööriistu, millel see funktsioon puudub.
- Paikade strateegia – tööriist peab võimaldama paindlikku konfigureerimist, et automatiseerida võimalikult palju väljavalitud paikade strateegias ettenähtud töösamme. Erinevate platvormide tõttu võivad siin olla suured erinevused. Muudatuste protseduuri raames ettevõetavad sammud peaksid olema tööriista poolt selgelt, vajaduse korral isegi auditeeritavalt dokumenteeritud. Hilisemad muudatused protsessis peaksid olema tööriistaga ühildatavad
- Jaotamine– kõik paigad ei sobi igale süsteemile. Tööriist peaks võimaldama grupeerida süsteeme ja rakendusi vabalt defineeritavate atribuutide baasil,

nt lähtuvalt turbevajadusest, asukohast ja organisatsiooni allüksusest. Nendest atribuutidest saab tuletada IT süsteemiprofiile, mis vastavad asutuse standardiseeritud süsteemitüüpidele.

- Tagasipööre (rollback) – ükski tarkvara pole täiuslik. Hoolimata kõikidest eeltestidest võib tekkida vajadus sisseviidud paigad tühistada. Selle protseduuri automatiseerimine säästab vea esinemise korral aega ja raha! Kui vigaseid muudatusi ei saa aegsasti ja vähese vaevaga tühistada, võib see asutust tõsiselt kahjustada.
- Seisundi hindamine – muudetud riist- või tarkvara korrektseks jaotamiseks kõikidele süsteemidele peab olema automaatsüsteem. Ka üldise tarkvara jaotamise puhul võib esineda probleeme süsteemi ühendamise või käideldavusega. Süsteem võib erinevate süsteemiolekute tõttu paigast keelduda. Seega on oluline, et muudatuste tööriist tuvastaks kõikide süsteemide paikade oleku (patch status). Olenevalt strateegiast peaks tööriist probleemide esinemise korral kas jätkama tehnilise paikadeprotsessiga ülejäänud IT-süsteemide juures või jätma teatud süsteemigrupid vahele või lõpetama paikade protsessi.

M 2.426 Turvapaikade ja muudatuste halduse integreerimine äriprotsessidesse

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, muudatuste haldur

Rakendamise eest vastutavad: muudatuste haldur

Olenevalt tehtavast muudatusest võib olla vajalik mõnda rakendust või IT-süsteemi taaskäivitada, mille tagajärjel ei saa seda rakendust või süsteemi mõnda aega tootmisprotsessis kasutada. Pealegi ei saa isegi hoolikalt tehtud testid alati välistada probleeme riist- või tarkvaramuudatuste jaotamisel vajalikesse rakendustesse ning võib esineda koguni töö seiskumist ja koos sellega ka süsteemi täielikku avariid. Hoolimata tehtud testidest on sel põhjusel oluline arvestada ka täiesti eraldi asjassepuutuvate tööprotsesside hetkeolekuga. Näiteks võib olla mõistlik mõnda riist- või tarkvara muudatust paar päeva edasi lükata vaatamata sellele, et asjassepuutuv süsteem on hetkel liigitatud turbe seisukohast kriitilisse kategooriasse. Vastav süsteem võib pakkuda olulisi, asutuse jaoks vajalikke teenuseid. Juhtkond võiks paikade ja muudatuste halduri põhjustatud äriprotsesside katkemist pidada suuremaks probleemiks kui lahendamata turvaprobleem.

Riist- ja tarkvaramuudatuste jaotamiseks tuleb seega teavitada kõiki osapooli saabuvatest muudatustest ja oletatavatest seisakuaegadest. Üksikute osapoolte hulka kuuluvad kõik osakonnad, mis vajavad vastavat süsteemi. Eriti oluline on kaasata muudatuste prioriteetide määramisse ja sobiva aja leidmisesse just need osakonnad, mille ülesanded sõltuvad vastavatest rakendustest ja IT-süsteemidest kõige rohkem. Lisaks muudatuste haldurile ja CAB-le peab olema veel vähemalt üks nõupidamistasand, mis otsustab vajaduse korral prioriteetide üle (vt M 2.422 Muudatustaotluste käsitlemine). See nõupidamistasand tuleb kokku panna asutuse juhtkonna baasil.

Kontrollküsimused:

- Kas asjassepuutuvaid osakondi informeeritakse eelseisvatest muudatustest?
- Kas muudatuste planeerimisel on arvestatud asjassepuutuvate äriprotsesside hetkeolekuga?
- Kas on olemas asutuse juhtkonna liikmetest koosnev nõupidamistasand, mis suudaks kahtluse korral otsustada riist- või tarkvaramuudatuste prioriteetide ja tööde ajakava üle?

M 2.427 Muudatustaotluste kooskõlastamine

Algatamise eest vastutavad: infoturbejuht, IT-juht

Rakendamise eest vastutavad: muudatuste haldur

Paikade ja muudatuste haldamisprotsessi edukus sõltub edukast suhtlemisest, kuna üksikute protsessisammudega, nagu kirjeldatud meetmetes M 2.421 Turvapaikade ja muudatuste halduse planeerimine ja M 2.422 Muudatustaotluste käsitlemine , tohib jätkata ainult siis, kui on olemas vastutavate osapoolte sellekohane luba. Riist- või tarkvarasse muudatuste sisseviimisele eelnevasse kooskõlastamisprotsessi tuleb olenevalt olukorras kaasata lisaks muutenõukogule (CAB) veel ka teisi sihtgruppe. Milliseid täpselt, see sõltub asutuse suurusest ja struktuurist. Üldjuhul tuleks kaasata riist- või tarkvaramuudatuse taotleja, IT konsultatsioonipunkt ja muudatuste puudutatava lõppkasutaja või valdkonna esindaja.

Tööprotsesside eest vastutav töötaja peab tundma riist- või tarkvaramuudatuste taotluste protseduuri, samuti seda, millised protseduurid peab taotlus läbima ja millist infot läheb taotluse protseduuri raames tarvis. Oluline aspekt on muudatustaotluse (RfC) sisu kvaliteet. Vajalik info koostatakse sageli blanketi kujul või erirakenduses sisestusblanketi abil. Seega tuleks eriti hoolikalt kindlaks määrata, milline info on vajalik ja kuidas peaks blankett välja nägema ning selle võimalike sihtgruppidega kooskõlastama. Lisaks tuleb paikade ja muudatuste halduse protsessi abil tagada, et tõsiste muudatuste puhul oleks kõigil vastutavatel spetsialistidel võimalik taotluse kohta arvamust avaldada, et vältida sihtgrupi vaatepunktist soovimatute muudatuste sisseviimist.

Teisest küljest ei tohi taotluse läbivaatamine kesta liiga kaua. Samuti peab olema võimalik käsitleda olulisi muudatusi kiirendatud korras. Seejuures peab olema vajaduse korral lubatud kindla definitsiooni alusel regulaarset paikade ja muudatuste haldamise protsessi lühendada.

Kontrollküsimused:

- Kas muudatuse sisseviimisele eelnevas kooskõlastamisprotsessis arvestatakse kõikide asjassepuutuvate sihtgruppidega?
- Kas on tagatud, et kõik muudatusest puudutatud sihtgrupid saavad tõendatavalt selle kohta arvamust avaldada?
- Kas on olemas kindlaksmääratud meetod, mis võimaldab oluliste muudatusnõuete käsitlemist kiirendada?

M 2.428z Skaleeritavus paikade ja muudatuste halduses

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: muudatuste haldur, administraator

Paikade ja muudatuste haldustööriista soetamisele kehtivad sageli teistsugused nõuded kui selle hilisemal kasutamisel. IT-maastik kasvab ja sinna lisanduvad uued IT-süsteemid, millega peab paikade ja muudatuste haldus oskama arvestada. Seega on oluline, et paikade ja muudatuste haldustööriist oleks skaleeritav. Milline skaleeritavus on süsteemi soetamisel vajalik, tuleb tuvastada planeerimisfaasis.

Skaleeritavust mõjutavad põhitegurid on olemasolevast IT infrastruktuurist lähtuv riist- või tarkvaramuudatuste jaotamisel nõutud kiirus ja vajadus vea korral IT-süsteeme massiivselt korraga taastada. Jaotamisprotsessi jaoks tuleb defineerida katkestuspunktid nendeks juhtudeks, kus selgub, et on tegeletud vigaste riist- või tarkvaramuudatuste jaotamisega. Kuna see võimalus sõltub olulisel määral teostamiskiirusest, tuleb kindlaks määrata, kus, kuidas ja millal on jaotamise teadlik katkestamine võimalik. Veendumaks, kas oodatav teostamiskiirus on tagatud, saab esmalt lähtuda IT infrastruktuuri tööväärtustest, nagu võrgu ribalaiused ja süsteemi koormus. Teostamise kiirust tuleb siiski enne süsteemi kasutuselevõttu testidega praktikas kontrollida. IT infrastruktuuris esineda võivatele nõrkadele kohtadele tuleb kiirelt reageerida, täiendades või muutes vajalikku konfiguratsiooni. Lõppväärtustele tuleb juurde arvutada IT infrastruktuuri oletatav kasv vahetult pärast kasutuselevõtu algust, et vältida kohest järjekordset süsteemi skaleerimis- ja ümberehitamisfaasi.

Esmalt tuleks koguda täiendavaid kogemusväärtusi ettevõtte enda seest ja kasutada neid täiendavate pidepunktidena süsteemi edasisel laiendamisel. Praktikas on end tõestanud asutuse füüsilisest ja geograafilisest IT-struktuurist lähtuv skaleeritavuse rakendamine. Kui asutuse paikade strateegia seda lubab, võib näiteks asutuse vastavates asupaikades kasutada jaotussüsteeme, mis saavad ja jaotavad tarkvaramuudatusi ainult vastava asukoha IT-süsteemide jaoks. Kui asutuse paikade strateegia on seevastu tsentraliseeritud ülesehitusega või kui paikade ja muudatuste haldamise tööriistade käitamine on tellitud väljast, on soovitatav valida selline skaleeritavus, et igas asukohas käitataks eraldiseisvaid süsteeme. Kui paikade ja muudatuste haldamise toetamiseks kasutatakse tarkvaratööriistu, tuleb jälgida, et need vastaksid skaleeritavusnõuetele.

Kontrollküsimused:

- Kas riist- või tarkvaramuudatuste jaotamisel on määratud katkestuspunktid juhuks, kui riist- või tarkvara võib sisaldada vigu?
- Kas enne paikade ja muudatuste haldustööriista kasutuselevõttu kontrollitakse hoolikalt selle töökiirust?

M 2.429z Muudatustaotluste tulemuste hindamine

Algatamise eest vastutavad: IT-juht, muudatuste haldur
Rakendamise eest vastutavad: muudatuste haldur

Haldusprotsessid, nagu paikade ja muudatuste haldamine, vajavad pidevat täiustamist, optimeerimist ja kohandamist asutuse muutuvate tingimustega. See, kuidas olemasolevaid meetmeid ellu viiakse, näitab muu hulgas ka paikade ja muudatuste haldamisprotsessi küpsust. Riistvara, tarkvara või konfiguratsiooni muudatustele eelnevad testid on mõeldud esmajoones kontrolliks, et veenduda, kas muudatused toimivad oma ettenähtud kasutusvaldkonnas või mitte. Kuna muudatused peavad reeglina kõrvaldama mõne tõrke, peab muudatustaotluse esitaja esitama sisseviidud muudatuse kohta oma hinnangu. Seetõttu on järeltestide tegemine täiesti möödapääsmatu. Järeltestide eelduseks on lähtesüsteemide valimine, mis kindlustab kvaliteedi. Lisaks tuleb tagada, et järelteste viiksid läbi sellised erialaselt pädevad kasutajad, kes tunnevad asutuse tööprotsesse ja oskavad võimalikke vigu hinnata. Kui muudatus oli tingitud turvakaalutlustest, peab järeltestid algatama muudatuste haldur ja läbiviijaks peab olema erialaselt pädev kasutaja. Järeltestide ja hindamiste tulemused dokumenteeritakse paikade ja muudatuste haldusprotsessi raames. Muudatuste haldurile, muutenõukogule ja turvahaldusele esitatakse andmed eesmärgiga täiustada protsessi.

Kontrollküsimused:

- Kas värskenduste hilisemaks kontrollimiseks viiakse läbi järelteste?
- Kas kvaliteedi tagamiseks valiti välja etalonsüsteemid?
- Kas järeltestide ja hindamiste tulemused dokumenteeritakse paikade ja muudatuste protsessi raames?

M 2.430 Turvapoliitikad ja eeskirjad infoturbe tagamiseks mobiilse töö ajal

Algatamise eest vastutavad: Infoturbejuht

Rakendamise eest vastutavad: Infoturbejuht, kasutaja

Piisav infoturve pole vajalik mitte ainult asutuse ruumides, vaid ka väljaspool asutust. Töötajad peavad ka äri- või erareisidel tundliku infoga hoolikalt ümber käima. Tuleks koostada turvapoliitika, mis kirjeldab aspekte, millega peavad töötajad äri- või erareisidel arvestama. See võib olla integreeritud ka mobiilsete IT-süsteemide turvalisse kasutamisse (vt M 2.309 Mobiilse IT-kasutuse turvapoliitika ja eeskirjad). Lisaks tuleks töötajatele koostada lühike ja ülevaatlik infoleht aspektidest, mida tuleks järgida mobiilse töö puhul.

Töötajate teavitamine võimalikest ohtudest

Töötajatele tuleb selgitada, et nad ei tohi ringi liikudes vahetada konfidentsiaalset infot võõraste isikutega. Eriti oluline on sidepartneri täpse identiteedi väljaselgitamine neil juhtudel, kus detailset infot on plaanis edastada telefoni teel (vt G 3.45 Sidepartnerite puudulik autentimine). Konfidentsiaalse info üle ei tohi ka arutada asutuseväliste isikute kuulmis- ja nägemisulatuses, samuti ei tohi seda neile edastada. Lisaks peab töötaja teadma, millist infot tohib teel olles töödelda. Selleks peab info olema liigitatud klassidesse, mis aitaksid kasutajatel võimalikult lihtsalt tuvastada neile kehtivaid piiranguid (vt M 2.217 Teabe, rakenduste ja süsteemide hoolikas liigitamine ja käitlus). Töötajaid tuleb muuhulgas informeerida järgnevatest aspektidest:

- Töötajad peavad enne reisi tutvuma sihtriigi turvaolukorra, sealsete tavade ja seadustega. Seejuures on näiteks abi välisministeeriumi riigi- ja reisiinfost.
- Võimalusel ei tohiks reisile kaasa võtta infot, mis pole hädavajalik. Kui seda ei saa vältida, peab see info olema käsipagasis. Pagasit ei tohi jätta järelvalveta.
- Tundlikku infot ei tohi jätta järelvalveta hotellitubadesse, nõupidamisruumidesse või võõrastesse bürooruumidesse. Seadme lukustamine kappi aitab ennetada juhuvargusi. Ülisuure turbevajadusega infot ei tohiks ka mitte hotelli enda seifis.
- Oma asutuse ja äripartneritega suhtlemiseks tuleks kasutada ainult turvalisi ühendusi. Kuna meile, samuti püsivõrgu ja mobiilsidetelefone saab pealt kuulata, peaks kommunikatsioon, kui on tarvis edastada ülisuure turbevajadusega infot, võimalusel toimuma *End-to-End* krüpteeringuga. Ka võõraste fakside puhul tuleb olla ettevaatlik, sest edastatud dokumente saab faksiaparaati salvestada ja hiljem välja printida, seega kopeerida.
- Töötajates peaks äratama kahtlust asjaolu, kui neile esitatakse reisi ajal ebatavaliselt palju küsimusi. Võõrastega ei tohiks kunagi rääkida ei reisi eesmärgist ega tööandjast.
- Digitaalsalvesteid sisaldavaid kinke, näiteks USB-mälupulki, tuleks käsitleda eriti ettevaatlikult, kuna need võivad sisaldada kahjulikku tarkvara. Äripartneritelt kinkide vastuvõtmine võib olla ka teistviisi problemaatiline, kuna kinkija võib oodata vastuteenet.

Andmekandjate ja dokumentide utiliseerimine

Ka liikuva töö puhul tekib tihti materjali, mida on tarvis utiliseerida ainuüksi juba seetõttu, et pagas ei muutuks üleliia raskeks. Kui institutsioonide siseruumides on vanade või kasutuskõlbmatute andmekandjate ja dokumentide utiliseerimiseks välja kujunenud kindlad protseduurid (vt M 2.13 Tundlike ressursside jäljetu hävitamine), siis liikuva töö puhul pole neid kahjuks alati võimalik rakendada. Seetõttu tuleks enne oma aja ära teeninud andmekandjate ja dokumentide hävitamist täpselt järele mõelda, kas need võivad sisaldada ka tundlikku informatsiooni. Kui võivad, tuleb vastavad andmekandjad ja dokumendid kahtluse korral siiski endaga kaasa võtta. Lisaks tuleb arvestada, et spetsialistid võivad ka rikkis andmekandjatelt väärtuslikku infot kätte saada. Seetõttu ei tohi selliseid, potentsiaalselt turbevajadusega infot sisaldavaid andmekandjaid lihtsalt niisama ära visata. Ka võõraste asutuste toimikute ja failide hävitajat (paberihunti) ei tohiks ilmtingimata pimesi usaldada, kuna pole selge, kuidas toimub jäätmete utiliseerimine või kes selle eest vastutab. Seega peab turvapoliitika sisaldama eeskirju selle kohta, mida töötajad peaksid teel olles vanade andmekandjate ja dokumentidega tegema.

Täiendavad kontrollküsimused:

- Kas on olemas turvapoliitika, mis kajastab infoturvet liikuva töö puhul?
- Kas igat töötajat on informeeritud sellest, millised on olulisemad turvameetmed äri- ja erareisidel?
- Kas töötajate tähelepanu juhitakse reeglitele, millest nad peavad era- ja ärireisidel kinni pidama?
- Kas on reguleeritud, mida peavad töötajad teel olles tegema vanade andmekandjate ja dokumentidega?

M 2.431 Korrakohased protseduurid informatsiooni kustutamiseks või hävitamiseks

Algatamise eest vastutavad: asutuse/ettevõtte juhatus, infoturbe spetsialist, IT-juht, organisatsiooni juht
Rakendamise eest vastutab: infoturbe spetsialist

Milline protseduur on sobiv andmete turvaliseks kustutamiseks või hävitamiseks, sõltub nii andmekandjate liigist kui ka andmete kaitsevajadusest. Informatsioon peaks seetõttu olema kaitsevajaduse järgi klassifitseeritud (vt M 2.217 Teabe, rakenduste ja süsteemide hoolikas liigitamine ja käitlus).

Paljudel põhjustel, näiteks partnerluse või väljasttellimise käigus edastatakse kolmandatele isikutele tundlikku teavet nii elektroonilistel andmekandjatel kui ka analoogkujul. Enne seda tuleb lepinguga kindlaks määrata, mis ajaks ja mil viisil tuleb need andmekandjad täielikult tagastada või hävitada. Andmete kustutamisel või hävitamisel tuleb kinni pidada paljudest seadustest, eeskirjadest ja reeglitest, mis võivad olenevalt asutuse liigist ja äriprotsessidest tugevasti varieeruda (vt M 2.340 Õiguslike raamtingimuste järgimine). Erinevat liiki andmete salvestamis- ja kustutamistähtajad tuleb kindlaks määrata ja nendest kinni pidada. Erinevat liiki andmekandjate puhul tuleb kasutada erinevaid meetodeid, et nendel olevat teavet turvaliselt kustutada või kogu andmekandja hävitada. Asutuse jaoks on tähtis omada ülevaadet kasutusel olevate andmekandjate kohta. Eristada võib analoogandmekandjaid, näiteks paberit, kirjutusmasina ja faksiaparaadi linte, ning digitaalseid andmekandjaid (elektroonilisi, magnetilisi, optilisi). Praktikas toimub analoogandmekandjatest vabanemine tihti kontrollimatult, näiteks prügikasti kaudu, kuna nendesse suhtutakse kui erilise kaitsevajaduseta bürootarvetesse.

Teabe turvaliseks kustutamiseks ja hävitamiseks vajalikud protseduurid peaks olema töötajate jaoks turvasuunistes kindlaks määratud (vt M 2.432z Eeskirjad informatsiooni kustutamiseks ja hävitamiseks). Millised meetodeid ja seadmeid erinevate andmekandjate kustutamiseks tuleb kasutada, on kirjeldatud meetmes M 2.167 Andmete kustutamiseks või hävitamiseks sobivate lahenduste valik . Suuremates asutustes võib abi olla näidisvormidest, kus küsitakse kogu olulist informatsiooni ja kõiki teostatavaid toiminguid (näiteks töötaja nimi, salvestatud andmete liik, hävitamise põhjus ja viis). Kuna digitaalsete andmekandjate tehnika ja mudelid muutuvad ja täiustuvad pidevalt, tuleb ka andmete turvaliseks kustutamiseks ja hävitamiseks kasutatavaid protseduure ja meetodeid pidevalt muutustega kohandada. Kui andmekandjate hävitamiseks kasutatakse väliste teenusetarnijate abi, peab kogu jäätmekäitluse protsess, alustades kogumiskohtadest, millele järgneb transport ja hävitamine teenusetarnija juures, olema vajalikul määral kindlustatud (vt M 2.436z Andmekandjate hävitamine välise teenusetarnija poolt). Lisaks sellele on otstarbekohane tõsta regulaarselt töötajate teadlikkust tundliku informatsiooni ja IT-komponentidega hoolika ümberkäimise alal (vt M 2.217 Teabe, rakenduste ja süsteemide hoolikas liigitamine ja käitlus).

Tundlike andmete selektiivsel kustutamisel tuleb jälgida, et kustutatud saaks mitte ainult kehtiv versioon, vaid ka eelnevad versioonid, ajutised failid, failide fragmendid jne. Vastutajad peavad teadma, kus operatsioonisüsteem ja rakendustarkvara töödeldavate andmete koopiaid talletavad. Struktureeritud andmete

talletamine teeb informatsiooni ülesleidmise lihtsamaks (vt M 2.138 Struktureeritud andmetalletus). Kogemused näitavad, et ikka ja jälle jääb informatsiooni kahe silma vahele, kui andmekandjad enne edasiandmist võõrastele selektiivselt kustutatakse. Seepärast on soovitatav selektiivsest kustutamisest loobuda. Kui andmekandjad vajavad parandamist, võivad konfidentsiaalsed andmed valedesse kätesse sattuda, kui andmekandjad ei ole enne turvaliselt kustutatud. Välist teenusetarnijat tuleb hoolikalt valida (vt M 2.252 Väljasttellitava teenuse sobiva tarnija valimine). Tuleb nõuda kirjalikku kinnitust, et andmekandjatel olevat informatsiooni ei loetaks ega kopeeritaks, kui see ei ole just vajalik parandustööde tegemiseks. Andmete kustutamisel ja hävitamisel tuleb jälgida, et andmekandjad, millel paiknevad kustutamisele kuuluvate andmete koopiad, saaks turvaliselt hävitatud. Nende hulka kuuluvad näiteks varuandmekandjad, aga ka RAID-süsteemid. IT-süsteemi kasutusest kõrvaldamise järel tuleb kustutada ja kasutuskõlbmatuks muuta ka varuandmekandjad, niipea kui nendele salvestatud andmeid enam ei vajata.

Nõuanne: paljusid eespool nimetatud probleeme ei teki juhul, kui andmed krüpteeritakse kohe salvestamisel sobiva krüpteerimistoote abil digitaalsele andmekandjale. Sülearvutite puhul on põhimõtteliselt soovitatav andmete täielik krüpteerimine. Serveri arhitektuuri puhul on täielik krüpteerimine tihti võimatu. Olenevalt tehnoloogiast võib serveri kõvaketaste täielik krüpteerimine minna kulukamaks kui hilisem kõvaketaste hävitamine. See kehtib eriti SAN/NAS arhitektuuride puhul. Ka analoogsete andmekandjate puhul on tihti olemas koopiad, näiteks vanad aktid kaua kasutamata laoruumides, mis tuleb samuti hävitada. Kõrge või väga kõrge kaitsevajadusega andmete korral tuleb kustutamine ja hävitamine protokollida, eriti analoog- ja digitaalsete andmekandjate likvideerimise käigus.

Kontrollküsimused:

- Kas asutuses kasutusel oleva teabe salvestamis- ja kustutamistähtajad on teada? Kas neist peetakse kinni?
- Kas asutuses kasutatavatele igat liiki andmekandjatele on olemas sobivad kustutus- ja hävitamismeetodid?
- Kas väliste teenusetarnijate kasutamisel andmete hävitamiseks on reguleeritud, kuidas toimub andmekandjate kogumine ja kuidas neid äraviimiseni hoitakse?
- Kas on tagatud, et andmete kustutamisel kustutatakse ka eelnevad versioonid, ajutised failid, failide fragmendid jms?
- Kas kõrge või väga kõrge kaitsevajadusega andmekandjate kustutamine ja hävitamine protokollitakse?

M 2.432z Eeskirjad informatsiooni kustutamiseks ja hävitamiseks

Algatamise eest vastutavad: andmekaitse eest vastutav töötaja, infoturbe spetsialist, IT-juht

Rakendamise eest vastutavad: töötajad

Kui andmekandjad likvideeritakse või ametlik säilitamistähtaeg on ületatud, tuleb nendele salvestatud informatsioon turvaliselt kustutada. Kindlad protseduurid aitavad ära hoida salvestatud andmete kuritarvitamist. Andmekandjatel olev informatsioon tuleb enne edasiandmist või likvideerimist kustutada nii, et informatsiooni taastamine ei oleks suure tõenäosusega võimalik. Ka andmekandja saamisel tuleb kontrollida, kas sellel olev info tuleb pärast enda kasutuseesmärkidel ümbertöötlemist ja teistele andmekandjatele salvestamist, näiteks arhiveerimise eesmärgil, usaldusväärselt kustutada.

Eesmärkide määratlemine

Selle suunise eesmärk on töötajate teadlikkuse tõstmine ja motiveerimine andmete kustutamise ja hävitamise alal. See peab pakkuma abi ja toetust sobivate meetodite ja vahendite valimisel kaitset vajavate andmete kustutamiseks või hävitamiseks. Milline on kõige sobivam protseduur andmete kustutamiseks või hävitamiseks, sõltub kasutatavast andmekandjast, selle salvestustehnoloogiast ja informatsiooni kaitsevajadusest. Eeskirjadest kinnipidamist tuleb regulaarselt kontrollida.

Reguleerimisala

Eeskirjades tuleks käsitleda hetkel kasutuskõlblikke ja asutuses kasutusel olevaid andmekandjaid. Eristada tuleks kõigepealt analoogseid ja digitaalseid andmekandjaid. Digitaalsed andmekandjad jagunevad elektromagnetilisteks (näiteks kõvakettad, disketid, magnetlindid), optilisteks (CD-d ja DVD-d), magnetoptilisteks (MO-ketas) ja välkmäludes (näiteks USB-mälupulgad). Kindlaks tuleb määrata laekuvate andmete kaitsevajadus. Lisaks sellele tuleb igat liiki andmekandjate jaoks välja valida ja siduvalt kindlaks määrata sobivad kustutusmeetodid.

Seadustest tulenevad ettekirjutused ja organisatsioonisisesed reeglid

Ülevaade tuleks anda sellest, milliseid õigusakte, näiteks andmekaitseseadusi, andmete kustutamisel ja andmekandjate hävitamisel tuleb järgida. Viidata tuleks aga ka normatiivse iseloomuga regulatsioonidele, näiteks ISO standarditele ja asutusesisestele nõuetele.

Vastutusalad

Selles osas määratakse kindlaks töötajate vastutusalad. Seejuures tuleb kindlasti eristada töötaja, esimehe, administraatori, revidendi, andmekaitse eest vastutava töötaja ja infoturbe eest vastutava töötaja rolle.

Kontaktisikud

Eeskirjadest peaks leidma kontaktisikute nimed ja nende kontaktandmed (telefon, e-post jne), et töötajatel oleks võimalik pöörduda nende poole andmete kustutamist puudutavate küsimuste tekkimisel, või sisaldama informatsiooni selle kohta, kust nad vajaliku info leiavad. Seejuures tuleks arvestada asjaoluga, et tihti tekitab segadust, kui on nimetatud liiga palju erinevaid kontaktisikuid. Seega võib olla

parem, kui tuuakse ära vaid väheste kontaktisikute nimed, kes siis kasutajad vajaduse järgi õigesse kohta suunavad (konsultatsioonipunkti kontseptsioon).

Protseduurid

Eeskirjades tuleb fikseerida, millised meetodid on olemas andmete turvaliseks kasutamiseks ja milliseid neist asutuses kasutatakse. Erinevate andmekandjate kustutamiseks kasutatakse tavaliselt erinevaid meetodeid. Eeskirjades tuleb kirjeldada, kuidas ja millal kasutajad informatsiooni peavad kustutama. Kui tekib vajadus kustutada andmed sellistelt andmekandjatelt, mida eeskirjades pole käsitletud, tuleb eeskirju järgida võimaluse ja mõistlikkuse piirides.

Uuendamine

Kuna tehnoloogia muutub pidevalt, tuleb ka eeskirju regulaarselt uuendada, et kirjeldatud kustutus- ja hävitusmeetodid sobiksid ka uut liiki andmekandjate jaoks. See kehtib ka andmekandjate kohta, mida senini ei ole käsitletud. Vajaduse korral tuleb välja arendada ja kasutada uusi meetodeid.

Kontrollküsimused:

- Kas on olemas eeskirjad andmete kustutamiseks või hävitamiseks?
- Kas andmete kustutamise või hävitamise eeskirjade täitmist kontrollitakse regulaarselt?
- Kas eeskirjad on päevakohased? Kas need käsitlevad kõiki hetkel kasutatavaid andmekandjate liike?

M 2.433w Ülevaade meetoditest andmete kustutamiseks ja hävitamiseks

Algatamise eest vastutavad: infoturbe spetsialist, IT-juht, organisatsiooni juht
Rakendamise eest vastutavad: infoturbe spetsialist, IT-juht, organisatsiooni juht

Informatsiooni kustutamiseks andmekandjatelt võib kasutada mitmesuguseid meetodeid. Millist meetodit valida, sõltub olulisel määral kustutamisele kuuluvate andmete kaitsevajadusest, aga loomulikult ka andmekandjate liigist. Analoogandmekandjate puhul võib informatsiooni näiteks üle kirjutada, välja lõigata või ära kustutada. Digitaalsete andmekandjate puhul võib andmed kustutada kustutusprogrammidega või üle kirjutada. Alljärgnevalt on tõhususe järjekorras kirjeldatud elektrooniliste andmekandjate kustutusmeetodid kaitseks jääkandmete taastamise eest.

Kustutuskäsu
Kustutuskäsud on operatsioonisüsteemis kasutatavad käsud andmete ja failide kustutamiseks, nagu Delete ja Erase. Kustutuskäskude kasutamisel tuleb silmas pidada, et selle käigus ei kustutata tavaliselt tegelikku faili informatsiooni, vaid üksnes viide sellele informatsioonile andmekandja „sisukorras". Fail ise jääb alles. On olemas meetodid ja programmid, mille abil on võimalik kustutatuks peetud informatsiooni taastada. Seda meetodit ei ole seetõttu soovitatav kasutada juhul, kui peab olema tagatud, et andmeid ei ole võimalik taastada. Tuleb leida meetodid ja mehhanismid, mis on efektiivsemad kui operatsioonisüsteemide standardkustutusmeetodid ja kustutavad ka kõrge kaitsevajadusega andmed nii, et neid pole enam võimalik taastada.

Üksikute failide ülekirjutamine
Lisaks kasutusel olevate operatsioonisüsteemide kustutuskäskudele on üksikute failide ülekirjutamiseks olemas tarkvaral baseeruvad vahendid. Nende kustutustööriistadega (wipe-tools) on võimalik kustutada üksikuid faile või salvestuspiirkondi täieliku ülekirjutamise abil sobivate andmemustritega. Seejuures tuleb aga silmas pidada, et failides sisalduvad andmed on tihti osaliselt või isegi täielikult taastatavad, kuigi failide kustutamiseks kasutati wipe-tools'i. Peamiselt on see tingitud sellest, et operatsioonisüsteemi või rakenduste kaudu salvestati andmete koopiad erinevatesse kohtadesse, mida kasutajad tihti ei tunne ega saa kontrollida. Nii võivad kustutatuks peetud andmed andmekandjale alles jääda ja neid on teatud meetodeid kasutades võimalik kätte saada.

Nende hulka kuuluvad näiteks järgmised:

- operatsioonisüsteemi või rakendusprogrammi loodud ja jälle kustutatud vahefailid (cache-failid) või ajutised failid;
- mingi programmi automaatselt loodud varukoopiad, näiteks teevad seda tihti Office'i programmid;
- saalefailid (vt M 4.325 Likvideerimisele kuuluvate failide kustutamine);

- andmete fragmendid, mis võivad olemas olla Windowsi operatsioonisüsteemide registri ja indeksi andmebaasis;
- file slack (file slack ehk andmenihe tähendab mõningate operatsioonisüsteemide puhul tavalist „täiteks vajalike andmete" salvestamist ilma kindla määratluseta andmekandja mälusektorisse) või cluster-tips-fragmendid.

Kuna vastavaid andmeid töötlevad operatsioonisüsteemid ja rakendusprogrammid, ei saa administraatorid ega kasutajad neid protsesse eriti mõjutada. Ka wipetehnikaid kasutavatel programmidel ei ole täit kontrolli kõikide nende andmejääkide üle. Seetõttu tuleb veendumaks, et andmekandjatele ei ole alles jäänud andmete koopiaid, kustutada andmekandja kas terviklikult või valida mõni teine, turvalisem kustutusprotseduur.

Vormindamine
Vormindamise teel valmistatakse elektrooniline andmekandja ette andmete salvestamiseks. Kõvaketaste puhul eristatakse madaltaseme vormindamist (low level formatting), mille käigus luuakse jäljed ja sektorid kõvaketta peal uuesti, ning loogilist ehk high level-vormindamist, mille teeb operatsioonisüsteem. Kuna madaltaseme vormindamise käigus muudetakse kõvaketta struktuuri ja vastupidiselt loogilisele vormindamisele kustutatakse ka jälgede ja sektorite jaotus ning seejärel kirjutatakse uuesti, ei saa teatud juhtudel kõvaketast pärast vormindamist enam kasutada. Kui kõvakettaid on vaja uuesti kasutusse võtta, tuleks eelkõige selgeks teha, ega kõvaketta garantii ei lähe madaltaseme vormindamise käigus kaduma. Madaltaseme vormindamise abil saab kõvakettad sõltumatult operatsioonisüsteemist jälle „algseisu" viia ja selle abil ka olemasoleva informatsiooni kustutada. Olemasolevate andmete kustutamise turvalisuses ei saa siiski kindel olla. Kustutamismeetodi kasutamine ei ole seetõttu soovitatav. Andmekandja mitmekordne ülekirjutamine on igal juhul usaldusväärsem. Loogilise vormindamise (HLF) käigus luuakse uuesti vaid failisüsteemi struktuur. Seetõttu ei sobi see informatsiooni usaldusväärseks kustutamiseks.

Andmekandjate täielik ülekirjutamine
Tavapärase kaitsevajaduse rahuldamiseks piisav füüsiline kustutamine on võimalik saavutada andmekandjate täieliku ülekirjutamisega. Seejuures kirjutatakse andmekandjad spetsiaalseid tarkvaravahendeid kasutades üks või mitu korda ette antud märkide või juhuslike numbritega üle. Andmekandjad peavad olema veatud ning on kasutatavad ka pärast ülekirjutamist.

Selle kustutamismeetodi usaldusväärsus ja turvalisus sõltub järgmistest faktoritest:

- Kasutajad peavad tarkvara õigesti kasutama. Vale kasutamine võib viia selleni, et andmekandjat ei kirjutata üle või kirjutatakse üle vaid osaliselt.
- Kas andmekandjad saavad täielikult ja usaldusväärselt kustutatud, sõltub suurel määral kustutusvahendite konfiguratsioonist. Seetõttu tuleb tagada nende optimaalne konfigureerimine ning välistada seadistuste muutmine volitamata isikute poolt.

- Kustutustarkvara peab tagama, et kõik andmekandja sektorid, ka kaitstud ja kahjustatud sektorid, saaks soovitud viisil üle kirjutatud. Erinevat liiki andmekandjate tehnoloogilise eripära (näiteks juba erinevate tootjate kõvakettad põhinevad erineval tehnoloogial) ja tehnika kiire arengu tõttu ei ole võimalik välistada, et mitte kõik tarkvaratooted ei täida seda nõuet. Tarkvara peab pärast ülekirjutamise lõppemist võimaldama edukat ülekirjutamist verifitseerida. Siiamaani puudub ühine seisukoht, mitu korda on vaja ülekirjutamisprotseduuri teha, et andmed oleks kindlalt kustutatud. Kriminalistikalabori uuringud on näidanud, et juba ühekordsel ülekirjutamisel sobivate märgijadade või juhuslike arvudega ei olnud andmeid võimalik enam taastada. Tavapärase kaitsevajaduse rahuldamiseks piisab niisiis ühekordsest ülekirjutamisest usaldusväärse tööriistaga. Protseduuri kordamisel kaitsemõju teoreetiliselt tõuseb. Suuremate kõvaketaste ülekirjutamine võib kesta väga kaua. Kõrgemate turvanõuetega andmete kustutamiseks tuleks ülekirjutamise protseduuri korrata kaks, veelgi parem kolm korda. Andmemustritena on soovitatav kasutada juhuslikke andmeid. Teine võimalus mitmekordsel ülekirjutamisel on kasutada teise ülekirjutamise käigus sellist andmemustrit, mis suudaks esimesel korral kasutatut täiendada.

Kustutamine kustutusseadmetega

Kustutusseadmete ülesanne on magnetilistele andmekandjatele salvestatud konfidentsiaalsete andmete hävitamine sellisel moel, et neid ei oleks enam võimalik taastada. Selleks on kustutusseadmed varustatud tugevate sama või vahelduva väljaga magnetitega, mille abil magnetväli demagnetiseerib seadme andmekandjad. Neid seadmeid nimetatakse ka demagnetiseerijateks. Kuna kustutusseadmetega kustutamisel on eranditult tegemist magnetilise mõjuga, saab kustutusseadmeid kasutada vaid magnetandmekandjate, näiteks magnetlintide, diskettide ja kõvaketaste kustutamiseks. Kustutusseadme magnetvälja mõjul lõhutakse andmekandjatele salvestatud magnetilised domeenid. Sobiva kustutusseadme kasutamisel ei ole andmekandjatelt pärast kustutamist enam võimalik informatsiooni leida. Sobivaks loetakse seejuures kustutusseadet, mille välja tugevus on tunduvalt tugevam kui andmekandja oma, mis võimaldab selle täielikult demagneetida. Seejuures tuleb tähelepanu pöörata hoolikale käsitsemisele, lisaks muule peavad andmekandjad olema korrektselt paigutatud ning valitud peab olema magnetilise mõju õige kestus. Igal juhul tuleb järgida kustutusseadmete kasutusjuhendit. Kustutusseadmega kustutamise eelis seisneb selles, et kogu andmekandja on võimalik väikese ajakuluga turvaliselt kustutada. Igatahes tuleb silmas pidada, et kõvakettaid ja erinevat liiki magnetlinte ei saa pärast kustutamist enam uuesti kasutada, sest koos kustutatud andmetega kustutatakse ka servorada (servo-track), mis juhib kirjutus-/lugemispead.

Elektrooniliste salvestusvahendite kustutamine

RAM-salvestid (SRAM ja DRAM) on muutmäluga salvestid, mille puhul toob toite väljalülitamine endaga kaasa andmete hävimise. Kui on olemas varupatarei, tuleb ka see eemaldada. Püsimälude puhul, nagu elektrooniliselt ümberprogrammeeritav EEPROM ja välkmälu (flash memory) tuleb seevastu andmete kustutamiseks kasutada hoopis elektripinget. EPROM-mälusid saab kustutada vaid kuni 30 minuti jooksul ultraviolettvalgusega kiiritades. Korrektse protseduuri väljaselgitamiseks

tuleb tutvuda tootja juhendiga. Siiski ei saa täielikult garanteerida, et pärast kustutamist on mälu igasugustest „andmejälgedest" tühi ja eelnevalt salvestatud andmete kohta ei ole võimalik teha ühtki järeldust. Seetõttu on soovitatav kogu salvesti enne kustutamist juhuandmetega täielikult üle kirjutada.

Välkmäluketaste kustutamine
Välkmälukettad on välk-EPROM-mäludel põhinevad pooljuhtsalvestid, mida kasutatakse kõvakettaajamite asemel arvutites, eriti aga sülearvutites. Välkmälukettaid saab nagu välk-EPROM-mälusidki tavapärase kaitsevajadusega andmete puhul kustutada turvaliselt sobiva kustutusprogrammiga ühekordse ülekirjutamise, kõrgema kaitsevajadusega andmete puhul kuni kolmekordse ülekirjutamise abil.

Andmekandjate hävitamine
Sobivate meetodite valimisel andmekandjate hävitamiseks tuleb tähelepanu pöörata nii analoogsetele andmekandjatele, nagu paber ja mikrofilm, kui ka digitaalsetele andmekandjatele (elektroonilised, magnetilised, optilised). Andmekandjate hävitamine võib toimuda nii lõikeseadmete, paberihuntide, lõikeveskite, stantside ja teiste sobivate seadmete abil, aga ka põletamise ja kokkusulatamise teel.

Analoogandmekandjate hävitamine
Meetodeid ja seadmeid, mis sobivad konfidentsiaalset informatsiooni sisaldavate analoogandmekandjate, näiteks paberdokumentide või mikrofilmide hävitamiseks, on kirjeldatud meetmes M 2.435z Sobiva dokumendipurusti valik .

Digitaalsete andmekandjate hävitamine
Sobivaid meetodeid ja seadmeid digitaalsete andmekandjate hävitamiseks on kirjeldatud meetmes M 2.167 Andmete kustutamiseks või hävitamiseks sobivate lahenduste valik . Optilisi andmekandjaid, nagu CDd või DVDd, ei ole võimalik üle kirjutada ega demagneetimise teel kustutada. Need tuleb hävitada sarnaselt kirjutuskaitstud või mitmekordselt mitte ülekirjutatavatele andmekandjatele (CD-ROMid või CD-Rid). Magnetandmekandjad, mida enam edasi ei kasutata, tuleks sobivaid seadmeid kasutades hävitada. Hävitamisele kuuluvad ka defektsed kõvakettad, mida ei saa enam üle kirjutada. Hävitamine võib toimuda paberihundis või termilisi meetodeid kasutades, näiteks põletamise või kokkusulatamise teel. Andmekandjate hävitamiseks vajaminevad seadmed on tihti suured, keerulised käsitseda ja kallid. Seepärast on andmekandjate hävitamise teenuse tellimine lähedal asuvatelt teenindusfirmadelt mõttekam, kui selleks vajalike seadmete soetamine. Kui andmekandjate hävitamine tellitakse väliselt teenusetarnijalt, peavad kogumiskohad, transport ja hävitamisprotsess teenuseosutaja juures olema vajalikul määral turvalised (vt M 2.436z Andmekandjate hävitamine välise teenusetarnija poolt).

M 2.434z Andmete kustutamiseks või hävitamiseks vajalike seadmete soetamine

Algatamise eest vastutavad: infoturbe spetsialist, IT-juht, organisatsiooni juht

Rakendamise eest vastutavad: varustusosakond, infoturbe spetsialist, IT-juht

Tavaliselt kasutatakse asutustes erinevat liiki andmekandjate hävitamiseks ja nendele salvestatud andmete kustutamiseks erinevaid tööriistu. Osasid neist kasutatakse töötajate töökohtadel, teisi tsentraalselt, näiteks IT tugikohtades.

Enne tööriista soetamist tuleb välja selgitada nõuded ja raamtingimused, et leida vastavaks rakendusjuhtumiks sobiv tööriist. Seadmete valikul andmete kustutamiseks või andmekandjate hävitamiseks tuleb tähelepanu pöörata nõudmistele, mis on kindlaks määratud meetmes M 2.167 Andmete kustutamiseks või hävitamiseks sobivate lahenduste valik . Nõuded andmete kustutamiseks ja andmekandjate hävitamiseks vajalikele tööriistadele tuleks dokumenteerida, et dokumentatsiooni põhjal oleks võimalik regulaarselt kontrollida, kas valitud tööriistad võimaldavad nende nõuete täitmist. Nõuded aktide hävitamiseks vajalikele tööriistadele on kirjas meetmes M 2.435z Sobiva dokumendipurusti valik . Elektrooniliste andmekandjate kustutamiseks ja hävitamiseks vajalikele tööriistadele esitatavad nõuded sõltuvad suurel määral andmekandjate liigist ja kasutusotstarbest. Kõige tähtsamaks tuleb pidada asutuse turvanõuete täitmist.

Muu hulgas tuleks välja selgitada järgmised asjaolud:

- Kas andmeid on võimalik nende kaitsevajaduse järgi usaldusväärselt kustutada?
- Kas mõni sõltumatu institutsioon on toote tunnustatud turvakriteeriumide, näiteks Common Criteria (CC) alusel sertifitseerinud või andnud loa selle kasutamiseks salastatud valdkondades?
- Kas toodet on hõlbus installeerida, konfigureerida ja kasutada?
- Kas toodet on võimalik selliselt konfigureerida, et kõik varem defineeritud turvaeesmärgid oleks saavutatavad?
- Kas tähtsaid konfiguratsiooniparameetreid on võimalik kaitsta volitamata kasutajate tehtud muudatuste eest?
- Kas toote dokumentatsioon sisaldab täpset tehniliste ja administratiivsete detailide kirjeldust?
- Kas toote jõudlus vastab kasutajate hulgale?
- Kas töötajad on ilma suurema koolituseta võimelised seadmeid efektiivselt, turvaliselt ja vigadeta kasutama?
- Kui suured on toodete soetamiskulud? Kui suured on eeldatavad käituskulud (hooldus, ekspluatatsioon ja kasutajatugi)?

Andmete mittetahtlik kustutamine võib häirida kogu äriprotsessi. Seepärast tuleks välja selgitada, kas nende seadmete liideseid ja juurdepääsukohti on võimalik piisavalt kindlustada. Neid nõudmisi on võimalik konkretiseerida rakendusprofiili näite põhjal kõvaketaste turvaliseks kustutamiseks.

Näide:

Kõvaketaste kustutamiseks pakub turg paljusid tööriistu. Olulised tunnused nende eristamiseks on järgmised:

- ülekirjutamiskordade arv;
- ülekirjutamismustrid;
- ülekirjutamismustrite vahetamine ülekirjutamiskordade kaupa;
- arvestamine kõvakettasisese kodeeringuga;
- verifitseerimisprotsess.

Kõvaketaste kustutustööriistade valikul peaks tähelepanu pöörama asjaolule, et valitud lahendus täidaks järgmised nõuded:

- Kasutusel olevate operatsioonisüsteemide ja rakenduste toetamine: tööriistal peaks olema täielik ühilduvus olemasoleva riistvara ja kasutatavate operatsioonisüsteemidega.
- Protokollimine: kustutusprotseduure peaks olema võimalik protokollida. Seaduslike ja lepinguliste raamtingimuste täitmiseks peaks olema võimalik tõendada, et andmekogumid teatud kindlaks ajaks kustutati.
- Juurutamise korrektsus: kustutustööriistade testimine on ikka ja jälle näidanud, et need on valesti juurutatud. Ilmnenud on järgmised vead:

1. kasutatakse valesid (mittesobivaid) ülekirjutusmustreid;
2. sektorid jäävad üle kirjutamata;
3. ei tehta vajalikku arvu kordi ülekirjutusprotseduure;
4. juhuslike arvude asemel kasutatakse ülekirjutusmustrina konstante.

Kuna kasutajatel on raske selliseid juurutamisvigu kindlaks teha, tuleks võimaluse korral soetada tooted, mida on testinud sõltumatud asutused. Eelistada tuleks teste, mille tegemise käigus avalikustatakse kõik testimiskriteeriumid, näiteks testid, mis põhinevad CC või ISO normidel. Kui värskeid testimistulemusi ei ole käepärast, tuleks selle asemel enne soetamist tutvuda IT-alaste ajakirjadega, mis korraldavad regulaarselt kustutustööriistade testimist.

Kontrollküsimused:

- Kas andmete kustutamiseks või hävitamiseks vajalikele tööriistadele esitatavad nõuded on dokumenteeritud?
- Kas valitud tööriistade vastavus nendele nõuetele on testitud?

M 2.435z Sobiva dokumendipurusti valik

Algatamise eest vastutavad: infoturbe spetsialist, organisatsiooni juht

Rakendamise eest vastutavad: varustusosakond, infoturbe eest vastutav töötaja

Dokumendipurustiga on võimalik purustada paberdokumente, aga ka kiipkaarte ja CD-sid selliselt, et fragmentidest pole enam nii lihtne seal eelnevalt olnud informatsiooni välja lugeda. Kas ja millise vaevaga on informatsiooni võimalik taastada, sõltub seadme kvaliteediklassist. ISKE-s on defineeritud viis dokumendipurustajatele määratud turvaastet. Turbeastmetesse jagamise aluseks on dokumendipurustite tekitatud osakeste suurus. Dokumendipurustajad, mis lõikavad materjali ribadeks, on suurema läbilaskevõimega kui need, mis materjali tükeldavad. Seepärast on nende kasutamine otstarbekas, kui purustamisele kuuluvate dokumentide hulk on suur, kuna see tagab ka purustatud osakeste parema segunemise. Ribadeks lõikamisel on aga vaja rohkem ruumi, mistõttu tuleb kogumismahutit regulaarselt tühjendada.

Turbeaste 1 (rahvusvaheline tähis DIN): osakeste suurus ei tohi tükkideks lõikamisel ületada 2000 ruutmillimeetrit, kusjuures 10% osakeste suurus võib jääda vahemikku 2000 kuni 3800 ruutmillimeetrit. Ribadeks lõikamise korral ei tohi ribade laius ületada 12 millimeetrit. Informatsiooni taastamine on võimalik ilma igasuguste abivahendite ja erialateadmisteta, kuid mõningase ajakuluga. Nimetatud turvaastmele vastavad seadmed ei ole ette nähtud kasutamiseks ettevõtetes ja ametkondades.

Turbeaste 2 (rahvusvaheline tähis DIN): osakeste suurus ei tohi ületada 800 ruutmillimeetrit, kusjuures 10% osakeste suurus võib jääda vahemikku 800 kuni 2000 ruutmillimeetrit. Ribadeks lõikamisel ei tohi maksimaalne riba laius ületada 6 millimeetrit. Informatsiooni taastamine on võimalik vaid abivahendite ja märkimisväärse ajakuluga. Turbeastmele 2 vastavaid seadmeid peaks kasutama vaid juhul, kui tükeldamist vajab suur hulk dokumente.

Turbeaste 3 (rahvusvaheline tähis DIN): tükeldatud osakeste suurus ei tohi ületada 320 ruutmillimeetrit, kusjuures 10% osakeste suurus võib jääda vahemikku 320 kuni 800 ruutmillimeetrit. Ribadeks lõikamisel ei tohi maksimaalne riba laius ületada 2 millimeetrit. Informatsiooni taastamine on võimalik vaid suurte kuludega (isikud, abivahendid, aeg).

Turbeaste 4 (rahvusvaheline tähis DIN): tükeldatud osakeste suurus ei tohi ületada 30 ruutmillimeetrit, kusjuures 10% osakeste suurus võib jääda vahemikku 30 kuni 90 ruutmillimeetrit. Informatsiooni taastamine on võimalik vaid eriseadmeid ja konstruktsioone kasutades.

Turbeaste 5 (rahvusvaheline tähis DIN): tükeldatud osakeste suurus ei tohi ületada 10 ruutmillimeetrit, kusjuures 10% osakeste suurus võib jääda vahemikku 10 kuni 30 ruutmillimeetrit. Informatsiooni taastamine on peaaegu võimatu.

Kõvaketaste purustamisel soovitatakse maksimaalselt 300-ruutmillimeetrilise ja CD-de ning DVD-de puhul maksimaalselt 200-ruutmillimeetrilise suurusega osakesi, kõrgema kaitsevajaduse korral peab purustatud osakeste suurus jääma alla 10 ruutmillimeetri (vt M 2.167 Andmete kustutamiseks või hävitamiseks sobivate lahenduste valik).

Sobiva turbeastme valikul peavad kasutajad optimaalsete kulude ja vajaliku turvalisuse saavutamiseks pöörama tähelepanu järgmistele asjaoludele:

- Mida väiksemateks osadeks andmekandjad purustatakse, seda suurem on hävitamise turvalisus. Turvalisust tõstab ka see, kui dokumendipurustaja on suure läbilaskevõimega – seetõttu toimub juba materjali hävitamise käigus purustatud osakeste segunemine.
- Väiksemateks osadeks purustamine muudab seadme läbilaskevõime väiksemaks. Soovitud läbilaskevõime saavutamiseks tuleb soetada võimsam ja sellest tingituna ka kallim dokumendipurustaja.

Kontrollküsimused:

- Kas konfidentsiaalse info hävitamiseks kasutatakse piki- ja ristilõikega dokumendihävitajat?
- Kas dokumendipurustaja valikul on arvestatud selle läbilaskevõimega?
- Kas osakeste suurus pärast purustamist vastab teabe kaitsevajadusele?

M 2.436z Andmekandjate hävitamine välise teenusetarnija poolt

Algatamise eest vastutavad: asutuse/ettevõtte juhatus, andmekaitse eest vastutav töötaja, infoturbe spetsialist

Rakendamise eest vastutavad: organisatsiooni juht

Kui andmekandjate hävitamiseks pöördutakse väliste teenusetarnijate poole, tuleb nendega sõlmida detailsed lepingud (vt M 2.253 Välise teenusepakkujaga sõlmitava lepingu koostamine). Kuigi andmekandjate hävitamine toimub välise teenusetarnija poolt, tuleb kindlaks määrata asutusesisesed eeskirjad, mis reguleerivad, kuidas peab toimuma andmekandjate kogumine ja kuidas neid deponeerida, kuni teenusetarnija neile järele tuleb.

Turvaline hoidmine tellija juures

Hävitamisele kuuluvad andmekandjaid tuleb hoida kaitstuna volitamata juurdepääsu eest, kuni neile järele tullakse. Andmekandjate kogumiseks võib asutuses paigaldada näiteks konteinerid, mis peavad olema nii kaitstud, et nendest ei saa ühtegi andmekandjat kätte. Nendest kogumiskonteineritest on eriti huvitatud ründajad, kuna need sisaldavad kontsentreeritud kujul konfidentsiaalset informatsiooni. Konteinereid ei tohiks mitte mingil juhul paigaldada üldkasutatavatesse koridoridesse. Siiski peaks kogumiskonteinerid olema paigaldatud töökoha lähedale, et töötajad ei hoiaks hävitamisele kuuluvaid andmekandjaid kaitseta, näiteks kirjutuslaua sahtlis, kuni nad need ükskord kogumiskohta annavad (vt M 2.13 Tundlike ressursside jäljetu hävitamine). Kui töötajad saavad kogumiskonteineri asukoha valimisel osaleda, aitab see kaasa üldisele omaksvõtule. Lisaks sellele peavad olema sobivalt kaitstud ka andmekandjate transport ja hävitamine. Samuti tuleb teenindusfirmaga sõlmida lepingulised kokkulepped. Nende kokkulepete täitmist tuleb regulaarselt kontrollida.

Turvalise transpordi kindlustamine

Tuleb tagada, et hävitamisele kuuluvad andmekandjad antakse üle vaid nende transpordiks volitatud isikutele. Selleks peab tellija nimetama kõigepealt isikud, keda on andmekandjate hävitamisprotseduuride teostamise alal instrueeritud ja kes on võimelised selle kulgu kontrollima. Transpordiga tegelevad isikud peavad suutma tõendada, et neil on volitused kogutud andmekandjate transportimiseks, et vältida konfidentsiaalsete andmete üleandmist volitamata isikutele. Andmekandjate üleandmine tuleb tõendada kirjalikult nii kohaletoimetamisel kui ka üleandmisel. Transportimisel tuleb kogu tee ulatuses tagada, et materjali transpordivad ainult selleks volitatud isikud. Kogu tee ulatuses ei tohiks transpordifirma töötajatel ega teistel isikutel olla võimalik transporditavale materjalile juurde pääseda. Näiteks võiks kasutada kinniseid või plommitud pakendeid.

Turvaline hoidmine teenusetarnija juures

Andmekandjate hävitamise teenust osutaval teenusetarnijal peavad olema välja töötatud toimivad turvaprotseduurid, mis tagavad hävitamisele kuuluvate andmekandjate muutmise lugematuks ning välistavad nendel oleva informatsiooni sattumise volitamata isikute kätte. Teenusetarnijal peab olema ajakohane, selgesti mõistetav turvakontseptsioon. Üldiseid nõudeid teenusetarnijatele ja tema töötajatele on kirjeldatud meetmes M 2.252 Väljasttellitava teenuse sobiva tarnija valimine . Hävitamisele kuuluva materjali kättesaamisel tuleb kontrollida, kas transpordiks üle antud kaup on täielikult kohale jõudnud, näiteks kas mahutite arv ja nende

kaal on sama, mis üleandmisel. Teenuseosutaja juures läheb hävitamisele kuuluv materjal tavaliselt kõigepealt lattu. Siin tuleb jälgida, et oleks tagatud toimiv juurdepääsukontroll, mis välistaks volitamata isikute juurdepääsu hävitamisele kuuluvatele andmekandjatele ja seadmetele. Andmekandjate hävitamiseks mõeldud seadmeid ja tööriistu tohivad kasutada vaid töötajad, keda on nende käsitsemise alal instrueeritud.

Kontrollküsimused:

- Kas hävitamisele kuuluvaid andmekandjaid säilitatakse kaitstuna volitamata juurdepääsu eest, kuni neile järele tullakse?
- Kas tellija on nimetanud ja instrueerinud isikud, kes hakkavad tegelema andmekandjate hävitamisprotsessi kontrolliga?
- Kas tellija kontrollib regulaarselt andmekandjate hävitamisprotsessi?
- Kas hävitamisele kuuluvatele andmekandjatele järeletulek ja nende transportimine on vajalikul määral turvatud?
- Kas välise teenusetarnija rakendatavad turvaprotseduurid on usaldusväärsed, arusaadavad ning hävitamisele kuuluvate andmekandjate kaitsevajadusele vastavad?

M 2.437 Samba-serveri kasutuselevõtu plaanimine

Algatamise eest vastutavad: Infoturbejuht, IT-juht

Rakendamise eest vastutavad: administraator, IT-juht

Samba-serveri mitmekülgsed kasutamisvõimalused nõuavad juba eelnevalt laialdast plaanimist, et tagada selle turvaline ja korrastatud seadistamine ja hiljem ka turvaline käitamine. Tuleb tagada, et kinni peetaks IT-süsteemidele eelnevalt kindlaks määratud infoturbe poliitikast (vt M 2.316 Serveri turvapoliitika kehtestamine) ja toimuks ka vastav teostus. Sõltuvalt kasutuskohast tuleb määratleda, kus ja millise funktsiooniga Sambat kasutatakse ja milline tarkvara tuleb veel võib-olla installeerida (nt OpenLDAP).

1. Stsenaariumid

Mõistmaks erinevaid ülesandeid, mida Samba on võimeline täitma, tuleks kõigepealt mõelda sellele, milliseid funktsioone võib arvuti Windowsi võrgus täita.

- Autonoomne arvuti - Autonoomne arvuti võib olla üksik tööarvuti või server, mis ei kuulu ühegi domeeni alla. Selline arvuti haldab iseenda kasutajaandmebaasi, mida ta ei ekspordi.
- Domeeni liige - Domeeni liige võib olla arvuti või server, mis kuulub kindlasse domeeni. Arvuti saab oma kasutajaandmebaasi domeenikontrollerilt.
- Domeenikontroller - Domeenikontrolleriks nimetatakse kasutajaandmebaasi eksportivat serverit. NT4 domeenimudelis (ka Samba korral) eristatakse esmast domeenikontrollerit (PDC – *Primary Domain Controller*) ja varundusdomeenikontrollerit (BDC – Backup Domain Controller). Uuemas *Active Directory* (AD) domeenimudelis ei paigutata kasutajaandmeid enam süsteemi kontohaldurisse (SAM – *Security Account Manager*), vaid koos paljude teiste lisaandmetega AD kausta. Oluliseks erinevuseks on, et enam ei eristata PDC-d ja BDC-d. Nüüd on ainult domeenikontroller. Iga domeenikontroller omab kirjutuspääsu AD-kataloogile, kuna kataloogiteenus toetab mitme AD-kataloogi vahelist infoühtlustust (*Multimaster Replication*). Lisaks sellele kasutatakse AD-domeenis teisi protokolle. Näiteks kasutatakse NetBIOS (*Network Basic Input/Output System*) asemel domeeninimede süsteemi (DNS – *Domain Name System*) ja edastusohje protokolli (TCP – *Transmission Control Protocol*)/internetiprotokolli (IP – *Internet Protocol*).

Samba-serverit võib kasutada allkirjeldatud stsenaariumites. Tuleb arvestada asjaoluga, et ühes ja samas olukorras on võimalik Sambat erinevalt kasutada:

- NT4 domeeni liikmena (domeeni liige)
- AD domeeni liikmena (domeeni liige)
- PDC-na NT4-ga ühilduvale domeenile (domeenikontroller)
- Samba PDC BDC-na NT4-ga ühilduvas domeenis (domeenikontroller). Sambasse ei ole olnud veel võimalik paigaldada protokolli, mis kasutaks NT4 PDC-d, et SAM-andmebaas BDC-ga ühtlustada. Seetõttu saab Samba BDC-d kasutada ainult Samba PDC-ga.

2. Funktsioonid

Kasutades Sambat NT4-domeeni või AD-domeeni liikmena, teostab Samba järgmisi funktsioone:

- andmeserver
- printimisserver

Kui Sambat kasutatakse NT4-ga ühilduvas domeenis PDC-na või Samba PDC BDC-d NT4-ga ühilduvas domeenis, saab Samba täita järgnevaid funktsioone:

- registreerimisserver
- andmeserver
- printimisserver

3. Winbind

Et kasutajad saaksid Samba vabastatud sisusid kasutada, peavad nad end serveril autentima. Selleks on vajalik, et Samba serveril oleks iga kasutaja jaoks olemas nii Windowsi kui ka Unixi kasutajakonto. Unixi kasutajakontot on teiste hulgas vaja selleks, et Samba saaks failisüsteemi ligipääsukontrolli jätta kerneli hooleks (vt M 4.332 Samba serveri pääsuõiguste turvaline konfiguratsioon). Seetõttu peab Windowsi domeeni liige kõigi oma gruppidega eksisteerima ka Unixi operatsioonisüsteemis. Teoreetiliselt on võimalik kõik domeeniliikmed käsitsi Unixi alla paigutada. Selle asemel tuleks aga kasutada Winbindi. Kui Unixi all ei eksisteeri Windowsi kasutajaid ega gruppe, siis on need võimalik Winbindiga luua. Winbindi kasutamisel Sambaga on võimalik vähendada nii võrgukoormust kui ka infosüsteemis olevate domeenikontrollerite koormust (vt M 4.333 Winbindi turvaline konfigureerimine Samba keskkonnas). Samba-serveri kasutamise plaanimisel tuleb seoses Winbindiga arvestada, et *ID-Mapping-Backend* „ads” toimib ainult siis, kui Samba käitus toimub turvarežiimis (*Security Mode*) „ads” (vt M 4.328 Samba serveri turvaline aluskonfiguratsioon).

Täiendavad kontrollküsimused

- Kas plaaniti, milline on Samba-serveri töö ja tema funktsioonid?
- Kui Winbindi kasutamine on vajalik, siis kas seda plaaniti vastavalt?

M 2.438z Väliste programmide turvaline kasutus Samba-serveril

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: Administraator

Paljusid funktsioone nagu uue kasutaja loomine Unixi‘s või printeristaatuse päring ei rakendata Sambas. Samba kasutab nende funktsioonide täitmiseks selle süsteemi programme, millele ta installeeritud on. Näiteks Unixi süsteemis uue kasutaja loomise korral käivitab Samba add user script kaudu spetsiifilise programmi. Kõik konfiguratsiooniparameetrid, mida Samba-väliste programmide käivitamiseks kasutab, lõpevad järgnevate märgijadadega:

- command
- script
- exec
- panic action
- program

Samba 3-s on umbes 40 sellist konfiguratsiooniparameetrit. Käsklusega

testparm -vs | grep -E “(command =)|(script =)|(exec =)|\ (panic action =)|(program =)” | wc -l

on võimalik kuvada hetkel kasutuses oleva Samba versiooni konfiguratsiooniparameetrite arv. Kui samba kasutab printerisüsteemiga suhtlemiseks Common Unix Printing System‘i (CUPS) Application Programming Interface‘i (API), siis ei ole vaikeseadistuses määratletud ühtegi nendest parameetritest, see tähendab, et ühtegi nendest parameetritest ei kasutata. Seda, kas Samba on CUPS teegiga tõlgitud ja ühendatud, on võimalik kontrollida järgneva käsklusega:

root# ldd $(which smbd) | grep ‘libcups’

Kui Samba ei kasuta printeritega suhtlemiseks CUPS-i API-d, siis eelseadistatakse mõningad printerisüsteemile spetsiifilised konfiguratsiooniparameetrid printing konfiguratsioonikaustas smb.conf standardväärtustega. Mõjutatud on järgnevad konfiguratsiooniparameetrid:

- print command
- lpq command
- lprm command
- lppause command
- lpresume command
- queuepause command
- queueresume command

Sambas varustatakse paljud selliste konfiguratsiooniparameetrite kaudu määratletud välised programmid root- õigustega. Sellest lähtuvalt tuleb kindlustada, et Samba käivitaks ainult programme, millel puudub kahjulik funktsioon süsteemile.

Käsklusega

user> testparm -vs | grep -E “(command =)|(script =)|(exec =)|\ (panic action =)|(program =)”

kuvatakse kõik Samba-väliste programmidega seotud parameetrid. Lisaks parameetritele kuvatakse ka hetkel kehtivad väärtused.

Täiendav kontrollküsimus:

- Kas enne väliste programmide Sambasse lisamist kontrollitakse nende võimalikku kahjulikkust?

M 2.439 Nõuete halduse kontseptsioon ja organisatsioon

Algatamise eest vastutavad: asutuse/ettevõtte juhtkond

Rakendamise eest vastutavad: asutuse/ettevõtte juhtkond, nõudehaldur

Tavaliselt on institutsioonis ülevaade nõuetest, mis on neis valdkondades ja äriprotsesside jaoks olulised. Tihtipeale ei ole need aga formuleeritud ülevaated, vaid erinevates struktuurides paiknev eri teave ja ekspertide teadmised. Tulenevalt suurest hulgast erinevatest nõuetest rahvusvahelises koostöös või äriprotsesside ja organisatsioonistruktuuride keerukusest võib kiiresti koguneda suur hulk erinevaid nõudeid. Seepärast on mõistlik koguda olemasolev teave erinevate seaduslike, lepinguliste ja teiste nõuete kohta kokku ja seda vajaduse korral täiendada. Selleks tuleb ametisse määrata vastavad isikud ja määrata kindlaks nende ülesanded nõuete halduses. Vastavat inimest kutsutakse sageli „nõudehalduriks". Olenevalt institutsiooni suurusest on mõttekas ametisse nimetada kas üks või mitu nõudehaldurit. Mõnedes ettevõtetes kasutatakse ka mõistet compliance manager, kes on institutsioonikeskne nõudehaldur. Kui kindlad reeglid seda ei nõua, ei pea selleks looma uut töökohta. Ülesande võivad endale võtta ka infoturbeosakond, auditi-, kontrolli- või õigusosakond.

Keskse nõudehalduri määramine kindlustab, et tal on ülevaade kogu institutsioonist, millest tulenevalt on võimalik juba varakult märgata ja vältida topelttööd ja konflikte. Mitu nõudehaldurit institutsiooni erinevates osakondades saavad aga paremini rahuldada nende hallatavate sihtgruppide vajadusi.

Lihtsuse mõttes viidatakse alljärgnevalt nõudehalduri rollile ainsuses. Nõudehalduri (hallatavate osakondade) ülesanded on järgmised:

- Kõik üldiseks äritegevuseks, informatsiooniks, nagu ka IT-süsteemide käituseks ja sinna juurde kuuluva füüsilise infrastruktuuri olulised seaduslikud, lepingulised ja muud nõuded peavad olema välja selgitatud ja dokumenteeritud (vt M 2.340 Õiguslike raamtingimuste järgimine).
- Erinevate osakondade andmed tuleb koguda, koondada ja konsolideerida struktureeritult.
- Identifitseeritud nõuete täitmiseks ja sobivate meetmete teostamiseks tuleb nimetada vastutavad isikud. Nõudehaldur peaks pidevalt kontrollima, kas kasutusele võetud meetmed võimaldavad täita esitatud nõudeid.
- Sageli tuleb nõuded kõigepealt interpreteerida ja neid institutsiooni vajaduste kohaselt tõlgendada, kuna enamik nõudeid ja seadusi väljendab pigem sihte ja ootusi kui teostamist.
- Kõik nimetatud nõuete liigid pärinevad konkreetselt sihtgrupilt, kes nõuab või kontrollib nõuetest kinnipidamist. Selleks et täita konkreetsed vajadused, tuleks nõuete väljaselgitamisel alati dokumenteerida ka vastav sihtgrupp. See säästab hiljem palju kohandamistööd. Seadusest tulenevate nõuete korral on mõttekas kindlaks määrata, milline instants (näiteks milline nõukogu) nendest kinnipidamist kontrollib ja millisel kujul tuleb selleks informatsioone täiendada.

Järgnevas tabelis leiate mõningad näited:

Nõuded	Sihtgrupp	Vastutav nõuete koguja

Andmekaitseseadus	Andmekaitse järelvalve	Ametkonna või ettevõtte andmekaitsespetsialist
Tööseadus	Töötajate esindus	Personaliosakond
Karistusseadustik	Kriminaaljälitus	Õigusnõuandja
Lepingud	Teenusepakkuja	Sisseost
	Klient	Turustamine
Muud nõuded	Koostööpartnerid	Tehniline osakond

Tabel. Nõuete liigitamine sihtgruppide ja nõudehaldurite alusel

Koostöö infoturbeosakonnaga
Infoturve on otsene või kaudne aspekt, mida tuleb arvestada pea kõigi nõuete korral. Seejuures on infoturbe spetsialist ainult vähestel juhtudel ka nõudehaldur. Nõudehaldur ja infoturbe spetsialist peavad seetõttu tegema tihedat koostööd, et esiteks kõigist osakondadest tulevad infoturbe nõuded oleks integreeritud nõudehaldusesse ja teiseks, et infoturbe seisukohast olulised nõuded rakendataks infoturbe meetmetes. Infoturbealased nõuded tulenevad esmajoones üldistest õiguseeskirjadest, osaliselt eriseadustest ja tegevus- või tööstusvaldkonna nõuetest, mis reguleerivad teatud süsteemide, teenuste ja tegevuste turvalisust. Siit tulenevad tsiviilõiguslikud kohustused, mille rikkumine (kaassüü) võib viia vastutava isiku vastutusele võtmiseni.

Näiteks:

- andmekaitseseadus,
- autorikaitse
- lepingud, ettevõtte üldtingimused jms,
- litsentsihaldus.

Infoturbealaste nõuetega arvestatakse äriprotsesside planeerimisel ja kontseptsioonis, rakendustes ja IT-süsteemides või uute komponentide hankimisel. Tüüpilised näited infosüsteemide etalonturbe kataloogides on meetmed, nagu M 2.419 Sobivate VPN-toodete valimine .

Kontrollküsimused:

- Kas institutsioonis on ülevaade seadusest tulenevatest, lepingulistest ja muudest nõuetest?
- Kas on kindlustatud, et meetmed spetsiifiliste nõuete täitmiseks on sobivad ja et neid teostatakse?

M 2.440 Windows 7 sobiva versiooni valimine

Algatamise eest vastutavad: Administraator, infoturbespetsialist

Rakendamise eest vastutavad: Administraator

Windows 7-l on erinevaid versioone nii kodukasutajale kui ka ettevõtetele, asutustele ja teistele organisatsioonidele. Versioonid erinevad üksteisest funktsioonide, hinna ja toetatavate litsentside poolest.

Kodukasutajale on mõeldud järgnevad Windows 7 versioonid:

- Windows 7 Starter
- Windows 7 Home Basic
- Windows 7 Home Premium
- Windows 7 Professional
- Windows 7 Ultimate

Ettevõtetele, asutustele ja teistele organisatsioonidele soovitab Microsoft järgnevaid Windows 7 versioone:

- Windows 7 Professional
- Windows 7 Ultimate
- Windows 7 Enterprise
- Windows 7 Starter: See versioon on ettenähtud vähenõudlikule kasutajale, kes kasutab arvutit minimaalselt ning kelle arvutil on väga väike jõudlus. Võimalused on piiratud ja olemas on ainult põhifunktsioonid.
- Windows 7 Home Basic: Versioon on mõeldud kodukasutajale. Võrreldes Windows 7 Home Premiumiga on võimalused piiratud. Kasutaja peab teiste hulgas loobuma Windows Aerost, Windows Media Centerist ja ka sisseehitatud varundusfunktsioonist.
- Windows 7 Home Premium: Versioon on mõeldud kodukasutajale. Windows 7 Home Premium versioon võimaldab kasutada Windows Aero klaasefekte ja laialdasi multimeediafunktsioone.
- Windows 7 Ultimate: Need versioonid on koostatud nii kodu- kui ka ärikasutajaid ja ametiasutusi silmas pidades. Neis on olemas kõik Windows 7 jaoks välja töötatud funktsioonid, nt kõvaketta krüpteerimine BitLockeriga ja laialdane võrgutugi.

Versiooniga Windows 7 Enterprise võrreldes pole Windows 7 Ultimate saadaval hulgilitsentsilepinguga.

- Windows 7 Business ning Windows 7 Professional: Versioonil Windows 7 Business on piiratud multimeediafunktsioonid. Samuti ei ole tootega integreeritud teatud turvafunktsioonid, nt ajamikrüpteering BitLockeriga ja rakenduste juhtimine AppLockeriga.
- Windows 7 Enterprise: mõeldud äriklientidele kasutamiseks, saadaval ainult hulgilitsentsilepinguga. Neis on olemas kõik Windows 7 jaoks välja töötatud funktsioonid, nt kõvaketta krüpteerimine BitLockeriga ja laialdane võrgutugi Microsofti litsentsimudel Windows Anytime Upgrade pakub tagantjärele kohandamist, mille puhul saab valida Windowsi erinevate redaktsioonide vahel.

Kohandamisel saab Windows 7 redaktsiooni Home Basic muuta redaktsiooniks Home Premium ning redaktsioonid Home Premium, Professional ja Business redaktsioonideks Windows 7 Ultimate.

32-bitiseid redaktsioone pole 64-bitisteks võimalik kohandada. 64-bitised versioonid pakuvad tõhusamat kaitset kahjurvara vastu, sest standardseadistuses saab neisse laadida vaid signeeritud draivereid. Lisaks on 64-bitistel versioonidel olemas Kernel Patch Protection, mis kaitseb Windowsi tuuma manipulatsioonide eest. Praegusaegsetel arvutitel on töömälu umbes 4 gigabaiti või rohkem ning seda saab hakata optimaalselt kasutama alates 64-bitistest versioonidest. Seetõttu tuleks alates Windows 7-st kasutada 64-bitist versiooni. Enne soetamist tuleb riist- ja tarkvara planeerimisel kontrollida, kas soodsam on osta 32-bitised, 64-bitised või nende kahe kombinatsioonist koosnevad litsentsid. Eriti oluline on analüüsida ühilduvust vanemate töös kasutatavate rakenduste ja spetsiaalse riistvaraga, sest need ei pruugi 64-bitise Windows 7-ga töötada.

Kontrollküsimused:

- Kas valiti sobiv Windows 7 süsteem?
- Kas Windows 7 versiooni valimisel arvestati kasutuskeskkonnaga (asutus, firma, kodukasutus) ja versioonist tulenevate võimalustega?

M 2.441 Uue tarkvara ühilduvuse kontroll koostööks Windows 7-ga

Algatamise eest vastutavad: IT-juht
Rakendamise eest vastutavad: administraator, infoturbespetsialist, IT-juht

Windows 7 erineb eelnevatest Windowsi versioonidest uute turvamehhanismide ning operatsioonisüsteemi omaduste poolest. Iga tarkvara ei täida neid nõudmisi. Sellest lähtuvalt ei saa varasematel Windowsi versioonidel kasutatud tarkvaralt eeldada, et see ühilduks ka Windows 7-ga.

Ühilduvuskontroll

Enne Windows 7 tarkvara soetamist tuleb kindlaks teha selle ühilduvus kasutatava Windows 7 versiooni konfiguratsiooniga. Sama kehtib ka operatsioonisüsteemi vanemalt süsteemilt Windows 7-le vahetamise korral. Kui planeeritakse varasemast teistsuguse riistvara kasutuselevõttu või operatsioonisüsteemi migreerimist, tuleb esmalt kontrollida ka kõikide asjassepuutuvate komponentide draiverite ühildumist.

Ühilduvuse kontrolli saab teostada järgmiselt:

- Taustauuring tootja kodulehel (https://winqual.microsoft.com), alapunktides „Certified for Windows 7” ja „Works with Windows 7”.
- Tarkvaratootja õiguslikult siduv kinnitus ühilduvuse kohta.
- Ühilduvuse kontroll testkeskkonnas.
- Järelpärimine Microsoftilt teadaolevate ühilduvuste või ühilduvusprobleemide suhtes.
- Infovahetus teiste kasutajatega.
- Uurimuse teostamine teadaolevate ühilduvuste või ühilduvusprobleemide suhtes.
- Tarkvara analüüsimine selliste toetatud diagnostikaprogrammidega nagu regmon, filemon või Windows 7 puhul procmon.

Ühilduvustest tuleks integreerida tarkvara testimis- ja vabastamismeetmetesse.

Kontrollküsimused:

- Kas Microsoft on kasutamiseks ettenähtud tarkvara Windows 7 jaoks sertifitseerinud („Certified for Windows 7”)?
- Kas on määratletud meetod tarkvara ühilduvuse kontrolliks?
- Kas ühilduvuse kontroll on tarkvara testimis- ja vabastamismeetoditesse integreeritud?

M 2.442 Windows 7 kasutamine kaasaskantavates arvutites

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: Administraator, kasutaja

Mobiilarvuti kasutamine on seotud tavaliste riskidega, mis tulenevad mobiilsest kasutamisest. Nagu kõigi teiste mobiilarvutite puhul, tuleb ka Windows 7-ga varustatud arvutite korral järgida moodulit B 3.203 Sülearvuti. Andmete krüpteerimise, varukopeerimine ja lokaalse tulemüüri tarvis on Windows 7 korral kasutada erinevad mehhanismid. Järgnevalt antakse nende valdkondade kohta soovitusi.

Andmete krüpteerimine

Mobiilarvutid paiknevad sageli kohtades, kus on tunduvalt madalam turvalisuse tase kui näiteks kaitstud bürooruumides. Seetõttu tuleks mobiilarvutil paiknevad konfidentsiaalsed andmed krüpteerida (vt M 4.29z Kaasaskantavatele IT-süsteemidele mõeldud krüpteerimistoote kasutamine). Teiste tootjate poolt valmistatud toodete kõrval võib krüpteerimiseks kasutada ka Windows 7 enda mehhanisme:

- Windows 7 versioonides Enterprise ja Ultimate võib kõvaketta partitsioonide krüpteerimiseks kasutada BitLockeri kõvaketta krüpteerimist. BitLockeri edukaks käivitamiseks Windows 7 stardiprotsessi ajal, saab administraator konfigureerida neli erinevat meetodit kasutaja autentimiseks: Autentimist ei toimu, PIN, USB pulk ja PIN ning USB pulk. Meetodid autentimist ei toimu, PIN, PIN ja USB pult eeldavad, et mobiilarvuti on varustatud TPM-iga (Trusted Platform Module). Koos TPM-iga tagab BitLocker süsteemi tervikluse ka buutimisprotsessi ajal.
- Krüptofailisüsteemi EFS (Encrypting File System) saab kasutada üksikute failide ja/või kataloogide krüpteerimiseks (vt M 4.147z EFS-i turvaline kasutamine Windows 'i keskkonnas).
- Offline -failide krüpteerimine. Offline -failid on põhimõtteliselt dokumentide koopiad, mis on võrgus kättesaadavad. Nad salvestatakse lokaalse arvuti andmebaasi, nii et ligipääs dokumentidele jääb alles ka siis, kui võrgust kättesaadavus on häiritud. Kogu offline -failide mälu, mis sisaldab kõigi kasutajate andmeid, krüpteeritakse arvutispetsiifilise võtmega. Krüpteerimine on kasutajale nähtamatu ja ainult administraatorid saavad seda aktiveerida või deaktiveerida.

BitLockeri kasutamine on soovitatav. EFS-i kasutamine on soovituslik, kui soovitakse, et mobiilsel arvutil olevad andmed oleksid krüpteeritud ka siis, kui arvuti on Windows 7 all sisse lülitatud. Sisselülitatud arvuti korral ei paku BitLocker kaitset. EFS seevastu hoolitseb üksikute failide ja ketaste krüpteerimise eest, kui need ei ole pidevalt dekrüpteeritud. Kui EFS-i poolt kaitstud failide või ketastega töötatakse, on ka need dekrüpteeritud. Meetod (BitLocker, Windows 7 EFS, offline -failide krüpteerimine ja krüpteerimine kolmandate programmidega) mobiilsel arvutil olevate andmete kaitseks tuleb kindlaks määrata vastavalt konkreetsele olukorrale ja juhtumile.

Andmete varukopeerimine

Andmekao vältimiseks tuleb kindla aja tagant teostada andmevarundus (vt M 6.32 Regulaarne andmevarundus). Windows 7-ga on võimalik varundada üksikuid

faile ja Windows Complete PC võimaldab luua varukoopia partitsioonidest (vt M 6.78 Andmete varundamine Windowsi klientsüsteemides).

Kui andmevarunduseks on konfigureeritud võrgukettad, saab varundus toimida ainult juhul, kui mobiilsel arvutil on võrguühendus varundusserveriga. Seetõttu tuleb ajad varukopeerimiseks vastavalt plaanida. Andmevarunduseks võib kasutada ka väliseid andmekandjaid (mälukaardid, USB mälupulgad). Sellisel juhul peab andmekandjale olema ligipääs nii andmevarunduseks kui ka taastamiseks. Seda tuleb arvestada väliste andmekandjate ligipääsupiirangute tehnilisel teostamisel (vt M 4.339 Vahetavate andmekandjate volitamata kasutamise tõkestamine Windows Vistas ja Windows 7-s). Meetod (Üksikute failide varundamine, Windows Complete PC varukoopia, programmid teistelt tootjatelt ja varundamise ajad ja kohad) mobiilsel arvutil olevate andmete varundamiseks tuleb kindlaks määrata vastavalt konkreetsele olukorrale ja juhtumile.

Lokaalne tulemüür

Vastupidiselt ettevõttesisestele statsionaarsetele lauaarvutitele, on mobiilarvutit võimalik otse internetiga ühendada. Sellisel juhul on kaitse lokaalse tulemüüriga kohustuslik. Windows 7 tulemüüriga pakub Windows kombinatsiooni „personaalsest tulemüürist“ ja IPSec lüüsist. Tulemüüri saab seadistada Windowsi turvakeskuse kaudu. Windows 7 tulemüüri täpsemaks konfigureerimiseks on kasutatav Management Console (mmc.exe) snap-in . Snap-In on konsooli lisamoodul, mida kasutatakse kindlate haldusülesannete teostamiseks. Windows tulemüüri abil saab kontrollida nii sisenevaid kui väljaminevaid andmevoogusid. Vaikeseadistuses blokeeritakse kogu sisenev andmevoog, välja arvatud konfigureeritud erandid (White List alged) ja väljaminev andmevoog, välja arvatud konfigureeritud erandid (Black List alged).

Windows tulemüüri vaikeseadistus sõltub antud Windows 7 versioonist. Windows 7 Enterprise ja Windows Professional 7 all on Windowsi tulemüüris avatud ainult vähesed pordid. Windows 7 Ultimate all on aga mitmed Windowsi teenused väljastpoolt kättesaadavad. Windows tulemüür kasutab Windows teenust Network Location Awareness (NLA). Administraator saab iga võimaliku võrgukeskkonna (võrgutüübi) tarvis Windows 7 tulemüürile konfigureerida erinevad suunised. Windows 7 eristab seejuures kolme võrguprofiili domeen, avalik ja privaatne võrk. Kui Windows 7 klient siseneb esimest korda uude võrku, siis küsib või Windows 7, millise võrguprofiiliga on tegemist. Selleks vajab kasutaja administraatori õigusi. Nende puudumisel valib Windows 7 avaliku võrgu. Kui võrk on domeen, mille liikmeks Windows 7 on, siis valib Windows 7 võrgukeskkonnaks automaatselt domeeni.

Juba üks kord liigitatud võrgud tunneb NLA teenus ära erinevate kriteeriumite järgi, näiteks vaikelüüsi (Default Gateway) MAC-aadress. Ainult haldusõigustega kasutaja saab klassifikatsiooni või Windows tulemüüri käitumist kindla klassifikatsiooni korral muuta. Standardolukorras annab Windows tulemüür võrguprofiilide domeen, avalik ja privaatne tarvis järgnevad seadistused.

Võrguprofiili domeeni korral kehtib:

- Windows 7 tulemüür aktiveeritakse.
- Windows 7 tulemüür saab seadistatud suunised Active Directory domeenist.
- Võrgutuvastus ja failide ning printerite lubamise konfiguratsioon põhineb Active Directory domeenist allalaetud grupipoliitikal.

Võrguprofiili „Avalik“ korral kehtib:

- Windows 7 tulemüür aktiveeritakse.
- Võrgutuvastus (NLA) deaktiveeritakse.
- Kõik failide ja printerite lubamised deaktiveeritakse, kaasa arvatud väliste andmekandjate lubamine.

Võrguprofiili „Privaatne“ korral kehtib:

- Windowsi tulemüür aktiveeritakse.
- Võrgutuvastus (NLA) aktiveeritakse.
- Kõik failide ja printerite lubamised deaktiveeritakse, kaasa arvatud meedia lubamine.

Tõenäoliselt saavad mobiilsed arvutid erinevates keskkondades ligipääsu võrgule.

Tüüpilised võrgukeskkonnad on ettevõtte LAN, kodune LAN ja internetiühendus avaliku WLAN-hotspoti kaudu. Windows 7 toetavad võrgukeskkonna automaatset tuvastamist ja tulemüüri seadistusi vastavalt hetke võrgukeskkonnale.

Kui kasutaja peab saama neid omadusi kasutada, peab ta vähemalt esimesel sisenemisel võrku omama administraatori õigusi. Kasutajat tuleb siis koolitada vähemalt võrgukeskkonna õiges määramise ja vajadusel ka reeglistiku määramise osas. Meetod (võrgukeskkonnast sõltuv reeglistik, kasutajapoolne võrgukeskkondade liigitamise võimalus) lokaalse tulemüüri kasutamiseks mobiilsel arvutil tuleb kindlaks määrata vastavalt konkreetsele olukorrale ja juhtumile. Selle käigus tuleb kontrollida, kas Windowsi enda tulemüür suudab toime tulla ka komplekssemate kasutusjuhtudega, nt koostöö virtuaalse privaatvõrguga (VPN), ning kas tulemüür saavutab soovitud kaitsetoime või tuleb siiski kaaluda mõne kolmanda tootja tarkvaralahendust.

Kontrollküsimused:

- Kas on kasutusele võetud meetmed mobiilarvuti andmete kaitseks?
- Kas andmete krüpteerimiseks kasutusele võetud meetmed on vastavuses konfidentsiaalsuse nõuetega?
- Kas andmete varundamiseks kasutusele võetud meetmed vastavad käideldavusnõuetele?
- Kas tulemüüri konfiguratsioon vastab nõuetele, mis tekivad vajalike ja lubatud kommunikatsioonisuhete tõttu?

M 2.443 Windows Vista SP1 kasutuselevõtt

Algatamise eest vastutavad: Administraator, IT-turbespetsialist

Rakendamise eest vastutavad: Administraator

SP1 on remondipakett, mis sisaldab tarkvara veaparandusi ja täiendusi Microsofti operatsioonisüsteemile Windows Vista. SP1 on saadaval nii Windows Vista 32-bitilise versiooni (x86) ja 64-bitilise versiooni (x64) jaoks. SP1 installeerimiseks toetab Microsoft meetodeid iseseisev pakett, värskendus ja DVD. Järgnevas tabelis on näidatud kõigi müügimeetodite omadused.

Müügimeetod	Omadused
Iseseisev pakett	- Windows Vistaga arvuti, kuhu kavatsetakse SP1 installeerida, ei pea olema internetiga ühendatud. - Allalaetud paketti saab tarkvara jagamise programmi abil korraga installeerida mitmesse Windows Vista arvutisse. - SP1 RC maht on 400 MB kuni 900MB, sõltuvalt sellest, mitut keelt süsteem toetab ja kas valiti 32-bitine versioon (x86) või 64-bitine versioon (x64).
Windows Update	- Windows Vistaga arvuti, kuhu kavatsetakse SP1 installeerida, peab olema interneti kaudu ühenduses Microsofti Update serveritega. 65 MB-ga on värskendus tunduvalt väiksem kui iseseisev pakett.
Windows Vista installeerimise DVD	- Sisaldab Windows Vista operatsioonisüsteemi SP1 tasemel. - Windows Vista installeerimiseks koos SP1-ga. - Pärast installeerimist tuleb Windows Vista 30 päeva jooksul aktiveerida.

SP1 allalaadimisel tuleb arvestada sellest tuleneva koormusega ettevõtte LAN võrgule. Võrgu koormus sõltub SP1 suurusest ja Windows Vista klientide arvust, kes seda üheaegselt alla laevad. Enne SP1 kasutamist Windows Vista tootmiskeskkonnas asuvas süsteemis tuleks seda testida testimiskeskkonnas võimalike mitteühilduvuste suhtes. Lisaks tuleb enne SP1 installeerimist Windows Vista kliendile kindlaks teha, kas kõvakettal on piisavalt vaba ruumi. Vajalik vaba ruum kõvakettal sõltub mitmetest faktoritest. Nende hulka kuuluvad näiteks, millisel viisil SP1 Windows Vista jaoks omandati ja näiteks mitut keelt toetatakse. SP1 installatsioonirutiin määrab vajaliku kõvakettaruumi. Viie keelega 32-bitise versiooni (x86) iseseisva paketti suuruseks nimetab Microsoft orienteeruvalt 4,5 GB. Vajadusel tuleb SP1 täpse mahu välja selgitamiseks pöörduda Micro-

softi poole. Enne SP1 installeerimist Windows Vistale tuleb kindlaks teha, kas eelnevalt on installeeritud kõik vajalikud Windows Vista tarkvarauuendused. *Microsoft Knowledge Base* artikli 935509 andmetel on nendeks BitLockeri uuendus 935509, SP1 installeerimise/deinstalleerimise uuendus 938371 ja Windows Vista installeerimistarkvara uuendus 937287 (seisuga kevad 2008). SP1 sisaldab lisaks veaparandustele ka mõningaid turvalisust mõjutavaid muudatusi. Nende hulka kuuluvad näiteks:

- Hoiatusteated, seniste ähvardavate RFM-ide (*Reduced Functionality Mode*) asemel, kui tahtlikult või tahtmatult rikuti nõudeid Windows Vista litsentsi aktiveerimisel (vt M 4.336 Hulgilitsentslepinguga Windows süsteemide aktiveerimine alates Windows Vistast või Windows Server 2008-st ja M 4.343 Hulgilitsentsilepinguga Windowsi süsteemide reaktiveerimine alates Windows Vistast või Windows Server 2008-st).
- EFS-iga krüpteeritud failid saab varundada tööriistaga „varundamine ja taaste“ (vt M 6.78 Andmete varundamine Windowsi klientsüsteemides).
- API-liides (*Application Programming Interface*) pakub täiustatud võimalusi 64-bitises keskkonnas kasutada ka teisi viirusetõrje programme peale *Kernel Patch Protection'i.*
- TPM-i (*Trusted Platform Module*) kasutamisel toetatakse BitLockeri *Multifactor* autentimist USB pulga ja PIN-i kaudu.
- Võimalik on ka teiste partitsioonide krüpteerimine BitLockeri kaudu (vt M 4.337 BitLockeri Drive Encryption kasutamine).
- Toetatakse SHA-256, AES-GCM ja AES-GMAC ESP-le (*Encapsulating Security Payload*) ning AH (*Authentication Header*), ECDSA, SHA-256 ja SHA-384 *Internet Key Exchange* (IKE) ning *AuthIP*.
- PRNG-dest (*pseudo-random number generator*) on kasutuses NIST SP 800-90 ECC (*Eliptical Curve Cryptography*).

Täiendavad kontrollküsimused:

- Kas on kindlaks määratud, millist SP1 versiooni vajatakse?
- Kas enne tootmiskeskkonda paigaldamist testiti SP1 testkeskkonnas võimalike mitteühilduvuste väljaselgitamiseks?
- Kas on kasutatav piisav ribalaius (Bandwidth), et SP1 internetist alla laadida ja organisatsiooni LAN-i installeerida?
- Kas vastaval Windows Vista kliendil on kõvakettal piisavalt vaba ruumi SP1 installeerimiseks?
- Kas enne SP1 installeerimist on Windows Vista kliendile installeeritud kõik vajalikud värskendused lähtuvalt Microsoft Knowledge Base artiklist 935509?

M 2.444 Virtuaalsete IT-süsteemide ressursside planeerimine

Algatamise eest vastutavad: IT-juht, infoturbespetsialist
Rakendamise eest vastutavad: administraator

Virtuaalsete IT-süsteemide planeerimisel tuleb lisaks meetmes M 2.315 Serveri kasutuselevõtu planeerimine antud serveri turvalise töö eeldustele silmas pidada ka muid punkte. Järgnevalt kirjeldatakse virtuaalsete IT-süsteemide planeerimise lisameetmeid.

Virtuaalsete IT-süsteemide tootjatugi

Tuleb kontrollida, et kõiki virtuaalsetel IT-süsteemidel käitavail rakendustel oleks valitud virtualiseerimisplatvormi jaoks olemas tootjatugi. Tootjad annavad oma tarkvara tavaliselt teatud operatsioonisüsteemi ja riistvaraplatvormi kombinatsiooni jaoks vabaks, kuid tagavad esineda võivate probleemide puhul toe ainult tarkvara tingimustekohase kasutamise korral. Kuna virtuaalse IT-süsteemi riistvaraplatvormi ei ole seni standardiseeritud, ei anna kõik tarkvaratootjad virtuaalsetele IT-süsteemidele täielikku tuge, vaid enamasti ainult teatud operatsioonisüsteemi ja virtualiseerimistoote kombinatsiooni jaoks näiteks vigade analüüsi ja kõrvaldamise puhul.

Virtuaalsete IT-süsteemide elutsükkel

Peale selle muutuvad väljakujunenud protseduurid (virtuaalsete) IT-süsteemide kasutuselevõtmise, inventariseerimise, käitamise ja kasutuselt kõrvaldamise jaoks ühes virtuaalses taristus käitamise puhul. Seetõttu tuleb järgmiste protsesside kohaldamine detailselt planeerida ja kindlaks määrata, pidades silmas järgmisi tingimusi:

- Kontrollitakse, kas kasutatavad operatsioonisüsteemid ja rakendused on virtualiseeritud IT-süsteemide käitamiseks sobivad.
- Tagatakse, et virtualiseerimistoote oleks IT-süsteemi jaoks sobiv.
- Ei tohi kasutada virtualiseerimisfunktsioone nagu näiteks snapshot 'id, mis võivad põhjustada probleeme rakendustega (vt M 4.347z Virtuaalsete IT-süsteemide snapshot'ide desaktiveerimine).
- Rakenduste jaoks ei tohi vaja minna riistvarakomponente nagu näiteks tarkvarakaitsemoodulid (Dongles) või ISDN-kaardid, mis ei suuda virtuaalset IT-süsteemi virtuaalses taristus käideldavaks teha.
- Kõik virtuaalsed IT-süsteemid peavad olema IT-koosluse inventariseerimisse täielikult kaasatud, vältimaks näiteks alalitsentseeritust või tundmatu kasutusotstarbega süsteemide käitamist.
- Füüsiliste IT-süsteemide kasutuselevõtuks vajalikud protseduurid ning planeerimis- ja käitamisettevalmistused tuleb ettenähtud viisil ja otstarbekohaselt virtuaalsetele IT-süsteemidele üle kanda. Kui füüsilised IT-süsteemid saab varustada näiteks kleepsuga, millele kantakse nimi ja IP-aadress, ei ole see virtuaalsete IT-süsteemide puhul võimalik. Neid parameetreid saab aga rakendada virtuaalsetele IT-süsteemidele nime andmisel.
- Koos serveri ja rakenduste käitajatega määratakse enne süsteemi käikulaskmist virtuaalse IT-süsteemi jaoks kindlaks realistlikud ja küllaldased jõudlus- ning ressursinõuded. Pärast jõudlusnõuete kindlaksmääramist tuleb kontrollitakse, kas juhuslikult esineda võivate tippkoormuste ajal võib ette

tulla jõudluspiiranguid: nii ei ole näiteks andmebaasi sisu töötlemise skriptid sageli ajakriitilised ja neid ei pea seetõttu teostama maksimaaljõudlusega.
- Tuleb kindlaks määrata, kuidas teostatakse virtuaalse IT-süsteemi töö ajal rutiinseid toiminguid. Sealjuures tuleb tagada, et sellised toimingud nagu virtuaalsete IT-süsteemide käivitamine ja peatamine, snapshot'ide loomine ja kustutamine ning lähtestamine oleks kooskõlastatud serveri käitajate ja rakenduste omanikega.
- Virtuaalsete IT-süsteemide jõudlust jälgitakse ja tagatakse jõudlusnõuete piisav täitmine.
- Tuleb kehtestada protseduur, millega protsessori jõudluse, põhimälu ja kõvakettamahu kasutamise kitsaskohad tuvastatakse õigeaegselt ja neile reageeritakse adekvaatselt.

Test- ja arenduskeskkonnad

Test- ja arenduskeskkondades, mille puhul teostatakse ainult virtuaalsete IT-süsteemide funktsionaalset analüüsi, ei ole vaja eelpoolmainitud tingimustest alati kinni pidada, kuid igal juhul tuleb organisatsioonis kehtestada protseduur, mis tagab, et virtuaalsete IT-süsteemide konfiguratsioon ja ressursside jaotus oleks kontrollitud ja vajadusel enne käikulaskmist kohandatud. Näiteks ei tohi virtuaalseid IT-süsteeme test- ja arenduskeskkonnast lihtsalt kopeerida ja kloonida, vaid nad tuleb uuesti installeerida. Kui IT-süsteemi ei installeerita uuesti, tuleb kopeeritava või kloonitava virtuaalse IT-süsteemi sobivust töö jaoks hoolikalt kontrollida.

Eriti oluline on kontrollida, kas teatud test- ja arenduskeskkonnas kasutatavad virtualiseerimisfunktsioonid (nagu näiteks skriptid külalistööriistades) on veel aktiivsed. Testid tuleb seejuures teostada keskkonnas, mis kasutab sama virtualiseerimislahendust kui sihtsüsteem. See peab tagama, et virtuaalse IT-süsteemi käitumine testkeskkonnas ei erineks käitumisest tegelikus töökeskkonnas.

Kontrollküsimused:

- Kas enne töövõrgus kasutuselevõttu kontrollitakse test-ja arenduskeskkondadest pärit virtuaalsete IT-süsteemide tööks sobivust?
- Kas on kehtestatud protseduur virtualiseerimisserverite ja virtuaalsete IT-süsteemide kasutuselevõtuks?
- Kas virtuaalsete IT-süsteemide puhul on kindlaks määratud, milliseid virtualiseerimisfunktsioone (nagu näiteks snapshot 'id) kasutada võib?
- Kas on tagatud virtuaalsete IT-süsteemide jõudluse jooksev jälgimine?
- Kas kõik IT-koosluse virtuaalsed IT-süsteemid on kaasatud inventariseerimisse?
- Kas on kehtestatud protseduur virtualiseerimisserverite ja virtuaalsete IT-süsteemide kasutuselt kõrvaldamiseks?

M 2.445 Sobiva riistvara valimine virtualiseerimiskeskkondade jaoks

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: finantsjuht

Enamlevinud operatsioonisüsteemi ja serveri virtualiseerimise lahendused esitavad aluseks olevale riistvaraarhitektuurile nagu virtualiseerimisserverite varustatus riistvarakomponentidega (võrguliidesed või massimälukaardid) konkreetsed nõuded, mida tuleb virtualiseerimisserverina kasutatavate serverisüsteemide ostmisel silmas pidada. Eri tüüpi virtualiseerimise (operatsioonisüsteemi-, hüperviisori- või hostipõhise serveri virtualiseerimise) puhul on riistvaranõuetes mõned järgnevalt kirjeldatavad põhimõttelised erinevused.

Operatsioonisüsteemi virtualiseerimise ja hostipõhise serveri virtualiseerimise nõuded

Operatsioonisüsteemi virtualiseerimise süsteemid ja nn hostipõhised serveri virtualiseerimise lahendused saab enamasti taandada installeerimiseks kasutatava alusoperatsioonisüsteemi kompleksse draiveritoele. Üks näide operatsioonisüsteemi virtualiseerimise kohta on *Sun Solaris Zones* , mis on integreeritud *Solaris*-operatsioonisüsteemi. Hostipõhised serveri virtualiseerimise näideteks on *Microsoft Virtual PC*, *Sun VirtualBox*, või *VMware Server*, mille saab sarnaselt traditsiooniliste teenustega installeerida ühilduvale operatsioonisüsteemile. Tavaliselt saab kasutada iga riistvarakomponenti (võrguliidesed, SCSI-kontrollerid jms), mida valitud operatsioonisüsteem toetab ja sel puhul saab kasutada arvukalt komponente.

Nõuded hüperviisoritoodetele

Tunduvalt rangemad nõuded virtualiseerimislahendusega kasutatavate riistvarakomponentide valimisele esitatakse hüperviisoritoodete puhul. Mainida tuleks näiteks *Microsoft Hyper-V*, *VMware ESX* või *XEN*, mis kujutavad endast virtualiseerimisele taandatud operatsioonisüsteemi ning on draiveritega varustatuse osas enamasti piiratud riistvaratoega või esitavad kasutatavale protsessorile erilisi nõudmisi. Näiteks saab virtualiseerimislahendust *XEN* kasutada piiranguteta ainult siis, kui protsessor sisaldab virtualiseerimisfunktsioone (*Intel VT*, *AMD-V*). Sama kehtib *Microsoft Hyper-V* puhul. Sõltumata kasutatava virtualiseerimislahenduse valimisest tuleb ühilduvust virtualiseerimiskeskkonna planeerimisel eelnevalt kontrollida. Operatsioonisüsteemi- ja hostipõhise serveri virtualiseerimise lahenduste puhul tuleb selgeks teha virtualiseerimistarkvara töötavus vastava operatsioonisüsteemi all koos valitud riistvaraga.

Riistvara valimine

Virtualiseerimislahenduse riistvaraplatvormiks valitakse sobivad füüsilised serverid. Virtualiseerimislahenduste autorid avaldavad oma toote jaoks kõlblike riistvarakonfiguratsioonide kohta regulaarselt uuendatud ühilduvusnimekirju, mis annab riistvara sobivuse kohta garantii. Selliseid nimekirju tuleb riistvara valimisel silmas pidada, eelkõige juhul, kui neid hakatakse kasutama tegelikus töös. Lisaks ei tagata hooldusle pingutes sageli tootjasertifikaadita virtualiseerimistarkvara puhul kokkulepitud tugiteenuseid ja garantiisid üldse või tehakse seda puudulikult. Juba töötavate ja probleemivabalt toimivate keskkondade puhul tuleb kontrollida, mil määral tagab tootja oma virtualiseerimistootele toe olemasoleva riistvara puhul ka siis, kui see on sertifitseerimata.

Täiendavad kontrollküsimused:

- Kas virtualiseerimislahenduse ühilduvust kasutatava riistvaraga on kontrollitud?

- Kas on tagatud, et kasutatava virtualiseerimislahenduse tootja annab antud füüsilise tarkvara puhul garantii?

M 2.446 Haldustoimingute jaotus virtualiseerimisserverite puhul

Algatamise eest vastutavad: infoturbespetsialist

Rakendamise eest vastutavad: administraator

Virtualiseerimistaristute puhul lisanduvad tavalistele rollidele ja haldustoimingutele (vt M 2.38 Administraatorirollide jagamine) arvutuskeskuse töös ka muud administratiivsed ülesanded. Administraatorite rolli eripära virtuaalses taristus seisneb selles, et neil võivad olla käitatavate virtuaalsete IT-süsteemide suhtes väga laialdased volitused. See tähendab, et neil:

- on kontroll emuleeritava riistvarakonfiguratsiooni üle,
- nad saavad virtuaalseid IT-süsteeme võrgus siduda,
- nad saavad eraldada virtuaalsetele IT-süsteemidele mäluressursse salvestusvõrgust ja
- neil on enamasti juurdepääs virtuaalsete IT-süsteemide konsoolidele.

Administraatorirollide jaotus võimaldab erinevate administraatorirühmade vastastikust kontrolli tööjaotusega arvutuskeskuse funktsioneerimisel. Nii saab mõnede virtualiseerimistoodete nagu *CitrixXENCenter*, *Microsoft System Center Virtual Machine Manager* või *VMware vSphere* puhul määratleda administraatorirollid, mis eraldavad teatud kasutajarühmadele virtuaalses taristus teatud õigused. Seejuures saab näiteks teatud kasutajarühmadel takistada virtuaalseid IT-süsteeme virtuaalsest taristust eksportimast. Peale selle saab anda või ära võtta virtuaalsete IT-süsteemide sisse- või väljalülitamise õigust. Tuleb kontrollida, kas virtuaalselt käitatavate IT-süsteemide puhul on administraatorirollide jaotus vajalik. See võib osutuda vajalikuks näiteks siis, kui teatud administraatorite rühm ei tohi konfidentsiaalsuse huvides saada õigust eraldada võrke kõrgendatud kaitsevajadusega virtuaalsete IT-süsteemide jaoks. Kui vajatakse administraatorirollide jaotust, tuleb kasutada vastavate administraatorirollide definitsiooni antud virtualiseerimistaristu puhul. Mõned virtualiseerimistooted sellist võimalust ei paku. Sel juhul tuleb kontrollida, kas piisab administraatorirollide pelgalt organisatsioonilisest jaotusest näiteks eeskirja põhjal.

Täiendavad kontrollküsimused:

- Kas on kontrollitud, et administraatorirollide jaotus on virtuaalse infosüsteemi puhul vajalik?
- Kas administraatorirollide jaotus toimub organisatoorsete või võimalusel virtualiseerimistoote tehniliste vahendite abil?

M 2.447 Virtuaalsete IT-süsteemide turvaline kasutamine

Algatamise eest vastutavad: IT-juht, infoturbespetsialist

Rakendamise eest vastutavad: IT-juht, administraator

Virtuaalsete IT-süsteemide kasutuselevõttu korral tuleb arvestada mõningate iseärasustega, mis ületavad füüsiliste IT-süsteemide jaoks vajalikud meetmed (vt M 2.318 Serveri turvaline installeerimine). See tuleneb nii virtuaalsete IT-süsteemide dünaamilisusest ja paindlikkusest kui ka võimalusest, et mitu erinevaid andmeid töötlevat virtuaalset IT-süsteemi paiknevad ühel virtualiseerimisserveril üksteise kõrval. Virtuaalsed IT-süsteemid tuleb nagu füüsilised arvutidki kasutusele võtta vastavalt tüübile ja kasutusalale (rakenduseserver või klient aga ka näiteks kommutaator). Seetõttu tuleb füüsiliste süsteemide jaoks kasutatavaid meetmeid teostada ka virtuaalsete IT-süsteemide installeerimise ja hilisema käitamise korral. Lisaks tuleb arvestada, et rakendustele, kui need teisaldatakse iseseisvatelt füüsilistel IT-süsteemidelt virtuaalsetele IT-süsteemidele, võivad tekkida lisaohud. Näiteks võivad teatud juhtudel tekkida kitsaskohad töötlemiskiiruses või mälumahus. Seejuures võib olla vajalik olemasoleva installatsioonidokumentatsiooni sobitamine kasutussevõetava virtuaalse IT-süsteemiga. Virtuaalse IT-süsteemi kasutuselevõttu tuleb seega hoolikalt ette valmistada (vt M 2.444 Virtuaalsete IT-süsteemide ressursside planeerimine).

Enne virtuaalserveri kasutusele võtmist tuleks arvestada järgmiste punktidega:

- Kindlustada tuleb, et virtuaalsete IT-süsteemide virtualiseerimistarkvara konfiguratsiooni ning virtuaalsete IT-süsteemide sisseseadmist ja kustutamist teostaksid vastutavad administraatorid.
- Vastavalt nõuetele tuleb seadistada ka virtuaalsete IT-süsteemide ligipääsuõigused. Ka siin kehtib põhimõtte, et lubada tuleks ainult ilmtingimata vajalikud ligipääsuvõimalused. See ei kehti mitte ainult virtualiseerimisserveri haldustarkvarale, vaid ka andmetele, millega virtuaalset IT-süsteemi virtualiseerimisserveril esindatakse.
- Kindlustada tuleb, et virtuaalsete IT-süsteemide jaoks vajalikud võrguühendused oleksid virtuaalses tarindis olemas.
- Välja tuleb selgitada ja arvestada virtualiseerimise mõjuga virtuaalse IT-süsteemi administraatoritele ja sellel käitatavatele rakendustele (näiteks süsteemimonitooringu korral või virtuaalsete riistvararessursside kasutamisel).
- Sõltuvalt kasutusvaldkonnast peavad füüsilisel arvutil paiknevad erinevad virtuaalsed IT-süsteemid üksteisest rohkemal või vähemal määral eraldatud olema (vt M 3.70w Sissejuhatus virtualiseerimisse ja M 3.72w Virtualiseerimistehnika põhimõisted). See kehtib eeskätt juhtudel, kui virtualiseerimisserveril soovitakse käitada erineva turbevajadusega virtuaalseid IT-süsteeme.
- Mitme virtuaalse IT-süsteemi käitamine ühel füüsilisel arvutil võib drastiliselt mõjutada sellel käitatavate rakenduste vastusteaega, kättesaadavust ja arvuti andmetöötlusmahtu.
- Tuleb kontrollida, kas rakenduse käideldavusele ja andmetöötlusmahtudele esitatavad nõuded on kasutatava virtualiseerimislahendusega täidetavad

Selleks võib enne tootmissüsteemi laskmist kontrollida, kas virtuaalne IT-süsteem annab vastuvõetavad vastuseajad ja andmetöötluskiirused.

- Peale selle tuleks jälgida virtuaalsete serverite jõudlusega seotud omadusi, et kitsaskohtade korral oleks võimalik konfiguratsiooni kohe parandada. Monitooring võib toimuda nii virtuaalsete IT-süsteemide tasandil kui ka vastava virtualiseerimisserveri tasandil. Siinjuures tuleb silmas pidada, et läbi virtuaalsete IT-süsteemide saadud jõudlusnäitajad ei vasta alati reaalsusele. Mõningate virtualiseerimistoodete korral jagatakse virtuaalsele IT-süsteemile näiteks teatud osa protsessoriajast. Kui virtuaalne süsteem teatab nüüd (virtuaalse) protsessi koormuse, siis ei vasta see füüsilise protsessori koormusele, vaid ainult süsteemile omistatud protsessoriaja koormusele.

Kontrollküsimused:

- Kas administraatorite ligipääsuõigusi virtuaalsetele IT-süsteemidele piiratakse vajalikul määral ning kas lubatakse ainult reaalselt vajalikud ligipääsuõigused?
- Kas virtuaalsete IT-süsteemide jaoks vajalikud võrguühendused on olemas?
- Kas virtualiseerimiskeskkonna, virtuaalsete IT-süsteemide ja nendel käitatavate rakenduste administraatorid on tutvunud virtualiseerimise mõjudega?
- Kas virtuaalsete IT-süsteemide ja nendel käitatavate rakenduste isolatsioon ja eraldatus on piisaval määral tagatud?
- Kas on välja selgitatud nõuded virtuaalsete IT-süsteemide käideldavusele ja andmetöötlusmahtudele?

_ Kas virtuaalseid IT-süsteeme monitooritakse jooksvalt?

M 2.448 Virtuaalsete taristute funktsiooni ja konfiguratsiooni kontroll

Algatamise eest vastutavad: IT-juht, infoturbespetsialist

Rakendamise eest vastutavad: administraator

Virtualiseerimisserveri konfiguratsioonifailid sisaldavad virtuaalse masina käitamiseks vajalike virtuaalse taristu kohta käivat informatsiooni. Siia juurde kuuluvad iga virtuaalse IT-süsteemi ressursside jaotus ja virtuaalsete IT-süsteemide võrkude defineerimine.

Virtuaalsete IT-süsteemide konfiguratsiooni monitooring

Virtuaalsete IT-süsteemide konfiguratsioon serverite ja operatsioonisüsteemide virtualiseerimiseks virtuaalses taristus määrab virtuaalse IT-süsteemi omadused. Samuti on kindlaks määratud millised protsessiressursid, kui palju põhimälu ja kui palju kõvakettaruumi virtualiseerimisserveri poolt virtuaalse IT-süsteemi kasutusse antakse. Peale selle määratakse serveri virtualiseerimisel, mille korral virtualiseeritakse kogu riistvara, kindlaks lisaks konfiguratsioonile ka riistvaraemulatsiooni omadused. Siia kuuluvad näiteks:

- massmäluseadmed ja võrgukaardid,
- ligipääs ajamitele (diskett, CD/DVD jne) ja ülejäänud virtuaalse IT-süsteemi käsutusse antav riistvara ning
- virtuaalse IT-süsteemi ühendamine füüsilise võrguga.

Kui virtuaalse IT-süsteemi konfiguratsiooni muudetakse, ei pruugi need teatud juhtudel saada ligipääsu kiiresti vajaminevatele ressurssidele. On ka võimalik, et virtuaalne IT-süsteem saab ligipääsud ressurssidele, millele ta tegelikult ligipääsu omada ei tohiks. Sellise mittelubatud ligipääsu näiteks oleks ligipääs kõigile ettevõtte arendusosakonna töötajate palgaandmetele. Sellest lähtuvalt on virtuaalse IT-süsteemi konfiguratsioonifailid lähtuvalt oma terviklusest tihtipeale suure turbevajadusega. Tuleks kindlaks määrata, kuidas peaks toimuma nende konfiguratsioonifailide kontroll volitamata muudatuste suhtes. Sõltuvalt virtualiseerimisserveril käitatavate virtuaalsete IT-süsteemide turbevajadusest tuleks mõelda automaatsete kontrollide (näiteks kontrollsumma meetod) või virtualiseerimisserveri administraatorite poolt läbiviidava regulaarse kontrolli peale.

Virtuaalse taristu funktsioonide monitooring

Virtualiseerimisserveril defineeritakse virtuaalsed võrgud reeglina nende võrkude abiga, mis ühendavad virtuaalse IT-süsteemi füüsilise võrguga. Need virtualiseerimisserveri võrgukonfiguratsioonid võivad väärkonfiguratsiooni või valede kaabliühenduste tõttu avada tahtmatuid suhtluskanaleid, mis tavaolukorras ei oleks kasutatavad. Sellekohane näide oleks kõrge turbevajadusega ERP-süsteemi ekslik ühendamine klientide sissehelistamiseks ettenähtud DMZ-tiga. Seepärast tuleb regulaarselt kontrollida, et kaablite asetust ja virtualiseerimisserveri loogilist sisseseadmist puudutav võrgukonfiguratsioon vastab plaanidele. See hõlmab võrgustiku ja virtualiseerimiserverite sidumist salvestusvõrguga. Mõningate virtualiseerimistoodete korral eristatakse ressursse, nagu näiteks võrguühendusi, ainult nime alusel, mis on peaaegu vabalt valitav. Need ressursid omistatakse nüüd virtuaalsetele IT-süsteemidele võrgu kaudu selle nime alusel. Omistatus jääb sageli alles, kui virtuaalne IT-süsteem teisaldatakse ühelt virtualiseerimisserverilt teisele . Kui füüsiliselt või loogiliselt erinevad võrguühendused on märgitud

sama nimega, võib virtuaalne IT-süsteem ühendada ennast vale võrguga. Teatud juhtudel võivad sellel olla raskekujulised tagajärjed, kui vea tõttu konfiguratsioonis on näiteks segamini aetud *internet* ja *intranet.* Seepärast tuleb võrkudele valida konkreetsed ja väljendusrikkad nimed ja regulaarselt kontrollida, kas antud võrgujaotus on õige. See võib toimuda funktsioonitesti kaudu, näiteks virtuaalsele süsteemile määratud võrgu kättesaadavustesti kaudu.

Täiendavad kontrollküsimused:

- Kas on kindlustatud, et virtuaalse taristu konfiguratsioonifaile kontrollitakse regulaarselt volitamata muudatuste suhtes?
- Kas kontrollitakse, et võrgujaotus vastab dokumentides kirjeldatule?
- Kas võrkudele valiti piisavalt konkreetsed ja väljendusrikkad nimed?

M 2.449z Konsooli kaudu virtuaalsetele IT-süsteemidele juurdepääsu minimaalne kasutamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator

Mitmed laialt levinud lahendused IT-süsteemide virtualiseerimiseks võimaldavad ennast kas lokaalselt virtualiseerimisserveril või võrgu kaudu kaugtööjaamast klienttarkvara abiga virtualiseerimistarkvaral sisse logida (näiteks Citrix XenCenter või VMware Console). See klienttarkvara võimaldab virtualiseerimistarkvara virtualiseerimisserveril sisse seada ning aitab seda hooldada ja monitoorida. Serveri virtualiseerimise toodete juures tuleb seda aga kasutada ka ligipääsuks virtuaalse masina konsoolile. Tavaliselt ei ole see nende toodete korral virtuaalsete IT-süsteemide arhitektuuri tõttu teistmoodi realiseeritav, kuna virtuaalsel IT-süsteemi puudub füüsiline konsool. Näiteks on sel moel võimalik jälgida virtuaalse masina käitusolekut ka buutimisprotsessi ajal. Serveri virtualiseerimisel koosnevad virtuaalsed IT-süsteemid ainult virtuaalsetest riistvarakomponentidest. Seadmed nagu võrgukaardid, massmälu ja graafikakaardid tuleb virtualiseerimistarkvara poolt emuleerida. Võrgukaartide ja massmäluseadmete emuleerimisel on reeglina võimalik virtuaalsete IT-süsteemide käsklused edastada vastavale füüsilisele seadmele. Seetõttu ei tule neid täielikult emuleerida. Graafikakaardid tuleb reeglina aga täielikult virtualiseerimistarkvara poolt emuleerida. Seetõttu teeseldakse jõudluse põhjustel virtuaalsele IT-süsteemile, et graafikakaart on pidevalt olemas. Alles ligipääsul virtuaalse IT-süsteemi konsooliliidesele käivitatakse tarkvaras tegelik emulatsioon. Reeglina seob see virtualiseerimisserveri protsess- ja salvestusressursid. Kuna konsooliligipääsud virtuaalsetele IT-süsteemidele mõjutavad tugevalt virtualiseerimisserveri haldustarkvara, tuleb need minimeerida. Virtuaalseid IT-süsteeme ei tohiks seega juhtida otse konsooliligipääsude kaudu vaid pigem võrgu, näiteks RDP või X-Windowsi SSH-tunneldamise kaudu.

Kontrollküsimused:

- Kas konsooliligipääsud virtuaalsetele IT-süsteemidele on minimeeritud, et nad ei saaks mõjutada virtualiseerimisserveri jõudlust?
- Kas virtuaalseid IT-süsteeme juhitakse võrgu, näiteks RDP või X-Window kaudu SSH-tunneldamise abiga?

M 2.450w Sissejuhatus DNS-i põhimõistetesse

Algatamise eest vastutavad: infoturbespetsialist

Rakendamise eest vastutab: infoturbespetsialist

DNS (Domain Name System) on võrguteenus, mis teisendab IT-süsteemide hostinimed IP-aadressideks. Teisendus toimub siis, kui selgitatakse välja hostinimega kokkukuuluv IP-aadress. Kui aga selgitatakse välja IP-aadressi juurde kuuluv hostinimi, siis nimetatakse seda tagurpidiseks teisenduseks.

Domeeni nimeruum

DNS on jaotatud andmebaas, mis haldab puukujulise struktuuriga domeeni nimeruumi. Puu koosneb sõlmedest ja lehtedest, mida nimetatakse label 'iteks. Punktidega eraldatud label 'ite ühendamine annab kokku domeeninime. Domeeni nimeruum on jaotatud erinevateks domeenideks. Juure kõige ülemist kihti kujutatakse punktina ja seda nimetatakse root 'iks. Sellele järgnevad tipptaseme domeenid, nt com , edu , de , at ja seejärel teise astme domeenid, nt info. Domeeni nimeruumis salvestatakse infot IP-aadresside ja domeeninimede seoste kohta. DNS-i võib vaadelda kui arvutivõrgu telefoniraamatut, mille põhiülesanne on nimede teisendamine. Näiteks piisab domeeninime www.bsi.bund.de sisestamisest brauserisse, et DNS leiaks domeeni nimeruumist üles sellega kokkukuuluva IP-aadressi. Otsingu tulemusena saab brauser ennast ühendada vastava veebilehega.

Resolver

Klientrakendused vajavad DNS-i kasutamiseks Resolverit. Tihtipeale on Resolver osa operatsioonisüsteemist. Kui klientrakendus vajab nimeteisendust, esitab ta Resolverile päringu. Resolver pakib päringu DNS-iga ühilduvasse pakki, saadab selle DNS-serverile, interpreteerib vastuse ning suunab andmed vastavale rakendusele tagasi. DNS-i jõudluse suurendamiseks salvestab Resolver vastuse andmed teatud ajaks vahemällu. Niikaua kui andmed paiknevad vahemälus ja esineb korduv teisendus, DNS-serverile päringut ei esitata.

DNS-server

DNS-serverid on rakendused, mis haldavad domeeni nimeruumi ühe kindla osa andmeid. Info on salvestatud nn tsoonifailidesse. Kui üks DNS-server haldab mitut domeeni, nt domeeni bund.de ja sinna alla kuuluvat alamdomeeni bsi.bund.de, salvestatakse need eri tsoonidesse. Infot tsooni kohta saab DNS-server ülemfailidest. Ülesannete põhjal võib eristada kahte DNS-serveri põhitüüpi:

- Advertisingu DNS-server,
- Resolvingu DNS-server.

Advertisingu DNS-serverid vastutavad tavaliselt internetist tulevate ja enda domeenide kohta käivate päringute töötlemise eest. Kui päringus soovitud domeeniinfo on neisse juba salvestatud, saadavad nad ise vastuse. Kui info ei ole salvestatud, juhivad nad päringu edasi mõnda teise DNS-serverisse. Advertisingu DNS-serveri põhiülesanne on võimaldada endasse salvestatud domeeniinfot kasutada. Resolvingu DNS-serverid seevastu töötlevad tavaliselt institutsiooni sisevõrgust laekuvaid päringuid. Kui vajalik domeeniinfo on neisse salvestatud, saadavad nad asjakohase vastuse nagu Advertisingu DNS-serverid. Kui ei ole salvestatud, ei saada Resolvingu DNS-serverid päringut teistesse DNS-serveritesse edasi, vaid teevad nimeteisenduse ise. Nimi Resolving vihjabki juba sellele, et sellise DNS-serveri põhiülesanne on Resolver-funktsioon. Neid kahte funktsiooni eristatakse selle mooduli kõigis ohukataloogides ja meetmetes. Terminit „DNS-server" kasutatakse nii Advertisingu kui ka Resolvingu DNS-serveri

kohta käivate üldistavate seletuste ja kirjelduste korral. DNS-servereid, mis kasutavad päringutele vastamiseks enda tsooniinfot, nimetatakse autoriteetseteks serveriteks. Olukorrale, kus DNS-serverile esitatakse päring, mis ei puuduta tema enda tsooni/tsoone ja mille kohta serveril ei ole infot vahemälus, võib DNS-server reageerida kolmel moel:

- Delegeerimine - Delegeerimine tähendab, et osa domeeni nimeruumi infost paigutatakse alamdomeenidesse. Näiteks kui DNS-server saab päringu bund.de kohta, saadab ta selle edasi vastutavale DNS-serverile. Kuna DNS-server peab tundma kõiki delegeeritud tsoonide eest vastutavaid DNS-servereid, võib ta päringu otse neile edasi juhatada.
- Teisendamine juur-nimeserveri kaudu - Kokku on olemas 13 DNS-juurserverit (Root-DNS-Server). Nendel DNS-juurserveritel on salvestatud info selle kohta, millised DNS-serverid on tipptaseme domeenide jaoks autoriteetsed. Kui soovitud andmed paiknevad väljaspool hallatavat domeeni ja andmeid ei ole ka vahemälus, tuleb rakendada rekursiivset teisendust, alustades juur-nimeserverist. Selline tööpõhimõte vastab Resolvingu DNS-serverile.
- Edastamine (forwarding) - Kui DNS-server ei suuda soovitud infot tarnida, saadab ta päringu edasi ühele eelkonfigureeritud DNS-serverile.

Kommunikatsioon

Nagu juba eespool kirjeldatud, kasutavad rakendused DNS-serveritega suhtlemiseks Resolver-liidest, olenemata sellest, kas tegemist on Advertisingu või Resolvingu DNS-serveriga. Resolver saadab nimeteisendust vajavate rakenduste nimel DNS-serverile päringu ja interpreteerib saadud vastust, et see siis rakendusele tagasi saata. Põhimõtteliselt eristatakse kahte liiki päringuid:

- Iteratiivsed päringud: iteratiivne tähendab, et kui DNS-server saab päringu ja ta pole päringuga küsitavaid andmeid ise salvestanud, saadab ta selle päringu edasi järgmisele vastutavale DNS-serverile. Päringu saanud DNS-server on seega Advertisingu DNS-server. Päringut esitav Resolver peab ise tegema kogu nimeteisenduse. www.bsi.bund.de nimeteisendus läbi DNS-juurserveri näeks välja järgmine (DNS-juurserverid vastavad ainult iteratiivsetele päringutele ning on seega Advertisingu DNS-serverid). Esimese sammuna küsib Resolver DNS- juurserverilt Advertisingu DNS-serveri kohta, mis vastutab .de eest. Teise sammuna tuvastab Resolver .de eest vastutava Advertisingu DNS-serveri kaudu DNS-serveri, mis vastutab bund.de eest. Seejärel küsib see bsi.bund.de eest vastutava Advertisingu DNS-serveri kohta. Lõpuks saab bsi.bund.de eest vastutav Advertisingu DNS-server saata Resolverile www.bsi.bund.de IP-aadressi.
- Rekursiivsed päringud: rekursiivse päringu korral on teisendamine umbes samasugune. Erinevus seisneb selles, et kogu eespool kirjeldatud nimeteisenduse võtab enda peale Resolveri eest vastutav DNS-server. Seega on

siin tegemist Resolvingu DNS-serveriga. Klientsüsteemi Resolver peab esitama ainult ühe päringu.

Advertisingu DNS-server aktsepteerib ainult iteratiivseid päringuid, seevastu Resolvingu DNS-server aktsepteerib nii iteratiivseid kui ka rekursiivseid päringuid. Rekursiivsed päringud tähendavad iteratiivsete päringutega võrreldes DNS-serverile suuremat koormust.

Tsooniedastused

Kuna DNS-i vajavad paljud võrgurakendused, tuleb vastavalt spetsifikatsioonile (RFC 1034) iga tsooni jaoks kasutada vähemalt kahte autoriteetset DNS-serverit. Kuna iga DNS-serveri jaoks eraldi kooskõlas olevate ülemfailide (master files) haldamine oleks liiga töömahukas, kasutatakse nende sünkroniseerimiseks tsooniedastust. DNS-serverit, mis hangib domeeniinfo otse ülemfailidest, nimetatakse primaarseks DNS-serveriks või ülem-DNS-serveriks (Primary/Master DNS-Server). Iga järgnevat DNS-serverit nimetatakse sekundaarseks või alluvaks (slave) DNS-serveriks ning see saab oma andmed tsooniedastusel primaarselt DNS-serverilt. Sekundaarne DNS-server kontrollib regulaarselt, kas tema tsooni domeeniinfo on muutunud või ta saab infot muudatuste kohta primaarselt DNS-serverilt. Sel juhul käivitab sekundaarne DNS-server domeeniinfo värskendamiseks tsooniedastuse.

Caching-Only DNS-Server

Caching-Only DNS-Server on Resolvingu DNS-serveri erijuht. Tavaliselt on DNS-server autoriteetne ühe või mitme tsooni jaoks, seda olenemata sellest, kas tegemist on Advertisingu või Resolvingu DNS-serveriga. See tähendab, et ta on selle tsooni kohta käiva domeeniinfo saanud ülemfailist, st ülem-DNS-serverilt tsooniedastusega. Seevastu Caching-Only DNS-serverid ei ole mitte ühegi tsooni jaoks autoriteetsed, nemad ise ei salvesta mitte ühtegi tsooni. Enamasti kasutatakse neid päringute vastuvõtuks ja nimeteisenduseks. Caching-Only DNS-servereid kasutatakse sageli institutsioonisiseste Resolvingu DNS-serverite edasisaatjatena (forwarder 'itena), kui need peavad teisendama internetist pärinevat domeeniinfot.

Turbeaspektid

DNS-i korral on olulise tähtsusega eelkõige terviklus ja käideldavus. Aina tähtsamaks on muutumas aga ka konfidentsiaalsus, vt nt M 2.451 DNS-i kasutamise planeerimine . Enamasti korraldatakse DNS-ile suunatud ründeid eesmärgiga manipuleerida nimeteisendust vajavaid teenuseid.

M 2.451 DNS-i kasutamise planeerimine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: infoturbespetsialist

DNS-serveri turvalise kasutamise üks põhieeldusi on põhjalik planeerimine. Selleks tuleb esmalt välja töötada kontsept, mis peaks muu hulgas sisaldama punkte selle kohta, kuidas DNS üles seada ning milline domeeniinfo vajab kaitset. Planeerimine ei puuduta aga mitte ainult neid valdkondi, mida seostatakse turbega selle klassikalises tähenduses, vaid ka täiesti tavapäraseid igapäevatöös kajastuvaid turbeaspekte. Viiteid DNS-i põhimõttelise struktuuri kohta leiate meetmest M 2.450w Sissejuhatus DNS-i põhimõistetesse .

Riistvara valimine

Riistvaral, milles DNS-serverit käitada soovitakse, on suur mõju loodava süsteemi koguvõimsusele. Seejuures mängib rolli, kui mitut päringut peab DNS-server keskmiselt töötlema, kas tegemist on Resolvingu DNS-serveriga, mis aktsepteerib rekursiivseid päringuid, või Advertisingu DNS-serveriga, mis aktsepteerib ainult iteratiivseid päringuid, ning kas DNSSEC-d (DNS Security Extensions) plaanitakse kasutada või mitte. DNS-serveri jaoks on oluline piisav põhimälu, et vältida olukordi, kus server paigutab salvestatavad andmed kõvakettale, sest see pikendab serverilt saadavate vastuste laekumise aega. DNSSEC kasutamisel tuleb jälgida, et krüptograafiliste operatsioonide korral sobiva andmetöötluskiiruse säilitamiseks valitaks suurema kiirusega protsessor. Planeerimisel välja valitud põhimälu ja protsessori jõudlusnäitajad tuleb üle kontrollida käituskatses, sest tegelikku jõudlust saab täpselt välja selgitada alles jooksvas kasutuses.

Domeeniinfo nähtavus

DNS-server haldab oma autoriteetse tsooni infot. Osa infost on mõeldud avalikkusele, nt veebi- või meiliserveri IP-aadress. Osa domeeniinfost puudutab aga institutsioonivõrgu sisemist struktuuri. See info võib anda aimu võrgukomponentide funktsiooni ja asukoha kohta. Seega tuleks Advertisingu ja Resolvingu DNS-serveri eristamise abil domeeniinfo nähtavust piirata, nagu on kirjeldatud jaotises „Eraldiseisvad DNS-serverid". IT-koosluse nimeruum tuleks jagada avalikuks ja institutsioonisiseseks alaks. Avalik ala peaks sisaldama ainult sellist domeeniinfot (tavaliselt IP-aadressi ja hosti nime), mis tagaks väljastpoolt ligipääsetavate teenuste tõrgeteta töö.

Tavaliselt on need järgmised:

- veebiserver,
- meiliserver,
- DNS-server,
- VPN-i ühenduspunktid.

Asutuse sees ei ole nähtavust enamasti vaja piirata. Mis domeeniinfo on väljapoole nähtav ja mis mitte, tuleb kindlaks määrata DNS-i kasutamise planeerimisel.

Eraldiseisvad DNS-serverid

DNS-servereid on võimalik eristada nende ülesannete alusel. Põhimõtteliselt on neid kahte tüüpi:

- Advertisingu DNS-server,
- Resolvingu DNS-server.

Advertisingu DNS-serverid vastutavad tavaliselt internetist tulevate päringute töötlemise eest. Resolvingu DNS-serverid töötlevad seevastu sisevõrgust laekuvaid päringuid. Kuna tegemist on kahe erineva ülesandega, siis tuleks need serverid ka üksteisest lahutada. Nii Advertisingu kui ka Resolvingu DNS-serverite jaoks on soovitatav sisse seada eraldi füüsilised serverid. Advertisingu DNS-server haldab ainult väljast kättesaadavat domeeniinfot ja toetab ainult iteratiivseid päringuid, Resolvingu DNS-server haldab siseringile nähtavat infot ja toetab nii iteratiivseid kui ka rekursiivseid päringuid. Kui Advertisingu ja Resolvingu DNS-serveri eristamine on liiga mahukas ettevõtmine või ei ole erinevatel tehnilistel põhjustel eraldi serverite sisseseadmine võimalik, võib kasutada ka lihtsamat konfiguratsiooni. BIND DNS-server võimaldab näiteks domeeniinfole määrata erinevad kihid (views). Nõnda saab DNS-server hallata sisevõrgust laekuvate päringute jaoks eraldi päringute kihti (view 'd), millesse on salvestatud kogu IT-koosluse domeeniinfo. See on Resolvingu DNS-server. Teine päringute kiht (view), mille lähtekohaks on internet, saab omale ainult selle osa domeeniinfost, mis kinnitati klassifitseerimisel avalikult ligipääsetavaks infoks. See on Advertisingu DNS-server. Selline disain pakub nõrgemat turvet kui kaks eraldiseisvat DNS-serverit ning see, kas suurem risk on vastuvõetav, tuleb iga juhtumi korral eraldi läbi mõelda.

DNS-serveri paigaldamine võrgustruktuuri

DNS-serveri paigutus võrgus sõltub organisatsiooni võrgutaristust. On olemas mõningad põhireeglid, millest tuleb kinni pidada:

- Primaarne ja sekundaarne DNS-server tuleb paigutada erinevatesse IPalamvõrkudesse. Lisaks ei tohi neid ühendada sama võrguühenduselemendi külge. Sellise lahenduse korral ei mõjuta IP-alamvõrgu ega võrguühenduselemendi rivist väljalangemine nimeteisenduse käideldavust, vt G 1.2 IT-süsteemi avarii.
- Advertisingu DNS-server tuleks paigutada demilitariseeritud tsooni (DMZ) (vt B 3.301 Turvalüüs (tulemüür)).
- Resolvingu DNS-serverid vastutavad institutsioonisiseste IT-süsteemide päringute eest. Pikkade vastuse laekumise aegade ja liigse võrgukoormuse vältimiseks tuleks need seetõttu paigutada institutsiooni usaldusväärse võrgu sees võimalikult lähedale päringuid esitavatele IT-süsteemidele.

Peale selle ei tohi Resolvingu DNS-serverid olla kättesaadavad välistele IT-süsteemidele.

- Kui info nähtavust piiratakse, peaks Advertisingu DNS-server domeeniinfo avalikult ligipääsetavat osa haldama demilitariseeritud tsoonis (DMZ).
- Kui siseste nimeserverite puhul kasutatakse interneti domeeninimeruumi teisendamiseks edasisaatjat (forwarder), ei tohiks seda paigutada sisevõrku.
- Kui firmasisesesse võrku paigaldatakse Caching-Only DNS-serverid, tuleks klientsüsteemide Resolverites keelustada domeeniinfo vahesalvestamine. Vahesalvestamise võtab enda kanda Caching-Only DNS-server. Keskse mälu abil minimeeritakse päringute arv. Lisaks on vahemälu mürgitamise

eduka ründe korral võimalik kustutada Caching-Only DNS-serveri vahemälu ja sellega ka võltsitud andmed.
- IT-kooslustes on turvalüüside kasutamine tänapäeval standardiks. DNSvõrguliikluse aktsepteerimiseks tuleb turvalüüsides ja pakettfiltrites sisse seada asjakohased reeglid, vt M 4.98 Side piiramine miinimumini paketifiltritega ja M 5.118z DNS-serveri integreerimine turvalüüsi koostisse .
- Planeerimisel tuleks tähelepanu pöörata sellele, et avataks võimalikult vähe marsruute ja porte.

Näite selle kohta, kuidas paigaldada DNS-server võrku koos turvalüüside ja paketifiltritega, leiate meetmest M 5.118z DNS-serveri integreerimine turvalüüsi koostisse.

Resolver

Resolverid on levinud operatsioonisüsteemide standardsed koostisosad juba algusest peale ja neid ei ole vaja eraldi välja valida ega hankida. Siiski tuleks tagada, et siseste IT-süsteemide Resolverid kasutaksid nimeteisenduseks Resolvingu DNS-servereid. Kindlasti ei tohiks nad esitada standardseid päringuid välistele DNS-serveritele. Lisaks tuleks seejuures kindlaks määrata Resolverite poolt kasutatavad DNS-sufiksid, nt bsi.bund.de. Sellega muudetakse hostx 'i nimeteisendusel domeeninime ülejäänud osa automaatselt FQDN-nimeks (Fully Qualified Domain Name) hostx.bsi.bund.de.

Domeeninimede haldus

Planeerimise käigus tuleb kindlaks määrata isik, kes vastutab interneti domeeninimede halduse eest. Vastutav isik peab tagama meetme M 2.298z Interneti domeeninimede haldus .

Kontrollküsimused:

- kas institutsioonisiseste ja -väliste IT-süsteemide päringute jaoks on sisse seatud eraldi DNS-serverid?
- kas domeeniinfo nähtavust on piiratud?
- kas on olemas plaan DNS-serveri paigutamiseks IT-koosluse võrku?
- kas siseste hostide Resolverid kasutavad nimeteisenduseks Resolvingu DNS-serverit?
- kas interneti domeeninimede haldamise jaoks on määratud vastutav isik?
- kas DNS-serverite riistvara on piisava jõudlusega?

M 2.452 Sobiva DNS-serveritoote valimine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator, infoturbespetsialist

Uute DNS-serveritoodete soetamisel on võimalik valida sellised tooted, mille käitamise turvalisus on suur ning personalikulu, samuti tehniline ja organisatoorne kulu võimalikult väike. Lisaks pakuvad erinevad DNS-serveritooted erinevaid funktsioone ja erinevat kasutusmugavust. Soetamisel tuleks arvestada järgmiste aspektidega:

- DNS-serveritoode peab olema end praktikas juba tõestanud.
- Kui valitavate toodete hulgas leidub mõni selline, mille jaoks on olemas piisaval hulgal koolitatud personali ja mis täidab kõik funktsionaalsusega seotud nõuded, tuleks kasutada just seda DNS-serveritoodet.
- On olemas DNS-serveritooteid, mille juurutamine ei ühti DNS-i standarditega (RFC 1034, 1035 jne). Eriti just siis, kui tarkvara „monokultuure" tahetakse vältida ja plaanitakse kasutada erinevaid DNS-serveritooteid, tuleks valik teha alles pärast ühilduvuse kontrollimist.
- DNSSEC kasutamise puhul tuleb jälgida, et DNS-serveritoode toetaks seda tehnoloogiat.

Tsooniinfo süntaksi kontrollimine

DNS-serveritooted abistavad administraatorit süntaktiliselt õigete tsoonifailide koostamisel erineval määral. DNS-serveritoote soetamisel tuleb otsustada, kuidas peaks olema korraldatud ülemfailide (master files) kontrollimine. Kui ülemfaile toimetatakse käsitsi, võib tööd lihtsustada mõni tsooniinfot kontrolliv tarkvaralahendus. Selleks võib näiteks BIND DNS-serveri puhul kasutada tööriista Named-Checkzone. Kui tsooniinfo töötlemiseks kasutatakse graafilist kasutajaliidest, tuleb näiteks nelja silma põhimõtte abil tagada, et sisestatud info võetaks kasutusele süntaktiliselt korrektse tsooniinfona.

Täiendavad kontrollküsimused:

- kas väljavalitud DNS-serveritoote jaoks on olemas piisav hulk koolitatud personali?
- kui palju aitab DNS-serveritoode administraatorit süntaktiliselt õigete ülemfailide koostamisel?

M 2.453 DNS-serverite kasutusest kõrvaldamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

Kui DNS-serverit ei taheta näiteks domeenist loobumise tõttu enam kasutada, tuleb kasutusest kõrvaldamisel arvestada teatud punktidega. Kasutusest kõrvaldamise plaan peab muu hulgas takistama sellise olukorra teket, kus domeeni nimeruumi jäävad alles viited DNS-serverile, mida seal enam pole.

Andmete kustutamine/ andmekandjate utiliseerimine

Kõikide hõlmatud arvutite andmed tuleb enne arvutite taaskasutusse võtmist turvalisel moel kustutada (vt M 2.167 Andmete kustutamine või hävitamine). Ka riistvara utiliseerimise puhul tuleb tagada, et see vastaks kõikidele turvanõuetele (vt M 2.13 Tundlike ressursside jäljetu hävitamine).

DNS-serveri kustutamine domeeni nimeruumist

Kui DNS-server pole ülemdomeenis registreeritud, pole edasised sammud vajalikud. Kui DNS-server on ülemdomeenis registreeritud, tuleb kasutusest kõrvaldamisest teatada ülemdomeeni administraatoritele, et nad kustutaksid ülemdomeenist ära kõik kasutusest kõrvaldatud DNS-serveri tsoonisissekanded.

Süsteemi kustutamine võrgukooslusest

Kustutada tuleb kõik võrgu- ja operatsioonisüsteemi tasandi viited. Kui kasutusest kõrvaldatud server on institutsiooni sisesüsteemidesse kantud standardse DNS-serverina, tuleb need sissekanded kustutada. Samuti tuleb kustutada tsooniedastused, mis on konfigureeritud kasutusest kõrvaldatud DNS-serveri ja veel alles jäävate DNS-serverite vahel.

Täiendavad kontrollküsimused:

- kas DNS-serveri kõvakettad on turvaliselt kustutatud?
- kas DNS-serveri riistvara utiliseeriti nõuetekohaselt?
- kas registreeritud DNS-serveri puhul registreering kustutati?
- kas kõik kasutusest kõrvaldatud DNS-serverile viitavad konfiguratsioonid on klientsüsteemidest eemaldatud?

M 2.454 Rühmatarkvarasüsteemide turvalise kasutamise planeerimine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator, infoturbespetsialist

Enne rühmatarkvarasüsteemi juurutamist tuleb otsustada, millisel otstarbel süsteemi kasutama hakatakse ja millise info jaoks see mõeldud on. Kasutusviisist sõltub, millist riist- ja tarkvara tuleb soetada. Samuti määrab kasutusviis kindlaks planeerimistöö tüübi ja mahu. Ka väljatöötatav infoturbepoliitika sõltub üsna olulisel määral planeeritud rakendusstsenaariumist.

Rühmatarkvarasüsteemide puhul saab eristada järgmiseid rakendusviise:

- Kasutamine intranetiserverina ja rühmatarkvaraklientide kaudu juurdepääsuks: selle stsenaariumi puhul peetakse peamiselt silmas sisesüsteemina ja kontorisiseseks suhtluseks (e-post, tähtaegade kooskõlastamine, rühmatöö koordineerimine) kasutamist.
- Kasutamine intranetiserverina ja veebiklientide kaudu juurdepääsuks: selle stsenaariumi puhul pääsetakse rühmatarkvaraserverile ligi brauseri kaudu. Kuna rühmatarkvaraserveri veebiliidese puhul kasutatakse täiesti teistsuguseid turvamehhanisme, vaadeldakse veebiliidese turvalist konfigureerimist omaette stsenaariumina.
- Kasutamine DMZ-na (demilitariseeritud tsoonina) ehk perimeetervõrguna: rühmatarkvaraserverit saab DMZ-i raames kasutada ka avalikult ligipääsetava infoserverina. Sellise kasutusviisi puhul nõuab süsteemi konfigureerimine serveri kerge ligipääsetavuse tõttu erilist tähelepanu.
- Kasutamine väliste teenusepakkujate rühmatarkvararakenduste puhul (näiteks pilvandmetöötlus): sel puhul pöördutakse väliste teenusepakkujate pakutavate rühmatarkvararakenduste poole. Turvalisuse aspektist lähtuvalt tuleb sel puhul pöörata erilist tähelepanu kolmanda osapoole salvestatud andmete konfidentsiaalsusele ning teenuse kättesaadavusele.

Nende üksikstsenaariumide sees võib veel täpsemalt eristada, milliseid rühmatarkvara funktsioone kasutada tahetakse. Põhimõtteliselt tuleb funktsioonide kasutamist turvaaspekte silmas pidades eraldi planeerida. Rühmatarkvarasüsteemide kasutusotstarbest olenevalt erinevad ka nõuded ülekantavate andmete konfidentsiaalsusele, käideldavusele, terviklikkusele ja siduvusele.

Põhimõtteliselt tuleb rühmatarkvara ressursside planeerimisel silmas pidada järgmiseid aspekte:

- Tuleb välja selgitada, millist infot millist teed kaudu rühmatarkvarasüsteemi kaudu edastatakse ning milline on selle info ja sellega seotud äriprotsesside kaitsevajadus.
- Tuleb kindlaks määrata, milliseid rühmatarkvarakomponente ja -teenuseid kasutatakse ning milliste pääsuõigustega millised kasutajad (rollid) neid kasutama hakkavad.

- Rühmatarkvara kasutuskontseptsiooni puhul tuleb samuti kindlaks määrata, millised krüptograafilised turvamehhanismid eelkõige meilide puhul kasutusele võetakse (vt M 5.108z Rühmatarkvara või meilisüsteemi krüptograafiline kaitse).
- Võõrastes võrkudes suhtlemise võimaldamiseks tuleb planeerida, kuidas kasutada kergesti ligipääsetavaid servereid. Need serverid peavad paiknema demilitariseeritud tsoonis või vähemalt turvalüüsi taga (vt B 3.301 Turvalüüs (tulemüür)).

Planeerimisel tuleb samuti kindlaks määrata, kuidas tagada ettenähtud failiedastus organisatoorsete eeskirjade või tehniliste rakenduste abil.

Siia kuuluvad näiteks järgmised punktid:

- Administraator peab rühmatarkvarakliendid konfigureerima nii, et kasutaja oleks ilma lisatoiminguteta maksimaalselt turvatud (vt M 5.57 Rühmatarkvara/meiliklientide turvaline konfiguratsioon).
- Andmeedastus tohib olla võimalik alles pärast seda, kui saatja on ülekandesüsteemis edukalt tuvastatud ja autenditud.
- Kasutajaid tuleb enne rühmatarkvarasüsteemide kasutuselevõttu vastavate rakenduste kasutamise suhtes koolitada. Neile tuleb tutvustada asutuse andmevahetuseeskirju.

Põhimõtteliselt ei tohi siseaadressile saadetavaid sõnumeid väliste radade või aadresside kaudu edastada. Eranditest tuleb kõiki töötajaid teavitada. Näiteks võib välisteenistuse töötajate või lihtsalt palju reisivate töötajate jaoks edastada e-kirju välistesse juurdepääsupunktidesse. Rühmatarkvararakenduste ja eelkõige meilide ülekandmine ühe asutuse erinevate asukohtade vahel peab toimuma turvaliste kanalite, nt VPN-i või oma püsiliini kaudu.

Rühmatarkvara turvalise kasutuse kontseptsiooni väljatöötamisel tuleb silmas pidada veel järgmisi punkte:

- Rühmatarkvarasuhtluse puhul tuleb aktiivsisu käitlemist pidevalt planeerida. Kõiki eeliseid ja puudusi kaaludes tuleb kindlaks määrata kogu organisatsioonis kehtivad ühtsed toimimisviisid.
- Tuleb otsustada, kas eemalviibimisteateid („kontorist väljas” -teated) kasutada või mitte, sest nende tõttu võib isikuinfot asutusest väljapoole sattuda.
- Tuleb kaaluda meilifiltrimehhanismide kasutamist rämpsposti (soovimatute reklaammeilide) tõrjumiseks.
- Kalendrifunktsiooni ja ülesannete nimekirja kasutamise puhul tuleb kindlaks määrata, kes ja milliste pääsuõigustega neile juurde võib pääseda. See on eelkõige oluline siis, kui koostööd tehakse asutuse teiste üksustega.
- Planeerimise puhul tuleb arvesse võtta, kas kasutajad kasutavad ühist arvutit. Sellele vastavalt tuleb nendel arvutitel profiilid määrata ja neid turvata.
- Kui asutuses kasutatakse vestlus-, kiirsõnumivahetus-, audio või videokonverentsiteenuseid, tuleb välja töötada nende kasutamiskontseptsioon.

Rühmatarkvara puhul rakendatakse väliste teenusepakkujate (näiteks meiliteenuse pakkujate) kasutamisel moodulis B 1.11 Väljasttellimine (Outsourcing) kirjeldatud turvasoovitusi. Eelkõige tuleb välja selgitada, milliseid turvameetmeid teenusepakkujad kasutavad (vt M 2.123z Rühmatarkvara või meiliteenuse pakkuja valimine). Ikka ja jälle vaieldakse selle üle, kas ja mil määral võib teenistuslikke rühmatarkvararakendusi, eelkõige meili, kasutada isiklikuks otstarbeks. Mõistlikes piirides toetatakse seda paljudes asutustes, kuna see motiveerib töötajaid. Üldiselt soovitatakse aga rühmatarkvara eeskirjade puhul kokku leppida, milliseid reegleid rühmatarkvara kasutamise puhul nii üldiselt kui eraviisiliselt meili ja muude rühmatarkvarateenuste kasutamisel järgida. Rühmatarkvarasüsteemide kasutamise puhul tuleb asutustes ühtlasi kindlaks määrata, milliseid rühmatarkvararakendusi kasutajad kasutada tohivad. Lisaks mitmesugustele teenustele, mida asutuses kasutatavad rühmatarkvarasüsteemid pakuvad, võivad nad pääseda ligi ka teistele tööarvuti kaudu kasutatavatele rühmatarkvararakendustele nagu veebimeil või internetikalender. Tuleb selgelt kindlaks määrata, milliste sisemiste või väliste rühmatarkvararakenduste kasutamine on töötajatele lubatud. Selle otsuse rakendamist kirjeldatakse allpool veebimeili näitel. Põhimõtteliselt tuleb lähtuda sellest, et töötajad tohivad kasutada ainult asutuses lubatud programme ja välisteenuseid.

Veebimeili all mõeldakse pakkumisi, mille puhul pääseb brauseri abil ligi veebipõhistele meiliteenustele. Mitmesugused meiliteenuse pakkujad pakuvad vastavaid lisaprogramme kas juba tootesse integreeritult või lisamoodulitena. Veebimeili eeliseks on see, et postkastile pääseb juurde igast internetiühendusega arvutist üle kogu maailma ilma vajaduseta investeerida infrastruktuuri. Samas on aga näiteks viirusetõrje või krüpteerimise puhul asutuse infoturbepoliitikat keerulisem järgida kui sisemises meiliserveris. Peale selle on konfidentsiaalsete meilide lugemise või paroolide teadasaamise oht veebimeili puhul märksa kõrgem.

Asutuse või ettevõtte võrgust veebimeili kasutamise puhul tuleb tingimata mõelda kahjurvaratõrjele. Praeguste viirusehoiatuste puhul võib veidi aega minna, enne kui viirustõrjeuuendused kõigi klientideni jõuavad. Sel juhul võiks takistada juurdepääsu veebimeilile vähemalt seni, kuni vastutajad on veendunud piisava kaitse olemasolus. Veebimeili kasutamise kohta tuleb asutuses või ettevõttes kehtestada eeskirjad. Selleks on mitmeid variante:

- Asutused võivad otsustada veebimeili kasutamise üldse ära keelata. Sellest tuleb muidugi töötajatele teada anda. Keeldu võib lisaks tehniliselt toetada teadaoleva teenusepakkuja filtreerimisega , kuid samas tuleb endale aru anda, et kasutajad leiavad alati uusi viise, kuidas sellistele teenustele juurde pääseda.
- Võib anda soovituse kasutada veebimeili sisevõrgust saadetavate erameilide puhul. Sellega välditakse olukorda, kus keelust hoolimata kasutatakse ametimeili isiklikel eesmärkidel (mis võib juhtuda näiteks kiirustamise või lihtsalt praktilisuse tõttu).

- Samuti on asutusi, kus veebimeili kasutamine on tööga seotud meilivahetuse jaoks väga erinevatel põhjustel ametlikult lubatud. Nii on terve hulk väiksemaid asutusi, millel pole oma meiliserverit ja mis kasutavad välissuhtluseks veebimeili. Samuti võib veebimeil olla praktiline lahendus, mille abil lugeda meile komandeeringus viibides, kui ligipääs kaugpöörduse abil pole lubatud. Veel üks põhjus veebimeili kasutamiseks võib peituda selles, et asutus ei soovi teatud meilide väljapoole sattumist. Samuti võib olla, et veebimeili aadress tuleb sisestada saitidele, kust on oodata rämpsposti, st teatud allalaadimiste, uudisgruppide jms puhul. Veebimeili kasutamise puhul tuleb järgida peatükis M 5.96 Veebmeili turvaline kasutamine .

Kontrollküsimused:

- Kas rühmatarkvarasüsteemide turvaliseks kasutamiseks on olemas pidepunktid?
- Kas on kindlaks määratud, millist liiki infot tohib kaitsevajadust silmas pidades milliste raamtingimuste puhul rühmatarkvarateenuste kaudu edastada?
- Kas on olemas eeskirjad rühmatarkvarateenuste isiklikel eesmärkidel kasutamise kohta?
- Kas on olemas eeskirjad veebimeili kaudu suhtlemise kohta?

M 2.455 Infoturbepoliitika kehtestamine rühmatarkvara jaoks

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: administraator, infoturbespetsialist

Nagu iga asutuses või ettevõttes kasutuseloleva klient-server-süsteemi puhul tuleb ka rühmatarkvaraserverite ja -klientide puhul välja töötada sobiv turvajuhend, mis kirjeldaks rühmatarkvara administraatoritele ja kasutajatele mõeldud reegleid:

- Rühmatarkvarasüsteemide jaoks välja töötatud turvajuhend peab olema kooskõlas asutuse või ettevõtte üldise turvajuhendiga.
- Tuleb otsustada, millal vajatakse näiteks võrgu- või meiliühenduse (näiteks interneti teel juurdepääsu) puhul kommunikatsiooniturvet ja kindlaks määrata vastavad mehhanismid.
- Turvajuhendit tuleb kõigile otseselt või kaudselt asjassepuutuvatele töötajatele tutvustada. Kõige parem on tutvustada juhendit asutusesisese koolituse käigus. Turvajuhendit tuleb regulaarselt uuendada ja sellest vastavaid isikuid tuleb siis ka teavitada.

Arusaadavuse huvides on mõttekas jaotada rühmatarkvaraeeskirjad kasutajale ja administraatoritele mõelduteks. Rühmatarkvara kasutajale mõeldud turvajuhendis tuleb näiteks kindlaks määrata:

- millised kasutajad millistele rühmatarkvaraserveritele juurde pääsevad või mitte (välistusnimekiri),
- milliste õigustega milline kasutaja millisele rühmatarkvaraandmebaasile juurde pääseb,
- millist infot millisele suhtluspartnerile edastada tohib,
- kuidas edastatud infot (sõltuvalt kaitsevajadusest) turvata , eelkõige reguleerides, millal tuleb ülekantavaid faile krüpteerida või digiallkirjastada.

Administraatoritele mõeldud rühmatarkvara turvajuhend peab muuhulgas reguleerima:

- kuidas peavad administraatorid rühmatarkvara komponente adekvaatse turbe saavutamiseks konfigureerima,
- millised teised serverid rühmatarkvaraserverile juurde tohivad pääseda,
- kust rühmatarkvaraserverile juurde tohib pääseda.

Näiteks Microsoft Exchange'i puhul tuleks rühmatarkvara turvajuhendis kindlaks määrata, millised kasutajad milliste õigustega millistele Exchange'i objektidele juurde tohivad pääseda. Kuna Microsoft Exchange'i süsteemid on väga tugevasti Windowsi keskkonda integreeritud, eriti Active Directory puhul, tuleb järgida Windowsi turvajuhendit.

Täiendavad kontrollküsimused:

- Kas rühmatarkvarasüsteemide kohta on olemas kehtiv turvajuhend?
- Kas kõiki kasutajaid teavitatakse rühmatarkvarasüsteemide uutest või muudetud turvameetmetest?

M 2.456 Rühmatarkvarasüsteemide turvaline haldamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator, IT-juht

Rühmatarkvarasüsteemide haldamine nõuab hoolikat planeerimist. Selle juures tuleb tähelepanu pöörata administratiivsete ülesannete ja vastavate administ raatorikontode piisavale lahushoidmisele. Rühmatarkvarasüsteemide haldamisel tuleb silmas pidada allpool kirjeldatud turvalisusaspekte.

Administraatorite määramine

Rühmatarkvarasüsteemide sujuvaks toimimiseks tuleb määrata ja välja koolitada administ raatorid . Meiliteenuste administraatoreid kutsutakse ka *postmaster*iteks. Nende ülesannete hulka kuuluvad:

- kohalikul tasandil rühmatarkvarateenuste pakkumine,
- rühmatarkvarasüsteemide kaitse kuritarvituste eest,
- kontrollimine, kas välised suhtluskanalid toimivad,
- rühmatarkvaraprobleemide puhul kontaktpunktina toimimine nii lõpp kasutajate kui lüüsiteenuste pakkujate jaoks.

Nende ülesannete realiseerimiseks seatakse sisse postkastid *postmaster@ ja abuse@*, mis tuleb sisse seada ka kõigi meililiikluses osalevate alamdomeenide jaoks. Kõik veateated saab aadressil *postmaster@* edastada administraatoritele, kes peavad vea allika kõrvaldama. Samuti peavad administraatorid hooldatavate IT-komponentide logides vigade esinemist ennetavalt kontrollima ja need kõrvaldama. Meiliteenuste kuritarvitusest teatatakse administraatoritele tavaliselt aadressil *abuse@*. Kui sellesse postkasti saabub kaebusi välistelt meilikasutajatelt, näiteks võrgust rämpsposti saatmise kohta, tuleb neid operatiivselt kontrollida ja kaebuste põhjused kõrvaldada. Vastasel korral riskitakse sellega, et meiliteenuse funktsionaalsus võib näiteks musta nimekirja sattumise tõttu kannatada saada. Peale selle tuleb vastavalt organisatsiooni struktuurile ja suurusele määrata üks või mitu isikut, kes vastutaksid pakutavate suhtlusteenuste hooldamise eest . Lisaks serveri käigushoidmisele tuleb teenindada ka kasutaja määratud suhtluskliente. Kõik teenindajad või nende esindajad peavad kasutajatele telefonitsi ja meilitsi pidevalt kättesaadavad olema.

Pääsuõigused

Pääsuõiguste andmisel tuleb lähtuda järgmistest põhimõtetest (vt M 4.355 Kasutajahaldus rühmatarkvarasüsteemide puhul):

- Pääsuõiguste struktuur peab olema selge. Kõik administratiivsed ülesanded ja pääsuõigused tuleb piisavalt dokumenteerida.
- Ulatuslike pääsuõiguste tõttu tuleb eriti hästi kaitsta administratiivset juurdepääsu rühmatarkvarasüsteemidele, eraldades ainult õigusi, mis on administratiivse tegevuse jaoks tingimata vajalikud.

- Administratiivsed ülesanded tuleb hoolikalt ära jaotada ning vastavatele isikutele dokumenteeritult üle anda. Tuleb kontrollida,kas rühmatarkvarasüsteemide puhul saab ülesannete jaotamise toetamiseks ära kasutada kasutusel olevaid administraatorirolle.
- Tavaliselt määratakse rühmatarkvarasüsteemi esimesel installeerimisel üldadminist raator, kellel on juurdepääs kõigile rühmatarkvara komponentidele ja andmebaasiobjektidele. See tuleb alginstallatsiooni käigus ära muuta. Pääsuõigusi tuleb jaotada varem kindlaks määratud administratiivse mudeli põhjal.

Rühmatarkvarasüsteemi piisav dimensioneerimine

Rühmatarkvaraserverite käsutuses peab olema piisavalt mäluruumi ja võimsust. Kolm peamist tegurit, millele tähelepanu pöörata, on protsessori, mälumahu ja andmekandjate valik. Rühmatarkvarasüsteemi piisavat dimensioneeritust tuleb regulaarselt kontrollida.

Rühmatarkvara dokumentatsiooni kasutamine

Tarkvaratootjate käsutuses on tavaliselt hulgaliselt dokumente ja infot, sh palju võrgudokumentatsiooni. Administraatoritele peab teada olema eelkõige turvalisust puudutav dokumentatsioon, samuti peavad nad sellele juurde pääsema. Eriti võrgudokumentatsiooni puhul tuleb regulaarselt kontrollida, kas on saadaval uusi versioone ja turbejuhiseid .

Rühmatarkvaraserverite turvaline konfigureerimine

Rühmatarkvaralahenduse installeerimise järel tuleb nii tarkvara kui ka serverija kliendikomponendid turvaliselt konfigureerida. Enne, kui administraator pärast rühmatarkvara edukat installeerimist konfigureerimisega jätkab, tuleb rakendada üldisi administreerimissoovitusi. Rühmatarkvara konfigureerimise puhul tuleb eelkõige silmas pidada:

- vajalikul määral pääsuõiguste piiramist,
- rühmatarkvaraliideste ja teiste komponentide turvalist konfigureerimist,
- suhtluslogi turvalist konfigureerimist ja adekvaatse logimise sisseseadmist.

Rühmatarkvara klientide turvaline konfigureerimine

Pärast seda, kui rühmatarkvarakliendid on asutuse sees installeeritud või jaotatud, tuleb klienditarkvara vastavalt konfigureerida, et tagada rühmatarkvarakeskkonna turvaline kasutus meetme M 5.57 Rühmatarkvara/meiliklientide turvaline konfiguratsioon alusel.

Rühmatarkvarasüsteemide puhul andmebaasi turvaline konfigureerimine

Rühmatarkvarasüsteemid kasutavad kogu olulise info püsivaks salvestamiseks tavaliselt andmebaasi. Kui andmebaasi ja rühmatarkvara süsteemikomponendid ei ole installeeritud samale arvutile, suhtlevad rühmatarkvarasüsteem ja andmebaas kohtvõrgu kaudu ülekantavate päringute abil. Seetõttu peab juurdepääs andmebaasile olema võimalikult hästi kaitstud. Sellise andmebaasi puhul on tegemist kriitilise komponendiga, mida tuleb tingimata volitamata juurdepääsu eest kaitsta. Andmebaas peab olema turvaliselt installeeritud ja seda peab turvaliselt kasutama. Selleks rakendatakse moodulis B 5.7 Andmebaasid esitatud soovitusi.

Täiendavad kontrollküsimused:

- Kas administraatori ülesanded ja talle antud õigused on piisavalt dokumenteeritud?
- Kas rühmatarkvarakomponendid on pärast installeerimist turvaliselt konfigureeritud?

M 2.457 Interneti turvalise kasutamise kontseptsioon

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: infoturbespetsialist, IT-juht

Peaaegu iga asutus kasutab tänapäeval internetti. Kuigi internetil on palju eeliseid, sageneb üha enam ka selliste teadete arv, mis kajastavad interneti kasutamisega seotud ohtusid. Ohtude minimeerimiseks tuleks igat uut interneti rakendamise varianti enne kasutuselevõttu hoolikalt planeerida ja hoolitseda selle eest, et kõikide IT-komponentide installimine, võrkuühendamine ja konfigureerimine toimuks turvaliselt. Interneti turvalise kasutamise kontseptsioon peaks esmalt selgitama, milliseid internetiteenuseid tohivad töötajad kasutada, milliseid reegleid tuleb sealjuures järgida ja kuidas tuleb kaitsta organisatsioonisiseseid IT-süsteeme. See kontseptsioon tuleb juurutada organisatsiooni üldisesse IT-turbestrateegiasse ning seetõttu tuleb see kooskõlastada infoturbeosakonnaga.

Planeerimine

Tuleb kindlaks määrata, millised internetiga seotud andmeside liigid on lubatud (vt M 2.459 Internetiteenuste ülevaade). Selleks on vaja välja selgitada, mis eesmärkidel soovitakse internetti kasutada. Institutsioonile tuleb välja valida sobivad ja vajalikud internetiteenused. Need võivad suuresti erineda. Näiteks võib organisatsioon otsustada, et juurdepääs internetile antakse ainult väga vähestele töötajatele, piirates omakorda ka nende kasutusvõimalusi, samuti võib ta otsustada, et igal töökohal on võimalik kasutada kõiki saadaolevaid internetirakendusi. Turbevaldkonnaga tuleb arvestada juba väga varajases planeerimisfaasis, et loodav arhitektuur saaks võimalikult turvaline. Juhtudel, kus teatud valdkondade jaoks soovitakse interneti kasutamine ära keelata või lubada seda ainult piirangutega, oleks mõistlik selleks otstarbeks sisse seada eraldiseisvad internetiarvutid (vt B 3.208 Interneti-PC). Interneti kasutamise turbestrateegia peab andma vastused järgmistele küsimustele:

- kes saavad juurdepääsu internetile?
- millised on interneti kasutamise tingimused, st mis otstarbel tohib internetti kasutada?
- mis teenuseid tohib internetis kasutada?
- mis andmeid tohib ja mida ei tohi internetis edastada?
- kas kasutajaid on tarvis koolitada? Kui jah, kuidas peaksid need koolitused välja nägema?
- kuidas tagatakse kasutajatele tehniline tugi?

Iga internetiteenuse kasutamine peab olema reguleeritud ning iga kasutajagrupi ja/või IT-süsteemide grupi kohta peab olema selge, milliseid turbetingimusi need peavad järgima. Kasutusse tuleks lubada ainult sellised teenused, mis on tööülesannete täitmiseks tõepoolest hädavajalikud. Teenuseid, mille kasutusõigusi ei ole konkreetselt kindlaks määratud, ei tohi kasutada enne, kui kehtestatakse vastavad reeglid või kohandatakse olemasolevaid. Siia alla kuuluvad näiteks turbekontseptsioon ja kasutajatele mõeldud kasutussuunised. Lisaks tuleb kindlaks määrata interneti eraotstarbelise kasutamise kord. Erinevate internetiteenuste kasutamise kohta vastu võetud otsused tuleks, samamoodi nagu otsuste langetamise põhjendused, selgelt kirja panna.

Ajakohasus

Interneti kasutamise kontseptsiooni tuleb regulaarselt, st vähemalt kord aastas, ajakohastada, sest see valdkond areneb väga kiiresti. Interneti kasutamise kontseptsiooni tuleks ajakohastada koos internetiühenduse loomise kontseptsiooniga, sest nende mõlema valdkonna turve on tihedalt seotud. Organisatsiooni eesmärkide, strateegiate ja ohuastme muutumisel tuleb kontrollida, millised on nende mõjud interneti kasutamise kontseptsioonile.

Täiendavad kontrollküsimused:

- kas interneti kasutamise kohta on olemas ajakohane kontseptsioon?
- kas seda kontseptsiooni kontrollitakse pidevalt ja täiendatakse vajaduse korral?

M 2.458 Interneti kasutamise reeglistik

Algatamise eest vastutavad: infoturbespetsialist, IT-juht, personalijuht

Rakendamise eest vastutavad: infoturbespetsialist, IT-juht

Ametkondade ja ettevõtete jaoks peab interneti kasutamine olema sätestatud kohustusliku reeglistikuga. See peab sisaldama kõikide töötajate interneti kasutamisega seotud õigusi ja kohustusi. Lisaks võib teatud internetiteenustele (nt meiliteenustele) kehtestada eraldi reeglid, mida tuleb loomulikult samuti järgida. Iga töötaja peab neid reegleid tundma ja regulaarselt üle kordama. Seega on mõistlik teha interneti kasutamise reeglistik ja muud reeglid intraneti kaudu kättesaadavaks. Interneti kasutamise reeglistik peaks kajastama vähemalt järgmisi aspekte:

- Kasutajaid tuleb lühidalt ja arusaadavalt informeerida interneti kasutamisega seotud riskidest.
- Kasutajad peavad teadma, kuidas internetiga vastutustundlikult ümber käia. Nad peavad oskama õigesti kasutada brauserit ja tüüpilisi internetiteenuseid, et vältida kasutusvigu ja ebaturvalist käitumist. Loomulikult peavad nad tundma ka organisatsioonisisest reeglistikku. Eriti tuleb neile selgitada võimalikke ohtusid ja kohustuslikke turbemeetmeid (vt M 3.77 Interneti kasutamisega seotud teadlikkuse suurendamine).
- Reeglistik peab määrama internetiteenuste kasutamise raamtingimused. Näiteks võib see sätestada, et internetipõhised tõlkimisteenuseid võib kasutada avalikkusele ligipääsetavate dokumentide jaoks, kuid mitte konfidentsiaalse info jaoks. Sellega seoses tuleb ka kindlaks määrata, kas internetiteenuseid tohib kasutada eranditult tööasjus või ka eraviisiliselt, nt lõunapauside ajal.
- Lisaks tuleb kindlaks määrata, mis rakendustega tohib internetiteenuseid kasutada. Reeglistik peab kehtestama nõude, et kasutajad ei tohi internetiteenuste rakendamiseks installida tarkvara, mille kasutamine pole heaks kiidetud. Siia alla kuuluvad ka brauseri täiendused (pluginad). Administraatorid peavad kasutajate brauserid seadistama selliseks, et maksimaalne turve saavutataks kasutaja sekkumiseta (vt M 5.45 Veebibrauserite turvaline kasutamine).

Konfidentsiaalset infot või sellist infot, mis võib jätta organisatsioonist vale mulje, ei tohi edastada ebaturvaliste internetiteenuste kaudu. Seega ei tohi seda infot jätta ei veebiserverile ega levitada meililistides. Teisalt jällegi tuleb kasutajatele selgitada, et keelatud on ka sellise info volitusteta allalaadimine või muul moel aktiivne hankimine. Näiteks ei tohi veebiserveritelt otsida faile, mille sisu võib olla solvav. Tuleb kindlaks määrata, millist sisu loetakse solvavaks. Reeglistik peab ka kindlaks määrama, kuidas käia ümber internetist saadud infoga. Kasutajate tähelepanu tuleb juhtida sellele, et võõra info kasutamisel tuleb arvestada autoriõiguste ja kasutustingimustega. Lisaks pole kõik allikad usaldusväärsed. Isegi kui ebausaldusväärsest allikast pärinevad andmed ei sisalda kahjulikku tarkvara, võib ka valeinfo kontrollimatu kasutamine siiski kahju tekitada. Valeinfot võivad sisaldada ka esindusliku välimusega veebilehed. Seega tuleb ka reguleerida, mis tingimustel tohib kohtvõrgust pärinevaid andmeid saata läbi interneti. Selleks tuleb

luua kriteeriumid, mis aitavad töötajatel otsustada, millist infot võib interneti kaudu edastada ja millist mitte. Siia alla kuuluvad ka reeglid selle kohta, kas ja kuidas andmeid nende edastamisel või levitamisel kaitsta.

Kõik töötajad peavad teadma, milliseid veebilehti ja -teenuseid nad tohivad kasutada ning kuidas kasutada neid turvaliselt ja ettenähtud viisil (vt M 3.78 Korrektne käitumine internetis). Veebilehtede kasutamine eeldab sageli registreerimist. Selleks sisestatav kasutajanimi, meiliaadress ja muu info võimaldavad teha järeldusi isiku ja organisatsiooni kohta. Tuleb selgitada, kas organisatsioonile viitamine on lubatud või mitte. Kui ei ole lubatud, tuleks kehtestada nõue, et internetiteenuste jaoks ei tohi kasutada ametlikke meiliaadresse. Läbivalt tuleb reguleerida, milliseid isiklikke ja organisatsiooni puudutavaid andmeid tohib avalikustada, et vältida näiteks soovimatute reklaamikampaaniate tulva ja inimestega manipuleerimise (*social engineering*) ründeid (vt M 2.313 Turvaline sisselogimine internetiteenustesse). Lisaks tuleb kasutajatele selgitada:

- mis andmed logitakse;
- kes on kontaktisikuks turbeprobleemide korral;
- et brauseri ja muude programmide konfiguratsiooni ei tohi omavoliliselt muuta.

Olenevalt olukorrast ja kasutuskeskkonnast tuleb reguleerida võib-olla ka teisi aspekte. Interneti turbereeglistik peab lühidalt tutvustama kasutatavaid sideteenuseid ja loetlema ka kõik muud asjakohased reeglid. Loomulikult tuleb seejuures arvestada ka seadustega, eriti andmekaitsenõuetega. Protsessi tuleb võimalikult vara kaasata ka andmekaitsespetsialist ja töötajate esindaja. Võib-olla on mõttekas lasta kasutajal allkirjaga kinnitada, et ta on interneti kasutamise reeglitest teadlik ja järgib neid sideteenuste kasutamisel.

Täiendavad kontrollküsimused:

- kas interneti kasutamise kohta on olemas turbereeglistik?
- kas interneti kasutamise turbereeglistik on kõigile töötajatele teada?

M 2.459w Internetiteenuste ülevaade

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: erialaspetsialist, infoturbespetsialist, IT-juht

Internet on üleilmne arvutivõrk, mille taristuga saab pakkuda ja kasutada erinevaid teenuseid. Kaks kõige olulisemat ja vanemat teenust on World Wide Web ja E-Mail. Peale nende on palju muid teenuseid. Kõige olulisemad ja tuntumad internetiteenused on järgmised.

World Wide Web (WWW)

WWW töötati välja hüpertekstisüsteemina, mille hajutatud info on omavahel ühendatud. Infole ligipääsemiseks saab kasutada veebibrauserit. Linkidega saab liikuda sõnalt sõnale või dokumendist dokumenti. WWW pakub kogu maailmas mitmekülgset infot, nt tekste, pilte, graafikuid, rakendusi, mänge, heli ja videoid. Peale kiire infokogumise saavad eraisikud ja organisatsioonid end WWW-s esitleda, avaldada oma materjale ja teenuseid pakkuda. Siiski tuleb alati arvestada ka sellega, et pakutav info võib olla vale. Pealegi on oht, et veebilehtede kaudu levitatakse kahjulikke programme, mis võivad näiteks koguda või võltsida konfidentsiaalseid andmeid.

E-Mail

E-post võimaldab saata elektroonilisi sõnumeid paljudele adressaatidele üle kogu maailma. Krüpteerimata ja allkirjastamata e-kirjad on seejuures võrreldavad postkaardiga, sest nende sisu saadetakse teele ilma kaitseta ja kujul, mida saab üsna lihtsasti muuta. E-post on üks levinud meetod kahjuliku tarkvara levitamiseks.

Internetifoorum

Internetifoorumis suheldakse tavaliselt mõnel konkreetsel teemal. Teema kohta saab teha postitusi ning teised huvilised saavad neid postitusi lugeda, neile vastata ja neid kommenteerida. Paljud internetifoorumid lubavad suhtluses osaleda alles pärast eelnevat sisselogimist ja/või registreerimist. Foorumis käitumist reguleerib foorumi netikett ehk foorumi käitajate kindlaks määratud käitumisreeglid. Foorumi administraatorid võivad suhtlusest kõrvaldada need kasutajad, kes foorumi reegleid eiravad. Sellele vaatamata võivad internetifoorumisse tehtud postitused jääda loetavaks pikaks ajaks. Foorumeid saab muu hulgas kuritarvitada sellega, et sinna postitatakse teadlikult kas valeinfot või tehakse halvustavaid sissekandeid. Lisaks on postitusi võimalik täiendada linkidega, nt lisainfole viitamiseks, kuid nende abil viidatakse sageli ka kahjuliku tarkvaraga veebilehtedele.

Uudisteserverid/netiuudised

Uudisteserveri kaudu saab vahetada ja lugeda uudiseid, nn netiuudiseid. Uudistegruppides saavad sama huviga isikud kogu maailmast üksteisega suhelda. Olenevalt kavatsusest otsitakse infot teatud teemade kohta või probleemide lahendamiseks. Teemad sorteeritakse uudistegruppidesse, mis saavad endale süstemaatilise ülesehituse küsimuste ja vastustega. Uudiseid tavaliselt tellitakse, kuid tellijaid ei kontrollita ja tellimusi ei kinnitata. Seega võivad protsessis osaleda kõik, st ka anonüümse või vale identiteediga kasutajad. Uudiseid saab lugemiseks salvestada lokaalselt või avada uudisteserveris. Olenevalt teemast vajab lokaalne salvestamine väga palju mäluruumi, kuid võimaldab info kiiremat töötlemist ja otsingut kogu tekstist.

Jutuajamine (chat)

Jutuajamine internetis tähendab kahe või enama suhtluspartneri sünkroonset suhtlemist interneti kaudu reaalajas. Levinud internetivariandid on Internet Relay Chat (IRC), veebijututoad (webchat) ja kiirsuhtlus (instant messaging). Jutuaja-

miseks kasutatakse sageli mõne jututoa haldaja avalikke jututube (chatrooms). Mitmed jutuajamisviisid nõuavad eelnevat registreerimist, kuid identiteedi saavad kasutajad endale ise vabalt valida. Sel põhjusel on olemas jututube, kuhu on ligipääs ainult neil osalejatel, kes on ennast kõigepealt registreerinud või kelle osalemise on heaks kiitnud administraator. Selleks, et volitamata isikud ei saaks jututoa kasutamist kuritarvitada, on lisaks võimalik edastada jututoa aadress ainult teatud kasutajatele või sisse seada era-jututoad. Ka võib administraator vestlust jälgida, kasutajaid hoiatada ja neid vestlusest välja lülitada. Kõiki sissekandeid saab salvestada ühtsesse logisse.

Blogi/veebilogi

Blogi on veebilehel peetav päevik, millele on ligipääs kas piiratud lugejaskonnal või kõigil huvilistel. Termin veebilogi ehk lühidalt blogi tuleneb nimest World Wide Web ja nimetusest logi ehk logiraamat . Eraisikud või organisatsiooni ülesandel tegutsevad isikud kirjutavad seal oma elukogemustest või muudel teemadel. Olenevalt blogi haldaja valitud seadistustest saab igale sissekandele jätta kommentaare ja teema üle arutleda. Blogisissekanded võivad kiirelt levida ja kauaks ajaks arhiveerituks jääda. Kuna need sissekanded kajastavad arvamusi, tuleks õigel ajal kaaluda, kas need on ikka mõeldud avalikkusele. Kui blogi tahetakse kasutada organisatsiooni jaoks, peaks selle sisu jälgima ja regulaarselt hooldama keegi vastutav töötaja. Kuna kommentaarid ja teated ei pruugi olla ainult positiivsed, aga negatiivsete märkuste kustutamist võidakse pidada arvamuse manipuleerimiseks, tuleb mõelda, mida teha kommenteerimisfunktsiooniga.

Twitter

Twitter on mikroblogimisteenus, mille kaudu saab avaldada maksimaalselt 140 märgi pikkuseid teateid. Twitteri kaudu edastatakse infot reaalajas. Paljud kasutajad kasutavad Twitterit mobiiltelefonis (kõikjal ja igal ajal). Kasutajad peavad end registreerima, kuid valitud identiteeti üldjuhul ei kontrollita. Registreeritud kasutajad saavad sissekandeid kommenteerida ja neile vastata. Registreerimata kasutajatel on vaid sissekannete lugemise õigus. Peale eraisikute levitavad Twitteri kaudu teateid ka organisatsioonid. Igale postitusele ehk säutsule (tweet) saab lisada võtmesõna, nn sildi, mis aitab märksõnaotsinguga seda kiiremini üles leida. Lisaks saab sellega analüüsida, mis teemad on Twitteris eriti populaarsed. Soovitusi Twitteri turvalise kasutamise kohta leiate meetmest M 5.156 Twitteri turvaline kasutamine .

Internetipangandus

Internetipangandus võimaldab teha pangatoiminguid internetis. Kõik ülekanded toimuvad elektrooniliselt, luues juurdepääsu vastavale pangaarvutile. Juurdepääsuks kasutatakse brauserit ja panga veebilehte või internetipanganduse rakendust. Kasutajal on see eelis, et paljud pangaga seotud tegevused ei sõltu enam pangakontorite asukohast ega lahtiolekuaegadest. Internetipanganduse suurim oht on see, et kliendi kontodele võivad ligi pääseda ründajad. Tavaliselt püüavad ründajad selleks saada oma valdusesse autentimisinfot, kasutades nt andmepetturlust (phishing), või suunata kliente manipuleeritud veebilehtedele, nt Trooja hobustega.

Kiirsõnumivahetus (instant messaging)

Kiirsõnumivahetus on üks internetisuhtluse variant. Kaks või enam osalejat kasutavad selleks kiirsõnumiteenust. Kiirsõnumid on soodne ja kiire alternatiiv telefonile, SMS-idele ja meilidele. Paljud teenused pakuvad peale puhta tekstisuhtluse ka lisafunktsioone, nt failide saatmist või eraldi jutukanaleid. Kiirsõnumivestluse sõnumeid ei pea ilmtingimata kohe lugema ja neile saab vastata viivitusega, kuid vahetu kontakt on võimalik. Kiirsõnumite kasutamine nõuab registreerimist, kuid

andmeid seejuures tavaliselt ei kontrollita. Tunnus, mis võib koosneda kasutajanimest, sõnumisaatja numbrist või sõnumisaatja ID-st, tuleb esmalt edastada võimalikele sidepartneritele. Sidepartnerid lisatakse kontaktide nimekirja. Sageli on võimalik näidata ka kasutaja seisundit, nt kas ta on eemal, hõivatud või suhtlemisest eriti huvitatud. Paljudes kiirsõnumiteenustes saab seisundi näitamise välja lülitada. Suhtluskontaktidelt saadud linke tohib avada ainult siis, kui on kindel, et need on tõesti saatnud sidepartner ja link ei juhi kahjuliku tarkvarani. Samuti ei tohiks avada faili, mille saatmist pole kokku lepitud. Kiirsõnumiteenuste oluline puudus on see, et erinevad teenusepakkujad kasutavad erinevaid protokolle. Potentsiaalsed sidepartnerid peavad kasutama sama süsteemi, et omavahel suhelda.

Internetitelefon

Internetitelefoniks või ka IP-telefoniks nimetatakse kõne edastamist avalike IP-võrkude, esmajoones interneti kaudu. Kõne edastamist IP-võrkude kaudu kasutatakse erinevates valdkondades ja seetõttu rakendatakse ka erinevaid turbenõudeid (vt B 4.7 IP-kõne (VOIP)). Internetitelefon on IP-kõne (Voice over IP, VoIP) üks variantidest. Interneti kaudu helistamiseks võib kasutada tarkvaralisi telefone, mis registreeritakse sama moodi nagu sõnumiteenused tsentraalses kataloogis. Üha rohkem kasutatakse ka kompaktseid ja soodsaid VoIP-lüüse, mis võimaldavad tavalistes telefonides kasutada internetis helistamise teenuseid. Lisaks on interneti kaudu helistamiseks olemas ka spetsiaalsed riistvaralised lõppseadmed (hardphones). Interneti kaudu helistamiseks peab lüüsina kasutatav IT-süsteem olema sisse lülitatud ja ühenduses internetiga. Lisaks saab kasutada kiirsõnumisüsteeme ja mobiilseid seadmeid.

Skype

Skype on interneti kaudu helistamise tarkvara, kuid sellel on ka kiirsõnumi funktsioon. Skype'iga saab helistada, andmeid edastada ja videokonverentse korraldada. Niipea kui sidepartnerid oma arvuti või nutiseadme internetti ühendavad, on nad oma Skype'i numbri kaudu kättesaadavad. Pideva kättesaadavuse tagamiseks peaks seega arvuti või nutitelefonalati töötama. Kui kasutaja arvuti või nutitelefon lakkab töötamast, ei ole ka Skype kasutamine võimalik.

Sotsiaalvõrgustikud

Sotsiaalvõrgustikud on veebikeskkonnad, mille kaudu saavad kasutajad omavahel suhelda ja andmeid vahetada. Olenevalt keskkonnast saab seal peale isiklike andmete postitada ka pilte ja kasutada erinevaid rakendusi. Sisu kujundamine on kasutajate ülesanne. Sotsiaalvõrgustikus kasutatud identiteet võib olla fiktiivne või vale või on selle loonud volitamata isik tegeliku omaniku teadmata. Võrgustik tekib kasutajatevahelise sotsiaalse tegevuse tulemusena ning see salvestatakse suhtluskeskkonna spetsiaalsete funktsioonidega tarkvara andmekogusse. Sotsiaalvõrgustike turvalise kasutamise soovitused leiate M 5.157 Sotsiaalvõrgustike turvaline kasutamine .

Interneti-TV/WebTV

Interneti-TV tähendab telesaadete ja filmide edastamist interneti kaudu lairibarakendusena. Interneti-TV ei taga kvaliteetset ülekannet. Ülekande kvaliteet sõltub kasutaja internetiühendusest ja lõppseadmest. Lisaks on internetis teenuseid, mis võimaldavad telesaateid salvestada. Salvestatud saadet saab videofailina alla laadida või vaadata brauseri aknas.

Internetiraadio/Webradio

Internetis pakutavaid raadiosaateid nimetatakse ka internetiraadioks või veebiraadioks. Ülekandeviisina on tavaliselt kasutusel voogaudio, mis eeldab vastava tarkvara olemasolu. Paljud raadiojaamad kasutavad sellist ülekandeviisi, et jõuda

kuulajateni, kes ei saa saateid kuulata ei satelliidi ega tavaraadioga. Veebiraadiote kuulamine ei piirdu ainult internetti ühendatud arvutitega. Kasutada võib ka eraldi veebiraadioseadmeid, mis on marsruuteri kaudu internetti ühendatud, kuid on ka mitmeid teisi seadmeid (mobiiltelefonid, mängukonsoolid).

Veebimälu

Veebimälu (nimetatakse ka online -kõvakettaks) saab kasutada info salvestamiseks internetti. Salvestatud infole pääseb ligi erinevatest IT-süsteemidest. Veebimälule ligipääsuks saab kasutaja kasutada erinevaid IT-süsteeme ja mälu teiste kasutajatega jagada. Veebimälu kasutamiseks peavad kasutajad end tavaliselt registreerima. Olenevalt teenusest tuleb kasutaja IT-süsteemi installida võib-olla mõni rakendus, et veebiketast saaks kasutada sama moodi nagu lokaalset kõvaketast (siit ka nimetus online -kõvaketas). Mõned teenused toetavad selliseid avatud standardeid nagu WebDAV-i (Web-based Distributed Authoring and Versioning), mille tugi on paljudes operatsioonisüsteemides ja mille tarbeks pole vaja lisarakendusi installida. Tavaliselt pääseb infole ligi ka läbi veebirakenduste. Selleks, et teised kasutajad andmekaustadele ligi pääseksid, tuleb igaühele selge luba anda, kuid on ka vaba juurdepääsuga kaustu (public-folder). Kui kõrvalised isikud teavad autentimiseks vajalikku parooli, pääsevad nad ligi kogu salvestatud infole.

Internetipoed

Internetipoodidesse pääseb võrku ühendatud arvuti või nutiseadme kaudu. Brauseris saab kauba välja valida, see pannakse virtuaalsesse ostukorvi ja tellitakse. Mobiilsetes lõppseadmetes saab sageli lisarakendusi endale välja valida otse eraldi rakendusest ja need lõppseadmesse installida. Kui ründajal õnnestub pakkuda veebipoes kahjulikku tarkvara või tarkvara andmeedastuse ajal muuta, võib tal õnnestuda kasutaja IT-süsteemi kompromiteerida.

Turbeaspektid

Mõned internetiteenustega seotud tüüpilised turbeaspektid on järgmised:

- Paljude internetiteenuste kasutajatunnust saab registreerimisel vabalt valida. Seetõttu on võimalik kasutada valeidentiteeti.
- Tavaliselt on lubatud ka nõrgad paroolid, mis teevad võimalikuks identiteedi varguse.
- Infot edastatakse kiiresti ja suures mahus sageli liiga vara või selleks volitusi omamata, samuti usutakse infot, ilma et seda kontrollitaks.
- Paljude internetiteenuste kasutustingimused lubavad sisestatud kasutajainfot kasutada reklaami otstarbel.

M 2.460 Väliste teenuste reguleeritud kasutamine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, infoturbespetsialist, IT-juht, organisatsiooni juht
Rakendamise eest vastutavad: töötajad

Internetis pakutakse paljusid huvitavaid teenuseid, millest võib kasu olla nii isiklikus elus kui ka tööl, sest need soodustavad näiteks suhtlemist kolleegidega või muudavad meie töö lihtsamaks. Nende teenuste hulka kuuluvad veebimeil, grupikalender, kaughooldustarkvara, internetis kasutatavad tekstitöötlussüsteemid ja kontoritarkvara, aadressiraamatu haldus, andmete salvestamine jne. Paljusid selliseid teenuseid saab kohe ilma suurema vaevata kasutama hakata ja neist võib organisatsioonis paljude tööde juures kasu olla. Kõik töötajad peavad siiski mõistma, et nad tohivad kasutada ainult neid väliseid teenuseid, mille on nende organisatsioon heaks kiitnud. Väliste teenuste omavolilise kasutamisega kaasnevad ohud on võrreldavad kinnitamata tarkvara installeerimisega: võivad tekkida erinevad turbe- ja andmekaitseprobleemid (vt G 3.105 Väliste teenuste volitamata kasutamine).

Töötajatele tuleb selgitada probleeme ja turberiske, mis selliste teenuste volitamata kasutamisega kaasneda võivad. Seda võib teha näiteks siseürituse raames või sisevõrku riputatud juhenditega, millele on lisatud konkreetsed näited. IT etalonturbe abivahendite hulgast leiate näidisdokumendi, mida võib kasutada eeskujuna, kuidas kaastöötajaid väliste IT-teenuste volitamata kasutamisest informeerida.

Kui töötajad tahavad oma töö kergendamiseks väliseid teenuseid kasutada, tuleks põhjuseid ja lahendusi otsida ennekõike organisatsiooni sees. Näiteks tuleb uurida, kas organisatsiooni enda IT-osakond suudaks pakkuda võrreldavat teenust või kas on võimalik sõlmida kasutusleping usaldusväärse teenusepakkujaga.

Kontrollküsimused:

- Kas väliste teenuste kasutamine on kõikidele töötajatele arusaadavalt reguleeritud?
- Kas kõik töötajad mõistavad, millega tuleb väliste teenuste kasutamisel, nt veebimeili puhul, arvestada?

M 2.461 Bluetooth'i turvalise kasutamise planeerimine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht
Rakendamise eest vastutavad: infoturbespetsialist, IT-juht

Bluetooth'il on suur arv erinevaid rakendusprofiile, mistõttu saab seda rakendust kasutada väga erineval otstarbel. Selleks, et tagada Bluetooth'i turvaline käitamine, peab institutsioon juba eeltööna Bluetooth'i kasutust planeerima. Institutsioon peab määratlema üldise strateegia, kui paljusid erinevaid Bluetoothi funktsioone ja kasutajaprofiile rakendama hakatakse. Tavaliselt on tarvis eristada kahte liiki Bluetooth-seadmeid:

- lõppseadmeid, millel on olemas Bluetooth'i funktsioonid (lühidalt: Bluetooth-lõppseadmed), nt mobiiltelefonid, nutitelefonid, sülearvutid jne ning
- lisaseadmeid, millel on olemas Bluetooth'i funktsioonid (lühidalt: Bluetooth-lisaseadmed), nt hiir, klaviatuur, peakomplekt jne.

Bluetooth-lõppseadmetel on reeglina olemas kõik funktsioonid, mida on kirjeldatud Bluetooth'i spetsifikatsioonides ning rakendatavaid turvafunktsioone saab ise vabalt valida. Bluetooth-lisaseadmed täiendavad Bluetooth-lõppseadmeid oma spetsiaalsete funktsioonidega. Olemasolevaid turvafunktsioone suudavad need reeglina kasutada siiski vaid piiratud kujul. Bluetooth-lisaseadmed rakendavad selleks otstarbeks reeglina Bluetooth-lõppseadmete erinevaid kasutajaprofiile. Bluetooth-lisaseadmete kasutusotstarve on enamasti määratletud seadmeliigiga. Nii nt saab Bluetooth-peakomplekti kasutada eranditult kõne edastamiseks ja Bluetooth-klaviatuuri saab kasutada üksnes andmesisestuseks. Lõppseadmete kasutusvõimalused on seevastu palju laiemad. Bluetooth-liidesega mobiiltelefone saab näiteks kasutada sülearvuti külge ühendatuna nagu modemeid ning kahe Bluetooth-lõppseadme vahel on võimalik andmeid vahetada. Seetõttu tuleb esmalt välja mõelda, millisel otstarbel Bluetooth-seadmeid institutsioonisiseselt ja -väliselt kasutama hakatakse. Järgmise sammuna tuleb määratleda, millistes valdkondades tohib ja millistes valdkondades ei tohi Bluetooth'i kasutada ning välja töötada ka vastavad raamtingimused. Valdkondades, kus töödeldakse institutsiooni toimimise seisukohalt kriitilise tähtsusega infot, tuleks Bluetooth'i toega andmesisestusseadmete kasutamine keelata, kuna vastasel korral muutuvad võimalikuks *Keylogging* -tüüpi ründed. Sel põhjusel peavad eksisteerima selged reeglid, milliseid Bluetooth'i funktsioone institutsiooni erinevates valdkondades kasutada tohib ja milliseid mitte. Ka neil juhtudel, kus Bluetooth-funktsioonide kasutamine on teatud kindlates ruumilistes piirides ära keelatud, võib siiski esineda olukordi, kus vastavates ruumides asuvad jätkuvalt Bluetooth-liidestega varustatud seadmed. Vältimaks olukordi, kus neid seadmeid võidakse väljastpoolt kasutama hakata, tuleb seadmete Bluetooth-liidesed kas desaktiveerida või keelata Bluetooth-liidestega seadmete nagu mobiiltelefonide või pihuarvutite kaasavõtmine teatud ruumidesse. Eelnevale lisaks tuleb otsustada, millised on üldkehtivad kohustuslikud turvafunktsioonid, mis peavad kaitsma nii Bluetooth-seadmeid kui ka Bluetooth-seadmete vahelist kommunikatsiooni (vt M 3.79 Sissejuhatus Bluetooth'i põhimõistetesse ja tööpõhimõtetesse). Vastavus on Bluetooth-seadmete turvalise konfiguratsiooni ja turvalise käitamise vundamendiks (vt M 4.362 Bluetoothi turvaline konfigureerimine ja M 4.363 Bluetooth-seadmete turvaline käitamine). Kindlasti tuleb välja

töötada ka kasutamisreeglid, mis kirjeldavad, mida Bluetooth-seadmete ja nende turvafunktsioonide kasutamisel peab järgima.

Bluetooth'i kasutamise raamtingimised tuleb sisse töötada institutsiooni turvapoliitikasse. Bluetooth'i funktsiooniga seadmete turvaliseks käitamiseks peab arvestama järgmiste olulisemate punktidega:

- Seadme vastutav kasutaja peab täiel määral mõistma traadita kommunikatsioonisüsteemide tööpõhimõtteid ja selle taga peituvat tehnoloogiat.
- Kasutatava tehnoloogia turvalisust tuleb regulaarselt hinnata. Samuti tuleks regulaarselt hinnata kasutatavate lõppseadmete (nt mobiiltelefonide, sülearvutite, pihuarvutite) turvaseadistuste tõhusust. Turbe seisukohast olulised paigad ja värskendused tuleb paigaldada võimalikult kiiresti.
- Tuleb määratleda, kas Bluetooth'i kasutamine on lubatud või keelatud. Turvakaalutlustest lähtuvalt võib olla nt mõttekas Bluetooth'i kasutamine tööotstarbelistes IT-seadmetes kas täielikult või teatud valdkondades ära keelata.
- Edastatavate andmete turvamiseks tuleb välja töötada ettekirjutused, mis reguleerivad muu hulgas adekvaatsete krüpteerimis- ja autentimis- protseduuride valimist, konfigureerimist ja võtmete haldamist.

Bluetooth'i kasutamise turvasuunised

Kasutajatele tuleb edastada lihtsad ja selgesti mõistetavad Bluetooth'i kasutamise turvasuunised. Nendes suunistes tuleb muu hulgas selgitada, milline on töötaja vastutus seoses Bluetooth-funktsioonide kasutamisega, millised seadistused mõjutavad Bluetooth-seadmete turvalisust ning seda, milliseid seadistusi peavad/tohivad tegema/teha kasutajad ja milliseid ainult administraatorid. Eelnevale lisaks tuleb veel ka defineerida see, millist liiki andmeid tohib läbi Bluetoothi edastada. Paljudes seadmetes, mida inimesed kasutavad, nt mobiiltelefonides või pihuarvutites, on olemas Bluetooth-liidesed, mis on seadme soetamise hetkel enamasti sisselülitatud. Bluetooth-liideste kasutamine ja keelamine peab olema väga selgelt reguleeritud ning olukorras, kus seda lubatakse, peavad eksisteerima selged raamtingimused. Selleks et vältida kasutajate koormamist liigsete detailidega, on mõistlik koostada eraldi Bluetooth'i kasutajapoliitika. Sellises kasutusjuhises tuleks kirjeldada Bluetooth'i kasutamise eripärasid, muu hulgas näiteks:

- millistes raamtingimustes tohib Bluetooth-funktsioonidega seadmeid kasutada,
- kuidas toimub Bluetooth-lõppseadmete korrektne installeerimine ja rakendamine,
- mida tuleb teha Bluetooth-seadmete (oletatava) kompromiteerimise puhul, esmajoones, kelle poole üldse tuleb pöörduda.

Bluetooth'i käitamise turvalisus tugineb suuresti Bluetooth-paroolide kvaliteedile. Seetõttu tuleb Bluetoothi paroolide valimisel olla ülimalt hoolikas ning selle olulisusest tuleb piisavalt teavitada nii kasutajaid kui ka administraatoreid (vt

M 3.80 Bluetooth'i kasutamise teadlikkuse tõstmine *).* Oluline on täpselt kirjeldada, kuidas tuleks ümber käia klientsüsteemide turvalahendusega. Siia valdkonda kuulub nt nõue, et ühtki turvalisust puudutavat konfiguratsiooni ei tohi muuta. Lisaks peaks kasutusjuhises sisalduma üheselt mõistetav nõue, et Bluetoothkomponentide kooskõlastamata külgeühendamine on keelatud. Lisaks peaks juhis sisaldama juhtnööre ka tundliku info, nt konfidentsiaalsete andmete käitlemise kohta, nt selle kohta, milliseid andmeid tohib läbi Bluetooth'i edastada ja milliseid mitte. Kasutajatele tuleb selgitada Bluetooth'iga kaasnevaid ohtusid, samuti Bluetooth'i kasutajapoliitika sisu ja mõju.

Täiendavad kontrollküsimused:

- Kas Bluetooth'i kasutamise kohta on olemas aktuaalne turvapoliitika?
- Kas Bluetooth'i turvalise kasutamise raamtingimused on dokumenteeritud?

M 2.462z Bluetooth-seadmete soetamise valikukriteeriumid

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: infoturbespetsialist, IT-juht

Bluetooth-seadmed erinevad üksteisest selle poolest, milliseid spetsifikatsioone need täidavad, milliseid rakendusprofiile need pakuvad ning erinev on ka tootjate poolt valitud Bluetoothi rakendamise viis. Seetõttu tuleks välja töötada erinevad kriteeriumid, mida Bluetooth-seadmete valikul arvestada. Alustuseks tuleks valikust välja jätta kõik sellised seadmed, mille puhul on teada, et nende Bluetooth-rakendustes on turvaaugud. Internetis on antud teema kohta palju lehti, kus vastavaid seadmeid üles loetletakse. Lisaks oleks tarvis välja selgitada, millised kasutajaprofiilid peavad Bluetooth-seadmetes olema ja milliseid profiile ei tohiks neis olla, st millised tuleks desaktiveerida. Bluetooth-seadmetes on erinevad kasutajaprofiilid, mida läheb tarvis seadmefunktsioonide täitmiseks. Nii näiteks on kõikidel Bluetooth-hiirtel ja -klaviatuuridel olemas vastav HID-Profile, kuna see on kõikidele kursoriseadmetele hädavajalik (vt M 3.79 Sissejuhatus Bluetooth'i põhimõistetesse ja tööpõhimõtetesse). Mobiiltelefonide puhul seevastu võiks näiteks turbe seisukohast eelistada seadmeid, millel puudub SIM Access Profile, mis võimaldab juurdepääsu telefoni SIM-kaardile, sest selle puudumise korral ei ole ka rünneteks potentsiaalset pidepunkti. Kõikidel juhtudel tuleks lõppseadmete valimisel jälgida, et need vastaksid vähemalt Bluetoothi spetsifikatsioonile 2.1, kuna alates sellest versioonist on seadmetes olemas olulised turvafunktsioonid, nt Secure Simple Pairing. Samuti tuleks tagada, et ei kasutatakse seadmeid, mille spetsifikatsiooni versioon on vanem kui 2.1, kuna need kasutava nõrku turvafunktsioone (vt M 4.362 Bluetoothi turvaline konfigureerimine). Bluetooth-seadmete olulised turbealased kriteeriumid on kokkuvõtvalt järgnevad:

- Bluetooth Special Interest Group (SIG) ei tegele mitte ainult Bluetooth-spetsifikatsioonide edasiarendamisega, vaid kontrollib ja sertifitseerib ka Bluetooth-seadmete koostalitlusvõimet. Sellele vaatamata on võimalik soetada väga paljusid tooteid, millel puudub Bluetooth-SIG kvaliteedinõuetele vastav sertifikaat. Selliste toodete koostalitlusvõime teiste seadmetega on ilmselt tavapärasest madalam. Seetõttu tuleks seadmete soetamisel jälgida, et neil oleks Bluetoothi ametlik kvaliteeditunnus.
- Valikut tehes tuleks arvestada, et sugugi mitte kõigis Bluetoothi toega seadmetes ei ole võimalik Bluetooth-liidest desaktiveerida.
- Bluetooth'i spetsifikatsioon näeb ette kolm võimsusklassi, mis määravad seadmete maksimaalse saatmisvõimsuse ja leviala. Langetades otsuseid võimsusklasside 1 kuni 3 kasuks tuleks arvestada, et mida suurem on seadme leviala, seda kättesaadavam on seade ka ründajatele.
- Bluetooth'i toega lisaseadmetes, nt peakomplektides on Bluetooth'i PIN-kood reeglina eelseadistatud ja kindlalt ette antud. Kuna selline olukord kujutab endast väga suurt turvariski, tuleks võimalusel alati soetada sellised seadmed, mille PIN-koodi saab ise muuta.
- Bluetooth-seadmed peaksid täitma versiooni 2.1 + EDR spetsifikatsioone. Sellega tagatakse, et seadmes on olemas turvarežiimi nr 4 ja *Secure Simple*

Pairing funktsioonid.

Enne soetamist tasuks üle kontrollida, kas Bluetooth-seadmetes on olemas kõik vajalikud profiilid. Kui seadmes puudub nt A2DP profiil (*Advanced Audio Distribution Profile*), ei ole võimalik läbi Bluetooth-liidese edastada kõrgekvaliteedilisi audioandmeid.

M 2.463z Bluetooth-lisaseadmete seadmekogu kasutamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator, kasutaja

Mõningate lõppseadmete standardkonfiguratsioon ei pruugi Bluetoothi moodulit sisaldada ja mõningate seadmete moodulid ei pruugi jällegi vastata Bluetoothi uusimatele spetsifikatsioonidele. Selleks, et kirjeldatud lõppseadmeid kiiresti kõige uuema Bluetooth-tehnoloogiaga varustada, võib olla abiks tsentraalse Bluetooth-seadmekogu sisseseadmine. Seadmekogu on lahendus, mis võimaldab hallata erinevaid Bluetooth-seadmeid. Seadmekogusse võib koondada alustuseks nt Bluetooth-hiired ja -klaviatuurid, GPS-vastuvõtjad, mis suudavad teiste seadmetega läbi Bluetooth-liidese ühendusse astuda ning lõpetuseks kõikvõimalikud adapterid (USB-pulgad ja sülearvutite pistikkaardid), mis võimaldavad lõppseadmetel Bluetoothi kasutada. Viimast tuleks hoolikalt jälgida Bluetooth-hiirte ja -klaviatuuride korral, kuna need vajavad sidetehnoloogia tööks alati ka Bluetooth-adapterit.

Bluetooth-adapter on sageli ka piisavalt ühene tõestus, mille alusel seadet Bluetooth-seadmete hulka liigitada ja arvesse tuleb võtta, et need peavad olema turvaliselt konfigureeritud. Lisaks tuleks Bluetooth-hiirte ja -klaviatuuride kasutamisel järgida soovitusi, mis kajastuvad meetmes M 4.254z Juhtmeta klaviatuuri ja hiire turvaline kasutuselevõtt . Praeguseks on saadaval juba suur hulk tooteid, mis suhtlevad omavahel läbi Bluetooth-liidese. Bluetoothi turvamehhanismide korrektsel rakendamisel ja konfigureerimisel pakuvad need üldjuhul suuremat kaitset kui tootja tehnikaga raadiosidel töötavad süsteemid. Piisavalt pika võtme kasutamist Bluetooth-ühenduse loomisel tuleks ennekõike kontrollida klaviatuuride puhul. Lisaks peaksid andmesisestusseadmed vastama Bluetoothi spetsifikatsioonile 2.1 + EDR, kuna alates sellest versioonist on võimalik kasutada funktsiooni Simple Secure Pairing (vt M 4.362 Bluetoothi turvaline konfigureerimine), mis tagab Bluetooth-ühendusele suurema turvalisuse ning kaitseb tõhusamalt võimalike klahvilogeri rünnete vastu. Kõik seadmekogusse kokku kogutavad seadmed peaksid vastama institutsioonis defineeritud kriteeriumitele (vt M 2.462z Bluetooth-seadmete soetamise valikukriteeriumid).

Iga kord, kui Bluetooth-seade töötajale väljastatakse, tuleb teda informeerida, kuidas Bluetooth-seadet ja selle turvafunktsioone korrektselt kasutada. Selleks tuleks koostada infoleht Bluetoothi kasutamise turvasuuniste kohta, kus kajastuvad muu hulgas ka juhised Bluetooth-lõppseadme installeerimise ja kasutamise kohta. Lisaks tuleks dokumenteerida info selle kohta, kes, millal ja millise Bluetooth-seadme laenutas ning mis otstarbel. Töötaja peab talle väljalaenutatud Bluetooth-seadme kättesaamist kinnitama oma allkirjaga. Allkirjaga kinnitab töötaja ka seda, et on Bluetoothi kasutamisega seotud turvanõuetest teadlik ja kohustub neid järgima. Ka Bluetooth-seadme tagastamine tuleb plangile üles märkida.

Mõningatel juhtudel on võib-olla mõistlik Bluetooth-seadmekogu ja juba olemasolev mobiiltelefonide seadmekogu kokku liita (vt M 2.190z Mobiilikogu sissesead-

mine). Paljudesse tänapäeva mobiiltelefonidesse on Bluetooth juba standardina sisse ehitatud, mis tähendab, et mobiiltelefonides tuleb teha täpselt need samad turvaseadistused, mis kõikides teistes Bluetooth-seadmetes.

Kontrollküsimus:

- Kas tsentraalsesse seadmekogusse tagastatud Bluetooth-seadmetes taastatakse nendele ette nähtud standardne seadistus?

M 2.464 Infoturbesuuniste loomine terminaliserveri kasutamiseks

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator

Terminaliserveri süsteemi kasutamisel tuleb luua vastavad infoturbesuunised. Siin kirjalikult ära toodud meetmed ja sihid peavad peegeldama turvalise terminaliserveri keskkonna tingimusi ja nõudeid. Suuniseid tuleb kontrollida nende aktuaalsuse suhtes ning vajadusel kohandada. Terminaliserverit puudutavad määratlused saab täiendavalt kokku võtta juba olemas olevas suunises või selle jaoks eraldi loodud dokumendis. Terminaliserveri suuniste dokument võib olla infoturbepoliitika või mõne muu dokumendi osa. Suunis peaks teiste hulgas sisaldama järgmiseid punkte:

- Miinimumnõuded, mida kliendid peavad täitma, et neid oleks võimalik terminaliserverile ligipääsuks kasutada.
- Keskkond, millesse need kliendid omavad ligipääsu. Eriti hoolikalt tuleks reguleerida ligipääsuvõimalusi eemal asuvate töökohtade korral, näiteks internetikohvikust või sülearvutiga ebaturvalise WLAN ühenduse kaudu (vt M 2.389 Avalike pääsupunktide turvaline kasutus *).*
- Lisaseadmed, mida võib kliendiga ühendada (printer, USB-pulk, teised lõppseadmed).
- Sisesed või välised võrgud, millega võib terminaliserveri keskkonda ühendada.
- Informatsioon või allavoolu teenused, millele on võimalik terminaliserveri süsteemide kaudu ligi pääseda ja kellel on see lubatud.
- Kõigile terminaliserveri komponentidele tuleks kindlaks määrata turvameetmed ja standardkonfiguratsioon.
- Turbeprobleemide kahtluse korral peab sellest informeerima infoturbevolinikku, et ta saaks teha edasised sammud (vt B 1.8 Turvaintsidentide käsitlus *).*
- Nii terminaliserveri administraatoreid kui ka kasutajaid tuleks teavitada või koolitada ohtude ja vajalike turbemeetmete suhtes, mida terminaliserveri-arhitektuuri kasutamine endaga kaasa toob.
- Peale selle tuleks suunises kirjeldatud meetmete teostust ka regulaarselt kontrollida.

Suunised terminaliserveri keskkonna kasutajale

Vältimaks kasutajate liigset koormamist andmetega on mõttekas kasutajatele luua eraldi terminaliserveri keskkonna suunised. Nendes tuleks lühidalt kirjeldada terminaliserveri kasutamise eripära, näiteks:

- Millisest sise- või välisvõrgust võib terminaliserveri süsteemi siseneda?
- Milliste raamtingimuste korral võivad kasutajad ennast keskkonda registreerida?

- Kas tohib kasutada organisatsioonile tundmatuid kliente ning kui jah, siis kuidas?
- Mida tuleb ette võtta terminaliserveri või kliendi oletatava kompromiteerimise korral? Keda tuleb teavitada?

Oluline on konkreetselt kirjeldada kliendipoolsete turbelahendustega ümberkäimist. Siia hulka kuuluvad näiteks järgmised põhimõtted:

- turbekriitilisi konfiguratsioone ei tohi muuta ega saata kolmandatele isikutele,
- kasutada tohib ainult lubatud tarkvaraversiooniga terminalitarkvara

Terminaliserverile ligipääsul kaugvõrgu kaudu tuleb veenduda, et:

- alati oleks aktiveeritud viiruseskanner,
- olemasolevat personaalset tulemüüri ei tohi välja lülitada (vt M 5.91 Interneti-PC personaalse tulemüüri installeerimine),
- kasutaja poolt kinnitatud kliendiautentimise kontroll turvalüüsi kaudu, kuna vastasel juhul lubatakse ainult piiratud ligipääs.

Terminaliserveri seansse võib kasutamise ajal katkestada tahtlikult või toimub see ühenduse katkemise tagajärjel. Juba eelnevalt käivitatud rakendused toimivad tavaliselt edasi ja seanssi on võimalik hilisemal ajahetkel jätkata. Et hooldustöid mitte takistada ja vältimaks andmekadu regulaarsete taaskäivitustsüklite tõttu, tuleb kasutajasuunistes kindlaks määrata turvalisuse tagavad käitumisviisid, lisaks tuleks tähelepanu pöörata ka järgmistele punktidele:

- Seansid, mis ühendushäirete tõttu katkesid, tuleks nii ruttu kui võimalik taastada.
- Kasutajate tähelepanu tuleks juhtida terminaliserveri seanssi maksimaalsele kestvusele.
- Hiljemalt kasutusaja lõpus tuleb teostatud programmid kasutaja poolt lõpetada ja ennast terminaliserveri seansist välja logida.

Peale selle peaks direktiiv sisaldama andmeid klassifitseeritud informatsiooni, näiteks salastatud andmete kasutamise kohta ning määrama, milliseid andmeid tohib terminaliserveri süsteemis kasutada ja milliseid klientidele üle kanda. Kasutajaid tuleks muuta terminaliserveri ohtude ning terminaliserveri suunise sisu ja mõju suhtes tundlikumaks.

Suunised administraatoritele

Lisaks peaks olema loodud terminaliserveri spetsiifilised suunised administraatoritele, mida võib kasutada ka administraatorite koolituse alusena. Selles peaks olema kindlaks määratud, kes vastutab erinevate terminaliserveri komponentide halduse eest, millised on osalevate administraatorite vahelised liidesed ja millal ja millist informatsiooni tuleb vastutavate isikutega jagada. Tavaliselt vastutab

terminaliserverite farmi käitamise eest mõni teine organisatsiooniüksus, kui see, kes vastutab klientide halduse eest või identiteedi- ja õigushalduse eest või see kes vastutab primaarse kaitse eest. Lisaks peaks administraatoritele mõeldud terminaliserveri suunis hõlmama terminaliserveri infrastruktuuri käituse põhiaspekte, näiteks:

- Turvalise terminaliserveri konfiguratsiooni kindlaksmääramine ja klientsüsteemide turvalise standardkonfiguratsiooni defineerimine.
- Olemasolevate terminaliserveri haldusserverite konfigureerimine.
- Meetodid individuaalsete kasutajaõiguste administratiivseks kasutamiseks ligipääsuks failidele ja rakendustele.
- Meetodid individuaalsete kasutajaõiguste administratiivseks kasutamiseks ligipääsuks allavoolu teenustele (*Backend*) ja võrkudele.
- Terminaliserveri seansside loomisel ebaturvalise võrgu kaudu kasutatava krüpteerimismeetodi valik ja seadistamine.
- Tegevus seansi katkemisel
- Taaskäivitustsüklite reguleerimine, ennetamaks mälulekkeid, protsessiprobleeme ja haldusakende läbiviimist.
- Logiandmete regulaarne analüüs
- Testide läbiviimine ning võrgu- ja süsteemikoormuse monitooring.
- Asendussüsteemide kasutuselevõtt
- Meetmed terminaliserverite kompromiteerimisel

Administraatoritel on terminaliserverite kasutamisel võimalus seansse dubleerida (*shadowing*). Siinjuures tuleb arvestada andmekaitseseaduse nõuetega. Seansi järelvalve ilma kasutaja loata rikub tema õigust privaatsusele. Selle funktsiooni kasutamine tuleb seega administraatori suunistega reguleerida. Kõik terminaliserveri kasutajad, olgu nendeks siis kasutajad või administraatorid, peaksid oma allkirjaga kinnitama, et nad on infoturbesuunist lugenud ning et nad peavad seal määratletud juhistest kinni. Ilma kirjaliku loata ei tohiks keegi seda süsteemi kasutada. Allkirjaga kinnitatud avaldused tuleb säilitada, näiteks personalitoimikus.

Täiendavad kontrollküsimused:

- Kas terminaliserveri administraatoritele ja kasutajatele koostati infoturbesuunised?
- Kas terminaliserveri kasutamise suuniseid kontrollitakse nende aktuaalsuse suhtes ning kas neid uuendatakse vajadusel?
- Kas kõik kasutajad ja administraatorid peavad kinnitama, et nad on terminaliserveri infoturbesuunist lugenud ja seal määratletud juhised endale selgeks teinud?

M 2.465 Terminaliserveri vajalike ressursside analüüs

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator

Et kindlustada terminaliserveri kättesaadavus on olulise tähtsusega süsteemiressursside õige dimensioneerimine. Protsessijõudlus, andmete läbilaskvus salvestussüsteemi ja nende suurus on tunnused, mis kirjeldavad terminaliserveri jõudlust ning samas mõjutavad ka sellise mitmekasutajasüsteemi stabiilsust. Vastutasuks on terminaliserveri klientide jõudlus vähemtähtis, kuna nemad võtavad enda kanda ainult kuvamise ja sisestuse haldamise. Mida rohkem on ühel terminaliserveril kasutajaid, seda rohkem protsesse peab olema võimalik korraga käivitada ja käitada. Kui jõutakse teatud piirideni, võib terminaliserver uute kasutajate ligipääsu keelustada, juba sisselogitud kasutajate jaoks võib server reageerida liiga aeglaselt või täielikult rivist välja langeda.

Skaleeritavus

Eelkõige terminaliserveri süsteemid võivad väga ruttu jõuda kasutatava tehnika jõudluse piirideni. Siinjuures tuleb pöörata tähelepanu asjaolule, et mitte ükski IT-süsteem ei ole suvaliselt laiendatav ja on sõltuv vastavast kasutusjuhtumist. Teatud koormuspiirist alates tekivad piirangud. Teatud juhtudel on neid piiranguid võimalik kõrvaldada. Samas on selgunud, et serverikoormuse järjekordsel tõstmisel võivad tekkida piirangud mõnes muus kohas.

Piiravateks faktoriteks võivad olla:

- Paigaldatavate protsessorite arv
- Põhimälu adresseeritavus süsteemiarhitektuuri kaudu
- Mäluhaldus operatsioonisüsteemi kaudu
- Massmälusüsteemide kiirus
- Ettevõtte/asutusesisese siini ribalaius

Praktikas on ennast õigustanud sellised kontseptsioonid nagu serverivõrgud (Terminaliserveri farm), mille turvalist teostust on kirjeldatud meetmes M 6.142z Redundantsete (ressurssi osaliselt või täielikult dubleerivate) terminaliserverite kasutamine . Otsused, mis selle meetme põhjal langetatakse, mõjutavad aga süsteemiressursside edukat dimensioneerimist. Nii võib vajaliku jõudluse kasutusse andmine ja sellega seotud rivist väljalangemise turvalisus toimuda kas serveri liiasuse või serveris paiknevate komponentide liiasuse kaudu.

Nõueteprofiili loomine

Tegelikult vajatavate ressursside väljaselgitamiseks on sobilik teostada sihtkeskkonna põhjalik analüüs. Siinkohal ei saa mälukasutuse kohta järeldusi teha mitte ainult ühe rakenduse alusel, mida kasutaja teostab. Samuti tuleks arvestada tagaplaanis jooksvate rakendustega nagu viirusetõrjeprogrammid, failikäivitusmehhanismid ja ekraanidefektid. Seepärast peab esmalt kontrollima, milliseid programme kasutatakse, milliseid ülesandeid ja millisel viisil nendega lahendatakse ja kui kiiresti peavad rakendused kasutajate ülesannete täitmiseks reageerima. Vajadusel võib kasutada automatiseeritud teste või kasutajagruppides läbiviidavaid teste.

Kontrollküsimused:

- Kas kontrolliti, milliseid rakendusi tuleks terminaliserveril kasutada ja millised ülesanded tuleks kustutada?
- Kas kontrolliti, milliseid jõudluse nõudlusi rakendused plaanitud kasutajaarvu juures terminaliserveri keskkonnale esitavad?
- Kas loodi strateegia terminaliserverite kasutamiseks, et tulla toime kasvavate kasutajaarvudega, suurema andmemahuga ja sellega seotud suurema serverikoormusega?

M 2.466 Migratsioon terminaliserveri arhitektuurile

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator

Olemasoleva klientserver-arhitektuuri migratsioonil terminaliserveri toega keskkonda, tuleb enne teostust põhjalikult kontrollida, kas teisaldatavad rakendused on selleks sobilikud. Kui kontrolli käigus tekib sihtsüsteemis konflikte failide või ligipääsu vahel, võib oletada, et selle põhjuseks on vastava rakenduse puudulik või puuduv kasutajaseansside eraldus. Windowsil põhinevad serveri operatsioonisüsteemid võimaldavad spetsiaalse installeerimisrežiimi siseselt see eraldamine rakenduse eest ise ära teostada. Sedasi eraldatakse iga seanssi jaoks individuaalselt registreerimisandmebaas (*Windows-Registry*) ja tähtsates süsteemikataloogides paiknevad failid. Rakendused, mis tootja andmetel on terminaliserveril kasutamiseks sobilikud, näiteks Windows Terminaliserveri ja firma Citrix terminaliserveri lahenduste all on enamjaolt seadistatud nii, et neid saaks sellisel viisil installeerida. Kui kirjeldatud eraldustehnika on planeeritud terminaliserveri lahenduse korral saadaval, tuleks seda ka kasutada. Pärast rakenduste edukat installeerimist tuleb installeerimisrežiimist uuesti väljuda.

Nõudmiste analüüs

Suuresti erineva turbevajadusega rakendusi ei tohiks lihtsalt niisama ühel terminaliserveril käitada. Kas neid on võimalik koos ühel terminaliserveril käitada, sõltub kasutatavast tootest ja organisatsiooni või rakenduse nõudlusest ja ohtudest. Seetõttu tuleb hinnata, kuivõrd on vaatluse all olev terminaliserveri lahendus sobilik ühel terminaliserveril koos käitama erineva turbevajadusega rakendusi. Lisaks tuleb kasutusele võtta sobivad meetmed, et kindlustada kõigile rakendustele sobiv turbetase. Kõige suurema turbevajadusega rakendus kättesaadavuse, konfidentsiaalsuse ja tervikluse alal määrab, milline on kõigi sellel terminaliserveril käitatavate rakenduste turbeaste. Kui vajaliku turbeastet ei ole võimalik kõigi rakenduste jaoks saavutada, tuleks kasutusele võtta eraldi IT-süsteemid. Kui vajatakse palju erinevaid rakendusi, on võimalik need vastavalt kasutajate vajadustele gruppidesse jagada. Kui soovitakse rahuldada suurt hulka erinevaid nõudmisi ühe või mõne vähese IT-süsteemi kaudu, kasvab informatsioonisüsteemi keerukus ja samuti ka tõenäosus, et rakendused hakkavad üksteist segama. Siinjuures on soovitatav juba eelnevalt loodud kasutajagrupid ja rakendused erinevate süsteemide vahel sobivalt laiali jagada. Lisaks tuleb meetmetes M 2.465 Terminaliserveri vajalike ressursside analüüs ja M 5.162 Ribalaiuse planeerimine terminaliserverite kasutamisel välja selgitatud määrasid võrrelda võrguinfrastruktuuri jõudluse näitajatega, et ületamatuid kitsaskohti juba eelnevalt arvesse võtta.

Täiendavad kontrollküsimused:

- Kas rakendused on sobilikud terminaliserveril kasutamiseks?
- Kas on kindlustatud, et terminaliserveril paiknevad rakendused ei pääse keelatud viisil ligi kriitilistele süsteemiradadele ja registreerimisandmebaasile, näiteks spetsiaalse installeerimisrežiimi abil?
- Kas on arvestatud sellega, et erineva turbevajadusega rakendusi ei tohi ilma vastavate meetmeteta terminaliserveritel käitada?

M 2.467 Terminaliserveri regulaarsete taaskäivitustsüklite plaanimine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator

Kindlustamaks terminaliserveri vigadeta käituse, tuleks plaanida regulaarseid taaskäivitustsükleid. Reguleeritud väljalülitamise ja taaskäivitamise ajal on võimalik läbi viia skripti juhitud hooldustöid. Peale selle piiratakse selle tegevusega erinevate mälulekete mõju, mis aja jooksul võivad terminaliserevri jõudlust vähendada. Et jagada haldusserverite koormusi taaskäivituse ajal pikema ajaperioodi peale, ei tohiks suurtes terminaliserveri-süsteemides taaskäivitustsüklid toimuda kõigile terminaliserveritele üheaegselt. Peale selle tuleks taaskäivitusest välja jätta terminaliserverid, millel toimuvad samal ajal aktiveeritud seansid. Selle tarvis tuleb koostada taaskäivitusplaan, mis lähtub terminaliserveri hetke ülesehitusest.

Täiendav kontrollküsimus:

- Kas töötati välja plaan terminaliserveri reguleeritud taaskäivitamiseks?

M 2.468z Tarkvaralitsentsid terminaliserveri keskkonnas

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator

Kui seni klient-serveril põhineval võrguarhitektuuril kasutatud rakendused soovitakse teha terminaliserveril kesksel kättesaadavaks, tuleb enne teisaldamist kontrollida litsentsiõigusi puudutavaid lepinguid. Näiteks ei pruugi vigaselt litsentseeritud tarkvara korral toimida turbemehhanismid, kuna nad võivad teatud juhtudel kasutajate arvu määramise aluseks võtta installatsioonide arvu. Terminaliserveril tuleb rakendus ainult üks kord installeerida. Sõltuvalt rakenduste serveri kasutatavatest ressurssidest on see siis piiramatu hulga kasutajate poolt korraga kasutatav. Ka nn riistvara tongeli kaitsest on niimoodi võimalik mööda hiilida. Litsentseerimata tarkvara ebaseaduslik kasutamine võib endaga kaasa tuua tsiviilõiguslikke või isegi karistusõiguslikke tagajärgi. Sellest lähtuvalt peaksid terminaliserveril kasutatavad programmid olema kooskõlas omandatud litsentsidega ja sobivalt protokollitud. Mõned terminaliserveri-süsteemid lubavad litsentsiserveri abiga sisselogitud konkureerivaid kasutajaid juhtida. Lisaks on võimalik sellest kõrvalekalduvalt litsentsiõiguslikult jälgida teatud arvu registreeritud lõppseadmeid. Litsentsiserveri installeerimine ja aktiveerimine terminaliserveri teenuste kasutamiseks on selle tarkvaralahenduse korral lausa kohustuslik. Litsentsiserveri nõuetekohane toimimine on seega terminaliserveri kättesaadavuse koha pealt ülimalt olulise tähtsusega. Litsentsiserveri korrektset töötamist tuleks regulaarselt kontrollida ning selle rivist väljalangemise korral planeerida ja ette valmistada selle asendus. Suurte installatsioonide korral tuleb terminaliserver ettevaatuse mõttes seadistada liiasusega.

Kontrollküsimus:

- Kas terminaliserveril kasutatavad programmid on kooskõlas omandatud litsentsidega ning kas see on sobival viisil protokollitud?

M 2.469 Terminaliserveri keskkonnast komponentide korrastatud eemaldamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator

Kui terminaliserver, terminaliserveriga ühendatud klient või terminaliserveri keskkonna infrastruktuurikomponent tahetakse kasutuselt kõrvaldada, on vajalik järgnevate sammude hoolikas planeerimine. Sarnaselt meetmele M 2.320 Serveri nõuetekohane kasutuselt kõrvaldamine , tuleb kindlustada, et:

- tähtsad terminaliserveri keskkonna sisesed andmed ei läheks kaduma,
- et rakendusserveriga ühendatud rakendused, kliendid või allavooluteenused ei oleks mõjutatud ja et
- terminaliserverite ja kliendi infrastruktuuri andmekandjatele ei jääks konfidentsiaalseid andmeid.

Seetõttu on eriti oluline, et oleks ülevaade, millised andmed, kus kohas süsteemis salvestatud on ja kust neile ligi pääseb. Järgnevalt täpsustatakse terminaliserveri keskkonna jaoks vajalikke punkte lähtuvalt meetmest M 2.320 Serveri nõuetekohane kasutuselt kõrvaldamine .

Andmevarunduse maht:

Regulaarselt tuleks salvestada järgmine informatsioon:

- Kasutajaprofiilid
- Litsentsiserverile paigutatud informatsioon
- Autentimisinformatsioon,
- Kui olemas, siis ka seansi andmebaasi (*Session Directory*) konfiguratsioon
- IMA (*Independent Management Architecture*) andmesalvesti konfiguratsioon Citrix süsteemide korral
- Kasutatavad haldustööriistad
- Terminaliserveri olemasolevad, eelnevalt defineeritud, kontrollitud ja töökorras süsteemiolud
- Kliendi olemasolevad, eelnevalt defineeritud, kontrollitud ja töökorras süsteemiolud

Varusüsteemid

- Terminaliserverite hoolduseks ja kasutuselt kõrvaldamiseks terminaliserveri farmist on mõttekas defineerida standardarhitektuur. See tähendab, et terminaliserveri farmis kasutatakse ainult samalaadset serveririistavara, millel on sama tarkvaraaste. Standardarhitektuuril põhinevate IT-süsteemide eeliseks on, et osta võib tavalisi poest saadavaid varusüsteeme ja varuosasid on võimalik osta varuga. Defekti korral on vigane seade võimalik soodsalt ja aegsasti väljavahetada

Kasutajate teavitamine

- Kasutajaid peaks teavitama, kuidas ja kuna terminaliserverit kasutuselt kõrvalda tahetakse. Kui kasutajatel on terminaliserveril veel avatud seansse, tuleb neil paluda need eelnevalt lõpetada.

Süsteemi viidete eemaldamine

- Selleks, et mitte ühtegi seanssi äkiliselt ei lõpetataks, tuleb enne terminaliserveri väljalülitamist takistada, et kasutajad ei saaks ennast süsteemi sisse logida.

Andmete kustutamine välja lülitatud süsteemilt

Kui koormuse ühtlaseks jaotamiseks terminaliserverite vahel kasutatakse *Loadbalancer* i või teisi süsteemisiseseid koormusejaotussüsteeme, tuleks enne terminaliserveri väljalülitamist see juba eelnevalt koormusejaotusplaanidest eemaldada. Takistamaks tundliku informatsiooni jõudmist volitamata isikute käsutusse, tuleks terminaliserverilt kustutada järgmine informatsioon:

- Kasutajaprofiilid
- Autentimisinformatsioon,
- Sertifikaadid

Kui ei taheta eemaldada mitte ainult üksikut terminaliserverit, vaid kogu terminaliserveri keskkonda, tuleb kustutada järgmine informatsioon:

- Tundlikud andmed istungiandmepangas,
- IMA (*Independent Management Architecture*) andmesalvesti Citrix süsteemide korral,
- Citrix süsteemide ZDC (*Zone Data Collector*), kõik klientidel paiknevad ajutised failid, nagu *bitmaps* id ja kogu vahemälu.

Andmevarundusseadmete kustutamine

Pärast kasutuselt kõrvaldamist on soovitatav kõik andmevarundusseadmed kustutada . Erandi moodustavad siinkohal terminaliserveri andmevarundused, mida kasutatakse reduntantselt või mis teiste terminaliserverite omadega sarnanevad. Sellisel juhul võib teatud asjaoludel hilisemal ajahetkel olla vajalik salvestatud informatsioon ülejäänud terminaliserveritele tagasi kanda.

Informatsiooni eemaldamine

Enne terminaliserveri kasutuselt kõrvaldamist tuleks eemaldada kõik USB-mälupulgad ja mälukaardid ning informatsioon, mis ei ole salvestatud kõvakettale tuleks kustutada. Siia kuuluvad näiteks *Preboot eXecution Environment* (PXE) informatsioon ja Bios'i sissekanded. Eemaldada tuleks ka kaughalduskaardid ja kirjad.

Täiendavad kontrollküsimused:

- Kas terminaliserverite tegevuse lõpetamine on reguleeritud?
- Kas kasutajaid teavitati selle kohta, et nad enne terminaliserveri tegevuse lõpetamise oma seansid sulgeksid?
- Kui terminaliserveritel paikneb kasutajate andmeid, siis kas need salvestati?
- Kas väljavahetatavad terminaliserverid eemaldati võrgukoormuse jaotamise plaanidest?
- Kas enne terminaliserveri välja vahetamist hävitati andmekandjatelt kogu konfidentsiaalne informatsioon?

M 2.470 Kodukeskjaama nõudlusanalüüsi läbiviimine

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: infoturbespetsialist, administraator

Enne kui kodukeskjaam soetatakse või kui olemasolevat keskjaama täiendatakse, võiks läbi viia kodukeskjaama nõudlusanalüüsi. Ennekõike tuleks selgusele jõuda põhimõttelises küsimuses: millist funktsiooni peaks kodukeskjaam lisaks tavapärasele telefoniteenusele veel pakkuma? Lisaks tuleks selgitada, kuidas keskjaama rakendada. Mõeldav on näiteks keskjaama paigaldamine vaid klientidega kontakti hoidmiseks, majasiseseks suhtluseks või kõnekeskusena kasutamiseks. Samuti tuleks selgitada, milliseid sideteenuseid tegelikult vajatakse.

Kodukeskjaama valik sõltub muuhulgas ka lõppseadmete hulgast ja korraga kastutatavate ühenduste arvust. Tänu analüüsi tulemusele peaks asutusel olema võimalik kodukeskjaama soetamist planeerida ning valida välja sobilik ja turvaline kodukeskjaam. Nõudlusanalüüsi tulemused tuleks dokumenteerida ja kooskõlastada IT-valdkonna vastutavate töötajatega.

Nõudlusanalüüs peaks muu hulgas andma vastused järgmistele küsimustele:

- Kuidas tuleks kodukeskjaama kasutada: tavapärase keskjaamana, VoIPsüsteemina või hübriidjaamana? Kas võimalikuks alternatiiviks oleks IPühendus
- Kui palju sise- ja kui palju välisühendusi peaks keskjaamal olema? Kas ühenduste arvu on pärast keskjaama ostmist veel võimalik muuta?
- Kuidas toimib avalikku telefonivõrku (PSTN) ühendamine? Kas korraga toimuvate kõnede arv on määratud (ISDN või S2m-ühendus) või on neid võimalik määrata vastavalt vajadusele (IP-ühendus)
- Kui palju sisemisi sideühendusi peaks olema korraga võimalik kasutada?
- Milliseid ülesandeid peaks plaanitav kodukeskjaam täitma? Millised funktsioonid peaksid sel olema? Kas on funktsioone, mis peaksid tingimata olemas olema?
- Kas olemasolevad lõppseadmed suudavad koos kodukeskjaamaga kõiki nõutud funktsioone täita või tuleb soetada uued lõppseadmed?
- Kas kodukeskjaama nõudlustele piisab olemasolevast juhtmestikust või tuleb juhtmestikku uuendada?
- Kas tuleb soetada uus kodukeskjaam või saab olemasolevat keskjaama täiendada?
- Kas kodukeskjaama kättesaadavusele või salvestatud või töödeldavate andmete konfidentsiaalsusele või integreeritusele esitatakse erinõudeid?
- Kas kodukeskjaamale on hiljem võimalik paigaldada muid funktsioone (riist-, tark- ja/või püsivara)?
- Kas kavandatakse suhtlust mitme keskjaama vahel eesmärgiga ühendada omavahel ettevõtte või asutuse erinevaid asukohti või filiaale? Kas olemasolevad keskjaamad on plaanitava uue keskjaamaga ühildatavad nii, et kogu asutuse kõik nõutavad funktsioonid saaksid täidetud?

- Kuidas tagatakse kodukeskjaama (juurdepääsu), telefonivõrgu ja lõppseadmete turvalisus?
- Kas kodukeskjaama hooldamiseks on vaja sõlmida teenindus- ja hooldusleping? Kui kiiresti on võimalik jaama parandada ja rikkeid kõrvaldada?

Vastavalt nõudlusanalüüsi tulemustele tuleb defineerida ja määratleda kodukeskjaamale esitatavad nõuded. Kui teha lisaks ka turuanalüüs ja konsulteerida vajadusel kodukeskjaamadega tegelevate firmade ekspertidega, siis saab nõudlustele toetudes välja töötada konkreetse plaani ja soetada asutusele sobiv kodukeskjaam. Täpsema info leiate moodulite M 2.105w Kodukeskjaama soetamine ja M 2.471 Kodukeskjaama rakendamise planeerimine .

Kontrollküsimused:

- Kas kodukeskjaama rakendamisel järgiti sellele esitatud nõudeid?
- Kas kodukeskjaamale esitatavaid nõudeid kooskõlastati IT-valdkonna vastutavate töötajatega?

M 2.471 Kodukeskjaama rakendamise planeerimine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: IT-juht, administraator

Enne kodukeskjaama rakendamise planeerimist tuleks läbi viia ulatuslik analüüs, milles määratletakse keskjaamale esitatavad peamised nõuded (vt M 2.470 Kodukeskjaama nõudlusanalüüsi läbiviimine). Kodukeskjaama turvalise rakendamise põhiliseks eelduseks on vastava plaani olemasolu. Keskjaama rakendamist võib planeerida ülevalt alla ehk põhimõtte „üldisest üksikuni" järgi: konkreetseid osakomponente planeeritakse kogu süsteemist lähtuvalt. Planeerimine ei puuduta siinjuures mitte ainult neid aspekte, mida tavapäraselt turvalisuse mõistega seostatakse, vaid ka tavakäitamise aspekte, millest võivad tuleneda nõuded turvavaldkonnale. Seepärast tuleks asutuse kodukeskjaam kogu oma üksikute funktsioonidega üksikajalikult läbi analüüsida. Lisaks on vaja saada ülevaade sidesüsteemi ühendatud komponentidest. Samuti on väga oluline, et nõudlusanalüüsis määratletaks kodukeskjaama käitusviis kas tavapärase keskjaamana, VoIP-seadmena, hübriidjaamana või IP-ühendusena. Keskjaama rakendamise planeerimisel tuleks silmas pidada alljärgnevaid aspekte.

Kasutusjuhend

Kodukeskjaama turvaliseks ja efektiivseks rakendamiseks tuleb kindlaks määrata olemasolevatel turvaeesmärkidel põhinevad turvanõuded. Lisaks tuleks silmas pidada ka plaanitud rakendamise käigust tulenevaid nõudeid. Need spetsiifilised turvanõuded peavad olema kooskõlas kogu asutust hõlmava turvakontseptsiooniga (vt M 2.472 Kodukeskjaama (PBX) turvajuhendi koostamine).

Varustatus/lõppseadmed

Kodukeskjaama kasutuselevõtuks tuleks määrata vajalikud lõppseadmed. Lisaks tavapärasele kõnetelefonile pakuvad ka täiesti lihtsad keskjaamad tervet hulka mugavust pakkuvaid lisafunktsioone. Seejuures on nii tavapäraste kui hübriidsete keskjaamade puhul võimalik valida nii analoogse kui digitaalse variandi vahel ning selliste seadmete nagu modem, faks, ning traadita ning traadiga telefonide vahel. Keskjaama valikul tuleks lähtuda ka selle käsitsemisomadustest, käsitsemismugavusest ning seadme omadustest. Olenevalt telefonide konkreetsest kasutusvajadusest võib valida näiteks vabakäe- või tavatelefonide vahel.

Rakendused

Kodukeskjaamadel on mitmeid rakendusi, mis võivad sisaldada järgimist nõudvaid turvaaspekte. Turvakriitiliste rakenduste hulka kuuluvad sellised rakendused nagu näiteks sisselülitamine selleks, et teised kõnepartnerid võiksid lülituda juba peetavasse kõnesse, konverentsilülitus, mis võimaldab mitmel osalejal korraga seadme kaudu üksteisega ühendust võtta, ja enda telefonil teisele telefoniaparaadile tulnud kõne vastuvõtmine. Kasutamise planeerimisel tuleks otsustada, milliseid keskjaamarakendusi kasutama hakatakse.

Pädevused

Kuna kodukeskjaama kasutamiseks on vaja mitmeid komponente, tuleks välja selgitada, millised organisatsiooniüksused milliste ülesannete eest vastutavad, nt kes vastutab riistvara soetamise ja paigaldamise eest, kes tarkvara uuendamise eest, kes paroolide või kasutajatunnuste eest. Samuti tuleks välja selgitada, kas ja millised tööd tuleks tellida väliselt teenusepakkujalt.

Õigustatud kasutamine

Olenevalt välja valitud rakendustest tuleks koostada dokument, kus sätestatakse, kellel on õigus rakendusi kasutada. See võiks sisaldada järgmist:

- Kes milliseid funktsioone ja sideteenuseid võib kasutada?
- Kes otsustab, kuidas kasutatakse keskjaama integreeritud automaatvastajat ning kes ja millal tohib milliseid salvestusi kustutada?
- Kes vastutab muusika eest, mis kõlab siis, kui kõne on ootel või kui see suunatakse automaatselt edasi?
- Kas lõppseadmed konfigureeritakse kõik administraatori poolt või saab iga kasutaja õiguse seda ise teha?

Haldamine ja konfigureerimine

Kui nimetatud dokumendi koostamisel mõeldi kodukeskjaama konfigureerimise ja haldamise peale üldiselt, siis nüüd tuleks antud teemaga üksikasjalikumalt tegeleda. Esmalt tuleks selgitada, kuidas hakatakse süsteemi haldama ja milliseid seadistusi tuleks teha läbi keskse haldus- ja konfigureerimisüksuse ja milliseid otse lõppseadmetel. Keskselt võiks näiteks juurde ühendada lisaseadmeid, seadistada pääste- ja erinumbrid, aga ka hallata aadressraamatut, näiteks lisada kataloog LDAP-i kaudu. Otse lõppseadmetele võiks seadistada helinaid, klahvilukustusi, funktsiooniklahve või isiklikke telefoniraamatuid. Edasi tuleks selgitada, kes vastutab kodukeskjaama ja selle komponentide haldamise eest. Selle alla kuuluvad ka sellised ülesanded nagu turvapaikade installeerimine või süsteemiosa uuendamine, uute kasutajagruppide sisseviimine, pääsuõiguste ja kasutajagruppide muutmine, uue keskjaama funktsioonide aktiveerimine ja keerulisemate konfiguratsioonimuudatuste tegemine. Kodukeskjaam tuleb liita asutuse turvapaikade ja muudatuste haldamisega (vt B 1.14 Turvapaikade ja muudatuste haldus). Kodukeskjaama konfiguratsioonimuutmised tuleb logida, et hiljem oleks vajadusel võimalik tehtuga tutvuda (vt M 4.5 Kodukeskjaama (PBX) haldustööde logi).

Logimine

Planeerimisetapis tuleks otsustada, milline on vähim logitav info ja kui kaua tuleks logiandmeid säilitada. Lisaks tuleks kindlaks määrata, kas logiandmeid hoitakse otse keskjaamas või võrku salvestatuna kesksel serveril. Lisaks peaks logimine olema võimalik ka IP-seadmeühendusel. Otstarbekas oleks juba planeerimisetapis kindlaks määrata, kuidas ja millal andmeid analüüsitakse. Seejuures tuleks kontrollida, kuivõrd nõuab see andmekaitseseadusest kinnipidamist ja milliseid järeldusi võiks logitud andmetest teha. Kodukeskjaam edastab tavaliselt logiandmed telefoninumbrite kohta, millelt on välja ja sisse helistatud. Neid andmeid saab kasutada näiteks kulude arvutamiseks. Andmed tuleb vastava tarkvara abil varundada.

Andmevarundus

Kodukeskjaama konfiguratsioone, kasutatavate programmide aktuaalseid versioone ja logiandmeid tuleb regulaarselt varundada, et hädaolukorra korral oleks asendussüsteem võimalik lühikese ajaga üles ehitada. Selleks, et vastata maksimaalselt lubatava andmekao nõudmistele, tuleks määratleda kindlad turvaajad ja turvavormid. Vastavad määratlused tuleb liita keskse IT-valdkonna koguandmevarundusse (vt M 6.26 Kodukeskjaama (PBX) konfiguratsiooniandmete regulaarne varundus).

Hädaolukorraennetus

Selleks, et probleemidele oleks võimalik kiiresti ja tõhusalt reageerida, tuleb luua organisatsioonilised raamtingimused, et hädaolukorra korral kiiresti alternatiivsetele sidekanalitele ümber lülituda või vastu võtta hädaolukorraga seotud kõnesid. Oluline on pöörata tähelepanu ka töötajate koolitamisele. Töötajatel peaksid

olema teadmised kodukeskjaamaga seotud ohtudest, nad peaksid ära tundma hoiatusmärke ja -sümboleid ning hoiatustoone ja oskama kasutada vastavaid kommunikatsiooniteenuseid. Kuna side kättesaadavus ei ole oluliseks eelduseks mitte ainult äriprotsessides, tuleb kasutusele võtta erinevaid ettevaatusabinõusid (vt M 6.145 Kodukeskjaama (PBX) hädaolukorraks valmisolek).

Vastav plaan peaks olema juhtkonna tasandil heaks kiidetud ja kõik otsused dokumenteeritud nii, et nendega oleks võimalik hiljem tutvuda.

Täiendav kontrollküsimus:

- Kas kõik kodukeskjaamaga seotud plaanid on dokumenteeritud nii, et nendega oleks võimalik hiljem tutvuda?

M 2.472 Kodukeskjaama (PBX) turvajuhendi koostamine

Algatamise eest vastutavad: institutsiooni/ettevõtte juhtkond, infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: IT-juht, infoturbespetsialist

Asutuse kodukeskjaamale esitatavad turvanõuded tulenevad institutsiooni üldisest turvajuhendist. Olenevalt üldjuhendist tuleb nõudmisi täpsustada ja koostada kodukeskjaama turvajuhend. Seoses sellega tuleb kontrollida, kas lisaks asutuse üldisele turvajuhendile on veel teisi juhendmaterjale, nagu nt IT- või paroolijuhend, aga ka näiteks VoIP-i (voice-over-IP) kasutusjuhend, mida tuleks järgida. Turvajuhend peaks sisaldama olulist infot kodukeskjaama käitatavuse, aga ka salvestatud andmete salajasuse ja integreerituse kohta. Seejuures tuleks silmas pidada, et põhimõtteliselt esitatakse sideteenustele kõrgeid käitus- ja konfidentsiaalsusnõudmisi. Isikuandmete salvestamisel tuleks jälgida ka andmekaitsest ja säilitamiskohustusest tulenevaid nõudeid. Kahtluste korral ja revisjonide läbiviimisel on need turvaanalüüside aluseks. Kodukeskjaama turvajuhendit peavad tundma kõik isikud ja töötajaterühmad, kes tegelevad keskjaama soetamise, paigaldamise, rakendamise ja käitamisega. Turvajuhend peab olema nende tegevuse aluseks. Nagu kõikide teiste juhendite puhul, peab sellegi sisu ja rakendamist üldrevisjonide käigus regulaarselt kontrollima. Kodukeskjaama turvajuhend peaks keskjaama ja selle sideteenuste kasutajaid lühidalt ja arusaadavas vormis võimalikest ohtudest informeerima (vt M 3.82 Kodukeskjaama turvalise kasutamise koolitus). Seejuures tuleks tähelepanu pöörata ka tehnikavaldkonna uusimatele arengutele ja hiljuti teatavaks saanud ohtudele. Taoline teave peaks äratama kasutajas huvi ja motiveerima teda juhendist kinni pidama.

Kodukeskjaama tavapäraste rakenduste kõrval (nt kolmanda isiku kõnest osavõtt, päring, kinnise liini korral taashelistamine, koputamine, aga ka lülitumine juba toimuvasse kõnesse, konverentsilülitus, ja kõne juurdetoomine) on tänu tavapärase kodukeskjaama IT-süsteemidega ühendamisele hübriid- ja VoIP-seadmetel veel palju muid infotehnoloogial baseeruvaid funktsioone. Näiteks on võimalik kõneuudiseid ja fakse edastada meili teel, võtta arvuti kaudu kõnesid vastu ja saata neid edasi ning vaadata, kas soovitud isik on kättesaadav. Turvajuhendis tuleb seepärast määratleda, milliseid kodukeskjaama funktsioone ja rakendusi hakatakse kasutama. Lisaks tuleks määratleda, kes millisel eesmärgil milliseid teenuseid võib kasutada. Seoses sellega tuleb kindlaks määrata ka see, millises ulatuses tohib keskjaama isiklikuks otstarbeks kasutada. Samuti tuleb jälgida turvameetmeid, mis reguleerivad vajaliku turvariistvara ja -tarkvara valimist ja paigaldamist, aga ka kodukeskjaama ja selle lõppseadmete turvalise konfiguratsiooni nõudeid. Hübriidseadmete või VoIP-süsteemi kasutamisel tuleb lisaks järgida ka neile süsteemidele kehtivaid juhendeid. Mõnel juhul võib olla otstarbekas anda kasutajatele õiguse mõningaid kindlaid konfiguratsiooniseadeid ise otse lõppseadmel läbi viia – näiteks võiks neil olla õigus telefoni lõppseade äraoleku ajaks välja lülitada. See peaks olema juhendis sätestatud, sest vastasel korral on see keelatud.

Lisaks oleks mõttekas sätestada juhendis näiteks järgmised punktid:

- Regulatsioonid juurdepääsu füüsiliseks kontrollimiseks: põhimõtteliselt

peaks kodukeskjaam olema paigaldatud eraldi turvaalale, näiteks lukustatavasse arvutiruumi. Seejuures tuleks reguleerida seda, kellel on õigus antud ruumi siseneda või kellel on keskjaamale juurdepääsu õigus. Juurdepääs haldusele, mis toimub tavaliselt haldusarvuti, aga ka üksikute lõppseadmete kaudu, peaks olema ainult keskjaama käitavatel isikutel (vt M 2.27z Kodukeskjaama (PBX) hooldus).

- Administraatorite töö regulatsioonid: tuleks määratleda, millise skeemi järgi jagatakse haldusõigusi. Seejuures tuleks ka kaaluda, kas administraatori IT-süsteeme puudutavad tööülesanded tuleks lahutada kodukeskjaama eest vastutava töötaja tööülesannetest. Lisaks tuleks määratleda, milline administraator võib milliseid õigusi kasutada ja kuidas ta need õigused saab.

Järgmise sammuna tuleks määrata juurdepääsuteed, mille kaudu administraatorid süsteemidesse pääseksid. Mõeldavateks variantideks on juurdepääs otse kodukeskjaamale, haldusvõrgu või kaughoolduslliideste kaudu. (vt M 5.14 Sisemiste kaugpöörduste turve ja M 5.15 Väliste kaugpöörduste turve).

Lisaks vajab reglementeerimist ka see, milliseid protsesse hakatakse dokumenteerima ning millises vormis ja kuidas dokumentatsiooni hooldada.

Siia kuuluvad järgmised paigaldamist ja konfiguratsiooni puudutavad andmed:

- Kuidas kogu kodukeskjaama ja lõppseadmeid paigaldada.
- Vaikeseadete kontrollimine ja olenevalt ohustatusest nende muutmine, samuti paroolide muutmine.
- Kodukeskjaama ja lõppseadmete kasutamine ja konfigureerimine.
- Konfiguratsiooni dokumenteerimine ja turvamine.

Samuti tuleks esitada nõudeid seadme turvaliseks käitamiseks:

- Haldamise kindlustamine (haldusele juurdepääs on ainult keskjaama käitaval personalil).
- Kodukeskjaama kõigi sisselogimiskatsete registreerimine, nende logimine ja kaughooldusportide regulaarne kontroll.
- Käitamiseks ja hoolduseks lubatud tööriistad.
- Mittekasutatavate juurdepääsuvõimaluste likvideerimine.
- Pääsuõiguste jagamine.
- Tarkvara uuendamise ja konfiguratsiooni muutmise juhised.
- Andmevarundus ja varundatud andmete taastamine.
- Regulatsioonid selle kohta, kuidas reageerida avariidele, tehnilistele riketele (kohalik tugi, kaughooldus) ja turvajuhtumitele.

Samuti peaks olema turvajuhendis osutatud, kuidas toimub keskjaama komponentide jäätmekäitlus. Osa kõneandmeid ja muid isikuandmeid on ju salvestatud keskjaama andmekandjatele. Sageli on lõppseadmetele märgitud kiirvalikuklahvide kombinatsioonid, IP-aadressid, telefoninumbrid või muu tehniline teave. Üksikud komponendid tuleb hävitada nii, et andmeid ei oleks võimalik taastada. Kodukeskjaama turvajuhendi rakendamise eest vastutab IT-käitus, dokumendi muudatused ja sellest kõrvalekalded tuleb kooskõlastada IT-turbespetsialistiga.

Kontrollküsimused:

- Kas on olemas toimiv kodukeskjaama turvajuhend?
- Kas kõigile töötajatele on kodukeskjaama turvajuhendit tutvustatud?

M 2.473 Kodukeskjaama (PBX) teenusepakkuja valimine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: kodukeskjaama eest vastutav töötaja, IT-juht, administraator

Peaaegu alati on vaja, et kasutaja saaks valida ja võtta kõnesid vastu isikutelt, kelle lõppseade ei ole ühendatud sellesama keskjaamaga, mis tema oma.

Järgnevalt tuuakse paar näidet:

Selleks, et oleks võimalik helistada isikutele, kelle lõppseade ei ole ühendatud asutuse kodukeskjaamaga (nt asutuse teistes asukohtades olevad lõppseadmed, mobiiltelefonid ja kõnepartnerid väljastpoolt), peab kodukeskjaam olema läbi kliendiliini ühendatud PSTN-iga (public switched telephone network ehk kanalikommutatsiooniga avalik telefonivõrk). Selle teenuse võib tellida keskjaama teenusepakkujalt (service provider).Keskjaama teenusepakkuja loob füüsilise ühenduse institutsiooni kodukeskjaama ja PSTN-i vahel, samuti korraldab ühenduse PSTN-iga. Erandiks on IP-seadmeühendused, mille puhul kasutatakse vaid internetiühendusi ja mille ühendamine PSTN-iga kuulub tervenisti keskjaama teenusepakkuja pädevusse. Kuna keskjaama teenusepakkuja vahendab keskjaama välisühendust, on teenusepakkuja valik väga oluline, samuti on tähtis tema pakutavad teenused ning korraga kasutatavate ühenduste arv.

Teenusepakkuja valikul võiks silmas pidada järgmist:

- Ühendamise viis - Kas kodukeskjaam ühendatakse PSTN-iga ühe või mitme ISDN-i baasühendustega või läbi S2m primary rate interface' i (ISDN-i primaarkonfiguratsioon, PRI). Kas IP-seadmeühendus on võimalik?
- Erinevate asukohtade liitmine võrku - Kuidas ühendatakse erinevates kohtades asuvad keskjaamad?
- Referentspaigaldus või -kliendid - Kas keskjaama teenusepakkujal on kogemusi asutustega, kelle nõudmised sarnanevad sellele juhtumile?
- Teenindusmeeskonna suurus ja kvaliteet - Kui kiiresti on tehnikud võimelised kohale tulema? Millise reageerimisaja pakkuja garanteerib?
- Riistvara - Kas kliendilt nõutakse eraldi riistava soetamist? Kas seda on võimalik osta või üürida? Millised on olemasolevad väljastellimis- ja teenusetasemelepped?
- Maht - Kas teenusepakkuja on võimeline tõendama, et ta saab pakkuda nõutud arvu väljaminevaid liine?
- Liiasusega liinid - Kas kodukeskjaama saab kõrgendatud kaitsevajaduse korral ühendada mitme füüsiliselt sõltumatu liini ja trassiga PSTN-iga liiasusega?

Lisaks turvaaspektidele tuleks tähelepanu pöörata ka lepingulistele ja finantsilistele aspektidele:

- Lepinguline seotus teenusepakkujaga - Kui kaua on klient teenusepakkujaga seotud? Millised on ülesütlemise tähtajad? Kas hiljem on võimalik hakata kasutama teise teenusepakkuja teenuseid?

- Paindlikkus ja valmisolek - Kas keskjaama teenusepakkuja on varem regulaarselt pakkunud uusi tooteid, teenuseid ja tariife? Kas kliendil on võimalik hakata kasutama üksikuid tooteid või teenuseid üksteise järel?
- Tariifimudelid - Kas on tariifimudeleid, mis vastaksid võimalikult hästi asutuse teenusekasutusele, nagu nt kindlad hinnad (internetiühenduse kuutasu) või diferentseeritud hinnad? Kas on soodushindu välismaale helistamiseks, kui kindlatele numbritele helistatakse sageli? Kuidas arvestatakse kõne pikkust (sekundilise või minutilise täpsusega)?

Kõik kokkulepitud teenused peavad olema täpselt ja ühemõtteliselt arusaadavalt kirjalikus vormis sätestatud.

Kontrollküsimus:

- Kas keskjaama teenusepakkujaga tehtud kokkulepped on kirjalikult sätestatud?

M 2.474 Kodukeskjaama (PBX) komponentide turvaline kasutuselt kõrvaldamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator

Mõnele kodukeskjaama komponendile salvestatakse selle kasutamisel konfidentsiaalset infot, mille hulka kuuluvad isikuandmed nagu nt telefoniraamatud ja kontaktandmed, aga ka kõneandmed. Traadita kohtvõrgu korral kuulub sinna hulka eriti autentimisinfo, mida kasutatakse traadita kohtvõrgule juurdepääsuks (vt M 2.390 Traadita kohtvõrgu komponentide kasutusest kõrvaldamine). VoIP-komponentidele võib olla olenevalt nende kasutuseesmärgist salvestatud erinevat tundlikku teavet nagu nt IP-aadressid ja muu võrgu ülesehitusest pärinev info, aga ka asutuse kõikide töötajate telefoninimistud (vt M 2.377 Turvaline IP-kõne komponentide kasutusest kõrvaldamine). Erinevatele komponentidele lokaalselt salvestatud ja veel kasutuses olevad andmed tuleks kas väljastpoolt kindlustada või arhiveerida (nt magnetlintidel, CD-l või DVD-ROM-idel) või kanda üle asendussüsteemi (vt B 1.4 Andmevarunduspoliitika ja B 1.12 Arhiveerimine). Komponentide kasutuselt kõrvaldamisel või nende asendamisel tuleks jälgida, et andmekandjaid, millele on salvestatud isikuandmed, käideldaks ettenähtud moel. Seda eriti siis, kui komponendid eraldatakse ja antakse kolmandele isikule edasi (nt müüakse). Ka juhul, kui seade vahetatakse garantiiajal välja või antakse tootja kätte või teenindusfirmasse parandamiseks, tuleks konfidentsiaalsed andmed enne seadme väljaandmist loetamatuks muuta. Sel eesmärgil tuleks andmekandjad kas füüsiliselt hävitada või siis tuleks andmekandjal olevad andmed nii kustutada, et neid ei ole võimalik taastada (vt B 1.15 Andmete kustutamine ja hävitamine).

Tihti on komponentide välisküljele märgitud kiirvaliku numbrid, IP-aadressid, telefoninumbrid või muu tehniline teave. Ka need tuleb enne seadme jäätmekäitlusesse andmist kõrvaldada. Lisaks tuleks jälgida, et kasutuselt kõrvaldatud komponendi pääsuõigused oleksid ära võetud, et kõrvalised isikud ei saaks neid kasutada. Sidesüsteemi komponentide turvalisele jäätmekäitlusele tuleks osutada ka turvajuhendis.

Täiendavad kontrollküsimused:

- Kas kodukeskjaama komponentidel olevad andmed kustutatakse enne nende jäätmekäitlusesse andmist?
- Kas vastavas turvajuhendis on viidatud keskjaama komponentide turvalise jäätmekäitluse vajalikkusele?

M 2.475 Lepingu koostamine väljast tellitava infoturbespetsialistiga

Algatamise eest vastutab: ametiasutuse/ettevõtte juhtkond
Rakendamise eest vastutab: ametiasutuse/ettevõtte juhtkond

Kui infoturbespetsialisti teenus tellitakse väljast, tuleks arvestada alljärgnevate aspektidega. Eriti just väikestes ettevõtetes ja ametiasutustes ei pruugi olla mõttekas kasutada infoturbespetsialisti ametikoha täitmiseks enda töötajat, vaid tellida teenus väljast. Selleks tuleb esmalt välja valida sobiva kvalifikatsiooniga ekspert. Juhiseid infoturbespetsialisti vajaliku kvalifikatsiooni ja tööülesannete kohta leiate standardist BSI 100-2 ja meetmest M 2.193 Infoturbeks sobiva organisatsioonilise struktuuri rajamine . Enne organisatsioonivälise infoturbespetsialisti ametisse nimetamist tuleb teenusepakkuja ja organisatsiooni vahel sõlmida leping, milles on võimalikult täpselt kindlaks määratud infoturbespetsialisti tööülesanded ning vastastikused õigused ja kohustused.

Organisatsioonivälise infoturbespetsialisti palkamine on seega väljasttellimise erijuhtum. Lepinguga tuleks reguleerida vähemalt järgmisi aspekte:

- organisatsioonivälise infoturbespetsialisti kvalifikatsiooninõuded;
- töötaja asendamise kord ja minimaalsed ressursid;
- organisatsioonivälise infoturbespetsialisti tööülesanded;
- teavitus-, aruandlus- ja eskalatsioonijuhised (töörollid);
- tööd telliva organisatsiooni teavituskanalite kaasamine;
- töökohad, tööruumid, kohaloleku- ja kättesaadavusajad;
- sisenemis-, juurdepääsu- ja kasutusõigused;
- töötaja õigus pöörduda otsesest ülemusest kõrgema astme üksuse poole ning töötaja aruandluskohustused organisatsiooni juhtkonna ees;
- tööde tellija koostöökohustused;
- konfidentsiaalsuslepped;
- huvide konfliktide lahendamine;
- lepingu rikkumise tagajärjed;
- töösuhte lõpetamine, nt tööülesannete ja -dokumentide üleandmine;
- töötasu.

Lepinguga tuleb organisatsioonivälist infoturbespetsialisti kohustada tööd tegema ja luua talle tingimused, mis võimaldavad tal teha oma tööd vähemalt sama hästi, kui seda teeks organisatsioonisisene infoturbespetsialist. Organisatsioonivälise infoturbespetsialisti teenuse kasuks otsustamisel tuleb arvestada ka mooduliga B 1.11 Väljasttellimine (Outsourcing) . Eriti tuleks võtta arvesse meedet M 2.226 Asutusevälise personali kasutamise protseduurid .

Kontrollküsimused - Organisatsioonivälise infoturbespetsialisti kasuks otsustamisel:

- Kas sõlmitav teenusleping sisaldab kõiki infoturbespetsialisti tööülesandeid ning nendega seotud õigusi ja kohustusi?

- Kas infoturbespetsialistil on vajalik kvalifikatsioon?
- Kas sõlmitav teenusleping sisaldab kõiki töölepingu lõpetamist reguleerivaid sätteid, k.a neid, mis reguleerivad tööülesannete ja -dokumentide üleandmist tööandjale?
- Kas sõlmitav teenusleping sisaldab kõiki konfidentsiaalsusleppeid?

M 2.476 Interneti turvalise ühendamise kontseptsioon

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, infoturbespetsialist, IT-juht
Rakendamise eest vastutavad: IT-juht, infoturbespetsialist

Erinevates institutsioonides kasutatakse väga erinevaid sise- ja välisvõrke. See valdkond hõlmab enamasti ka IT-süsteemide ja võrkude ühendamist internetiga. Kõik ühendused avatud väliste võrkudega kätkevad endas ohte, sest need võivad muutuda väravaks kahjurvarale, kõikvõimalikele rünnetele ja andmete väljavoolule. Seetõttu tuleb koostada kontseptsioon, millega määratakse kindlaks internetiühenduse liik ja selle usaldusväärne turve. Ohtude minimeerimiseks tuleks ka igat uut interneti rakendamise varianti enne kasutuselevõttu hoolikalt planeerida, samuti tuleb hoolitseda selle eest, et kõikide IT-komponentide installimine, võrku ühendamine ja konfigureerimine oleks turvaline. Interneti turvalise ühendamise kontseptsioon peab esmajoones vastama küsimusele, kuidas kaitstakse sisevõrgus paiknevaid IT-süsteeme. Samuti tuleb kindlaks määrata interneti kasutamise raamtingimused, st kes tohib milliseid internetiteenuseid ja mis tingimustel kasutada (vt M 2.457 Interneti turvalise kasutamise kontseptsioon). Muu hulgas tuleb langetada otsus, milliseid internetiga seotud andmeside liike ja internetiteenuseid lubatakse (vt M 2.459w Internetiteenuste ülevaade). Internetiühendusele esitatavad nõuded olenevad institutsiooni internetikasutuse eesmärkidest, nt veebiserveri käitamiseks on tarvis palju rohkem ribalaiust ja internetiühenduse käideldavusnõuded on palju suuremad kui neil juhtudel, kus internetti kasutatakse ainult aeg-ajalt teabe hankimiseks veebiteenuste kaudu. See kontseptsioon tuleb juurutada organisatsiooni üldisse infoturbestrateegiasse ning seetõttu ka infoturbeosakonnaga kooskõlastada.

Töökorraldus

Interneti kasutamiseks läheb tarvis suurt hulka erinevaid IT-komponente. Seetõttu tuleb kindlaks määrata, mis osakonnad vastutavad erinevate ülesannete täitmise, nt kasutajatunnuste loomise, kasutajate haldamise või veebilehe sisu muutmise eest. Probleemide kiireks ja efektiivseks lahendamiseks (nt selleks, et internetiteenuse kasutamine hädaolukorras kiiresti välja lülitada) tuleb välja töötada ka töökorralduse raamtingimused. Sobiva internetiteenuse pakkuja (Internet Service Provider – ISP) ja vajaliku ühendustehnika valimiseks tuleks üksikute internetiteenuste puhul dokumenteerida ka vajalik ribalaius ja reaktsiooniaeg (vt M 2.176z Sobiva internetiteenuse pakkuja valimine). Võrgustruktuuri kohandamist planeerides tuleb välja selgitada, milliseid teisi IT-süsteeme ja võrguühendusi võib interneti kasutamine mõjutada. Samuti tuleks kindlaks määrata, kuidas toimida internetist pärit andmetega, nt kas allalaaditud faile tohib teistes süsteemides edasi töödelda või tuleb need arhiveerida. Kontseptsioon peab sisaldama turvanõudeid selle kohta, kas internetis olevale infole ligipääsemiseks või info edasisaatmiseks teistele internetis olevatele arvutitele on vaja seda volitamata lugemise ja muutmise eest kaitsta.

Turvaline ühendus internetiga

Kui kohtvõrgus (LAN) soovitakse kasutada ka World Wide Webi (WWW), e-posti või muid internetiteenuseid, tuleb LAN ühendada ebausaldusväärse

võrguga, nt internetiga. Selle tagajärjel hakkavad institutsiooni seni suletud võrku mõjutama märkimisväärsed ohud ja seda juba enne, kui jõutakse installida ja kasutusele võtta esimene internetirakendus. Ründajad, kes kasutavad oma töös internetti, võivad internetiprotokollides, -teenustes ja -komponentides otsida võimalikke turvaauke, samuti võivad nad üritada andmevahetust pealt kuulata (sniffing), võltsida saatjaandmeid (spoofing) ning sisevõrku tungida. Nendele ohtudele saab vastu astuda, kui kasutada tugevat võrguühendust, sobivaid seadmeid, turvalisi konfiguratsioone ja kontrollitud käitamist.

LAN-i ühendamiseks ebausaldusväärse võrguga võib valida arhitektuuri, mis koosneb neljast tsoonist:

- Esimese tsooni moodustab sisevõrk. See sisaldab kõiki klientsüsteeme ning ka taristu ja rakenduste servereid, mida on tarvis LAN-i lokaalseks autonoomseks käitamiseks.
- Teises tsoonis asub turvalüüs (vt B 3.301 Turvalüüs (tulemüür)), mis kaitseb LAN-i internetist tulevate rünnete eest. Samuti asuvad selles tsoonis internetipõhiseid teenuseid osutavad serverid, mida omakorda kaitstakse paketifiltritega, st serverid asuvad demilitariseeritud tsoonis. Demilitariseeritud tsoonid (DMZ) on võrgu üleminekukohtadesse sisse seatud vahevõrgud, millega kaitstakse sisemisi võrgustruktuure. Tsoonides paiknevatesse serveritesse on võimalik teha üksnes kontrollitud pöördusi. Sel juhul saab teenuseid osutada nii WAN-is kui ka LAN-is. Neid kahte võrku saab omavahel ühendada proksiserveritega.
- Kolmanda tsooni moodustavad interneti ühendamiseks vajalikud komponendid. Kõige lihtsamate variantide korral kuulub sellesse tsooni üksainus marsruuter, mis on ühendatud internetiteenust osutava teenusepakkuja võrguga. Suurte käideldavusnõuete korral tuleb selleks ette näha liiasusega ühendus.
- Neljandas ehk haldustsoonis kogutakse ja töödeldakse kõiki haldusandmeid tsentraalselt. Selles tsoonis võib paikneda ka ajaserver, mida kasutatakse kõikide võrgus asuvate süsteemikellade sünkroniseerimiseks. Kõik ülejäänud aspektid peaksid olema juba kaetud turvalüüsi valdkonna läbitöötamisega (vt M 2.71 Turvalüüsi (tulemüüri) turvapoliitika).

Ajakohasus

Interneti ühendamise kontseptsiooni tuleb regulaarselt, st vähemalt kord aastas, ajakohastada, sest see valdkond areneb väga kiiresti. Turvalise internetiühenduse tagamiseks tuleks interneti turvalise ühendamise kontseptsioon koostada koos turvalüüsi kontseptsiooniga (vt M 2.70 Turvalüüsi (tulemüüri) kontseptsiooni väljatöötamine). Organisatsiooni eesmärkide, strateegiate ja ohuastme muutumisel tuleb kontrollida, millist mõju avaldab see internetiühendusele.

Kontrollküsimused:

- Kas interneti ühendamise kohta on olemas ajakohane kontseptsioon?
- Kas interneti ühendamise kontseptsiooni kontrollitakse pidevalt ja täiendatakse vajaduse korral?

M 2.477 Virtuaaltaristu planeerimine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

Virtuaaltaristu kasutuselevõtule peab kindlasti eelnema detailne planeerimine, sest tegu on väga keerulise valdkonnaga. Seetõttu tuleb juba kontseptsiooni valimisel ja projekteerimise eeltööna täpselt analüüsida hädavajalikke raamtingimusi.

Virtualiseerimistehnoloogia kindlaksmääramine

Esimese planeerimistööna tuleb välja selgitada, millised IT-süsteemid tulevad virtualiseerimiseks üldse kõne alla, ja selle põhjal otsustada, milline on virtualiseerimistaristu baastehnoloogia (serveri või operatsioonisüsteemi virtualiseerimine).

Selleks tuleb analüüsida järgmisi olulisimaid kriteeriume:

- Serveri virtualiseerimine, mille puhul kujutatakse serverit virtuaalselt täismahus koos selle riistvarakomponentidega, sobib väga hästi eriti neil juhtudel, kus on tarvis käitada väga erinevate ülesannetega virtuaalseid IT-süsteeme. Serveri virtualiseerimist kasutavate süsteemide korral on võimalik erinevate operatsioonisüsteemidega (Windows, Linux, Solaris) töötavaid masinaid käitada koos ühes virtualiseerimisserveris, sest iga virtuaalne süsteem saab jätkuvalt kasutada oma operatsioonisüsteemi tuuma. Serveripõhise virtualiseerimisega on võimalik saavutada virtuaalsete IT-süsteemide väga tugev kapseldus. See tähendab näiteks seda, et virtuaalne IT-süsteem ei kasuta ühtki virtualiseerimisserveri ega ka mis tahes teise virtuaalse IT-süsteemi operatsioonisüsteemi komponenti ega tarkvarateeki. Serveripõhisel virtualiseerimisel on virtuaalsed süsteemid ka palju tugevamalt üksteisest isoleeritud kui operatsioonisüsteemi virtualiseerimisel, st funktsioonide vastastikmõjud on enamjaolt välistatud.
- Operatsioonisüsteemi virtualiseerimine võimaldab hõlpsalt ühes virtualiseerimisserveris käitada suurt hulka ühesuguseid servereid. Seetõttu saab operatsioonisüsteemi virtualiseerimisega saavutada suure tihenduse (virtuaalsete IT-süsteemide suhe virtualiseerimisserveritesse). Ent operatsioonisüsteemi virtualiseerimisega ei saa enamasti ühes serveris virtuaalsete süsteemidena koos käitada erinevaid operatsioonisüsteeme, sest virtuaalsed IT-süsteemid kasutavad virtualiseerimisserveri operatsioonisüsteemi tuuma ja tarkvarateeke. Ühe operatsioonisüsteemiperekonna piires on see mõnede toodete puhul siiski ka osaliselt võimalik.

Virtuaalsed IT-süsteemid ei ole üksteisest nii tugevalt isoleeritud kui serveripõhisel virtualiseerimisel. Näiteks kasutatakse tarkvarateeke ühiselt ning virtuaalsed IT-süsteemid kasutavad ühe ja sama operatsioonisüsteemi tuuma. Lisaks pole virtuaalsed IT-süsteemid sageli kas üldse või on väga nõrgalt kapseldatud, sest need kasutavad virtualiseerimisserveri tark- ja riistvarakomponente. Operatsioonisüsteemi virtualiseerimisega kaasnev virtuaalsete IT-süsteemide nõrk kapseldus viib selleni, et erineva kaitsevajadusega virtuaalseid IT-süsteeme ei saa niisama lihtsalt ühes serveris koos käitada. Seevastu serveripõhisel virtualiseerimisel on olukord enamasti hoopis teine, sest selle korral on virtuaalsed IT-süsteemid palju tugevamalt kapseldatud. See, kas erineva kaitsevajadusega virtuaalseid IT-süsteeme saab käitada koos ühes virtualiseerimisserveris või mitte, ei olene

üksnes rakendatavast tootest, vaid ka organisatsiooni, täpsemalt virtuaalsete IT-süsteemide erinõuetest ja -ohtudest. Seetõttu tuleb juba planeerimise käigus hinnata, kas kõne alla tulev virtualiseerimistehnoloogia sobib erineva kaitsevajadusega virtuaalsete IT-süsteemide käitamiseks ühes virtualiseerimisserveris või mitte.

Virtualiseerimistoote valimine
Kui virtualiseerimistehnoloogia on välja valitud, tuleb analüüsida reaalsete toodete sobivust konkreetse kasutusvaldkonna jaoks. Selle valdkonna olulised nõuded tulenevad näiteks virtuaalkeskkonnas vajaminevatest protsessorite liikidest ja funktsioonidest ning vajalike seadmeemulatsioonide ja liideste käideldavusnõuetest.

Juba võimalikult varajases planeerimisetapis tuleks analüüsile tuginedes ära otsustada ka see, millist tehnoloogiat kasutatakse virtuaalsete IT-süsteemide ühendamiseks arvutuskeskuse võrguga. Selleks saab valida kas serveri füüsiliste võrgukaartide ühendamise virtuaalsete IT-süsteemidega või virtuaalsete süsteemide ühendamise nn virtuaalse kommutaatoriga. Sellest valikust oleneb, kuidas rakendatakse meetmetes M 2.141 Võrgukontseptsiooni väljatöötamine ja M 5.61 Sobiv füüsiline segmenteerimine ning M 5.62z Sobiv loogiline segmenteerimine . Nii on juba varajases tööetapis teada, mis nõuded kehtivad nii virtualiseerimisserveri ülesehituse kui ka selle juurde kuuluva taristu kohta. Pärast seda, kui töökeskkonnale esitatavad nõuded on teada, saab nende põhjal välja valida sobiva virtualiseerimislahenduse ja sellega hästi ühilduvad IT-süsteemid.

Arvutuskeskuseülene planeerimine
Ühes virtualiseerimisserveris saab käitada suurt hulka virtuaalseid IT-süsteeme. Nendes virtuaalsetes IT-süsteemides, mis on enamasti erinevate operatsioonisüsteemidega töötavad serverisüsteemid, saab omakorda käivitada suurt hulka erinevaid rakendusi. Nendel rakendustel on jällegi tarvis suurt hulka baasteenuseid, nt DNS-i, autentimiseks vajalikke kataloogiteenuseid või andmebaasiteenuseid. Seetõttu peab virtualiseerimisserveritel olema juurdepääs kõikidele nendele ressurssidele, mida läheb tarvis kas virtualiseerimisserveril endal või mõnel virtuaalsel IT-süsteemil. Virtualiseerimisprojekti planeerimisel tuleb arvestada allnimetatud aspektidega.

Virtualiseerimisserveritel on tarvis:

- füüsilisi ühendusi kõikide võrkudega, mille keskkonnas virtuaalseid IT-süsteeme käitatakse;
- ühendusi salvestusvõrkudega, et tagada juurdepääs massmälu komponentidele;
- juurdepääsu taristutele, nt DNS- ja DHCP-serveritele ning kataloogiteenuse serveritele.

Seetõttu tuleks virtualiseerimislahenduse planeerimisse võimalikult vara kaasata ka kõik nende teenuste eest vastutavad administraatorirühmad. Nii saab projektis juba algusest peale kasutada nende oskusteavet ja nad saaksid ka ise sõnastada projekti jaoks vajalikke nõudeid.

Töörollide ja vastutusalade planeerimine

Kuna virtualiseerimisserverid võimaldavad sageli virtuaalsetel IT-süsteemidel ja nendes süsteemides käitatavatel rakendustel pääseda juurde arvutuskeskuse põhiteenustele, nt võrkudele ja salvestusvõrkudele, moodustavad virtualiseerimisserverid virtuaalsete IT-süsteemide vaatevinklist ka ise osa arvutuskeskuse taristust. Seetõttu on soovitatav võrkude ja salvestusvõrkude juurdepääse reguleerivaid ettekirjutusi ja nõudeid kohandada virtuaaltaristu vajadustega. Näiteks kui salvestivõrgu segmenteerimisele ja salvestusressursside juurdepääsule on kehtestatud meetmest M 5.130 Salvestisvõrgu (SAN-i) kaitse segmenteerimise abil lähtuvad nõuded, tuleb tagada, et neid nõudeid saaks rakendada ka virtuaaltaristus. Virtualiseerimisserverite juurdepääs salvestusressurssidele peab olema võimalikult laialdane. Need serverid peavad ilmtingimata ise juurde pääsema väga paljude virtuaalsete IT-süsteemide salvestusressurssidele, sest muidu ei saaks nad virtuaalsetele IT-süsteemidele võimaldada nende ressursside kasutamist. Ent siiski tuleb järgida ka moodulisse B 3.303 Salvestisüsteemid ja salvestivõrgud kuuluvate meetmete nõudeid. Meetmeid peaks siinkohal siiski saama võtta rakendatava virtualiseerimistehnoloogia vahenditega. See tähendab, et virtualiseerimisserveri administraatoritel on kohustus tegelda nüüdsest ka selliste tööülesannetega, millega varem tegelesid üksnes salvestivõrgu või -komponentide administraatorid. Sama kehtib võrguadministraatorite tööülesannete kohta. Virtuaalsete IT-süsteemide ühendused infokoosluse erinevate võrkudega määratakse virtualiseerimisserveris kindlaks virtualiseerimisserveri administraatorite poolt, sest nemad defineerivad virtuaalsete IT-süsteemide ja virtualiseerimisserveri füüsiliste võrguühenduste seosed. See on traditsiooniliselt olnud võrguadministraatorite töö. Juhul kui ühes virtualiseerimisserveris soovitakse käitada erinevate võrkude virtuaalseid IT-süsteeme, peavad korrektsete võrguseoste ja nende seire eest vastutama virtualiseerimisserveri administraatorid. Lisaks tuleb tagada, et virtualiseerimisserveris käitatavate virtuaalsete IT-süsteemide puuduv kapseldus ja isolatsioon ei õõnestaks eesmärki, mis püstitati võrgu segmenteerimisega: suurendada turvet süsteemide jaotamisega arvutuskeskuse eri valdkondadesse. Seetõttu tuleb virtuaaltaristu planeerimisel, juhul kui see on vastava virtualiseerimislahenduse puhul vajalik, otsustada, kuidas hakkavad virtualiseerimisserveri administraatorid täitma võrgu- ja salvestivõrguadministraatorite tööülesandeid. Lisaks tuleb analüüsida, kas virtualiseerimisserverite administraatorid võiksid võrguühenduste ja salvestivõrguühenduste haldamisega seotud töid delegeerida võrgu- ja salvestivõrguadministraatoritele. Kehtivate reeglite rakendamise kohustus ja vastutus peab olema reguleeritud väga selgelt ja täpselt.

Taristu kohandamine virtualiseerimisega

Klassikalistes infokooslustes on serverid ühendatud sageli ainult ühe, harva ka mitme võrguga. Kui aga virtualiseerimisserveris soovitakse käitada erinevates võrkudes paiknevaid virtuaalseid IT-süsteeme, tuleb virtualiseerimisserver ühendada ilmtingimata mitme võrguga.

Seetõttu on soovitatav võtta moodulite B 3.302 Marsruuterid ja kommutaatorid ja B 4.1 Heterogeensed võrgud :

- M 2.141 Võrgukontseptsiooni väljatöötamine
- M 2.142 Võrguplaani väljatöötamine
- M 4.81 Võrgutoimingute audit ja logimine

- M 4.206 Kommutaatori portide turvamine
- M 5.61 Sobiv füüsiline segmenteerimine
- M 5.62z Sobiv loogiline segmenteerimine
- M 5.77z Alamvõrkude rajamine

ning kohandada neid virtualiseerimisserveri eripära ja nõuetega. Siinkohal tuleb arvestada, et virtualiseerimisserverid peavad suutma virtuaaltaristus täita kõikide virtuaalsete IT-süsteemide ühenduspöördusi. Näiteks kui kommutaatori portides kasutatakse MAC-filtreid (vt M 4.206 Kommutaatori portide turvamine), tuleb nende filtrite konfiguratsiooni kohandada virtuaaltaristu nõuetega. Kui neid filtreid ei kasutata, ei saa virtuaalseid IT-süsteeme, millel on mõne virtualiseerimistehnoloogia puhul olemas ka enda MAC-aadress, niisama ühest virtualiseerimisserverist teise ümber tõsta. Kuna seda funktsiooni läheb aga tarvis virtuaalsete IT-süsteemide jaotamiseks virtualiseerimisserveris, et parandada süsteemi jõudlust, võib selline olukord, kus filtreerimisreeglid jäetakse kohandamata, ohustada virtuaalsete IT-süsteemide käideldavust.

Virtualiseerimistehnoloogiate kasutamisest tingitud lisanõuetega tuleb kindlasti arvestada ka moodulisse B 3.303 Salvestisüsteemid ja salvestivõrgud kuuluvate meetmete võtmisel:

- M 2.525 Salvestisüsteemide turvapoliitika väljatöötamine
- M 4.275 Salvestisüsteemide turvaline kasutamine
- M 5.130 Salvestisvõrgu (SAN-i) kaitse segmenteerimise abil

Virtualiseerimisserveri kasutuse planeerimine

Kasutuse planeerimisel tuleb meetme M 2.315 Serveri kasutuselevõtu planeerimine kõrval arvestada ka täiendavate eripäradega. Need eripärad tekivad sellest, et virtualiseerimisserveris on enamasti tarvis korraga käitada mitut virtuaalset IT-süsteemi. Seetõttu tuleb välja selgitada, kui palju läheb virtuaalsete IT-süsteemide tööshoidmiseks tarvis protsessorivõimsust, põhimälu ja vaba kõvakettaruumi. Samuti tuleb välja selgitada, milliseid võrguühendusi läheb virtualiseerimisserveri ja virtuaalsete IT-süsteemide jaoks tarvis (vt M 5.135 Turvaline meediatransport SRTP abil).

Sobivate virtualiseerimisserverite valimiseks tuleb välja selgitada, kui suurt jõudlust ja kui palju ressursse planeeritud virtuaalsed IT-süsteemid vajavad. Selle teabe põhjal on võimalik kindlaks määrata vajaminev virtualiseerimisserverite arv ja nende võimsus. Aktiivselt käitatavate füüsiliste IT-süsteemide migreerimisel virtuaalkeskkonda ei piisa tegeliku ressursivajaduse hindamiseks virtualiseeritavate IT-süsteemide ressursivajaduse kokkuliitmisest. Jõudluse arvutamiseks tuleks hoopiski virtualiseeritavaid süsteeme mõõta ja tuletada mõõdetud füüsiliste serverite jõudlusnäitajate põhjal virtualiseerimisserverile esitatavad jõudlusnõuded.

Ressursside planeerimisel ei tohi piirduda mitte üksnes kõikide virtuaalmasinate ressursivajadusega, vaid arvesse tuleb võtta ka virtuaaltaristu ressursivajadusi, mida läheb tarvis virtualiseerimistarkvara tööshoidmiseks. Selle tagajärjel suureneb massmälu vajadus, nt läheb massmälu tarvis virtualiseerimisserveri ekraanitõmmiste, seisundilogide ja saalimisfailide salvestamiseks. Protsessori- ja põhimäluressurssi kasutatakse ka virtualiseerimisserveri hypervisor'i jaoks.

Katsetus- ja arenduskeskkondades võib eelloetletud nõuetest ka kõrvale kalduda. Selliste keskkondade planeerimisel tuleb arvestada, et ei tekiks soovimatuid vastastikmõjusid tootmissüsteemidega. Seetõttu tuleb katsetuskeskkonnad tootmiskeskkondadest piisavalt eraldada.

Virtuaaltaristu käideldavus

Virtualiseerimisserveri planeerimise käigus on soovitatav arvestada, et käideldavusnõuded võivad osutuda tavapärasest rangemaks, sest virtualiseerimisserveris käitatakse suurt hulka IT-süsteeme. Kui virtualiseerimisserver peaks lakkama töötamast, ei tööta seejärel ka enam ükski selles serveris käitatav IT-süsteem. Kõikide virtualiseeritud IT-süsteemide käideldavusnõuded kanduvad üle virtualiseerimisserverile (kumulatsiooni põhimõte). Seetõttu on oluline analüüsida, kas virtualiseerimisserverite jaoks tuleks valida kõrgkäideldav või veatolerantne arhitektuur või kas mitmest virtualiseerimisserverist loodud virtuaaltaristus peaksid olema mehhanismid, mis kompenseeriksid ühe või ka mitme virtualiseerimisserveri töö katkemise.

Kontrollküsimused:

- Kas virtualiseerimisserverite ja virtuaalsete IT-süsteemide kasutamise reeglid on kooskõlas IT-süsteemide, rakenduste, võrkude ja salvestivõrkude kasutusreeglite ja -suunistega?
- Kas erinevate administraatorirühmade (rakenduste-, serveri-, võrgu- ja salvestivõrguadministraatorite) tööülesanded on selgelt üksteisest lahutatud?
- Kas vastutus virtuaaltaristu komponentide (virtualiseerimisserverite, virtuaalsete IT-süsteemide, salvestivõrgu, võrgu) eest on selgelt määratletud ning kas vastutavatel töötajatel on olemas piisavad tehnilised lahendused?
- Kas virtuaaltaristu on piisava liiasusega, et vastata käideldavusnõuetele?

M 2.478 Mac OS X turvalise kasutuse planeerimine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: infoturbespetsialist, administraator

Mac OS X süsteemide reguleeritud ja turvaline juurutamine eeldab ulatuslikku planeerimist. Selles meetmes keskendutakse projekti sujuvaks juurutamiseks olulistele tarkvaraaspektidele. Maci süsteemi riistvarakomponendid on Apple'i ette antud ja seega piisavalt ülevaatlikud. Suur erinevus varasemate ja praeguste Maci süsteemide vahel seisneb aga protsessoris. Alates versioonist Snow Leopard (10.6) ei toeta Mac OS X enam PowerPC tüüpi protsessorite kasutamist. Mac OS X 10.6-t ei saa installida vanematesse Apple'i arvutitesse, milles puudub Inteli CPU. Kui PowerPC-dega Apple'i arvutitelt soovitakse üle minna Inteli protsessoriga Apple'i arvutitele, tuleb kontrollida, kas tegu on universaalsete rakendustega, st nendega, mis töötavad nii PowerPC kui ka Inteli protsessoritega arvutites. Platvormi vahetamisel, st mõne teise operatsioonisüsteemi vahetamisel Mac OS X vastu, tuleb samuti kõigepealt kontrollida, kas Mac OS X jaoks on saadaval samad või samaväärsed rakendused ning kas nende puhul on tagatud koostöö juba olemasolevate süsteemidega (nt Lotus Domino või Microsoft Exchange'i serveriga). See ei puuduta üksnes neid rakendusi, mida käitatakse otse kliendis, vaid ka serverirakendusi, mille puhul kehtivad teatud eeldused. Näiteks vajab osa veebipõhistest rakendustest ActiveX-i. ActiveX-i Mac OS X-s kasutada ei saa. Tarkvara, mis Mac OS X-ga ei ühildu, saab käitada tarkvara virtualiseerimislahendusega. Seda võib siiski pidada vaid hädavariandiks, sest ühelt poolt seab see suuremaid nõudmisi riistvarale ning teiselt poolt on see palju keerulisem kui rakenduse käitamine virtualiseeritud keskkonnas. Olemasolevate tarkvaralitsentsilepingute puhul tuleks kontrollida, kas need hõlmavad ka Mac OS X süsteeme. Kui ei hõlma, tuleb edaspidi litsentsilepinguid sõlmides tähelepanu pöörata ka sellele, et valitaks tarkvara, mida saaks käitada erinevatel platvormidel, st sõlmida litsentsilepingud, mis lubavad tarkvara käitada ka teistel platvormidel. Mac OS X-ga töötavate süsteemide juurutamisel tuleb kontrollida ka seda, kas olemasolev väline riistvara, nt printerid, plotterid, kaardilugejad ja muud seadmed, ühilduvad Mac OS X-ga ning kas nende seadmete jaoks on olemas vajalikud draiverid. Samuti tuleb kontrollida, kas seadmed toetavad Mac OS X-s kasutatavaid võrguprotokolle, mida läheb tarvis erinevate IT-süsteemide ühendamiseks. Näiteks kui jagatud võrgu failisüsteemina kasutatakse Andrew File Systemi (AFS) protokolli, tuleb juba varem välja valida Mac OS X-ga kokku sobiv klient.

Kasutajate kontseptsioon

Kasutajate kontseptsiooniga määratakse kindlaks, milliste volitustega peavad kasutajad täitma oma tööülesandeid. Kasutajate kontseptsiooni koostamisel tuleb vahet teha lokaalsete ja domeeniüleste kasutajakontode vahel. Nii lokaalsete kui ka domeeniüleste kasutajakontodega seotud volitusi tuleb väljastada võimalikult suurte piirangutega. Sel viisil vähendatakse kasutajakonto tahtlikust või ka tahtmatust väärkasutusest tingitud kahju. Mac OS X-s tuleb iga kasutaja jaoks luua igapäevatöös kasutatav standardsete kasutajaõigustega konto. Kui Mac OS X kliendid integreeritakse kataloogiteenusega, tuleks järgida moodulit B 5.15 Üldine kataloogiteenus . Juhul kui tegu on heterogeense võrguga, mille kataloogiteenuse alusena kasutatakse Windowsi serverit, tuleb arvestada ka mooduliga B 5.16 Active Directory .

Haldamiskontseptsioon

Haldamiskontseptsioon tuleb koostada enne Mac OS X juurutamist, kui seda

pole veel tehtud. Haldamiseks tuleb ette näha kahe erineva konto kasutamine. Mac OS X eristab kasutaja- ja administraatorikontosid. Töötaja, kes on end sisse loginud kasutajakontosse, ei saa muuta süsteemi seadistust, installida rakendusi kõikidele ligipääsetavatesse kataloogidesse ega teisi kasutajakontosid hallata. Seevastu administraatorikontodel on kõik need volitused olemas. Võimaluse korral peaksid administraatorid kasutama oma töös standardkasutaja õigustega kasutajakontot. Administraatorivolitustega kontot tuleks kasutada vaid juhtudel, kus standardsest kasutajakontost enam ei piisa. Mac OS X-s on administraatorivolitusi nõudvad tööd märgistatud väikse tabaluku sümboliga. Tabaluku sümboli peal klõpsates küsib süsteem administraatori pääsuandmeid ning pärast nende sisestamist saab teha administraatorivolitusi nõudvaid muudatusi. Kui tööd on tehtud, peaks administraator uuesti klõpsama tabaluku sümbolil, et ennast administraatorivolitustega kontost välja logida ja standardvolitustega kontos edasi töötada. Erilahendusena on Mac OS X-s ka *root* -konto, mis on standardseadistuses desaktiveeritud. Administraatorikonto ja *root* -konto erinevad teineteisest selle poolest, et administraatorikonto ei anna õigust kustutada andmeid olulistest süsteemikaustadest. Nii saab administraator küll süsteemi laialdaselt ümber seadistada, kuid mitte tervet operatsioonisüsteemi täielikult kasutuskõlbmatuks muuta. Ent administraatorikontoga töötades on võimalik aktiveerida ka *root* -konto. Seetõttu ei piisa süsteemifailide juhusliku kustutuse vältimiseks üksnes *root* -konto desaktiveerimisest.

Logimiskontseptsioon

Rünnete ja ebareeglipäraste sündmuste tuvastamiseks tuleks sisse lülitada süsteemi logimisvõimalused ja neid ka kasutada. Meetmed M 4.106 Süsteemi logimise aktiveerimine (Unix) ja M 4.25 Logimine Unix-süsteemis kehtivad ka Mac OS X kohta, sest see põhineb Unixil. Logimisfunktsiooni mõistlikuks kasutamiseks tuleks esmalt analüüsida, millised Mac OS X-ga töötava kliendi programmid on olulised. Kõik tööprotsesside jaoks olulised rakendused tuleks siduda võimalikult suure logimisastmega, et kõik (hoiatus)teated saaksid logitud. Nii on tõrke tekkimisel ka piisavalt infot vea kõrvaldamiseks. Näiteks kui klienti kasutatakse peamiselt meilide saatmiseks, tuleks kõik meiliprogrammi tööga seotud teated suunata mõnda kesksesse kohta, kus neid ka analüüsitakse.

Andmete talletamine, varundamine ja krüpteerimine

Tuleb kindlaks määrata koht, kuhu kasutajate andmed salvestatakse (vt M 2.138 Struktureeritud andmetalletus). Juhul kui kõik olulised andmed salvestatakse serveritesse, võib klientarvuti lokaalsete kõvaketaste krüpteerimisest loobuda. Nii saab ka andmete varundamist rakendada tsentraalselt, mis tähendab, et ka lokaalsest andmevarundusest on võimalik loobuda. Need võimalused sõltuvad aga väga tugevalt kohapealsetest oludest. Näiteks kui ühes kliendis rakendatakse mõnda spetsiaaltarkvara, mille funktsiooni taastamine võimaliku defekti korral tähendab väga palju tööd, tuleks siiski regulaarselt varundada konkreetset klienti. Lisateavet andmevarunduse kohta leiate meetmetest M 6.146 Andmete varundamine ja taastamine Mac OS X klientsüsteemides ja M 6.32 Regulaarne andmevarundus ning moodulist B 1.4 Andmevarunduspoliitika . Kaasaskantavate arvutite puhul tuleb rakendada vähemalt ajutist lokaalset andmetalletust. Selleks tuleb planeerida kliendi andmetalletus ja selle (krüptograafiline) kaitse (vt M 4.29 Kaasaskantavatele IT-süsteemidele mõeldud krüpteerimistoote kasutamine) . Juhtudel, kus piisab kasutajakataloogi krüpteerimisest, võib kasutada FileVaulti (vt M 4.372 FileVaulti kasutamine Mac OS X-s). Kui turbe seisukohast olulisi andmeid salvestatakse mujale kui kasutaja kettaajamitele, tuleks ka need krüpteerida. Lisateavet

andmete turvalise talletamise ja transportimise kohta leiate meetmest M 4.379 Andmete turvaline talletamine ja transportimine Mac OS X-s . Tavapärasest suurema kaitsevajaduse korral sellisest kaitsest enamasti ei piisa ja tuleb kasutada täiendavaid turvarakendusi, nt krüpteerimisprogrammi, mis krüpteerib kogu kliendi kõvaketta.

Täiendavad kontrollküsimused:

- Kas on tagatud, et administraatorid kasutavad kõikide haldamisega mitteseotud tööülesannete täitmiseks väheste õigustega kasutajakontot?
- Kas Mac OS X jaoks on olemas kasutajate ja haldamiskontseptsioon?
- Kas Mac OS X jaoks rakendatakse logimiskontseptsiooni?

M 2.479 Mac OS X turvapoliitika planeerimine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: IT-juht, administraator

Mac OS X kasutuselevõtu üks olulisim töökorralduslik ülesanne on asjakohase Mac OS X turvapoliitika kavandamine ja sõnastamine. See turvapoliitika peaks lähtuma meetmest M 2.322 Klient-server-võrgu turvapoliitika kehtestamine ja määrama kindlaks Mac OS X klientide puhul rakendatavad turvanõuded. Kõik kasutajad ja muud isikud, kes on seotud klientide soetamise ja käitamisega, peavad seda turvapoliitikat tundma ning sellest oma töös juhinduma. Nagu kõikide suuniste puhul, tuleb ka turvapoliitika sisu ja rakendamist regulaarselt üldise auditi käigus kontrollida. Mac OS X turvapoliitikas sõnastatud nõuded rakendatakse ellu operatsioonisüsteemi turvaseadistustega. Neil juhtudel, kus üksnes tehniliste meetmete võtmisest turbe tagamiseks ei piisa, tuleb neid täiendada ja toetada töökorralduslike meetmetega. Võimaluse korral tuleks töökorralduslikele meetmetele alati eelistada tehnilisi lahendusi. Turvapoliitika peab lähtuma ettevõttes või ametiasutuses seni kehtinud turvapoliitikast ja ei tohi sellega vastuollu minna. Mac OS X turvapoliitika koostamine hõlmab enamasti olemasolevate suuniste mugandamist või täiendamist. Sealjuures tuleb ilmtingimata pöörata tähelepanu sellistele Mac OS X spetsiifilistele tehnoloogiatele nagu FileVault ja Time Machine. Mac OS X taristu planeerimisel tuleb üldjuhul lähtuda institutsiooniülesest turvapoliitikast. Samas peab toimima ka nn tagasiside, st alamvaldkonna turvapoliitika mõjutab omakorda institutsiooniülest turvapoliitikat. Mac OS X turvapoliitika koostamisel on oluline jälgida, et tööde käigus arvestataks kõikide seadustest tulenevate ettekirjutustega. Mac OS X turvapoliitika tuleb dokumenteerida ja klient-server-võrgu kasutajatele vajalikus mahus teatavaks teha. Seda turvapoliitikat peaksid tundma ja rakendama kõik administraatorid. Järgnev teemade loetelu annab üldise ülevaate valdkondadest, mida tuleks käsitleda vastava turvapoliitika väljatöötamisel. Olenevalt institutsiooni konkreetsetest kasutusvaldkondadest tuleb muidugi arvestada veel ka lisaaspektidega.

Konfigureerimis- ja haldusstrateegia

Esmalt tuleks otsustada, kas konfigureerimise ja halduse üldstrateegia on oma olemuselt liberaalne või piirav, sest kõik edasised otsused olenevad suurel määral sellest valikust. Tavapärase turbevajadusega klientide puhul võib valida suhteliselt liberaalse üldstrateegia, mis lihtsustab enamasti ka nende konfigureerimist ja haldamist. Siiski on ka niisugustel kasutusjuhtudel soovitatav, et strateegia oleks ainult nii liberaalne, kui see on parasjagu vajalik. Suure turbevajadusega klientide puhul võiks üldjuhul eelistada piiravat strateegiat. Kui kliendi kas või ainult ühe põhiväärtuse – konfidentsiaalsuse, käideldavuse või tervikluse – turbevajadus on väga suur, tuleks kliendile kindlasti valida piirav konfigureerimis- ja haldusstrateegia.

Füüsiline turvalisus

Mac OS X turvapoliitika koostamisel tuleb käsitleda ka füüsilist turvalisust, sest neid operatsioonisüsteeme kasutatakse muu hulgas ka kaasaskantavates arvutites. Füüsilise turvalisuse tagamiseks tuleb rakendada moodulis B 3.201 Klient esitatud soovitusi.

Vastutusalad

Mac OS X turvapoliitikas peavad sisalduma Mac OS X süsteemide käitamisega tegelevate töötajate vastutusalad. Iga administraatori puhul tuleb kindlaks määrata tema konkreetne vastutusala. Erinevad vastutusalad võivad olla näiteks järgmised:

- turvaparameetrite muutmine;
- logiandmete analüüs;
- pääsu- ja süsteemiõiguste andmine;
- paroolide vahetamine ja deponeerimine;
- andmete varundamine ja andmete taastamine varukoopiatest.

Kui klient-server-võrgu puhul antakse kasutajatele õigused ka haldustoimingute tegemiseks, peavad administraatorite kõrval vastutust kandma ka kasutajad. Tavaliselt piirdub selline vastutus siiski vaid pääsuõiguste määramisega enda failidele, juhul kui need tuleb eraldi määrata ja hierarhias kõrgemal asuva kataloogi eelseadistused neile ei kehti. Lõppkasutajaid tuleb koolitada, et nad teaksid, kui suur on iseseisvalt haldustoiminguid tehes nende vastutus ja mille eest nad vastutavad. Seevastu süsteemide haldusega peaksid siiski tegelema vaid piisava koolituse saanud võrguadministraatorid. Hädaolukorraks valmisoleku planeerimise raames tuleb tagada ka sobiv töötajate asendamise kord.

Side turvalisus

Turvapoliitika peab käsitlema ka andmeedastuse turvet. Turvapoliitika koostamisel on soovitatav esmalt sõnastada andmeedastuse põhinõuded (eesmärk) ning seejärel töötada välja erinõuded, mis lähtuvad kohapealsetest konkreetsetest oludest. Siinkohal tuleb tähelepanu pöörata eelkõige autentsus-, konfidentsiaalsus- ja käideldavusnõuete täitmisele. Tuleb otsustada, millised Mac OS X süsteemi võrguteenused tehakse kättesaadavaks teistele IT-süsteemidele. Kuna igast aktiveeritud võrguteenusest võib saada rünnete sihtmärk, tuleks teenuste valikul piirduda miinimumiga. Ebavajalike võrguteenuste väljalülitamise kohta leiate lisateavet meetmest M 5.165 Mac OS X mittevajalike võrguteenuste desaktiveerimine . Nõuete täitmisel tuleks arvestada ka Mac OS X enda töölaua tulemüüri kasutamise võimalusega (vt M 5.166 Mac OS X isikliku tulemüüri konfiguratsioon *).*

Krüpteerimine

Tuleb otsustada, kas, millist infot ja kuidas krüpteeritakse. Andmeid on soovitatav krüpteerida eelkõige kaasaskantavates IT-süsteemides. Mac OS X tarkvara hulka kuulub ka FileVault, millega saab krüpteerida kasutajakatalooge. Lisateavet FileVaulti kohta leiate meetmest M 4.372 FileVaulti kasutamine Mac OS X-s . Selle asemel võib kõvaketta täielikuks krüpteerimiseks kasutada ka kolmandate tootjate tarkvara. Krüpteeritud failisüsteemide rakendamiseks tuleks koostada eraldi kontseptsioon ja võimalikult täpselt dokumenteerida kõik konfiguratsiooni üksikasjad, sest vastasel juhul võivad krüpteeritud failisüsteemis hoitavad andmed näiteks krüptovõtme või paroolifraasi kaotuse või väärkonfiguratsiooni korral jäädavalt kaotsi minna.

Andmevarundus

Andmekadude ennetamiseks tuleb kõikidest olulistest Mac OS X klientide andmetest teha regulaarselt varukoopiaid. Selleks tuleb kindlaks määrata andmete salvestuskoht ja andmevarunduse sagedus. Need otsused tuleb kaasata üleorganisatsioonilisse andmevarunduse kontseptsiooni, st need otsused ei tohi sellega vastuollu minna. Andmete varukoopiaid tuleb vigade suhtes regulaarselt kontrollida. Lisateavet Mac OS X andmevarunduse kohta leiate meetmest M 6.146 Andmete varundamine ja taastamine Mac OS X klientsüsteemides .

Logimine

Nagu paljud teisedki Unixi süsteemid, pakub ka Mac OS X palju võimalusi turbesündmuste (nt õnnestunud ja/või ebaõnnestunud sisselogimiskatsete) logimiseks. Eeltööna tuleb langetada järgmised otsused:

- millised sündmused logitakse?
- kuhu salvestatakse logifailid?
- kuidas ja kui sageli analüüsitakse logisid?

Logimisfunktsiooni seadistuse kindlaksmääramisel tuleb arvestada süsteemiseire üldkontseptsiooniga. Unixi süsteemide logimise kohta leiate lisateavet meetmetest M 4.106 Süsteemi logimise aktiveerimine (Unix) ja M 4.25 Logimine Unix-süsteemis .

Täiendavad kontrollküsimused:

- Kas Mac OS X jaoks on olemas turvapoliitika?
- Kas Mac OS X turvapoliitika lähtub ettevõttes või ametiasutuses juba varem koostatud turvapoliitikast?
- Kas Mac OS X turvapoliitika on kasutajatele vajalikus mahus teatavaks tehtud?
- Kas Mac OS X turvapoliitika käsitleb kõiki olulisi valdkondi?

M 2.480w Exchange'i ja Outlooki dokumentatsiooni kasutamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator, arendaja

Microsoft on teinud enda TechNet Service'i veebilehel (http://technet.microsoft.com) kättesaadavaks suure hulga tasuta teavet. Sellelt veebilehelt võib leida Microsofti toodete dokumentatsioone, online- juhendeid, kasutusjuhendid jms. Lisaks viidatakse Microsofti TechNetis sageli ka teistele teabeallikatele.

Järgnevalt on esitatud mõningad näited:

- Microsofti TechNetis antakse juhiseid lisatarkvara kasutamise kohta. Enekõike tuleks pöörata tähelepanu turbeteabele, mida võib leida menüüst „Security". Olulised on ka Microsofti toodete turvajuhised, mis on kättesaadavad menüüst „Download Center". Selle meetme raames on eriti vajalikud valdkondade „Messaging" ja „Collaboration" turvajuhised.
- Arendajatele vajaliku teabe jaoks on loodud eraldi keskkond Microsoft Developer Network (http://msdn.microsoft.com). Selle kasutamine eeldab registreerimist, kuid on kasutajale siiski tasuta.

Exchange'i serveriperekonda kuuluvate toodete kõige värskema online- dokumentatsiooni leiate Microsofti TechNetist vastava versiooni alt. Kogu vajaliku teabe saab alla laadida Exchange Server TechCenterist. Sama kehtib ka Microsoft Outlooki dokumentatsiooni kohta, mille leiab Office TechCenterist. Turvet käsitlevate dokumentide ja juhiste korral viidatakse allikale Security Compliance Management Toolkit, mis sisaldab kõige uuemaid turvajuhiseid, turvalise installimise juhiseid, seirejuhiseid ning muid dokumente ja abimaterjale.

Outlook 2010 puhul sisaldab see näiteks järgmist:

- Versiooni Microsoft Outlook 2010 oluline dokumentatsioon, allalaaditavad materjalid ja juhised asuvad rubriigis „Outlook 2010 Ressource Kit" („Office 2010 Beta Resource Kit"). Infoturbe aspekte käsitletakse rubriigis „Security and protection for Office 2010 Beta".

Kontrollküsimus:

- Kas administraatorid teavad kõige uuemat Microsoft Exchange'i ja Microsoft Outlooki online -dokumentatsiooni?

M 2.481 Exchange'i kasutuse planeerimine Outlook Anywhere'i jaoks

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator, IT-juht

Outlook Anywhere võimaldab kasutajatel Exchange'ile juurde pääseda interneti kaudu. Tegemist on serveris töötava edastusteenuse, mitte klienttarkvaraga. Kuna internetis aset leidev andmeedastus on rünnetele palju vastuvõtlikum kui sisevõrgus toimuv andmeedastus, on soovitatav valida selline turbestrateegia, mis kaasaks protsessi võimalikult palju turvafunktsioone.

SSL-i kasutamine Outlook Anywhere'i jaoks

Kui Exchange'i andmetele soovitakse interneti kaudu juurdepääsemiseks kasutada Outlook Anywhere'i, tuleb installida kehtiv SSL-i sertifikaat (Secure Sockets Layer), mille on väljastanud klientarvuti operatsioonisüsteemi jaoks usaldusväärne sertifitseerimiskeskus (Certification Authority – CA).

SSL- offloading 'u kasutamine Outlook Anywhere'i jaoks

Juhul kui kasutatakse SSL-i proksit, mis tagab klientpöörduste serveri krüpteerimise SSL-iga, peab Outlook Anywhere'i jaoks olema korrektselt konfigureeritud nn SSL- offloading . Nii luuakse kogu ühendus SSL-iga täielikult SSL-i proksi abil, mis säästab väärtuslikku ribalaiust ja muid ressursse.

Autentimise konfigureerimine Outlook Anywhere'i jaoks

Outlook Anywhere'i autentimiseks tuleb välja valida sobiv autentimismeetod. Vältida tuleks olukorda, kus korraga on konfigureeritud nii standardne autentimine kui ka Windowsi autentimine, kusjuures viimane neist on turvalisem. Selle nõude konkreetne täitmine näeb versiooni 2010 puhul välja järgmine:

- Outlook Anywhere'i turvalise kasutuse tagamiseks tuleb järgida Microsofti TechNeti veebilehti, mis käsitlevad teemat „Understanding Security for Outlook Anywhere: Exchange 2010 Help". Konfiguratsiooniseaded leiate rubriigist „Managing Outlook Anywhere: Exchange 2010 Help", kus käsitletakse peamiselt aktiveerimist, desaktiveerimist, autentimist, krüpteerimist SSL-iga ja sertifikaatide haldamist.

Täiendavad kontrollküsimused:

- Kas Outlook Anywhere'i rakendamisel kasutatakse kehtivat SSL-i sertifikaati?
- Kas Outlook Anywhere'i jaoks on korrektselt konfigureeritud SSL- offloading ?
- Kas Outlook Anywhere'i jaoks on välja valitud ja konfigureeritud sobiv autentimismeetod?

M 2.482 Exchange'i süsteemide regulaarsed turvakontrollid

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator, revident, infoturbespetsialist

Microsoft Exchange'i süsteemi turvalisust on pikemas perspektiivis võimalik tagada ainult piisavate regulaarsete kontrollidega, mis tuvastavad väärkonfiguratsioone ja teisi kitsaskohti. Turvakontrolle peaksid tegema erinevad inimesed kindla intervalliga. Näiteks peaksid administraatorid kontrolle läbi viima suhteliselt lühikeste ajavahemike tagant (umbes kord kuus). Et kontrollimisprotseduur lähtuks kindlatest põhimõtetest, on soovitatav välja töötada kontrollnimekiri. Administraatorid saavad väiksemad tuvastatud probleemid enamasti ise kohe ära lahendada, suurematest probleemidest tuleb aga teavitada vajalikke instantse vastavalt nende jaoks kehtestatud protseduurireeglitele. Keskmise pikkusega ajavahemike tagant (mitme kuu möödudes) peaksid turvakontrolle tegema mõned teised organisatsioonisisesed töötajad (infoturbeosakonna töötajad, IT-revidendid). Pikkade ajavahemike tagant oleks mõistlik lasta teha kontrolle väljaspool enda organisatsiooni töötavatel isikutel. Kontrollide puhul tuleb arvestada alltoodud aspektidega.

Turbeinfo regulaarne kogumine

Administraatorid ja infoturbe eest vastutavad töötajad peavad ennast regulaarselt kursis hoidma nende vastutuse alla kuuluvate süsteemide võimalike muudatuste ja uuendustega. Selleks tuleb regulaarselt tutvuda eelkõige Microsofti teabeallikatega (vt M 1.1 Vastavus normidele ja eeskirjadele).

Revidentide kasutajakontode volitused

Kasutajakontodele, mis võimaldavad organisatsioonivälistel isikutel kontrollida süsteemi konfiguratsiooni, tuleks volituste määramisel anda vaid lugemisõigused. Revisjoni jaoks loodud kasutajakontodel ei tohi olla muudatuste tegemise õigust. Juhul kui revisjonide jaoks loodud kasutajakontode volitusi ei ole võimalik piirata lugemisõigusega, tohib juurdepääsu neile lubada vaid siis, kui järgitakse neljasilmapõhimõtet.

Volituste regulaarne kontrollimine

Exchange'i süsteemi volituste täiemahuline käsitsi kontrollimine pole üldjuhul võimalik, sest nende hulk on selleks liiga suur. Seetõttu on ilmtingimata tarvis, et oleks välja töötatud sobiv volituste kontseptsioon. Ent ka siis, kui see kontseptsioon on olemas, tuleb siiski regulaarselt kontrollida, kas volituste sisu langeb kontseptsiooniga kokku. Selleks võib olulistes kasutajarühmades teha pistelisi kontrolle. Volituste kontseptsioon peaks tagama sellised protsessid, mis suudaksid tõkestada volituste kokkukuhjamist. Kasutajate volitusi tuleb regulaarselt kontrollida.

Kontrollide puhul on oluline järgnev turbeteave:

- Kriitiliste volitustega kasutajad
- Kasutajate volitusi tuleb võrrelda volituste kontseptsiooniga.
- Kasutajate, rollijaotuse, rollide, profiilide ja volituste muudatuste tõendamine
- Siinkohal tuleks eriti hoolikalt kontrollida võimalikke muudatusi administratiivsetes objektides.

Värskenduste värskuse kontrollimine

Microsoft Exchange'i süsteemi installitud värskenduste puhul tuleb kontrollida nende värskust. Süsteemi installitud paikade (patches) versioone tuleb võrrelda saadaolevate paikadega. See eeldab, et kontrollija teab, millised paigad on Microsoft süsteemi jaoks juba avaldanud. Kontroll peab tuvastama ka värskendustega seotud vead ja hoiatavad süsteemiteated.

Sideliideste turvalisuse kontrollimine

Kontrollida tuleks erinevate sideliideste turvalisust (vt M 5.100 Exchange'i süsteemi siseneva ja väljuva side kaitse). Eriti hoolikalt tuleb siinkohal kontrollida, kellele on antud administraatorivolitused ning mis teenuseid ja funktsioone on võimalik kasutada.

Kontrollküsimused:

- Kas Exchange'i süsteemis tehakse regulaarselt turvakontrolle?
- Kas Exchange'i volitusi kontrollitakse regulaarselt vähemalt pisteliselt?
- Kas Exchange'i süsteemi on installitud kõige värskemad paigad?

M 2.483 Exchange'i süsteemide turvaline kohandamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

Kohandamisel konfigureeritakse ja muudetakse rühmatarkvarasüsteemi selliselt, et see vastaks institutsiooni erivajadustele. See protseduur nõuab enamasti küllaltki palju aega.

Turbe seisukohast tuleb arvestada järgmisega:

- Mugandamise (customizing) jaoks tuleb koostada eraldi kontseptsioon, milles kirjeldatakse võimalikult täpselt rühmatarkvarasüsteemi soovitud lõppseisundit. Samas kontseptsioonis tuleb kirjeldada ka mugandamiseks vajalikke tööprotsesse. Kontseptsioon tuleb kooskõlastada infoturbeosakonnaga.
- Kohandamisega võivad tegelda ainult piisavate erialateadmistega ja usaldusväärsed isikud.
- Rühmatarkvarasüsteemi konfiguratsioone ei tohi kohandada tootmissüsteemis, vaid katsetuskeskkonnas.
- Kohandamiseks tuleb juurutada protsessid, mis annaksid tegevuse kohta piisavat tagasisidet ja võimaldaksid kontseptsiooni kohandamise käigus vajaduse korral ka muuta.

Kontrollküsimused:

- Kas Microsoft Exchange'i kohandamise jaoks on koostatud kohandamiskontseptsioon?
- Kas Microsoft Exchange'i süsteemi kohandab selleks koolitatud personal?
- Kas on tagatud, et mugandamiseks vajalikke muudatusi ei tehtaks otse tootmissüsteemis?

M 2.484 OpenLDAP planeerimine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: IT-juht, administraator

OpenLDAP kasutuselevõttu institutsioonis tuleb hoolikalt planeerida. OpenLDAP kasutuse planeerimisel tuleb alati lähtuda meetmest M 1.1 Vastavus normidele ja eeskirjadele . Selle meetme põhjal langetatud otsustest, eelkõige sellest, kuidas hakatakse OpenLDAP-d kasutama, tulenevad ka OpenLDAP-le esitatavad nõuded. Konkreetne planeerimistöö oleneb kasutatavast taristust. OpenLDAP planeerimisel tuleb arvestada vähemalt järgmiste punktidega:

- Integreerimine teiste rakendustega
- OpenLDAP puhul eksisteerib suur hulk võimalusi, kuidas ja milleks seda teiste rakenduste või operatsioonisüsteemidega integreerida, nt:
- kasutajate haldamiseks Unixi ja Linuxi süsteemides saab kasutada Pluggable Authentication Module'i (PAM) ja Name Service Switchi (NSS);
- heterogeensetes võrkudes saab seda kasutada tsentraalse kataloogiteenusena või koos Active Directoryga, kui kasutatakse Sambat (vt B 5.17 Samba);
- aadressiraamatu ja sertifikaadikataloogina sellistes meiliprogrammides nagu Microsoft Outlook või Mozilla Thunderbird (vt B 5.3 Rühmatarkvara). Kui OpenLDAP-d soovitakse kasutada koos teiste rakendustega, tuleb nende planeerimine, konfigureerimine ja installimine kindlasti OpenLDAP-ga kokku sobitada. Selleks tuleb paralleelselt võtta erinevaid asjakohaseid IT-etalonturbe meetmeid. Teiste rakendustega integreerimise kohta leiate teavet ka rubriigi „OpenLDAP Frequently Asked Questions" (http://www.openldap.org/faq) eraldi lõigust asukohas Faq-O-Matic | OpenLDAP Software FAQ | Integration .
- Toimivate sõltuvussuhete tagamine. Selleks et OpenLDAP saaks täita kõiki standardi LDAPv3 kohaseid kataloogiteenuse funktsioone, peab OpenLDAP kindlasti juurde pääsema teiste rakenduste funktsioonidele. See kehtib eriti andmetalletuseks kasutatava Berkeley DB kohta, mille jaoks on OpenLDAP-d spetsiaalselt optimeeritud. Kõikide OpenLDAP funktsioonide täielik kasutuselevõtt saavutatakse vaid koostöös selle hierarhilise andmebaasiga. Siinkohal tuleb arvestada, et Berkeley DB ja OpenLDAP on kaks teineteisest sõltumatult välja arendatud tarkvararakendust. OpenLDAP vajab oma tööks Berkeley DB versiooni, millel on OpenLDAP tugi. Ülevaate OpenLDAP toega Berkeley DB versioonidest leiate OpenLDAP Administrator's Guide'i (http://www.openldap.org/doc) lisast „Recommended Versions". Samast lisast saate muu hulgas teavet ka teiste OpenLDAP tööks vajalike tarkvarapakettide kohta. Nendes materjalides nimetatud nõudeid tuleb järgida, eriti puudutab see Transport Layer Security mõne variandi, nt OpenSSL-i või GnuTLS-i installimist ning Simple Authentication and Security Layersi (Cyrus-SASL) installimist. Võimalikku alternatiivi GnuSASL-i OpenLDAP versioon 2.4 veel ei toeta. Ilma nende kahe toetava rakenduseta ei suuda OpenLDAP standardile LDAPv3 täiel määral vastata. Kui aga autentimist soovitakse kaitsta Kerberosega, tuleb installida kas Heimdali Kerberos või MIT Kerberos. Administrator's Guide'i lisas kajastatud kataloogiteenuse side jaoks mõeldud turbetarkvarast TCP Wrappers tuleks siiski loobuda ja eelis-

tada sellele mõnda muud, IP-filtril põhinevat lahendust (vt M 4.238 Lokaalse paketifiltri rakendamine).

- Konfiguratsioonimeetodi valimine. OpenLDAP toetab alates versioonist 2.3 kaht konfiguratsioonimeetodit. Klassikaline konfiguratsioon toimub staatiliselt konfiguratsioonifailiga (slapd.conf), mille serveriprotsess slapd käivitamisel endale sisse loeb. Uuemat konfiguratsioonimeetodit nimetatakse online -konfiguratsiooniks ja selle puhul salvestatakse konfiguratsiooniseadistused kataloogipuu spetsiaalsesse alasse („slapd.config").

Online-konfiguratsiooni eelised on:

- Online -konfiguratsiooni muudetakse LDAP operatsioonidega ja neid saab teha võrguühenduse kaudu, ilma et oleks tarvis juurdepääsu OpenLDAP-d käitava IT-süsteemi failisüsteemile.
- Haldustöid saab teha lihtsasti käsitsetava graafilise LDAP Clientiga.
- Online -konfiguratsiooni seadistust saab muuta ka serveri töö ajal ja muudatused rakenduvad kohe, st serveriprotsessi slapd ei ole tarvis taaskäivitada.
- Konfiguratsioon on võimalik kataloogi osana replikeerida teistesse serveritesse – see lihtsustab jaotatud kataloogiteenuste haldamist. Tänu sellele rakenduvad kõikides kooslusse kuuluvates serverites palju kiiremini näiteks pääsuõigustes tehtud muudatused. Samas tuleb jällegi arvestada, et kõik back-end 'id ja overlay 'd ei toeta online -konfiguratsiooni.

Staatiline konfiguratsioon kaitseb ka läbimõtlemata muudatuste tegemise eest ja piirab seeläbi turvaintsidentide teket. OpenLDAP planeerimisel tuleb valida, millist konfiguratsioonimeetodit kasutatakse, ning seejärel tuleb seda ka läbivalt ühtmoodi rakendada. Online -konfiguratsioon on seda mõttekam:

- mida laiaulatuslikum on kataloogiteenus,
- mida suuremad on selle käideldavusnõuded,
- mida rohkem servereid jaotatud kooslusse kuulub.
- kasutatavate back-end 'ide valik. Installimiseks ja konfigureerimiseks vajalike back-end 'ide valik oleneb kataloogiteenuse planeeritud kasutusvaldkonnast. Lisateavet back-end 'ide valiku kohta leiate meetmest M 2.485 Back-end 'ide valimine OpenLDAP jaoks .
- kasutatavate overlay 'de valik. Nii nagu back-end 'ide puhul, tuleb ka overlay 'de jaoks koostada nimekiri, milliseid neist hakatakse kasutama. Overlay 'de kasutamise üle otsustades tuleks läbi töötada OpenLDAP Administrator's Guide'i teemakohane peatükk. Iga overlay puhul tuleb eraldi kontrollida, kas see on eksperimentaalne või kas selle edasiarendamine on lõpetatud. Mõlemal juhul tuleks vastava overlay kasutamist tootmiskeskkonnas vältida. Lisaks tuleb iga overlay puhul asjakohasest dokumentatsioonist (nt Manpage) uurida, kas see toetab online -konfiguratsiooni. Overlay 'de valimisel tuleb arvestada, et nende käivitamise järjekord (nn virnastamine) võib mõjutada funktsioonide tööd. Näiteks võib see juhtuda olukorras, kus üks overlay muudab andmeid, kuid mõni teine overlay vajab neid siiski nende algsel kujul.

Kindlaksmääratud puustruktuuri tagamine Kataloogiteenuse planeerimisel määrati kindlaks selle struktuur, mis tulebki võtta OpenLDAP planeerimise aluseks:

- Tuleb välja valida sobiv nimemudel, juhul kui seda ei ole juba üldise planeerimise raames tehtud. X.500 standardi klassikaline nimemudel järgib organisatsiooni struktuuri ja kasutab selliseid nimetajaid nagu OrganizationalUnit (OU), Organization (O) ja Country (C) (nt OU = ria, O = riigiamet, C = ee). Selle kõrval rakendatakse aina rohkem ka interneti stiili järgivat nimemudelit. Selle nimemudeli puhul kasutatakse puustruktuuri ülemistel tasanditel vaid domeenikomponente DomainComponents (DC) ja selle koosteosi erinevalt ei tähistata (nt DC = ria, DC = riigiamet, DC = ee).
- Nimemudeli ja soovitud struktuuri jaoks tuleb välja valida sobivad skeemid. Need määravad kindlaks, mis andmeid andmebaasi millisel kujul salvestatakse ja millised on nende andmete seosed. OpenLDAP-s on kõik RFC-des defineeritud skeemid juba olemas ning lisaskeemid on saadaval internetis. Olemasolevatest skeemidest peaks tavakasutuseks enamasti piisama. Kui aga skeeme on tarvis laiendada, tuleb seda teha ülimalt ettevaatlikult, sest sellest sõltub kataloogiteenuse töö.
- OpenLDAP võimaldab overlay 'dega muu hulgas ka objektide atribuute piirata. Sel juhul jätab vastavalt konfigureeritud slapd-server skeemide põhjal objektidele lubatud toimingud täitmata (vt M 4.386 Atribuutide piiramine OpenLDAP puhul).
- Skeemid võivad osutuda vajalikuks ka olenemata sellest, milline puustruktuur on kindlaks määratud. Skeemid võimaldavad back-end 'idel ja overlay 'del, mis salvestavad oma andmeid LDAP vahendusel või LDIF-andmevormingus, töötada ilma vigadeta. Näiteks back-end nimega backmonitor vajab oma tööks skeemi nimega core.schema. Selliseid võimalikke sõltuvussuhteid tuleb kontrollida komponentide dokumentatsioonist ja nendega ka arvestada.
- OpenLDAP puustruktuuri kindlaksmääramiseks tuleb muu hulgas ära otsustada, kas dünaamilisi objekte overlay 'ga dds (dynamic directory services) lubatakse või mitte. Sellised objektid kustutatakse pärast defineeritud aja möödumist või teatud sündmuste mitteesinemisel kataloogiteenusest automaatselt. Overlay 'ga dynlist (dynamic lists) saab lisaks moodustada dünaamilisi rühmi. Dünaamilisi rühmi ei sisustata käsitsi, vaid need sisaldavad automaatselt kõiki objekte, mis vastavad defineeritud otsingukriteeriumile. Nii saab ilma suurema vaevata näiteks sisse seada rühmi ja loendeid, mis hõlmavad kõiki ühe korruse töötajaid. Dünaamilisi loendeid saab kasutada ka pääsuõiguste kontrollimiseks (vt M 4.387 OpenLDAP pääsuõiguste turvaline andmine) . Siinkohal tuleb olla ettevaatlik, sest ühelt poolt võib haldustööde maht küll väheneda, kuid teisalt võib pääsuõigustest kaduda täpne ülevaade.
- Kasutajapöörduste planeerimine. Vältida tuleb kasutajate juurdepääsu anonüümsete kasutajakontodega. Kui anonüümne juurdepääs on siiski hädavajalik, peaks kataloogiteenus sisaldama vaid madala turbeastmega andmeid. Kui juurdepääsu on tarvis võimaldada madala turbeastmega alamvaldkonnale, kuid kataloogiteenus sisaldab kõrgema turbeastmega andmeid, on soovitatav sisse seada kaks slapd-serveri teenust, millest üks võimaldab anonüümset juurdepääsu ja sisaldab vaid madala turbeastmega andmeid. Seda olukorda võib muu hulgas lahendada ka replikatsioonidega (vt M 4.389 OpenLDAP partitsioonid ja replikatsioonid) . Selleks replikeeritakse töötajate andmeid sisaldavast kataloogiteenusest ainult töötaja nimi ja avali-

kus telefoniraamatus kajastuv telefoninumber. Kasutajapöörduste planeerimise alla kuulub ka administraatorite vastutuse kindlaksmääramine. Näiteks võivad kataloogiteenuse erinevate andmebaaside eest vastutada erinevad administraatorid (vt M 2.407 Kataloogiteenuste administreerimise planeerimine).

Kliendi kasutamise planeerimine. OpenLDAP kasutamise planeerimisel ei tohi piirduda slapd-serveriga, vaid tuleb arvestada ka klientide valiku ja toetamisega. Sobivad rakendused on OpenLDAP-s saadaval ldap*-tööriistadena. Neid tööriistu juhitakse siiski üksnes käsuviibaga. Need eeldavad suuremahulisi koolitusi ja töötajad ei soovi neid enamasti kasutada. Praktikas kasutatakse enamasti graafilisi tarkvaratööriistu või lahendusi, kus klient on integreeritud rakendusega. Kui aga kataloogiteenuseid juhitakse LDAP-ga, võidakse olenevalt olukorrast kasutada ka selliseid klientprogrammi rakendusi, mille omadustega tuleb arvestada ka OpenLDAP planeerimisel. Samuti võib olla mõttekas panna slapd-server täitma funktsioone, mida LDAP spetsifikatsioon ette ei näe, kui klientidel asjakohased funktsioonid puuduvad. Selliseid funktsioone võimaldavad OpenLDAP-s kasutada overlay 'd:

- Overlay 'ga chain (chaining) võimaldatakse serveril iseseisvalt järgida referral 'eid (st viiteid hierarhias kõrgemal asetsevatele serveritele, replikatsioonidele jms), selle asemel et teatada kliendile aadress, mille alt see saaks ise neid otsida.
- Overlay 'ga valsort (value sorting) väljastab server otsingutulemused kliendile juba sorteeritud järjekorras.
- Jõudluse seadmine

Planeerimisel tuleb arvestada ka vajaliku jõudlusega, sest see võib väga tugevalt mõjutada käideldavust. Eelkõige tuleks välja selgitada kõige sagedamini otsitavad atribuudid.

Täiendavad kontrollküsimused:

- Kas OpenLDAP toetab kasutatavat Berkeley DB versiooni?
- Kas OpenLDAP puhul on võetud arvesse selle sõltuvussuhet teiste rakendustega ja kas asjakohased nõuded on täidetud?
- Kas OpenLDAP jaoks valitakse välja nõuetele vastavad back-end 'id ja overlay 'd?
- Kas OpenLDAP overlay 'sid kasutatakse õiges järjekorras?
- Kas OpenLDAP planeerimisel arvestatakse õigete klientrakenduste valiku ja toega?

M 2.485 Back-end 'ide valimine OpenLDAP jaoks

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: IT-juht, administraator

Installimiseks ja konfigureerimiseks vajalike *back-end* 'ide valik oleneb kataloogiteenuse planeeritud kasutusvaldkonnast:

- Kui OpenLDAP-ga hallatakse üht või ka mitut andmebaasi otse, tuleb välja valida *back-end* , mis sobib vastava andmetalletuse jaoks. Andmete haldamisel on OpenLDAP optimeeritud andmebaasihaldussüsteemi (DBMS) Berkeley DB kasutamiseks. Berkeley DB jaoks on olemas kaks *back-end* 'i: back-bdb ja selle edasiarendus back-hdb. *Back-end* back-hdb koormab IT-süsteemi küll rohkem ja seab suuremaid nõudmisi andmete vahesalvestamiseks kasutatavale andmesalvestile, kuid sel on rohkem funktsioone ning see võimaldab kataloogistruktuuri sees terveid osapuid ümber nimetada (*subtree renaming*). OpenLDAP arendusmeeskonna lähiperspektiiv näeb ette *back-end* 'ist back-bdb loobumist. Seepärast on soovitatav OpenLDAP uusinstallatsioonide puhul kasutada *back-end* 'i back-hdb.
- OpenLDAP suudab *back-end* 'iga back-ldif andmeid salvestada ka LDAP Data Interchange Formati (LDIF) andmevormingus. LDIF-andmevormingu puhul salvestatakse kogu andmebaas loetava teksti vormis tekstifailina. Seda liiki andmetalletus ei sobi suurte andmehulkade ja paljude kasutajate korral. *Online* -konfiguratsiooni puhul on aga back-ldif siiski hädavajalik, sest sufiks CN=config salvestatakse alati LDIF-andmevormingus.
- OpenLDAP-d saab kasutada täielikult või osaliselt, proksina, teiste LDAP-serverite jaoks. Sel juhul läheb tarvis kas *back-end'* i back-ldap või selle edasiarendust back-meta. Erinevalt *back-end* 'ist back-ldap on back-meta võimeline samal ajal tegema pöördusi mitmesse serverisse. *Back-end* 'il back-meta on rohkem funktsioone, kuid see-eest on seda ka palju keerulisem konfigureerida. Enamiku kasutusjuhtude korral piisab *back-end* 'ist back-ldap.
- *Back-end* 'i back-ldap läheb alati tarvis siis, kui slapd-server käivitab ise ldap operatsioone. Sellega on tegu näiteks juhul, kui slapd-server tühistab iseseisvalt viiteid või kui replikeerimiseks kasutatakse *push* -režiimi.
- Lisaks on mõeldav, et OpenLDAP kasutab relatsioonilise andmebaasi andmeid. Selleks läheb tarvis *back-end* 'i back-sql. Siinkohal tuleb arvestada, et relatsiooniline andmebaas ei sobi kataloogiteenuse andmete täielikuks salvestamiseks. OpenLDAP ühendamine relatsioonilise andmebaasiga võib olla mõttekas vaid juhul, kui sellisest andmeallikast soovitakse välja lugeda üksikut lisateavet, nt ühes loendis kajastuvat telefoninumbrit kataloogiteenuses, mis haldab kõiki institutsiooni kasutajaid.
- Vajaduse korral kasutatakse OpenLDAP-d andmete hankimiseks enda väljatöötatud rakendustest või selliste rakenduste juhtimiseks. Juhul kui andmeside puhul ei järgita LDAP standardit, läheb olenevalt sellest, milline on enda arendatud rakenduse liides, tarvis ühte järgmistest *back-end* 'idest: back-perl, back-shell või back-sock.

- Kui otsustatakse, et OpenLDAP käitamist on vaja seirata (*monitoring*), saab vastavad funktsioonid kasutusele võtta *back-end* 'iga back-monitor (vt M 1.1 Vastavus normidele ja eeskirjadele *).*

Teised *back-end* 'id, mida siin ei ole nimetatud, tuleks planeerimisest välja jätta. Need on kas vananenud (back-ldbm, back-tcl), ainult katsetamiseks mõeldud (back-passwd, back-null) või sellised *back-end* 'id, millel on OpenLDAP versiooni 2.4 jaoks esialgu ainult eksperimenteerimise staatus (back-dnssrv, back-ndb, back-relay).

Täiendav kontrollküsimus:

- Kas tootmiskeskkonnas kasutatakse ainult OpenLDAP jaoks vajalikke back-end 'e?

M 2.486 Veebirakenduste ja veebiteenuste arhitektuuri dokumenteerimine

Algatamise eest vastutavad: arendusosakonna juht , üksikute IT-rakenduste eest vastutavad töötajad

Rakendamise eest vastutavad: arendaja, administraator

Veebirakenduste efektiivseks hooldamiseks, arendamiseks ja laiendamiseks on tarvis tunda nende tarkvara arhitektuuri. Süsteemi spetsiifikat kajastava dokumentatsiooni kõrval (vt M 1.1 Vastavus normidele ja eeskirjadele , M 2.31 Volitatud kasutajate ja õiguste profiilide dokumenteerimine ja M 2.34 IT-süsteemi muutuste dokumenteerimine) tuleb veebirakenduste dokumenteerimisel arvestada mõningate eripäradega. Dokumentatsioon peab hõlmama kõiki veebirakenduse koostisosi. Veebirakenduse spetsiifikat käsitlevas dokumentatsioonis peaksid sisalduma vähemalt järgmised punktid:

- kõik sõltuvussuhted (nt raamistikud, teegid, operatsioonisüsteemid, riistvara) ja liidesed (nt taustsüsteemidega);
- kõik käitamiseks vajalikud komponendid, mis ei kuulu veebirakenduse koostesse, tuleb selliselt ka tähistada (nt sellised taustsüsteemid nagu andmebaas);
- dokumentatsioonist peab olema võimalik välja lugeda, millised komponendid vastutavad turbe eest. Järgnevalt on loetletud veebirakenduse minimaalsed kohustuslikud turbefunktsioonid:
- kasutajahaldus,
- rollide ja volituste kontseptsioon,
- autentimine,
- volitused,
- seansihaldus,
- logimine,
- transportimise turve;
- kui veebirakendus on integreeritud mõne juba olemasoleva võrgutaristuga, peab dokumentatsioon kajastama ka seda (vt M 5.169 Veebirakenduse süsteemiarhitektuur).

Kajastada tuleb ka kõiki krüptograafilisi funktsioone ja protseduure, vt moodul B 1.7 Krüptokontseptsioon .

Dokumentatsiooni tuleb värskendada ja kohandada juba alates veebirakenduse arendusetapist, et seda saaks kasutada projektis võimalikult vara ja sellest oleks võimalik välja lugeda, mille põhjal vastavad otsused on tehtud.

Kontrollküsimused:

- Kas veebirakenduse või veebiteenuse tarkvara arhitektuur dokumenteeritakse?
- Kas veebirakenduse puhul on dokumenteeritud kõik selle koosteosad ja sõltuvussuhted?
- Kas käitamiseks vajalikud komponendid, mis ei ole veebirakenduse koosteosad, on asjakohaselt tähistatud?
- Kas dokumentatsioon kajastab, millised veebirakenduse ja veebiteenuse komponendid vastutavad milliste turvamehhanismide eest?

- Kas rakendatavad krüptograadilised funktsioonid ja protseduurid on dokumenteeritud?
- Kas veebirakenduse arhitektuur dokumenteeritakse juba arendustegevuse käigus?

M 2.487 Veebirakenduste arendamine ja laiendamine

Algatamise eest vastutavad: erialaspetsialist, üksikute IT-rakenduste eest vastutavad töötajad

Rakendamise eest vastutavad: arendajad, varujad, arendusosakonna juht, katsetajad

Rakenduste (sh veebirakenduste) tõhusaks arendamiseks tuleb kehtestada reeglid ja tagada, et neid ka järgitaks. Eesmärk on vältida või vähemalt võimalikult kiiresti tuvastada arendus- ja laiendustööde raames tekkivaid nii kontseptsioonilisi kui ka programmeerimisega seotud vigu. Rakenduste arendus- ja laiendustööde puhul tuleks arvestada alltoodud punktidega.

Kindla mudeli järgimine arendustöödel

Arendustöödel tuleks järgida mõnda sobivat töömudelit (nt V-mudel XT, kosemudel, spiraalimudel). Siinkohal on oluline, et enne rakenduse kasutuselevõttu läbiks rakendus kõik vastava mudeli tööetapid. Rakendatav töömudel peaks koosnema vähemalt järgmistest või neile sarnastest faasidest.

- Vajaduste analüüs - Rakendusele esitatavate nõuete kindlakstegemisel tuleb arvestada ettevõtte turvapoliitika ja teiste ettevõtte eripärasid kajastavate nõuetega ning asjakohane info tuleb arendusmeeskonnale ka kättesaadavaks teha (nt sellised tööstusstandardid nagu PCI DSS või teave erivajadustega töötajate kohta). Siia alla kuulub ka krüptograafiliste algoritmide kasutamise kohustus ja nende kasutusnõuded ning turvalise programmeerimise suunised. Selles etapis on esmalt tarvis välja selgitada, milliseid andmeid hakkab planeeritav rakendus töötlema, ning seejärel tuleb need andmed turbevajaduse alusel liigitada. Rakenduse jaoks tuleb kindlaks määrata sobivad turbemehhanismid, mis kaitseks andmeid nii, nagu nende turbevajadus seda eeldab.
- Kontseptsioon ja disain - Kontseptsiooni koostamisel tuleb kindlaks määrata ja dokumenteerida rakenduse arhitektuur ja ülesehitus. Siin tuleks välja valida ka sobivad arendustehnoloogiad (nt programmeerimiskeeled, raamistikud). Kulude kokkuhoidmiseks ja turvaaukude vältimiseks tuleks arvestada ka arendajate teadmiste ja kogemustega. Arhitektuuris peaksid erinevad komponendid (nt volitamine, autentimine) olema eelistatult moodulite kujul, mida on võimalik uuesti kasutada. Moodulite tsentraliseeritud käideldavus ja kasutamine aitavad vältida liiasust nõudvaid lahendusi ja lihtsustavad hooldamist. Klient-server-arhitektuuri (nt veebirakenduse) korral tuleks tsentraalsed turvamehhanismid võimalusel vähemalt serveris tööle rakendada. Arvestada tuleks sellega, et turbenõuete täitmiseks peab piisama üksnes turvamehhanismidest ning katsetuste tarbeks peavad turbenõuded olema dokumenteeritud. Vastuvõetud otsused tuleb dokumenteerida piisavalt detailselt, et dokumentatsiooni põhjal oleks hiljem lihtne rakendust edasi arendada.
- Arendamine - Rakendusse kuuluvate komponentide turvaliseks arendamiseks tuleb järgida programmeerimise jaoks kehtestatud turvasuuniseid.Tuleb võtta arvesse, et dokumentatsiooni on tarvis arendustöö käigus pidevalt täiendada (nt lisada lähteteksti kommentaare ja kasutada dokumen-

tatsiooni koostamist toetavaid tarkvaratööriistu). Nii tagatakse, et lähtetekst on hiljem arusaadav ka teistele, mitte ainult arendajatele endile.Juba arendatud tootelahenduste, kasutusest välja jäetud lahenduste ja lünkliku dokumentatsiooni vältimiseks tuleks dokumenteerida ka arendustööde ajalugu (nt revisjonisüsteemiga).

- Katsetused - Katsetuste puhul tuleb tööfunktsioonide kõrval tähelepanu pöörata ka turbefunktsioonide korrektsele toimimisele. Siia alla kuulub muu hulgas turvakomponentide, nt volitamis-, autentimis- ja filtreerimiskomponentide töö kontrollimine. Turvamehhanismide töö kontrollimiseks tuleks teha penetratsiooniteste ning tavapärasest suurema turbevajaduse korral ka lähtekoodi analüüse (vt M 5.150 Penetratsioonitestide läbiviimine). Enne rakenduse kasutuselevõttu ei tule kontrollida mitte üksnes tööfunktsioonide toimimist, vaid ka seda, kas rakenduse funktsioone on võimalik kasutada vääralt. Seda võib kontrollida penetratsioonitestidega. Kuna katsetuste käigus tuleks järgida neljasilmapõhimõtet, peavad neid teste tegema inimesed, kes ei ole osalenud rakenduse kontseptsiooni väljatöötamises ega ka rakenduse arendamises. Katsetusi tuleb alati teha katseandmetega, mitte reaalsete töö- ega kliendiandmetega. Veebirakenduste puhul tuleks katsetustel kontrollida, kas need vastavad rakendatud standardile (nt HTML-i standardile). Nii on võimalik vältida rakenduse ettenägematuid, veebilehitseja väärast interpretatsioonist tingitud kõrvalmõjusid. Väga kasulikuks võib osutuda katsetamine erinevate veebilehitsejatega. Katsetuste planeerimisel ja tegemisel tuleks arvestada meetmega M 2.62 Tarkvara vastuvõtuprotseduurid .
- Integreerimine ja tarkvara juurutamine (deployment) - Enne rakenduse kasutuselevõttu igapäevastes tööprotsessides tuleb rakendusele ja vajaduse korral ka taustsüsteemidele luua turvaline konfiguratsioon. Selleks peab arvesse võtma võimalikke ühendusi rakenduse ja taustsüsteemide vahel (nt identiteedimälud, andmebaasid). Enne rakenduse kasutuselevõttu tuleb muu hulgas kontrollida ka seda, kas transpordikanal on kaitstud.
- Andmete kaitsmine volitamata manipulatsioonide eest - Rakenduse tundlikke andmeid salvestatakse sageli taustsüsteemidesse. Seepärast peaks rakenduse ja võimalike taustsüsteemide turbeaste olema ühesugune. Kasutajatele tohiks juurdepääsu taustsüsteemidele võimaldada üksnes rakenduses selle jaoks defineeritud liidestega. Lisaks tuleb tagada, et kolmandatel isikutel ei oleks rakenduse juurutamisel (*deployment*) võimalik rakenduse andmeid manipuleerida.
- Hooldus - Rakenduse hooldamiseks peab olema välja töötatud hooldusprotsess, mis näeb muu hulgas ette ka rakenduse regulaarsed turbekontrollid, mille abil saab tuvastada võimalikke turvaauke ja saadaolevaid paikasid (*patches*). Kui rakendust laiendatakse või kohandatakse, tuleb arvestada, et sellised tegevused ei tohi pärssida turbefunktsioonide tõhusust. Nende tööde järel tuleb turvamehhanismid spetsiaalses katsetuskeskkonnas uuesti üle kontrollida.

Programmeerimissuuniste rakendamine

Programmeerimissuunised aitavad kindlaks määrata ühtlase programmeerimisstiili ning tagada ühtlast turbeastet (nt turvateekide kasutamisega). See võimaldab lähteteksti paremaks ja arusaadavamaks muuta. Suuniseid rakendades on lihtsam märgata vigu ja kitsaskohti ning vähendada rakenduse võimaliku hilise-

ma laiendamisega kaasnevaid kulusid. Programmeerimissuunised pole mõeldud mitte üksnes organisatsioonisiseseks kasutuseks, vaid neid tuleks rakendada ka arendustegevuste väljasttellimisel.

Pikaajaline planeerimine turbemehhanismide arendamisel

Turbemehhanisme kavandades ja arendades tuleks arvestada ka sellega, mis suunas võivad areneda nii ründetehnikad kui ka standardid (nt HTML-i standard). Näiteks peaks filtreerimiskomponent, mis filtreerib välja kahjulikuks liigitatud - *tag* 'e, filtreerima välja ka tundmatud *tag* 'id. Tundmatuid *tag* 'e võidakse tulevikus (nt uue HTML-i standardi kasutuselevõtul) kasutada veebirakenduse turbemehhanismidest möödahiilimiseks.

Toote eripäradega seotud turbefunktsioonid

Kui veebirakendust kasutatakse eranditult mõne spetsiaalse veebilehitsejaga (vajaduse korral ainult ühe kindla tootjafirma tootega), tuleks arvestada ka selle veebilehitseja tootjaspetsiifiliste turbefunktsioonidega.

Rakenduse arendustööde väljasttellimine

Väljasttellimisel tuleb tagada, et firma, kellega leping sõlmitakse, täidab arendustegevuse raames vajalikke turbenõudeid. Selleks võib kehtestada kas konkreetse töömudeli või nõuda programmeerimissuuniste järgimist. Kui suure turbeastmega rakenduse arendustööd tellitakse väljast, tuleks tagada, et lähtetekst (nt projekti arhiiv) kuulub tööde tellija halduskontrolli alla. Tööde tellijal peab olema võimalik rakenduse lähtetekstile mis tahes ajal juurde pääseda ja mõista lähtetekstis tehtud muudatusi.

Arenduskeskkonna kindlaksmääramine

Tootmis-, katsetus- ja arenduskeskkonda tuleb käitada erinevates süsteemides. Nende keskkondade jaoks tuleks valida erinevad pääsuandmed. Katsetuskontode puhul tuleks laialdasi volitusi võimaluse korral alati vältida. Arendus- ja katsetuskeskkondade vastu toime pandud ründed ei tohi mõjutada igapäevatööks kasutatavat keskkonda.

Täiendavad kontrollküsimused:

- Kas rakenduse arendamisel järgitakse sobivat töömudelit?
- Kas rakenduste arendustööde käigus järgitavad töömudelid katavad kõik arendustööde etapid ning kas kõik need etapid läbitakse enne rakenduse kasutuselevõttu?
- Kas rakenduste arendustööde tegemiseks kehtestatakse programmeerimissuunised?
- Kas rakenduste turbemehhanismide kavandamisel ja arendamisel arvestatakse tulevastest standarditest ja võimalikest ründemeetoditest tulenevate arengusuundumustega?
- Kas rakendustega seotud arendustööde puhul on arendus-, katsetus- ja tootmissüsteemid üksteisest lahutatud?
- Kas rakenduse jaoks tehakse penetratsiooniteste, mille käigus kontrollitakse rakenduse loogikat?
- Kas rakenduse penetratsioonitestide puhul järgitakse neljasilmapõhimõtet?

M 2.488w Web tracking

Web tracking 'u all peetakse silmas kasutajaandmete analüüsi, nt veebilehe kasutajate tegevuste jälgimist. Näiteks saab analüüsi põhjal kasutajatele kuvada neid huvitavat reklaami ning külastatavusstatistika põhjal hinnata erinevate sissekannete populaarsust ja veebilehte selle järgi optimeerida. Selleks logitakse veebilehtede vahendusel selliseid kasutajaga seotud andmeid nagu kasutaja asukoht, tehingu seisund (nt ostu sooritamine veebilehel) ja veebilehe külastatavus. Kui selliste andmete hankimiseks palgatakse mõni väline teenusepakkuja, tuleb arvestada, et sellistel firmadel on võimalik neid andmeid siduda ka teiste klientide ja veebirakendustega. Võimalik on luua rakenduseüleseid detailseid kasutajaprofiile. Kasutajaandmete kogumiseks võib kasutada:

- (püsivaid) küpsiseid;
- web bug 'e (ühe piksli suurused pildid, nt meili sees, mille eesmärk on koguda päringustatistikat);
- brauserite sõrmejälgi (nt sellised atribuudid nagu installitud lisaprogrammid, ekraani eraldusvõime, ajatsoon, User Agent , HTTP Header);
- IP-aadressi logimist.

Nimetatud viise võib omavahel ka kombineerida, et kasutajaid kindlamalt identifitseerida. Enne kasutajaandmete analüüsimist, eriti kui need andmed võimaldavad tuvastada kasutaja isikut või kui seda teenust soovitakse sisse osta, tuleb kontrollida selle tegevuse seaduspärasust.

M 2.489 Windows Server 2008 süsteemiseire planeerimine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht
Rakendamise eest vastutavad: administraator, erialaspetsialist, revident

Windows Server 2008-ga kaasnevad uuendused

Windowsi serverite puhul tuleb rakendada seire- ja logimispõhimõtteid (vt M 1.1 Vastavus normidele ja eeskirjadele). Windows Server 2008 juurutamisega võeti kasutusele täiesti uus sündmusprotokolli moodul. Logifaili on suurendatud kuni ühe petabaidini, kuid paremaks on muudetud ka logide koostamise kirjutusvõimsust. Sündmusprotokolli moodul on põhimõtteliselt võimeline töötlema ja salvestama kümneid tuhandeid sündmusi sekundis. Uues moodulis muudeti ka sissekannete vormingut. Varasema.evt asemel võeti kasutusele XML-i vorming.evtx.

Lisaks nimetatud muudatuste ja uute sündmuste kasutuselevõtu on veel kaks olulist uuendust:

- Sündmuste kogumine ühte tsentraalsesse Windowsi süsteemi. Alates versioonist Windows Server 2008 on võimalik sündmuste koopiad koguda ühte tsentraalsesse arvutisse.
- Sündmuste ID-de uus numeratsioon. Turvet kajastavate sündmuste identifitseerimisnumbreid (ID-sid) muudeti uues moodulis väärtuse 4096 võrra, nii nt vastab vanale numbrile 528 Edukas rakendamine uus ID numbriga 4634. Seda tuleks arvesse võtta juba olemasolevate sündmuse-ID-de puhul, nt nende analüüsimisel skriptidega.

Planeerimine

Planeerimisel tuleb arvestada järgmiste meetmetega, sest need moodustavad Windows Server 2008 konfiguratsiooni tuuma:

- M 2.64 Logifailide kontroll
- M 2.110 Andmeprivaatsuse suunised logimisprotseduurides
- M 5.9 Serveri logi

Alates Windows Server 2008-st on võimalik eeldefineeritud sündmusi kajastavate logide koopiaid koguda ühte tsentraalsesse Windowsi süsteemi ja neid seal ühtlustada. Enne vajaliku konfiguratsiooni tegemist tuleks analüüsida logisid edasi saatva ja koguva arvuti mõningaid põhiaspekte. Seirekonfiguratsiooni tegemiseks on tarvis nii andmeallikana toimivas kui ka andmeid koguvas arvutis aktiveerida vajalikud teenused. Selleks tuleb esmalt kindlaks määrata, millised Windowsi serverites esinevad sündmused edastatakse tsentraalsesse süsteemi. Alles seejärel saab sisse seada nn abonemendid (subscriptions).

Abonementidega tuleb kindlaks määrata seire alla kuuluvad lähtearvutid, sündmuste tüübid ja vajaduse korral ka päringufiltrid. Seejärel on võimalik kasutusele võtta ka abonementide laiendatud funktsioonid, nt ribalaiuse optimeerimine. Siinkohal tuleb kindlaks määrata, kas abonemendi tüübi käivitab kogumis- või lähtearvuti. Olenevalt olukorrast võib selle otsuse tõttu osutuda vajalikuks muuta tulemüü-

ri reegleid. Planeerimisele järgneva käitusfaasi puhul tuleks arvestada meetmega M 4.344 Windows Vista, Windows 7 ja Windows Server 2008 süsteemi seire .

Kontrollküsimus:

- Kas seire jaoks on kindlaks määratud, millised Windowsi serverites esinevad sündmused edastatakse tsentraalsesse süsteemi?

M 2.490 Hyper-V-ga virtualiseerimise planeerimine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator, IT-juht, erialaspetsialist

Hyper-V on Microsofti enda virtualiseerimislahendus, mis kasutab hypervisor'it. Hyper-V kasutamisel tuleb serverite puhul tingimata arvestada mooduliga B 3.304 Virtualiseerimine. Olenevalt virtuaaltaristu eripäradest on modelleerimisel mõnikord tarvis tegemist teha väga laialdaste sõltuvussuhetega. Virtualiseeritavate serverite (külaliste) kõrval tuleb virtuaalse võrgutaristu jaoks üles ehitada ka virtuaalsed aktiivsed võrgukomponendid. Lisaks virtualiseerimist käsitlevas moodulis kirjeldatud raamtingimuste on Hyper-V kasutust planeerides vaja arvestada ka süsteemi eripärade põhjal vastu võetud otsustega. Hyper-V installitakse Windows Server 2008 keskkonda rollina. Pärast installimist saab operatsioonisüsteem Hypervisori keskkonnas endale virtuaalmasina ülesanded.

Operatsioonisüsteem

n-ö degradeerub puhtaks halduskonsooliks ja sellega hakatakse haldama ressursse teiste virtuaalmasinate jaoks. Hyper-V planeerimisel tuleb erilist tähelepanu pöörata külalissüsteemide turbeastmele. Windows Server 2008 host -süsteemi ja haldusüksuse turbeaste saadakse külaliste maksimaalse ja kumuleeritud turbevajaduse põhjal. Kui süsteemi laiendatakse ja lisandub mõni uus külalissüsteem, võib see tekitada olukorra, kus host -süsteemi turbevajadust on vaja tagantjärele kohandada. Seetõttu tuleks juhtudel, kus laiendusi on võimalik juba ette näha, sellega ka arvestada. Kuna teatud funktsioone ja omadusi saab tagantjärele muuta kas üksnes suure vaevaga või ei saa seda üldse teha, tuleks nendega arvestada juba planeerimisel. See puudutab ennekõike Server Core'i installatsiooni (vt M 1.1 Vastavus normidele ja eeskirjadele), mida sobib kasutada tavapärasest suurema turbevajaduse korral, sest see pakub vähem ründevõimalusi.

Server Core'i installatsioonist tuleks loobuda vaid juhul, kui on ette teada, et külalissüsteemide turbevajadused ei osutu tavapärasest suuremaks. Kasutajaliidese puudumise kaaluvad sageli üles Hyper-V eelised, nt väiksem ressursitarve, väiksem vajadus turvapaikade järele, vähem ründevõimalusi ja kaugpöördust võimaldavad haldustööriistad. Server Core'i alternatiivina võib installida ka versiooni Hyper-V Server 2008 R2. See on Server Core'i piiratud versioon, mis toetab üksnes Hyper-V rolli kasutamist ja mille muudetud litsentsimudelis puuduvad sisseehitatud külalislitsentsid. Kuna Hyper-V serveris on võimalik kujutada tervet taristut koos võrguga, tuleks selle haldamiseks luua erinevad rollid – nii ei saa administraatorid liiga suuri volitusi. Meetmes M 5.153 Võrgu planeerimine virtuaalsete taristute jaoks kirjeldatakse näiteks võrgusegmentide lahutamist virtualiseeritud süsteemide kaupa. Terviksüsteemi administraator, kel on võimalik muuta virtuaalsete võrgukaartide ühendusi, on võimeline võrku lahutavaid mehhanisme välja lülitama (vt G 1.4 Kahjutuli).

Seda saab vältida administraatorirollide planeerimisega:

Hyper-V administraatorirollid peavad kattuma füüsiliste ressursside (SAN-i, võrguühenduste) volitustega. Administraatorirollide juurutamiseks Hyper-V-s pakub Microsoft volituste haldurit (Authorization Manager, azman.msc). Selle tööriistaga saab administraatorirollide defineerimiseks omavahel kombineerida erinevaid protsesse (nt väliste Etherneti portide seostamine) ja valdkondi (nt külalissüsteemide rühmad). Töörollid tuleb kindlaks määrata juba planeerimisfaasis.

Virtuaaltaristu jaoks tuleb koostada integreeritud andmevarunduse kontseptsioon, mis arvestaks Hyper-V süsteemi eripäradega. Hyper-V-s on andmevarunduseks olemas VSS Writer (Volume Shadow Copy Service), mis varundab muu hulgas ka külalissüsteemide metaandmeid. Selleks peab see ühilduma rakendatava andmevarundustarkvaraga.

Kontrollküsimused:

- Kas Hyper-V-ga loodava virtuaalkeskkonna planeerimisel arvestatakse ka selle võimaliku suureneva turbevajadusega?
- Kas Hyper-V-ga loodud virtuaalkeskkonnas sisse seatud administraatorirollid kattuvad füüsiliste ressursside (SAN-i, võrguühenduste) volituste struktuuriga?
- Kas Hyper-V-ga loodud virtuaalkeskkonna jaoks on koostatud servereid ja külalissüsteeme integreeriv andmevarunduse kontseptsioon?

M 2.491 Windows Server 2008 rollide ja turvamallide kasutamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: erialaspetsialist, administraator

Windows Server 2008-ga kaasnevad uuendused

Rollide ja turvamallide kasutamist on Windows Server 2008-s mõneti muudetud. Näiteks on muudetud administratiivsete mallide failivormingut (vt M 2.368 Administratiivsete mallide kasutamine), lisaks on tehtud muudatusi ja täiendusi peamiselt grupipoliitikaobjektide ja haldustööriistade valdkonnas. Kõikidel juhtudel tuleb esmalt kindlaks määrata, kuidas vastavaid malle süsteemide jaoks kasutada.

Server Manager

Rollide ja funktsioonide põhikonfiguratsioon tehakse tsentraalse tarkvaratööriistaga Server Manager. Seda on eelmiste versioonidega võrreldes tunduvalt paremaks muudetud. Ent INF-failivormingus malle või muid malle (templates) ei saa Server Manageriga siiski töödelda.

Security Configuration Wizard

Alates versioonist Windows Server 2008 kuulub süsteemi kindlate koosteosade hulka ka Security Configuration Wizard (SCW) (vt M 1.1 Vastavus normidele ja eeskirjadele). Samas jällegi on SCW olulisus alates Server Manageri juurutamisest märkimisväärselt vähenenud, sest Server Manager võimaldab tsentraalset juurdepääsu peaaegu kõikidele serveri konfigureerimise seadistustele. Lisaks saab SCW-s malle koostada ja hallata kas väga piiratud kujul või ei saa seda üldse teha. SCW-ga koostatud XML-faile on küll põhimõtteliselt võimalik ka grupipoliitikaobjektideks migreerida, aga see protsess on väga töö- ja ajamahukas. Seetõttu sobib SCW pigem nn eraldiseisvate (stand alone) süsteemide haldamiseks.

Starter-grupipoliitikaobjektid

Starter-grupipoliitikaobjekte saab kasutada konfiguratsioonimallide koostamise alusena. Alates versioonist Server 2008 kuuluvad need objektid grupipoliitikate haldussüsteemis kasutatavasse grupipoliitikate struktuuri. Siinkohal tuleb arvestada, et Windows Server 2008 R2-s ja Windows 7-s starteri tüüpi objekte alguses ei olnud. Need tarnis Microsoft alles tagantjärele. Starteri tüüpi grupipoliitikaobjekte ei saa otse töödelda. Malli muudetava versiooni kasutamiseks tuleb valida suvandi „Starter Group Policy Object” alt suvand „New Group Policy Object”. Selle suvandi kasutamisel kopeeritakse soovitud objekt Active Directorys grupipoliitikaobjektide kausta. Starter-grupipoliitikaobjekti põhjal koostatud uus grupipoliitikaobjekt sisaldab kõiki selles kasutatud administratiivsete mallide ja defineeritud väärtuste poliitikaseadistusi. Kõik domeenis olemasolevad starter-grupipoliitikaobjektid salvestatakse domeeni Sysvol-kaustas asuvasse StarterGPO-de kausta.

Security Compliance Manager

Mallide tsentraalseks haldamiseks saab kasutada Microsoft Security Compliance Manageri (SCM). Tegemist on Microsofti pakutava Security Solution Acceleratori koosteosaga. SCM ühendab endas selliseid varasemaid tööriistu nagu Security Compliance Management Toolkit ja GPOAccelerator. Neid tarkvaratööriistu ei arendata enam edasi ja nende turustamine on lõppenud. Microsofti värskendatud mallid on veebiliidese kaudu kättesaadavad. Lisaks saab kasutada teiste tootjate malle. SCM põhineb starter-grupipoliitikaobjektidel.

Tegemist on eri valdkondadele mõeldud standardseadistusi sisaldavate mallidega, mis jagunevad kahte rühma:

- Enterprise Client (EC) - Need mallid on mõeldud kasutamiseks ettevõtete standardsüsteemides, mis on domeeni liikmed. Liikmesserveri konfiguratsiooni jaoks vajaliku malli nimi on WS08R2-EC-Member-Server.
- Specialized Security – Limited Functionality (SSLF) - Seda tüüpi mallid sobivad tavapärasest suuremate turbenõuetega süsteemidele, kus turbe suurendamiseks piiratakse olemasolevate funktsioonide kasutust. Tavapärasest suuremate turbenõuetega serverisüsteemides tuleb kasutada malli nimega WS08R2-SSLF-Member-Server.

SCM-i põhiülesanded on järgmised:

- turvaseadistuste tsentraalne haldamine nn baseline 'idena;
- domeeni turvaseadistuste tsentraalne haldamine;
- kolmandate tootjate baseline 'ide kasutamine;
- baseline 'ide eksportimine.

Security Compliance Manageriga saab koostada ja eksportida järgmisi vorminguid:

- Desired Configuration Management (DCM) Packs;
- ecurity Content Automation Protocol (SCAP);
- XLS (eeldab Excel 2007-t);
- Group Policy Objects (GPO).

Siinkohal tuleb arvestada, et töödelda tohib üksnes mallide koopiaid. Samuti tuleb kõiki Windows Server 2008 turvamalle hallata ja töödelda mõnes tsentraalses kohas. Valitud turvaseadistused tuleb dokumenteerida. SCM-i juurutamisega võeti baseline 'id tagantjärele kasutusele ka Windows 7-s, Windows Server 2008 R2-s ja Microsoft Office 2010-s. Kõikide süsteemide ja toodete puhul kehtib jätkuvalt EC- ja SSLF-mallide eristamise nõue. Lisaks Security Compliance Manageri installatsiooni saab kasutada ka lisatööriista LocalGPO, mis koostab lokaalsetest poliitikatest GPO varukoopiad (backups). Need varukoopiad sobivad ka teiste süsteemide aluskonfiguratsiooniks. Sama tööriist võimaldab ka vastupidist protsessi, st GPO varukoopiate muundamist lokaalseteks poliitikateks. Kui LocalGPO-d soovitakse kasutada, tuleb see vastava MSI paketiga tagantjärele juurde installida.

Kontrollküsimused:

- Kas Windows Server 2008 turvamalle hallatakse ja töödeldakse mõnes tsentraalses kohas?
- Kas mallide jaoks on kindlaks määratud kriteeriumid, kuidas neid erinevates süsteemides kasutada?
- Kas Windows Server 2008 jaoks väljavalitud turvaseadistused on dokumenteeritud?

M 2.492 Lotus Notesi/Domino keskkonna integreerimine olemasoleva turvataristuga

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: erialaspetsialist, administraator

Lotus Notesis/Dominos on olemas enda turvamehhanismid ning kasutada saab ka täiendavaid turvakomponente (nt spetsiaalselt Lotus Notesi/Domino jaoks kohandatud viirusetõrjetarkvara või spämmifiltreid). Institutsioon, kes planeerib Lotus Notesi/Domino esmakordset kasutuselevõttu (või Lotus Notesi/Domino platvormi uuendamist), peab ilmtingimata pöörama tähelepanu ka sellele, kuidas Lotus Notesi/Domino turvamehhanisme olemasoleva turvataristuga õigesti integreerida, et vältida nn turvasaarekesi. Selleks tuleb eelkõige kohandada Notesi/Domino keskkonna jaoks olulisi võrguüleminekuid, nt turvalüüse, *content scanner* 'eid, *content filter* 'eid ja viirusetõrjetarkvara, et need vastaksid Lotus Domino protokollide ja teenuste kasutamisest tingitud erinõuetele. Samas tuleb arvestada, et Lotus Notesi/Domino enda turvamehhanisme saab omakorda kasutada ka teiste turvakomponentide kohandamiseks ja perimeetriturbe probleemide kõrvaldamiseks. Seetõttu tuleb Lotus Notesi/Domino turvamehhanismide koostööd teiste olemasolevate turvakomponentidega kindlasti kontrollida juba enne platvormi kasutuselevõttu ja ka enne üleminekut uuemale versioonile.

Lotus Notesi/Domino koostöö turvalüüsidega

Lotus Domino servereid saab paigutada demilitariseeritud tsoonidesse (DMZ) ja kaitsta turvalüüsiga. Lotus Notesi/Domino serverikomponentide konkreetne paigutus on Lotus Notesi/Domino keskkonna turvaarhitektuuri üks osa. Seniste turvakomponentide ja Lotus Notesi/Domino koostöö tagamiseks võib tarvis minna asjakohast kontseptsiooni, eriti kui olemasolevaid turvakomponente on plaanis kasutada ka Lotus Notesi/Domino keskkonna jaoks. Selleks tuleb arvesse võtta nii Lotus Notesi/Domino teenuste valdkonnaspetsiifiliste kui ka Lotus Notesis/Dominos kasutatavate protokollide tehnilisi iseärasusi (nt seda, kas protokolli konfigureerimiseks saab kasutada turvalist ühendust või mitte)

Lotus Notesi/Domino koostöö spämmivastaste lahenduste, *content scanner* 'ite, *content filter* 'ite ja viirusetõrjetarkvaraga

Lotus Domino *web gateway* 'de ja Lotus Notesis/Dominos kasutatava viirusetõrjetarkvara valimisel tuleks otsustada selliste toodete kasuks, millel on spetsiaalne Lotus Notesi/Domino platvormi tugi. Spämmivastased lahendused, *content scanner* 'id, *content filter* 'id ja viirusetõrjetarkvara tuleb kohandada Lotus Domino teenuste ja kasutatavate protokollide nõuetega.

Lotus Notesi/Domino koostöö tsentraalse logimise ja automaatse logianalüüsi turvakomponentidega

Tsentraalsetes süsteemides tööle pandud logimisfunktsioon ja logide analüüsimine pakuvad muu hulgas kaitset Lotus Notesi/Domino enda turvalogimise manipulatsioonide vastu, mida võivad teha suurte volitustega kasutajad, administraatorid ja edukad ründajad. Seetõttu on turvalogide kirjutamine tsentraalsesse kaitstud süsteemikeskkonda (nt tsentraalsesse logiserverisse) väga oluline kaitsemeede päris mitmete ohtude korral, mida võivad põhjustada institutsiooni enda töötajad, kellele on antud suured haldusvolitused. Juhtudel, kus kasutatakse tsentraalseid logimissüsteeme ja logide analüüsimise süsteeme (nimetatakse ka Security Information and Event Monitoringuks või lühidalt SIEM-i lahendusteks), tuleb kindlaks määrata, milliste Lotus Notesi/Domino logimisvaldkondade jaoks on need mõel-

dud ja millised on Lotus Notesi/Domino eripäradega arvestavad analüüsikriteeriumid.

Täiendav kontrollküsimus:

- Kas Lotus Notesi/Domino keskkonna jaoks olulised võrguüleminekud, nt turvalüüsid, content scanner 'id, content filter 'id ja viirusetõrjetarkvara, on kohandatud Lotus Domino protokollide ja teenuste kasutamisest tingitud erinõuetega?

M 2.493w Litsentsihaldus ja litsentsiaspektid Lotus Notesi/Domino soetamisel

Algatamise eest vastutab: IT-juht

Rakendamise eest vastutavad: soetaja, erialaspetsialist

Lotus Notesi/Domino platvormi üha suureneva keerukuse ja kõikide suurte tarkvaratootjate levinud litsentsipoliitika tõttu on järjest raskem saada litsentside valdkonnast selget ülevaadet. Ent just litsentsiaspektid on Lotus Notesi/Domino puhul muutunud aina olulisemaks. Sobivate litsentside valimisega on küll võimalik märkimisväärselt raha kokku hoida, kuid nii tehniliselt kui ka töökorralduslikult on üha raskem kontrollida, kas sõlmitud on õiged litsentsilepingud ja kas nende nõudeid järgitakse korrektselt (et välistada või minimeerida vigu). Siinkohal tuleks kindlasti meeles pidada, et aktiveerimiskohustusega protsesside korral tuleb kogu arhiveerimisaja vältel säilitada ka vastavad programmikomponendid, sest nende puudumisel võib osutuda juurdepääs arhiveeritud andmetele kas võimatuks või ülimalt töömahukaks. Levinud tähtajalistes litsentsilepingutes on enamasti ka punkt, mis näeb ette, et pärast litsentsi lõppemist tuleb kõik programmi koopiad hävitada. Näiteks võib Notesi/Domino puhul arhiveerimiskohustus kehtida meilidele ja workflow 'dele, aga ka teistele komponentidele, nt enda arendatud rakendustele, mis töötavad Lotus Notesi/Domino platvormil.

Litsentside hankimise ja haldamise protsess

IT-osakond peab tagama, et litsentside hankimisel ja haldamisel rakendataks asjakohast protsessi, milles arvestatakse Lotus Notesi/Domino litsentside eripäraga. Sobiva litsentsi hankimine eeldab, et Lotus Notesi/Domino platvormi rakenduste töö eest vastutav isik, Lotus Notesi/Domino platvormi pooleliolevaid projekte koordineeriv projektijuht (nt arendus- ja katsetussüsteemide jaoks vajalike spetsiaalsete serverilitsentside tõttu) ning soetamise eest vastutav osakond teeksid koostööd. Litsentside soetamise ja haldamise protsessi puhul tuleb tagada selle nõuete uuendamine kindlate ajavahemike möödudes ja juhtudel, kus tootja on märkimisväärselt muutnud enda seniseid litsentsimudeleid. Litsentsihaldusprotsessiga ei tule tagada mitte üksnes pidev ülevaade kõikide litsentside hetkeseisundist, vaid ka litsentside strateegiline ja ennetav planeerimine, mille puhul arvestatakse muu hulgas ka värskenduste (upgrades) kaitse ja tootjafirmade pakutava toega.

Lotus Notesi/Domino litsentside eripärad virtuaalsete süsteemide puhul (näiteks Vmware)

Kui Lotus Notesi/Domino litsentse kasutatakse virtualiseerimistehnoloogia jaoks (nt mõnes virtuaalses masinas, mis ei kasuta kogu füüsilist riistvara, vaid ainult selle üht kindlat osa), võib lintsentside hankimisel olla mõistlik kasutada Passport Virtualisation Capacityt (endise nimega Sub-Capacity Licensing). Litsentsihaldusprotsessis tuleb nende võimalustega arvestada. Tehnilisi lahendusi läheb Lotus Notesi/Domino litsentside haldamisel tarvis alles siis, kui litsentse koguneb teatud arv. Litsentside haldamiseks sobivad institutsioonis juba olemasolevad vara- ja litsentsihaldusprotsessid ning abivahendid, aga ka eraldi Lotus Notesi/Domino platvormi jaoks sisse seatavad lahendused. Selleks saab kasutada (või peab kasutama, kui tootjaga sõlmitud leping selleks kohustab) tootja enda abivahendeid, nt IBM License Management Tool'i (ILMT).

Litsentsiaruanded ja -auditid

Litsentside puhul tuleb tagada, et lepingulised kohustused oleksid vajalikele osapooltele teada ja neid järgitaks. Teatud liiki litsentsimudelite korral eeldatakse, et klient peab koostama ja säilitama (arhiveerima) litsentsiaruandeid ning süsteemitööriistade kirjalikke ülestähendusi ja väljundeid. Kuna sellised kohustused on lepingus kindlaks määratud, tuleb neid ka hoolikalt täita. Nõuete täitmist tuleb regulaarselt kontrollida. Litsentsilepingutesse on sageli sisse kirjutatud ka litsentsiauditite kohustus, millega nõutakse, et auditi peavad tegema institutsioonivälised isikud, st kas tootjafirma või tootja volitatud sõltumatud audiitorid. Institutsioon peab tagama, et töökorralduses oleks sisse seatud ka litsentsiauditi protsess, mis toetab litsentsiauditite asjatundlikku ettevalmistust ja koostamist. Selle protsessi kavandamisel tuleb arvesse võtta tootjafirmaga kokku lepitud Lotus Notesi/Domino litsentsiauditite nõudeid.

Täiendavad kontrollküsimused:

- Kas litsentside hankimiseks ja haldamiseks rakendatakse asjakohast protsessi, milles arvestatakse Lotus Notesi/Domino litsentside eripäraga?
- Kas institutsioonis on juurutatud litsentsiauditi protsess, mis toetab litsentsiauditite asjakohast ettevalmistust ja koostamist?

M 2.494 Lotus Notesi/Domino keskkonna taristu jaoks komponentide valimine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

Uus, Eclipse'i tehnoloogial põhinev Notes Client (Standard Client, tuntud ka kui Full Client), aga ka serverikomponendid vajavad palju rohkem süsteemiressurssi kui versioonile 8 eelnenud Lotus Notesi/Domino platvormi komponendid. Alates versioonist 8.0 tuleb sellega kohandamisel (upgrade) kindlasti arvestada.

Seetõttu tuleb üle kontrollida ka nõuded, mille tootja on kehtestanud Domino ja Notesi komponente käitavate serverite ja klientide riistvarale, ning võimalike muudatuste korral olemasolevat IT-varustust muuta. Jõudlus- ja turbeprobleemide ning klienditaristus tehtavate suuremate muudatuste vältimiseks võib abi olla otsusest rakendada lõppkasutaja jaoks ka edaspidi Notes Clientit (Basic Client). Domino serveri uued teenused, nt Presence ja Instant Messaging, toovad endaga kaasa ka uued turvanõuded, mis mõjutavad turvataristu seniste komponentide, nagu tulemüüride ja IDS-ide/IPS-ide konfiguratsiooni ning võivad tekitada vajaduse uute komponentide soetamise järele, mis võimaldaksid neid teenuseid paremini kaitsta. Seetõttu tuleb juba eeltööna kooskõlastada turvataristu käitajate nõuded ning Lotus Notesi/Domino keskkonna jaoks mõeldud turvakomponentide soetamisele ja käitamisele kehtestatud nõuded.

Tähelepanu tuleks pöörata järgmistele turvataristu komponentidele:

- turvalüüsid;
- võrgupõhised rünnete tuvastamise ja vältimise süsteemid (NIDS/NIPS);
- serveripõhised rünnete tuvastamise ja vältimise süsteemid (HIDS/HIPS);
- serveripõhised kahjurvara eest kaitsvad komponendid;
- kliendipõhised isiklikud tulemüürid;
- kliendipõhised kahjurvara eest kaitsvad komponendid ja kliendipõhised HIDS-id (sageli koondatud kliendipõhiseks Security Suite 'iks);
- Content Security lahendused (ka eraldi seadmed);
- tundlike andmete lekkimist vältivad lahendused (Date Loss Prevention – DLP).

Enne igat Lotus Domino keskkonna redaktsiooni muutmist ja mis tahes olulisi muudatusi Domino teenuste kasutamises (nt uute teenuste töölelülitamine) tuleks kontrollida, kas selline tegevus on kooskõlas turvataristus Lotus Notesi/Domino turbe eest vastutavate komponentide tööga.

Kontrollküsimused:

- Kas asutuses on olemas protsess, mis tagab, et kasutatav riistvara vastab Lotus Notesi/Domino komponentide kõige uuematele nõuetele?
- Kas enne igat Lotus Domino keskkonna redaktsiooni muutmist ja enne mis tahes olulisi muudatusi Domino teenuste kasutamises (nt uute teenuste töölelülitamine) kontrollitakse, kas selline tegevus on kooskõlas turvataristus Lotus Notesi/Domino turbe eest vastutavate komponentide tööga?

M 2.495 Lotus Notesi/Domino komponentide kasutusest kõrvaldamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: infoturbespetsialist, administraator

Lotus Notesi/Domino keskkonna kasutustsükli puhul tuleb arvestada ka kasutusest kõrvaldamisega. Sellega kaasneb enamikul juhtudel ka komponentide asendamine, sest Lotus Notesil/Dominol põhinevad tööprotsessid ei muutu nii palju, et nt meili- ja veebiteenustest sooviks keegi lõplikult loobuda. Seetõttu rakendatakse kasutusest kõrvaldamist vaid uute toodete korral, nt kui migreerimisega minnakse üle uuele rühmatarkvarale või koostöölahendusele. Kui kasutusest kõrvaldamisega ei kaasne migreerimist, puudutab see enamasti ainult Lotus Notesi/Domino keskkonna üksikuid komponente (või taristukomponente ja nendes töötavaid Lotus Notesi/Domino komponente). Ühe komponendi kasutusest kõrvaldamisel tuleb alles jäävast keskkonnast kustutada kõik kasutusest kõrvaldatud komponendile suunatud viited (nt cross -sertifikaadid), samuti tuleb kohandada inventuuriloendeid ja andmebaase. Nii välditakse ründeid, mis põhinevad vanade referentside „taaskasutusel", st kasutusest kõrvaldatud komponendi identiteeti ärakasutamist võõra komponendi või süsteemi liitmiseks olemasoleva süsteemiga.

Litsentse ja litsentsihaldust tuleb kontrollida ja vajaduse korral muuta. Samamoodi nagu tuleb käituda kasutusest kõrvaldatud komponentide viidetega alles jäävas Lotus Notesi/Domino keskkonnas, tuleb vastavate komponentide andmed ja viited ära kustutada ka operatsioonisüsteemidest, võrgukooslusest, seire- ja turvakomponentidest (turvalüüsidest, IDS-idest, Content Security eraldi seadmetest, SIEM-i platvormidest, kahjurvara eest kaitsvatest komponentidest, võrguseirekomponentidest).

Sellisest ulatuslikust kustutamisest võib ka loobuda, juhul kui kasutusest kõrvaldatud komponent asendatakse Lotus Notesi/Domino koosluses uuega, mis võtab üle vana komponendi identiteedi, nt kui Domino server kantakse samal kujul üle võimsamale riistvarale.

Pärast edukat migreerimist tuleb enne kasutusest kõrvaldatud Lotus Notesi/Domino taristu füüsilist kõrvaldamist rakendada moodulis B 1.15 Andmete kustutamine ja hävitamine käsitletud nõudeid. Sama kehtib ka muuotstarbeliste taristute (nt arendustööde serverite) kohta. Tuleb arvestada, et arhiveeritud andmeid on tarvis ka pärast Lotus Notesi/Domino keskkonna kasutusest kõrvaldamist edasi säilitada ning tagada, et nendele andmetele pääsetaks juurde piisavalt lihtsalt ja kogu arhiveerimiseks ette nähtud aja vältel (arhiveerimistähtajad leiate arhiveerimiskontseptsioonist). Selleks läheb tarvis vastavaid ressursse (riistvara, tarkvara, litsentse).

Kontrollküsimus:

- Kas Lotus Notesi/Domino komponentide kasutusest kõrvaldamise protsess dokumenteeritakse (nt tööprotsesside dokumentatsioonis või käituskäsiraamatus)?

M 2.496 Logiserveri korrakohane kasutusest kõrvaldamine

Algatamise eest vastutavad: andmekaitsespetsialist, infoturbespetsialist

Rakendamise eest vastutab: administraator

Logiserveris kogutakse, töödeldakse, salvestatakse ja arhiveeritakse logiandmeid. Logides kajastuvad andmed võivad muu hulgas sisaldada IP-aadresse, kasutajanimesid ja IT-süsteemide nimesid. Seetõttu tuleb logiserveri korrakohasel kasutusest kõrvaldamisel tagada, et kõvaketastel ja teistel andmekandjatel ei oleks kaitset vajavaid andmeid. Kõik andmekandjad tuleb turvaliselt kustutada, olenemata sellest, kas need antakse edasi, suunatakse parandusse või kõrvaldatakse lõplikult kasutusest. Parandusse saatmisel ei piisa üksnes kõvaketaste formaatimisest või operatsioonisüsteemi kustutusfunktsioonide kasutamisest. Kõvakettad tuleb sobivate kustutusprogrammidega üle kirjutada nii, et nendel hoitud andmeid poleks võimalik ka erimeetoditega enam taastada. Lisateavet andmekandjate turvalise kustutamise ja hävitamise kohta leiate meetmest M 2.167 Andmete kustutamine või hävitamine .

Kui logiserver kõrvaldatakse kasutusest jäädavalt, tuleks peale andmekandjatel olevate andmete kustutamise andmekandja ka mehaaniliselt hävitada (purustada). Juhul kui andmekandjaid pole võimalik kohe kiiresti hävitada, tuleb neid kuni hävitamiseni hoida kohas, kus need on volitamata juurdepääsu eest kaitstud. Magnetilisi andmekandjaid saab kustutada ka elektromagnetiliselt – degausseriga. Kui andmekandjate kustutamine on mõne kolmanda osalise ülesanne, tuleb tellimust sisse andes arvestada muu hulgas ka andmekaitseaspektidega ja sõlmida vastav leping.

Täiendav kontrollküsimus:

- Kas logiserveri korrakohase kasutusest kõrvaldamise puhul on tagatud, et selle andmekandjad ei sisalda enam kaitset vajavaid andmeid?

M 2.497 Logimise turbekontseptsiooni koostamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: IT-juht, infoturbespetsialist

Logimise turbe tagamiseks tuleb koostada logimise turbekontseptsioon. Selles kontseptsioonis määratakse kindlaks kõik aspektid, mis aitavad logimist muuta turvaliseks, nt milliseid andmeid logitakse, kui pikalt tuleb logitavaid andmeid säilitada, kuidas neid analüüsida ja tsentraalse logimise korral läbi võrgu saata. Järgnevas loetelus on toodud üksnes mõned kõige olulisemad valdkonnad, mida see kontseptsioon peaks reguleerima. See loetelu ei ole täielik ning seda tuleb vastavalt asutuse konkreetsetele kasutusvaldkondadele kohandada ja täiendada. Detailsemad soovitused loetletud aspektide kohta leiate moodulist B 1.0 Infoturbe haldus . Turbekontseptsiooniga määratakse kindlaks, kuidas, kus ja mida tuleb erineva turbevajaduse korral logida. Selleks tuleb muu hulgas vastu võtta otsus, kas logimisfunktsioon pannakse tööle lokaalselt või tsentraalselt (vt M 3.90 Tsentraalse logimise põhitõed) . Enamasti on infokoosluse turvet puudutavatest sündmustest ülevaate saamine lihtsam siis, kui kasutatakse keskset logiserverit, mis kõik erinevad logid endasse kokku kogub ja neid analüüsib ning tagab ka seire. Otsuse langetamiseks tuleb muu hulgas kaaluda järgmisi aspekte:

- kas tsentraalne logimislahendus on ilmtingimata hädavajalik või saab logiandmeid ka lokaalselt salvestada ja analüüsida?
- kuidas tagatakse tsentraalse logimise korral serverite turve?
- kuhu tuleks keskne logiserver võrgus paigutada?
- millist sünkroniseeritud ja täpset aega kasutatakse logimisteadete jaoks?
- kuidas on korraldatud logiserverite turvaline kasutusest kõrvaldamine?

Asutusel tuleb vastu võtta otsus, milliseid IT-süsteeme, võrke ja rakendusi peab logimise turbekontseptsioon käsitlema. Üldjuhul tuleks logidesse üles kirjutada kõikide IT-süsteemide, nagu serverite, klientide, võrguühenduselementide ja turvalüüsidega seotud turbesündmused ja neid analüüsida, nagu on kirjeldatud meetmes M 4.430 Logiandmete analüüs . Selleks on soovitatav vastata järgmistele küsimustele:

- milliseid sündmusi peab logimine kajastama?
- milliseid teenuseid, rakendusi ja *host* 'e tuleb logida?
- millises andmevormingus on tarvis logiandmeid koguda ja analüüsida?

Kõikide logimisprotsessi funktsioonide ja omaduste optimaalseks kasutamiseks on oluline, et administraatorid saaksid asjakohase koolituse (vt M 3.89 Logimisprotsessi haldamise koolitus). Koolitustel tuleks käsitleda logiserveri komponentide juurutamist, käitamist ja haldamist. Olulised on muu hulgas järgmised punktid:

- kes ja mis eesmärgil tohib logiandmetele juurde pääseda?
- milliseid administreerimisülesandeid tohib delegeerida või peaks delegeerima?
- milliseid koolitusi on administraatoritele tarvis seoses logimisega?
- kuidas tagatakse järelevalve administraatorite tegevuse üle?

Kokku kogutud logiandmeid võib analüüsida nii lokaalselt kui ka mõnes keskses logiserveris (vt M 4.431 Logimise jaoks oluliste andmete valik ja töötlemine). Tsentraalse analüüsi korral tuleb logimisega seotud andmed edastada kesksesse serverisse läbi võrgu. Siinkohal on oluline, et IT-süsteemide vaheline andmeedastus oleks piisavalt turvaline (vt M 5.171 Turvaline andmeside keskse logiserveriga). Selleks tuleb arvestada järgmiste aspektidega:

- milliste mehhanismidega tagatakse logiandmete edastamise käigus logiandmete käideldavuse, konfidentsiaalsuse ja tervikluse säilimine?
- kas logiandmeid on võimalik edastada läbi andmevõrgu (*In-Band*) või tuleb selleks sisse seada eraldi logimis- ja haldusvõrk (*Out-of-Band*)?
- kas aja määratlemiseks on olemas piisavalt täpne lähtepunkt, mille põhjal kõik logiallikad sünkroniseeritakse?

Teatud sündmuste esinemisel või lävendiväärtuste ületamisel peaks süsteem väljastama asjakohase hoiatuse, nt meili või SMS-iga. Et hoiatussüsteemi oleks võimalik mõistlikult kasutada, on muu hulgas oluline, et hoiatavate teade hulk ei paisuks liiga suureks ja asjakohaseid isikuid teavitataks sündmustest võimalikult kiiresti (vt M 6.151 Logimise häirepoliitika). Soovitatav on vastata järgmistele küsimustele:

- milliseid filtreerimisseadistusi tuleks kasutada, et olulist teavet logiandmete seest üles leida?
- kuidas ja kui kaua logiandmeid arhiveeritakse ning kas see protsess vastab andmekaitsenõuetele?
- kuidas tuleks seadistada lävendiväärtusi, et tulemused ei oleks valepositiivsed (valehäire) ega valenegatiivsed (sündmust ei tuvastata)?
- kuidas tuleb hoiatustele reageerida?
- kuidas teavitatakse asjasse puutuvaid isikuid hoiatustest?

Logimisel tuleb järgida ka andmekaitsenõudeid, sest nendest võib oleneda, milliseid andmeid on lubatud ja keelatud logida ning kuidas logiandmetega korrektselt ümber käia (vt M 2.110 Andmeprivaatsuse suunised logimisprotseduurides). Logimise turbekontseptsioon peab olema kooskõlas institutsiooni üldkehtiva turvakontseptsiooniga. Kontseptsiooni tuleb regulaarselt ka uuendada ja muuta, võttes arvesse tehnilistes süsteemides või institutsiooni töökorralduses tehtavaid muudatusi.

Täiendavad kontrollküsimused:

- Kas logimise turbekontseptsioon on kooskõlas kogu institutsiooni hõlmava turvakontseptsiooniga?
- Kas logimise turbekontseptsiooni uuendatakse regulaarselt?

M 2.498 Reageerimine hoiatus- ja veateadetele

Algatamise eest vastutab: IT-juht
Täideviimise eest vastutab: IT-osakond

Hoiatus- ja veateadetele reageerimiseks tuleb institutsioonis juurutada hästi struktureeritud ja arusaadavad protsessid ning dokumenteerida nende protsesside tagamiseks võetavad meetmed. Asjakohased protsessid peavad kindlaks määrama, kes vastutab teadete läbitöötamise eest (töörollid või isikud) ja millisel moel teates kajastuvat infot kellelegi edasi antakse (nt meilid, SMS-id, trouble ticket 'id).

Kui institutsioonis on juba kasutusele võetud hoiatamiskontseptsioon, tuleb reageerimine võrguhalduse valdkonna hoiatus- ja veateadetele sellega integreerida. Allpool on toodud välja hoiatus- ja veateateid esile kutsuvad sündmused ja põhjused ning kirjeldatud, kuidas tuleks neile reageerida.

Hoiatusteated
Hoiatusteate ilmumise põhjused võivad olla erinevad:

- Võrgukontseptsioonis defineeritud ja võrguhaldussüsteemi salvestatud lävendiväärtusi võidakse ületada või mitte saavutada.
- Rakendatavaid teenuseid ei saa kasutada ette nähtud kvaliteediga.
- Võrguhaldussüsteemis tuvastatakse võrguliikluse anomaaliad.

Need võivad olla tingitud näiteks järgnevatest teguritest:

- Kasutusele võetud uued tööprotsessid vajavad oodatust rohkem ribalaiust.
- Internetis on mõni veebileht, mis huvitab korraga väga paljusid töötajaid, nt mõne mängu või jalgpalli MM-i otseülekande striimimine.
- Üks võrgus paiknevatest arvutitest on nakatunud kahjurvaraga, mis üritab luua andmesideühendusi keelatud portidega.
- Institutsiooni vastu pannakse toime väline rünne.
- Võrdõigusteenuseid (P2P) kasutatakse keelatud viisil, mille tagajärjel tekib internetiühenduses ülekoormus.
- Keegi üritab sisevõrku ühendada IT-süsteemi, ilma et tal oleks selleks volitusi.
- Kasutatakse keelatud protokolle (nt remote desktop 'i ühendus mõne väljaspool institutsiooni võrku asuva arvutiga).
- Keegi proovib järjestikku läbi erinevaid paroole, et end volitamata mõnda aktiivsesse võrgukomponenti sisse logida.

Olenevalt hoiatusteate põhjusest peavad vastutavad isikud võtma järgmisi asjakohaseid meetmeid:

- Kui hoiatusteade ilmub seetõttu, et mõnda lävendiväärtust ei saavutatud või see väärtus ületati, nt mõne veebilehe intensiivse kasutamise tõttu, saab

olukorra parandamiseks võtta kas tehnilisi või töökorralduslikke meetmeid. Kui võib oletada, et seda liiki sündmus enam ei kordu, pole tarvis ka spetsiaalseid abinõusid rakendada.
- Kahjurvarasse nakatumise kahtluse korral tuleb käivitada kahjurvara skaneerimine.
- Kui on alust arvata, et probleem võib korduda, tuleb välja selgitada, kas olukorda võiks parandada aktiivsete võrgukomponentide konfiguratsiooni muutmine, nt teenuste aktiveerimine ja desaktiveerimine. Kui tegemist on juba tuttava probleemiga, saab abi otsida tootja värskendustest (updates) ja paikadest (vt B 1.0 Infoturbe haldus).
- Juhul kui lävendiväärtuste vastu eksitakse pidevalt, tuleb kaaluda, kas võrgus kasutatavate teenuste töö parandamisele aitaks kaasa senisest võimsama riistvara kasutuselevõtt. Võrgu teatud lõikude puhul võib abi olla näiteks sellest, kui Fast Ethernetilt minnakse migreerimise teel üle suurema edastusvõimsusega ühendustele. Pärast meetmete võtmist tuleb ajakohastada ka võrguplaani andmed.
- Kui hoiatusteateid ei õnnestu vältida üksikute meetmete võtmisega, tuleb olenevalt olukorrast kaaluda topoloogia muutmist ja algatada võrgu kavandamise protsess (vt B 4.1 Heterogeensed võrgud). Teenuste puhul saab rakendada näiteks liiasust, kuid võib ka juhtuda, et võrgu topoloogiat tuleb laiendada.

Veateated
Veateated viitavad alati sellele, et mõni aktiivne võrgukomponent või teenus, mis kuulub võrguhaldussüsteemi seire alla, on lakanud töötamast. Töö katkemise põhjus võib, kuid ei pruugi olla seotud võõraste osaliste mõjutustega.

Selle tulemusena võib katkeda:

- võrgukeskkonnas teenuseid osutava IT-süsteemi (nt meiliserveri) töö;
- aktiivsete võrgukomponentide töö (nt kommutaatori ühe pordi defekt);
- passiivsete võrgukomponentide töö (nt ümberehitustööde käigus kogemata kahjustada saanud kaabel).

Vigade põhjused võivad muu hulgas olla järgmised:

- keskkonnamõjudest (nt liigsest kuumusest ja veest) põhjustatud riistvaradefekt või tehnilise taristu viga, nt elektrikatkestus;
- IT-süsteemi või aktiivse võrgukomponendi kokkujooksmine tarkvaravea tõttu;
- IT-süsteemi töö seiskumine selle vastu institutsiooni sees või väljast toime pandud eduka ründe tõttu;
- igapäevatöös kasutatavate süsteemide hävitamine turbemeetmete katsetamise tõttu, nt kui katse käigus ei käivitu varutoiteallikas.

Väga oluline on üles leida põhjused. Eesmärk peab olema selliste vigade vältimine või vähemalt nende kiire kõrvaldamine, kui need kõigest hoolimata

peaksid siiski korduma. Õigete põhjuste ja seoste leidmine võib mitme ebasoodsa asjaolu kokkulangemisel osutuda keeruliseks. Vigade kõrvaldamisel võib muu hulgas abi olla järgmistest meetmetest:

- defektse riistvarakomponendi väljavahetamine või kokku jooksnud tarkvara uuesti installimine;
- olenevalt olukorrast võib kõne alla tulla ka defektse riistvarakomponendi parandamine;
- kui töötamast lakanud süsteemi jaoks on olemas standby -süsteem (cold või hot standby), tuleks defektse süsteemi asemel kasutusele võtta vastav standby -süsteem.

Peamine eesmärk on kõrvaldada viga. Ent tuleb ka teada, kuidas selliseid vigu edaspidi vältida. Vigade analüüsimine ja vea kõrvaldamiseks võetud meetmed tuleb dokumenteerida.

Kontrollküsimused:

- Kas hoiatus- ja veateadetele reageerimiseks on juurutatud hästi struktureeritud ja arusaadavad protsessid ning kas vastavate protsesside tagamiseks võetavad meetmed on dokumenteeritud?
- Kas võrguhalduse vea- ja hoiatusteated on võimaliku olemasoleva hoiatuskontseptsiooniga integreeritud?

M 2.499 Logimise planeerimine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: IT-juht, administraator

Kuna turbesündmusi logitakse korraga infokoosluse väga erinevates süsteemides, tekib selle tagajärjel suur hulk logiandmeid. Logiandmed sisaldavad olulist teavet, mis võib aidata tuvastada nii riist- kui ka tarkvaraprobleeme ning nende asukohta. Logiandmeid on võimalik kasutada ka turbeastme suurendamiseks, sest nende põhjal saab tuvastada näiteks ründeid ja ka teisi turbevaldkonna probleeme. Logimisfunktsiooni turvalise töö tagamiseks on tarvis seda piisavalt hästi, st vajalikus mahus, planeerida. Näiteks tuleb koostada logimiskontseptsioon, milles määratakse kindlaks, kas institutsioon võtab kasutusele lokaalse või tsentraalse logimise. Lisaks tuleb reguleerida paljusid teisi valdkondi, nt logimisfunktsiooni haldamist ja kasutamist, hoiatamist ning tõendite säilitamist.

Logimiskontseptsioon

Logimiskontseptsiooniga määratakse kindlaks, kuidas, kus ja mida tuleb erineva turbevajaduse korral logida. Selle alla kuulub ka otsus, kas logimisfunktsioon pannakse tööle lokaalselt või tsentraalselt ning mida tuleb logitud sündmusi kajastava teabega peale hakata. Lisateavet logimiskontseptsiooni koostamise kohta leiate meetmest M 2.500 IT-süsteemide logimine .

Tsentraalse logiserveri asukoht võrgus

Tsentraalse logiserveri asukoht võrgus peab olema hästi läbi mõeldud, sest ühelt poolt peavad kõik IT-süsteemid sellele juurde pääsema, kuid teisalt tuleb tagada, et ebausaldusväärsetes võrkudes paiknevatel volitamata kasutajatel puuduks juurdepääs logiserverile. Üks sellekohane näide on turvalüüsi (tulemüüri) ees asuv perimeetrimarsruuter, mis on otse ühendatud internetiga ja mille logiandmeid soovitakse hallata ka tsentraalselt. Asukoha valimisel on oluline, et see ei tekitaks uusi kitsaskohti, nt võimalusi turvakomponentidest mööda hiilida. Logiandmete tavapärasest suurema turbeastme korral tuleks logiserver paigutada spetsiaalsesse logi- ja haldusvõrku. Selleks tuleb iga logitav IT-süsteem eraldi ühendada spetsiaalse logi- ja haldusvõrguga, nt võrgukaardiga. Sellise lahenduse puhul tuleks logiandmeid edastada ainult selle jaoks sisse seatud võrgus (võrgu eraldamine, Out-of-Band).

Turvaline andmeedastus tsentraalse logiserveri korral

Kui IT-süsteemide lokaalsed logiandmed kogutakse kokku tsentraalsesse logiserverisse, tuleb logiandmete edastamisel hoolitseda eelkõige tervikluse ja konfidentsiaalsuse säilimise eest (vt M 5.171 Turvaline andmeside keskse logiserveriga). Logiandmeid tuleb volitamata juurdepääsu (lugemise, muutmise, kustutamise) eest kaitsta näiteks krüpteerimisega. Mõeldavad on ka sellised mehhanismid, mis suurendavad andmete terviklust juba nende edastamise käigus. Näitena võib tuua andmete saatmise eraldi LAN-i (võrgu lahutamine, Out-of-Band), mille seest andmeid edasi enam ei saadeta ning millele on juurdepääs ebausaldusväärsetest võrkudest tõkestatud.

Haldamine

Logiandmeid ei kasutata mitte üksnes veaotsinguteks ja seireks, vaid ka kontrollimiseks, nt auditite ja revisjonide raames ning arvutitele tehtavate kohtueksper-

tiiside jaoks. Logiandmete kui tõendusmaterjali usaldusväärsuse tagamiseks tuleb neid kaitsta nii juhusliku kui ka ette kavatsetud muutmise eest. Seetõttu peaks juurdepääs nendele andmetele olema ainult volitatud töötajatel. Süsteemi haldajaks tuleb valida usaldusväärne administraator (vt M 3.10 Usaldusväärse administraatori ja tema asetäitja valimine). See on eriti oluline suure turbeastme korral, sest sellised logiandmed võivad sisaldada isikuandmeid. Administraatorite tegevusele on samuti soovitatav kohaldada seirefunktsioone, eriti kui on tegemist suure turbeastmega. Kuna logimine võib enamikul juhtudel puudutada ka isikuandmeid, tuleb tagada, et nii lokaalne kui ka tsentraalne logimisprotsess vastaks andmekaitsenõuetele. Näiteks võivad andmekaitsenõuded kehtestada piirangu, et logiandmeid tohib koguda üksnes eesmärgiga teha andmetest varukoopiaid või tagada igapäevatöö nõuetekohane toimimine (vt M 2.110 Andmeprivaatsuse suunised logimisprotseduurides). Logimiseks välja valitud protseduur ja logiandmete analüüsikriteeriumid tuleb dokumenteerida protseduuride loendis.

Kasutuseesmärk

Juba planeerimisel tuleks langetada otsus, mis eesmärgil logiandmeid infokoosluses kasutatakse. Logimisprotsessi tuleb kaasata kõik andmeallikad, mis on kooskõlas logimisele seatud eesmärgiga.

Infokoosluse logimise jaoks võivad olla olulised näiteks järgmiste IT-süsteemide andmed:

- aktiivsed võrgukomponendid (nt marsruutrid ja kommutaatorid);
- operatsioonisüsteemid;
- rakendused ja teenused (nt veebi-, meili-, failiserver),
- võrgu turvakomponendid (nt tulemüür, proksi, IDS);
- host 'ide turvakomponendid (nt turvalüüsid, viiruseskannerid);
- füüsilised juurdepääsusüsteemid.

Infokoosluse laiaulatusliku seire tagamiseks võib nende süsteemide logiandmed tsentraalselt koondada.

Hoiatamine

Tsentraalselt kokku kogutud logiandmed sobivad suurepäraselt hoiatussüsteemi täiendamiseks. Oluline on, et andmeid kogutaks ja analüüsitaks pidevalt ning võimalikult reaalajas. Selleks tuleb logiandmed kokku koguda (aggregation) ja korreleerida. Kokkukogumise all peetakse silmas ühesuguse sisuga logiteadete koondamist, st kaks ja rohkem kordi esinev teave kogutakse kokku üheks kandeks.

Korrelatsioon tähendab erinevate logiandmete seostamist. Infokoosluse vastu toime pandud ründeid on sageli võimalik tuvastada alles pärast erinevate logiandmete kombineerimist. Ründajad üritavad sageli oma tegevuse jälgi peita. Erinevatest allikatest pärit logiandmete võrdlemine suurendab võimalust, et tuvastatakse mõni sissekanne, mida ründajal ei õnnestunud eemaldada. Andmeid saab kokku koguda ja üksteisega seostada ainult mõnes tsentraalses kohas, kus ei koguta kokku mitte ühe, vaid erinevate süsteemide logiandmeid. Logiandmete mõistliku

analüüsi tagamiseks, mis võimaldaks neid andmeid kasutada ka hoiatussüsteemi töös, tuleb kokkukogumise ja korrelatsiooniga tuvastada olukord, kus logiandmed ei vasta enam terviklusnõuetele. Lisaks tuleks hoiatussüsteemiga integreerida vastav anomaaliakomponent, mis käivitab hoiatuse, kui seire alla kuuluva infokoosluse seisundis peaks esinema kõrvalekaldeid (vt M 6.151 Logimise häirepoliitika).

Tõendite säilitamine

Infokooslusest kogutud logiandmeid võidakse kasutada ka turvaintsidentide lahendamiseks (arvutite kohtueksperti isid). Sellise tegevuse eesmärk on kasutada logiandmeid kohtus tõendusmaterjalina. Kohtueksperti iside puhul üritatakse logiandmete põhjal rekonstrueerida juba toimunud turvaintsidenti, et selgitada välja sellest tekkinud kahju.

Kontrollküsimused:

- Kas logimisfunktsioonide kasutamiseks koostatakse logimiskontseptsioon?
- Kas logiserveri integreerimine infokoosluse võrguga on hoolikalt planeeritud?
- Kas tsentraalse logimisfunktsiooni korral on kõikidel logitavatel IT-süsteemidel juurdepääs logiserverile ning kas volitamata isikute juurdepääs logiserverile on tõkestatud?
- Kas logitavatest IT-süsteemidest kogutud logiandmete edastamisel tsentraalsesse logiserverisse on tagatud logiandmete tervikluse ja konfidentsiaalsuse säilimine?
- Kas kogutud logiandmetega ümberkäimisel järgitakse andmekaitsenõudeid?
- Kas logimisprotseduur ja logiandmete analüüsimise kriteeriumid on dokumenteeritud?
- Kas logiandmete seire leiab aset võimalikult reaalajas ning logiandmeid analüüsitakse regulaarselt?

M 2.500 IT-süsteemide logimine

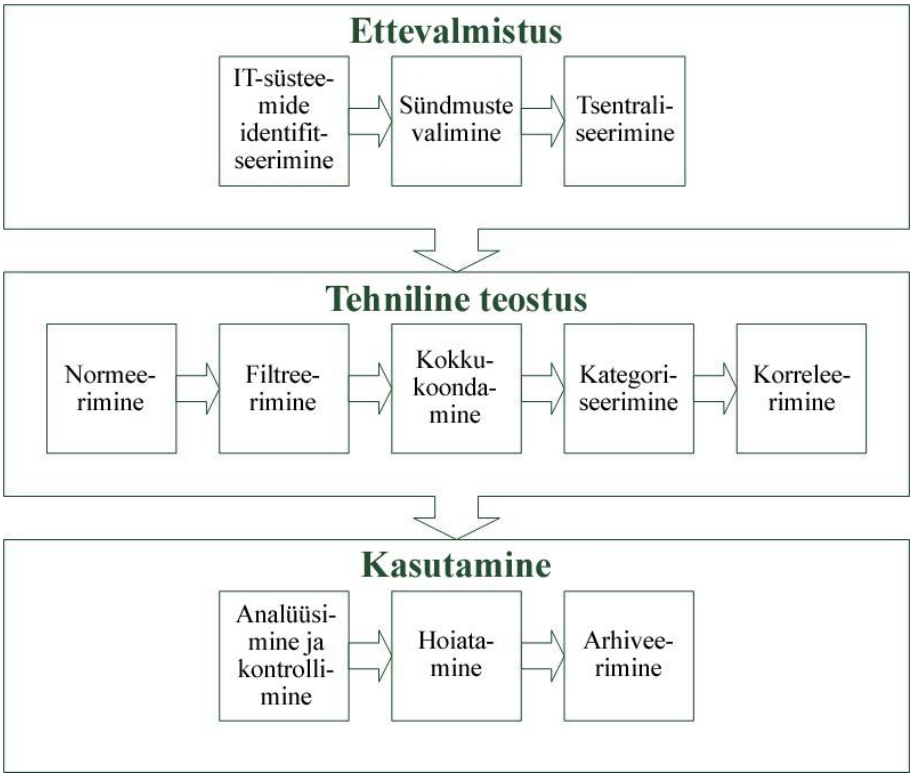
Algatamise eest vastutavad: infoturbespetsialist, IT-juht
Rakendamise eest vastutab: administraator

Andmetöötlussüsteemide turbega seotud sündmusi tuleb logida. Põhjusi selleks on mitu. Ühest küljest aitab sisselülitatud logifunktsioon varakult tuvastada ja kõrvaldada potentsiaalseid kitsaskohti. Teisalt saab logiandmete põhjal avastada turbenõuete rikkumisi ja uurida tagantjärele turvaintsidendi võimalikke tekkepõhjusi. Selleks kirjutatakse vaadeldavates IT-süsteemides aset leidvad sündmused logidesse. Iga institutsioon peaks kehtestama üldreeglid, kuidas IT-süsteeme, võrke ja rakendusi logida. Seejärel saab üldreegleid kohandada konkreetsete IT-süsteemide eripäradega. Lisateavet, kuidas konkreetsete IT-süsteemide, võrkude ja rakenduste logimist korraldada, leiate IT etalonturbe kataloogide erinevatest IT-süsteeme käsitlevatest moodulitest (vt M 1.1 Vastavus normidele ja eeskirjadele). Logimist käsitletakse põhjalikumalt moodulis B 5.22 Logimine . Selles moodulis vaadeldakse kõiki logimise ja seirega seotud eriohte ja nende vastumeetmeid, olenemata sellest, mis operatsioonisüsteeme parasjagu kasutatakse.

Sobiliku protsessi väljatöötamine ja realiseerimine on väga töö- ja ajamahukas. Seetõttu tuleks seda moodulit kasutada alati suuremate infokoosluste puhul ning juhtudel, kus infokoosluses soovitakse juurutada tsentraalselt töötavat logimist. Väikeste ja ülevaatlike infokoosluste puhul võib piisata ka üksnes selle meetme võtmisest. Esimese asjana tuleb institutsioonil enda jaoks koostada logimiskontseptsioon. Logimiskontseptsiooniga määratakse kindlaks, kuidas, kus ja mida tuleb erineva turbevajaduse korral logida. Logid peaksid üldjuhul alati kajastama kõiki administraatorivolitustega tehtud sisselogimisi. Kontseptsiooniga tuleb muu hulgas kindlaks määrata ka see, kuidas logitud sündmustega edasi toimida (vt M 4.431 Logimise jaoks oluliste andmete valik ja töötlemine). Järgnevalt tutvustatakse kontseptsiooni koostamise seisukohalt vajalikke aspekte.

Tsentraalne või lokaalne logimine
Logimise eesmärk on aidata mõista, miks ja kuidas leidsid IT-süsteemides, võrkudes ja rakendustes aset olulised muudatused, ning tagada seeläbi nende turve. Siinkohal on võimalik eristada lokaalset ja tsentraalset logimist. Tsentraalse logimise korral kogutakse erinevates IT-süsteemides kohapeal koostatud logiandmed kokku eraldi IT-süsteemi, kus neid analüüsitakse. See võimaldab logitud sündmusi välja valida, filtreerida ja analüüsida ühes keskses kohas. Sellise lahenduse eelis on muu hulgas ka see, et nii saab erinevate IT-süsteemide turbeprobleeme ja süsteemide vastu suunatud ründeid omavahel seostada ja suurendada seeläbi turvaintsidentide avastamist (vt M 3.90w Tsentraalse logimise põhitõed). Lokaalse logimise korral jäävad logid IT-süsteemidesse, kus need koostati. Seal on korraldatud ka nende valimine, filtreerimine ja analüüsimine. Võimalik hoiatusfunktsioon, mis teavitab turbesündmusest, käivitub samuti detsentraalselt vastavas IT-süsteemis. Logimise planeerimisel on tarvis erinevate IT-komponentide puhul kindlaks määrata, kas neis aset leidvaid sündmusi logitakse tsentraalselt või lokaalselt. Enamasti võib soovitada tsentraalset logimist.

Samas tuleb siiski ka arvestada, et kõikide IT-süsteemide puhul ei ole tsentraalne logimine



Logimisetapid
Logimisprotsessi etapid olenevad sellest, kas kasutatakse tsentraalset või lokaalset logimist.

Logimiskontseptsioon peab arvestama võimalike erinevate etappidega, mis hõlmavad järgmisi valdkondi:

- IT-süsteemide identifitseerimine
- asutusel tuleb vastu võtta otsus, milliseid IT-süsteeme, võrke ja rakendusi peab logimiskontseptsioon käsitlema.

Üldjuhul võiks lähtuda põhimõttest, et logida tuleb kõikide IT-süsteemide turbega seotud sündmused, nagu näiteks:

- kliendid, k.a kaasaskantavad IT-süsteemid;
- serverid;
- võrguühenduselemendid (marsruutrid ja kommutaatorid);
- oluliste tööprotsesside andmebaasid;

- kodukeskjaamad;
- turvalüüsid.

Kui institutsioon otsustab tsentraalse logimise kasuks, peavad rakendatavad IT-süsteemid seda toetama. Selleks tuleb enamasti logitavasse IT-süsteemi installida kas agent või mõni muu rakendus. See rakendus võtab info IT-süsteemis kajastatud sündmuste kohta vastu ja saadab selle otse tsentraalsesse logiserverisse.

Turbesündmuste valimine
Infokoosluses tuleks üldjuhul alati logida kõik turbesündmused.

Erilist tähelepanu tuleks siinkohal pöörata järgmistele sündmustele:

- kasutajavolitustega kasutajatunnuste alt tehtud ebaõnnestunud sisselogimiskatsed, nt vale parooli sisestamise tõttu;
- kasutajatunnuste blokeerimine;
- kasutajate ja administraatorite sisselogimised ebaharilikel kellaaegadel;
- riistvara töö katkemine ja tõrked;
- vead rakenduste töös ja rakenduste ülekoormamine, nt mälu täitumine ja oluliste tööprotsesside katkemine;
- andmed võrgu koormuse ja ülekoormuse kohta;
- ründetuvastussüsteemide (Intrusion Detection System) hoiatus- ja veateated;
- pöördused aktiivsetesse võrgukomponentidesse (kes logis millal sisse?).

See, milliseid sündmusi logida, oleneb muu hulgas ka vastavate IT-süsteemide turbevajadusest, mistõttu tuleb see institutsioonis juba varem kokku leppida ja kindlaks määrata.

Tsentraliseerimine
Logiandmed on soovitatav kokku koguda ühte kesksesse kohta. Lokaalse logimise korral võivad nendeks kohtadeks olla erinevad kataloogid, et logiandmete kogumisel säiliks ülevaade ja neid oleks vajaduse korral võimalik kiiresti üles leida. Seevastu tsentraalse logimise puhul tuleks turbesündmusi kajastavad andmed saata läbi turvalise kanali edasi tsentraalsesse serverisse ja salvestada seejärel mõnda andmebaasi.

Normeerimine
Kokkukogutud erinevad teated tuleb hilisema analüüsi tarbeks saada ühte andmevormingusse (normeerida), sest vormingu ja edastusprotokolli jaoks puudub ühtne standard. Normeerimisega on võimalik logide erinevaid andmevorminguid, nt Syslog, MS Eventlog, SNMP, Netflow ja IPFIX, üksteise suhtes kohandada ja seejärel koos analüüsida. Nii saab kõik erinevates andmevormingutes kogutud andmed ühtlustada ja neid seejärel ühes andmevormingus analüüsida.

Filtreerimine
Filtreerimisega saab logiandmete analüüsimisest juba võimalikult varajases etapis välja arvata vastava kasutusvaldkonna jaoks ebaolulised andmed. Turbesündmusi kajastavatest teadetest filtreeritakse välja nende informatiivne sisu ja see suunatakse järgmistesse tööetappidesse.

Kokkukoondamine
Kokkukoondamise (aggregation) eesmärk on logides esinevate korduvate sündmuste koondamine üheks andmehulgaks. Üks ja sama IT-süsteem võib korduvalt järjestikku koostada identse sisuga logisid, mistõttu piisab sageli üksnes esimese logi töötlemisest. Korduvate sündmuste esinemisel tuleks salvestada korduvate sündmuste hulk, et hiljem oleks võimalik kindlaks teha, kui sageli identse sisuga logiteateid koostatakse.

Kategooriate ja prioriteetide kindlaksmääramine
Kategooriad ja prioriteedid on olulised eelkõige tsentraalse logimise korral. Nende abil saab logiteadetes kajastuvat infot veelgi detailsemaks muuta.

Korreleerimine
Infokoosluse erinevatel IT-süsteemidel, nt turvalüüsidel, serveritel ja klientidel, on enda tööst üksnes piiratud ülevaade. Selle probleemi kõrvaldamiseks saab vastavaid logiandmeid korreleerida. Näiteks saab turvalüüside logiandmeid siduda marsruutrite logiandmetega.

Analüüsimine ja kontrollimine
Võimalikke turvaauke, manipuleerimiskatseid ja ebareeglipärasusi saab avastada vaid siis, kui peale logiandmete kogumise analüüsitakse ja kontrollitakse neid regulaarselt. Analüüs ei tuvasta mitte ainult turbega seotud sündmusi ja vigu, vaid annab ka infot hetkekoormuse kohta. Turvalisust mõjutavate sündmuste logimine on turvameetmena tõhus vaid siis, kui vastavaid logidesse kogutud andmeid kontrollib regulaarselt mõni revident, st isik, kelle ülesanne ei ole neid süsteeme hallata. Kui sõltumatu revidendi ametikoha loomine ei ole töötajate puuduse tõttu või tehniliselt võimalik, võib logifailide kontrollimise usaldada ka mõnele administraatorile. Selleks tuleks valida siiski mõni selline administraator, kes ei vastuta kontrollitavate süsteemide haldamise eest, sest muidu muutub administraatori töö kontrollimine väga raskeks. Kui regulaarselt on tarvis läbi vaadata suure mahuga logifaile, on mõttekas kasutada kontrollimiseks mõnda programmi, nt graafilise kasutajaliidesega analüüsiprogramme ja aruannete genereerijaid. Programm peaks võimaldama valida erinevate analüüsikriteeriumite vahel ja tõstma esile kriitilised logikanded (nt korduvad ebaõnnestunud sisselogimiskatsed) (vt M 2.64 Logifailide kontroll).

Hoiatamine
Kriitilisena määratletud sündmuste esinemisel või lävendiväärtuste ületamisel peaks süsteem väljastama asjakohase hoiatuse, nt meili või SMS-iga. Et hoia-

tussüsteemi oleks võimalik mõistlikult kasutada, ei tohi hoiatavate teadete hulk paisuda liiga suureks. Selleks tuleb lävendiväärtuste kindlaksmääramisel olla realistlik ja arvestada infokoosluse eripäradega.

Arhiveerimine
Tuleb kontrollida, millised on logifailidele seaduste või lepingutega ette nähtud säilitusajad. Sündmuste tagamaade väljaselgitamiseks võib olla andmetele kehtestatud minimaalne säilitusaeg, andmekaitsenõuete tõttu võib aga kehtida ka andmete kustutamise kohustus (vt M 2.110 Andmeprivaatsuse suunised logimisprotseduurides). Kui logiandmed arhiveeritakse, tuleb järgida moodulit B 1.12 Arhiveerimine .

Logitud sündmuste konfidentsiaalsus ja terviklus
Mõned andmeallikad genereerivad logiteateid, mis võimaldavad neid seostada konkreetse isikuga. Seetõttu peab juurdepääs logiandmetele olema üksnes volitatud isikutel. Samuti tuleb tagada, et logitud sündmusi poleks võimalik volitamata kustutada ega tagantjärele muuta. Sellised volitused tuleb jätta isikutele, kes logivad end süsteemi sisse revidendina. Kui tehniliselt on võimalik, tuleks ka administraatoritelt andmete kustutamise ja muutmise õigused ära võtta. Selleks tuleb rakendada asjakohaseid failisüsteemiõigusi, mis tõkestavad volitamata isikute juurdepääsu. Tsentraalse logimise korral tuleb logitud sündmusi kaitsta ka logiandmete edastamisel, nt krüpteerimisega või edastamisega läbi eraldi haldusvõrgu (Out of Band Management). Selliste kaitsemeetmete võtmine suurendab andmeedastuse ajal muu hulgas ka logiteadete terviklust ja konfidentsiaalsust. Tavapärasest suurema turbevajaduse korral tuleks analüüsida, kas logitavate sündmuste jaoks oleks mõistlik kasutada WORM-andmekandjaid (Write Once Read Many). Seda tüüpi andmekandjatele saab andmeid kirjutada ainult üks kord, st kord juba kirjutatud andmeid ei ole võimalik tagantjärele muuta.

Aja sünkroniseerimine
IT-süsteemide, võrkude ja rakenduste võimalike tõrgete ja nende süsteemide vastu suunatud rünnete tuvastamiseks tuleb kõikides IT-süsteemides ja virtuaallahendustes kasutada ühist kellaaega. Suure infokoosluse puhul tuleb kõikide süsteemide kellaaeg sünkroniseerida tsentraalse ajaserveriga. See rakendab sünkroonse aja tagamiseks näiteks Network Time Protocoli (NTP) (vt M 4.227 Lokaalse NTP -serveri kasutamine aja sünkroniseerimiseks). Kõik infokooslusse kuuluvad süsteemid saavad enda aja selle tsentraalse väärtuse põhjal sünkroniseerida.

Kontrollküsimused:

- Kas logimise jaoks on olemas kontseptsioon?
- Kas logitud sündmused on volitamata isikute juurdepääsu eest kaitstud?

M 2.501 Isikuandmete kaitse haldus

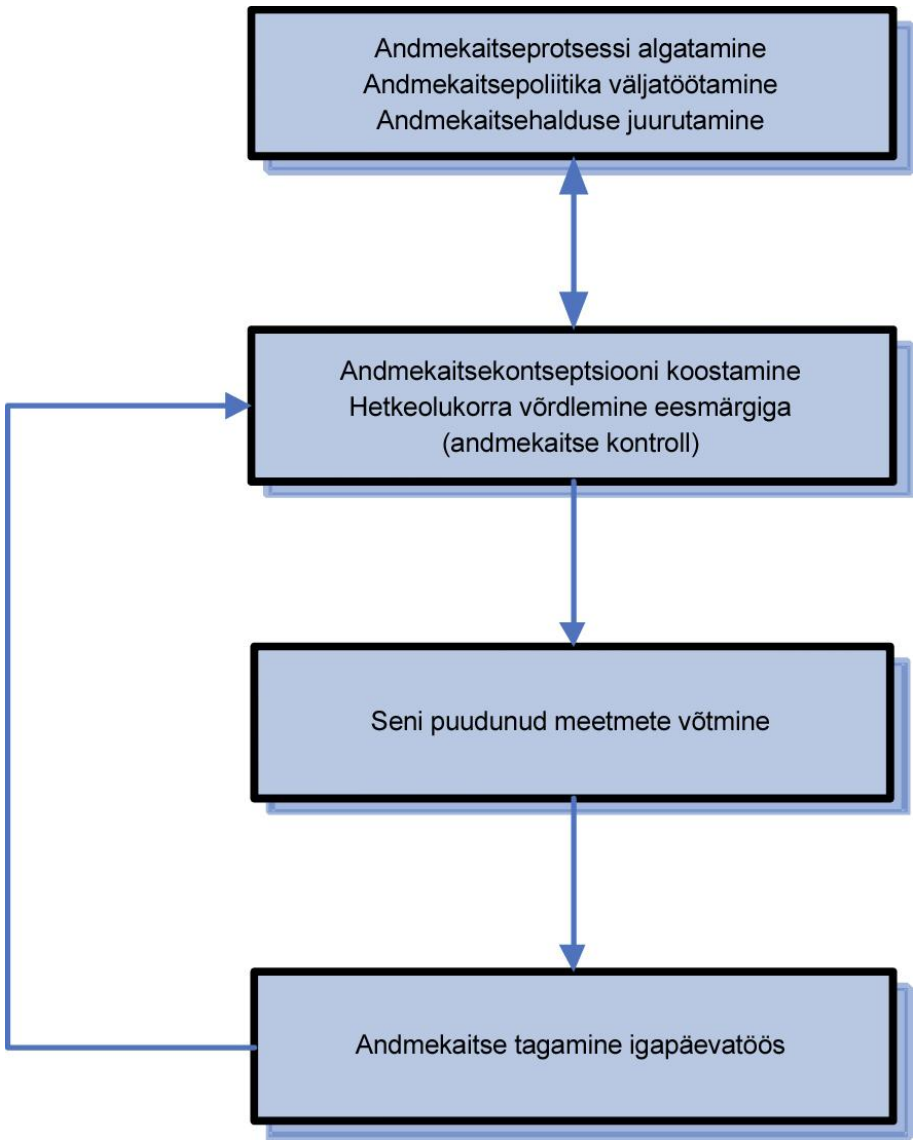
Algatamise eest vastutab: ametiasutuse/ettevõtte juhtkond
Rakendamise eest vastutavad: infoturbe spetsialist, isikuandmete töötlemise eest vastutav isik

Isikuandmete kaitse halduse all mõistetakse protsesse, mis võimaldavad täita andmetöötlusprotsesside planeerimisele, juurutamisele, kasutamisele ja kasutusest kõrvaldamisele kehtivaid seadustest tulenevaid isikuandmete kaitse nõudeid.

Isikuandmete kaitse haldus on isikuandmete kaitse aspektide rakendamine üleorganisatsioonilisel tasandil või suurte projektide puhul. Järgnevalt kirjeldatakse isikuandmete kaitse halduse protsessi, mida tuleb käsitleda kui näidet ja ühte võimalikku ettepanekut. Protsessi tuleks vaadelda eelkõige kui IT etalonturbest lähtuva infoturbeprotsessi üht osa, kuid ka kui eraldi protsessi, juhul kui põhieesmärk on käsitleda konkreetseid isikuandmete kaitse aspekte. On iseenesest mõistetav, et seda protsessi ei tuleks juurutada mitte iga valdkonna jaoks eraldi, vaid terves organisatsioonis korraga ja kõikide protseduuride jaoks, milles töödeldakse andmeid s.h isikuandmeid.

Isikuandmete kaitse protsess
Isikuandmete kaitse halduse tuuma moodustab isikuandmete kaitse protsess. Nii nagu infoturbeprotsess, on ka isikuandmete kaitse protsess tsükliline ning peab tagama, et isikuandmete kaitse seaduse nõudeid järgitaks pidevalt, st ka siis, kui töökeskkonnas esineb muudatusi. Protsess hõlmab organisatsiooni strateegiat, taktikat ja tööprotsessidega seotud ülesandeid. Järgnevalt kirjeldatakse protsessi toimimiseks vajalikke meetmeid. Protsess on koostatud nii, et isikuandmete kaitse haldust saaks juurutada ka sellistes organisatsioonides, kus isikuandmete kaitse rakendamiseks vajalik struktuur esialgu puudub.

Protsessi näitlikustab järgmine joonis.



Andmekaitseprotsess = Isikuandmete kaitse protsess
Joonis 1. Isikuandmete kaitse protsess

Järgnevalt kirjeldatakse isikuandmete kaitse protsessi üksikuid etappe ehk osaprotsesse.

Isikuandmete kaitse protsessi algatamine
Siia etappi kuuluvad strateegilist eesmärki kujundavad meetmed (eesmärk kuni viieks aastaks). See hõlmab järgmisi tegevusi. Isikuandmete kaitse poliitika väljatöötamine, enamasti tervele institutsioonile või ettevõttele kehtiva turvapoliitika osana.

Selle eesmärgid võivad olla muu hulgas järgmised:

- nõuete täitmine minimaalsete töökuludega (compliance);
- isikuandmete kaitse nõuded kui konkurentsieelis (USP: Unique Selling Proposition).

Isikuandmete kaitse halduse juurutamine, on enamasti turvahalduse üks osa. Selle olulised alamvaldkonnad on vastutusalade kindlaksmääramine (isikuandmete töötlemise eest vastutava isiku roll ja funktsioon võrreldes infoturbespetsialistiga ning nende kahe koostöö), protsesside defineerimine ja ressursside (personaliressursi) tagamine.

Isikuandmete kaitse kontseptsiooni koostamine
Isikuandmete kaitse kontseptsioon täiendab infoturbekontseptsiooni ja kehtib samamoodi kolm aastat (vt M 2.503 Isikuandmete kaitse kontseptsiooni aspektid).

Vajalike meetmete võtmine
See protsess hõlmab isikuandmete kaitse kontseptsiooniga kindlaks määratud, kuid seni veel rakendamata meetmete võtmist. Meetmete võtmiseks kasutatakse klassikalist projektihaldust, st koostatakse projekti- ja töögraafik.

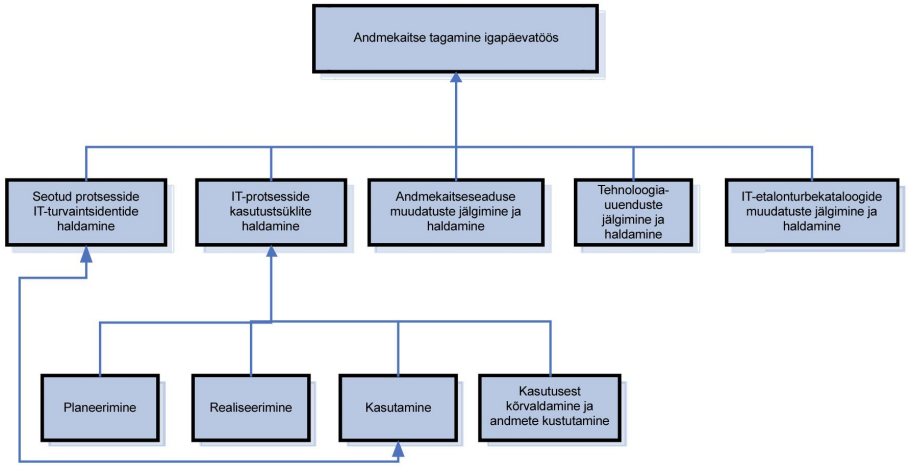
Isikuandmete kaitse tagamine igapäevatöös
Selle osaprotsessi ülesanne on reageerida isikuandmetega seotud tööprotsessides esinevatele muudatustele ja tõrgetele.

See puudutab eelkõige järgmist:

- isikuandmete kaitses eaduse muudatused;
- (IT-)protseduuride muudatused;
- igapäevastes tööprotsessides esinevad tõrked, mida võib liigitada turvaintsidendiks;
- tehnoloogiline areng ja seniste meetmete võtmise lihtsustamine.

Selle eesmärgi täitmiseks tuleb peale turbeprotsessi juurutada mitmeid alamprotsesse, mis suudaksid andmekaitsesse puutuvaid muudatusi ja tõrkeid iseseisvalt analüüsida ja lahendada. Nende protsesside tulemusi saab kasutada näiteks isikuandmete kaitse halduse struktuuri muutmiseks või isikuandmete kaitse kontseptsiooni ajakohastamiseks.

Alamprotsessidest annab ülevaate järgmine joonis.



*Andmekaitseprotsess = Isikuandmete kaitse protsess
Joonis 2. Valdkonna isikuandmete kaitse tagamine igapäevatöös, osaprotsessid

Turvaintsidentide haldamine
IT-protsesside jooksva töö käigus esinevate turvaintsidentide haldamisel tuleb vajaduse korral tähelepanu pöörata ka intsidentide võimalikele isikuandmete kaitse aspektidega seotud tagajärgedele. Selleks on kõige mõistlikum teha koostööd infoturbespetsialistiga, kes juhatab turvaintsidenti uuriva meeskonna tööd.

Isikuandmete kaitse halduse ülesanded võivad olla muu hulgas järgmised:

- tehniliste ja töökorralduslike meetmete seadmine tähtsuse järjekorda (probleemide analüüsi, lahendamise ja tõendite säilitamisega seotud andmekaitsenõuded);
- juriidiliste aspektidega tegelemine isikuandmete kaitse seaduse kohaselt.

Protsesside paremaks integreerimiseks oleks mõistlik, et isikuandmete kaitse halduse, st selle alamprotsessid, algataks turbehaldusosakond. Praktikas tähendab see näiteks seda, et isikuandmete töötlemisega seotud turvaintsidentide korral kaasatakse turvaintsidenti haldava meeskonna töösse automaatselt ka isikuandmete töötlemise eest vastutav isik. Nii saab tööks olulise teabe ja vajalikud tööprotsessid optimaalselt kokku sobitada. Turvaintsidentide haldamise raames tuleb ka kirjeldada, kus toimub ettevõttes või ametiasutuses andmekaitsega seotud turvaintsidentide haldamine ja kes töötajatest sellega tegelevad.

Isikuandmete kaitse aspektid IT-protsesside kasutustsüklite haldamisel
IT-toodete ja -protseduuride kasutustsüklite haldamiseks rakendatakse kasutustsükli mudelit, mis lähtub üldjoontes ISKE kasutustsükli mudelist ja IT etalonturbe kataloogidest. Erinevates faasides tuleb võtta moodulisse B 1.5 Andmekaitse . Eelnevale lisaks tuleks uusi IT-protseduure planeerides ja nende jaoks kontseptsioone koostades uurida, kas neile sobiksid ka PETlahendused (Privacy Enhancing Technologies). PET-d on tehnilised lahendused, mis aitavad järgida isiku-

andmete kaitse põhiaspekte, nt vältida andmete kuhjumist ning tagada eesmärgipärasus ja läbipaistvus. PET-d võivad olla sellised protokollid nagu P3P (Platform for Privacy Preferences) ja protseduurid, mis tagavad andmete anonüümsuse ja rakendavad pseudonüüme andmete edastamisel võrgus, andmetalletusel andmebaasides ja andmekaevandusprotsessides (Privacy Preserving Data Mining – PPDM). Siia kuuluvad ka programmide meeldetuletusfunktsioonid, mis aitavad järgida isikuandmete seatud kustutamistähtaegu.

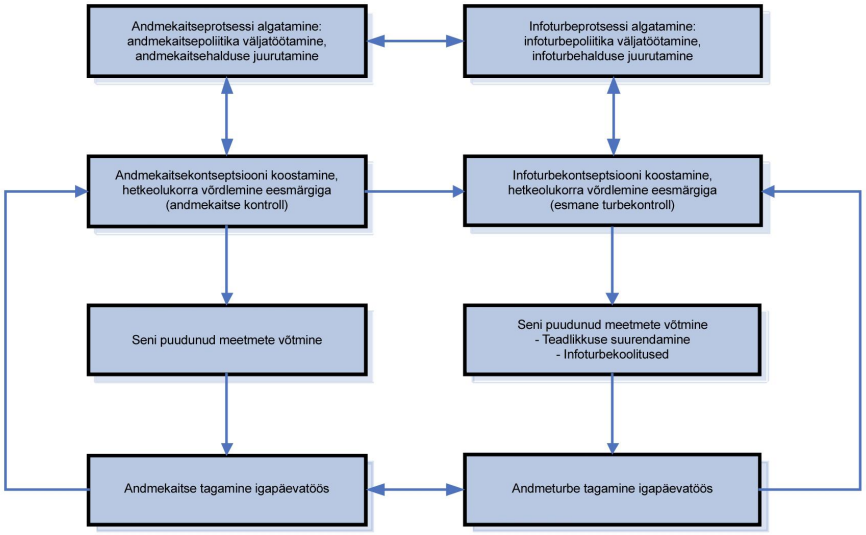
Isikuandmete kaitse seaduse muudatuste haldamine
Isikuandmete kaitse seaduses tehtavaid muudatusi tuleb jälgida, samuti tuleb analüüsida nende mõju isikuandmeid töötlevatele protsessidele. Selle alamprotsessi saab integreerida ka asutuse või ettevõtte üldise seadusandlikke muudatusi jälgiva ja haldava protsessiga.

Tehnoloogiauuenduste jälgimine
Nii nagu infoturbehaldus, võimaldab ka tehnoloogiauuenduste jälgimine hoida end kursis tehnika tasemega, eelkõige selle infoturbe- ja isikuandmete kaitse aspektidega. See alamprotsess annab koos kohustusliku isikuandmete kaitse seadusega impulsse isikuandmete- ja turbekontseptsiooni edasiarendamiseks.

ISKE kataloogide muudatuste jälgimine ja haldamine
Üldise muudatuste jälgimise protsessi raames tuleb arvestada ka võimalike muudatustega BSI standardites, ISKE kataloogides ning eriti selle isikuandmete käsitlevas moodulis. Peale uute ideede, kuidas isikuandmete kaitse- ja turbekorraldus kontseptsiooni edasi arendada, tuleks selle protsessiga kontrollida ning vajaduse korral ka kohandada infoturbehalduse liideseid.

Kokkuvõte
Eelnev näitlik protsessimudel pakub rohkelt võimalusi kasutada ära nii BSI standardite kui ka ISKE vastavate turbeprotsessidega seotud sünergiat. Sünergia võib tekkida näiteks protsesside ühitamisest, dokumentide ja dokumentatsiooni (nt isikuandmete kaitse- ja turbekontseptsiooni korraldused) integreerimisest ning lõppeda protsesside täieliku integreerimisega. See võib puudutada ka töötajaid, kes täidavad olulisi tööülesandeid, nt võib infoturbejuhi ametikoha liita isikuandmete töötlemise eest vastutava isiku omaga, eeldusel et töötajal on asjakohane kvalifikatsioon ja ta ei vastuta samal ajal IT-valdkonna kontseptsioonide väljatöötamise ega süsteemide käitamise eest (vältida tuleb huvide konflikti). Selline lahendus võib hästi sobida eelkõige väiksele organisatsioonile.

Võimalikud seosed on kujutatud joonisel 3.



*Andmekaitseprotess = Isikuandmete kaitse protsess

Joonis 3. Isikuandmete kaitse- ja andmeturbeprotsessi vastastikmõjude ja sünergia skeem

Kontrollküsimused:

- Kuidas on andmete salvestamine viidud vastavusse tehnika tasemega?
- Millistes olemasolevates IT-protseduurides ja kuidas saaks mõistlikult kasutada PET(eraelu kaitset soodustavad tehnoloogiad)-lahendusi?

M 2.502 Isikuandmete kaitse vastutusalade kindlaksmääramine

Algatamise eest vastutab: ametiasutuse/ettevõtte juhtkond

Rakendamise eest vastutab: ametiasutuse/ettevõtte juhtkond

Isikuandmete kaitse nõuete järgimine on ülimalt oluline kõikide selliste IT-süsteemide ja -protseduuride puhul, millega töödeldakse isikuandmeid. Isikuandmete kaitse aspektidega tuleb arvestada juba alates IT-protseduuri planeerimisest ning see tegevus tuleb integreerida infoturbehaldusega. Ainult nii saab tagada, et kõikide oluliste aspektidega on arvestatud ja kõik tööülesanded täidetakse tõhusalt.

Isikuandmete kaitse nõuete järgimist kontrollib ja nõustab Eestis Andmekaitse Inspektsioon (www.aki.ee). Täpsema loetelu isikuandmete kaitse aspektidega seotud ülesannete ja nende täitmiseks vajalike reeglite kohta leiate meetmest M 2.1 IT kasutajate vastutuse ja reeglite kehtestamine .

Isikuandmete kaitsega seotud ülesannete täitmiseks sobib väga hästi isikuandmete töötlemise eest vastutava isiku ametikoha loomine ja selle integreerimine infoturbehaldusega. Isikuandmete töötlemise eest vastutava isiku teenust võib ka sisse osta. Isikuandmete spetsialist (isikuandmete töötlemise eest vastutav isik) kontrollib isikuandmete kaitse nõuete järgimist, kuid moodustab samal ajal ka omamoodi ühenduslüli enda vastutusel isikuandmete kaitse nõudeid järgiva osakonna ja Andmekaitse Inspektsiooni vahel. Ka nendes valdkondades, mille jaoks eraldi isikuandmete töötlemise eest vastutavat isikut ametisse ei nimetata, tuleb aisikundmete kaitse nõuetest siiski kinni pidada. Selle ülesande võib enda kanda võtta infoturbehalduse osakond. Selleks tuleks sisse seada vähemalt organisatsioonisisene IT-revisjon ja isikuandmete kaitse kontrollimine (vt M 2.110 Andmeprivaatsuse suunised logimisprotseduurides).

Isikuandmete töötlemise eest vastutava isiku nimetamine ametisse

Isikuandmete töötlemise eest vastutava isikuna võib töötada ainult isik, kellel on vastavate ülesannete täitmiseks sobivad erialateadmised ning kes on piisavalt usaldusväärne. Tööülesannete täitmiseks peavad isikuandmete töötlemise eest vastutaval isikul olema vajalikud teadmised tehnoloogiast, töökorraldusest ja seadustest. Ta peab tundma andmealase enesemääratluse õigust, isikuandmete ja inimeste põhiõiguste seost. Lisaks peab isikuandmete töötlemise eest vastutav isik hästi tundma institutsiooni ja tal peavad olema väga põhjalikud teadmised infotehnoloogiast. Kui töötaja ei ole piisavalt kvalifitseeritud, tuleb talle anda võimalus end koolitada. Isikuandmete töötlemise eest vastutav isik peaks oma kogemuste põhjal tundma ametiasutuse või ettevõtte ülesandeid ja tööviise, et olla suuteline täitma alle määratud kontrolli- ja nõustamisülesandeid. Isikuandmete töötlemise eest vastutav isik ei pea ilmtingimata täitma ainult oma töökohustusi. Olenevalt töödeldavate andmete s.h isikuandmete mahust ja hulgast ning sellega seotud isikuandmete kaitse probleemidest võib tal olla ka muid tööülesandeid. See võib sobida eriti just väikestele ametiasutustele ja ettevõtetele, kuid alles pärast seda, kui töötaja on suutnud ennast kõigega kurssi viia ja erialased tööprotsessid on juurutatud. Seejuures tuleb kindlasti jälgida, et ei tekiks huvide konflikte ega liigset sõltuvust, mis võiks kahjustada tööülesannete täitmist. Huvide konfliktid on kerged tekkima eriti siis, kui isikuandmete töötlemise eest vastutava isiku töö ei piirdu üksnes enda tööülesannetega, vaid ta peab tegelema ka per-

sonali või infotehnoloogiaga või täitma tööülesandeid institutsiooni osakondades, kus töödeldakse suurel hulgal delikaatseid isikuandmeid, või kui on muu hulgas ka veel konfidentsiaalsusspetsialist. Seevastu isikuandmete töötlemise eest vastutava isiku ja infoturbespetsialisti ülesandeid on võimalik ühendada suhteliselt probleemivabalt.

Kui infoturbespetsialisti ametikoht on sisse seatud nii, et ta ei sõltu IT töö eest vastutavast osakonnast, on nende kahe ametikoha ühendamine isegi soovitatav. Selle ametikoha täitmiseks võivad sobida ka organisatsioonis õigusnõustamise või töökorralduse eest vastutavate osakondade juhid või kaastöötajad. Tulevase usaldusväärse koostöö tagamiseks tuleks isikuandmete töötlemise eest vastutava isiku ametisse nimetamise protsessi võimalikult vara kaasata ka töötajate esindajad.

Isikuandmete töötlemise eest vastutava isiku ametikoha loomisest tuleb kõikidele töötajatele teada anda. Teavitamise käigus tuleb töötajatele selgitada, et neil on võimalik nii isiklike kui ka tööalaste isikuandmete kaitse küsimustega pöörduda otse isikuandmete töötlemise eest vastutava isiku poole. Isikuandmete töötlemise eest vastutava isiku eduka töö tagamiseks on väga tähtis, et tema ametikoht oleks sõltumatu ja organisatsioonis hästi esile tõstetud. Isikuandmete töötlemise eest vastutav isik ei tohi töötada mitte ühegi sellise organisatsiooniüksuse alluvuses, mida ta peab kontrollima. Hierarhiliselt peaks isikuandmete töötlemise eest vastutav isik kuuluma juhatusse, nt alluma otse juhatusele või moodustama eraldi üksuse. See teave peab olema kajastatud organisatsiooni struktuuriskeemis ja seega kõikidele töötajatele teada. Isikuandmete töötlemise eest vastutaval isikul peab olema otsene ja alatine õigus võtta ühendust ametiasutuse või ettevõtte juhtkonnaga ning saada õigel ajal põhjalikku infot kõigest ametiasutuses või ettevõttes toimuvast, mis on otseselt seotud tema tööga. Teda tuleb kaasata isikuandmete kaitse valdkonna jaoks olulistesse protsessidesse, samuti tuleb teda teavitada isikuandmetega ümberkäimist puudutavatest plaanidest. Isikuandmete töötlemise eest vastutava isiku tööd peavad toetama nii ettevõtte/ametiasutuse juhtkond kui ka töötajad. Kui on tarvis, tuleb isikuandmete töötlemise eest vastutava isiku käsutusse anda abipersonal ning lisaseadmed ja -vahendid. Juhul, kui isikuandmete töötlemise eest vastutaval isikul läheb tarvis spetsiifilist tehnilist või õigusnõustamist, tuleb talle vastavates osakondades määrata kindlad kontaktisikud, kelle poole ta saab vajaduse korral pöörduda.

Isikuandmete töötlemise eest vastutav isik peab hoolitsema selle eest, et ettevõte või ametiasutus täidaks piisaval määral isikuandmete kaitse nõudeid. Ta täidab oma ülesandeid peamiselt nõustamise ja kontrollimisega. Esmaülesanne on nõustamine. Isikuandmete töötlemise eest vastutav isik on kõikide isikuandmete kaitset puudutavate küsimuste korral töötajate usaldusväärne kontaktisik. Vigade või tegematajätmiste avastamisel peaks isikuandmete töötlemise eest vastutav isik esmalt koos asjaosalistega püüdma leida tulemuslikke lahendusi.

Siinkohal on oluline, et töötajatele teadvustataks isikuandmete töötlemise nõuete järgimise positiivseid tagajärgi ja selle kasulikkust. Õige rakenduse korral on isikuandmete kaitse töödes abiks ega mõju koormavana. Kui mõni ametiasutus või ettevõte kogub liiga palju isikuandmeid, kustutab need liiga hilja ära või edastab neid volitamata, ei riku ta mitte üksnes isikuandmete kaitse seadust, vaid kulutab ka oma tööprotsesside täitmiseks ettenähtust rohkem aega ja raha. Isikuandmete kaitse nõuete järgimine on esmajoones kodaniku- ja kliendisõbraliku käitumise tunnus, sest see muudab protseduurid läbipaistvaks. Isikuandmete töötlemise eest vastutaval isikul on õigus teha enda valitud ajal etteteatamiseta kontrolle. Sellega seotud tööülesannete täitmiseks on tal õigus pääseda kõikidesse asjakohastesse ruumidesse ja ta võib tutvuda kõikide dokumentidega, mis sisaldavad isikuandmeid või mis puudutavad nendega ümberkäimist. Seevastu tutvumine personaliaktide, arstipaberite, riiklike abirahade maksmist kajastavate paberite ja turbeprotsessidega on lubatud üksnes asjakohaste isikute loal.

Personalihalduse valdkonda kontrollides ja nõustades tuleb arvestada nende sõltumatusega. Samas ei tähenda see, et kontrolle ei tohiks üldse teha. Isikuandmete töötlemise eest vastutav isik peab ametiasutuse või ettevõtte juhtkonnal aitama isikuandmeid kaitsta ja vältida vahejuhtumeid, mis võiksid kahjustada institutsiooni mainet. Ta peaks suhtlema ka töötajate esindusega. Hea koostöö pole vajalik mitte ainult isikuandmete töötlemise konfidentsiaalsuse seisukohalt. Erialase pädevuse tagamiseks peab isikuandmete töötlemise eest vastutav isik end pidevalt täiendama. Väga kasulik on ka kogemuste vahetamine sama tegevusvaldkonna kolleegidega ja sarnaseid ülesandeid teistes ametiasutustes või ettevõtetes täitvate isikuandmete töötlemise eest vastutavate isikutega.

Isikuandmete töötlemise eest vastutava isiku tööülesanded olenevad kõige muu kõrval ka ametiasutuse või ettevõtte suurusest, ülesehitusest ja liigendusest. Järgnev kataloog annab ülevaate isikuandmete töötlemise eest vastutava isiku võimalikest tööülesannetest nii ametiasutustes kui ka ettevõtetes:

Peamised tööülesanded

- Nõustada juhtkonda ja kõiki töötajaid isikuandmete kaitsega seotud küsimustes
- Teha etteteatamisega ja etteteatamiseta kontrolle

Ülevaated ja registrid

- Pidada andmetöötlussüsteeme kajastavaid registreid või kontrollida registripidamist
- Tagada ülevaade kõikidest failidest ja protseduuridest, milles salvestatakse või töödeldakse isikuandmeid
- Täita seadustest tulenevaid teavitamiskohustusi
- Kontrollida volitatud töötleja poolt isikuandmete kaitse seaduse nõuetekohast täitmist

Koostöö

- Koostada juhiseid, ringkirju ja muid ametlikke dokumente, mis reguleerivad ümberkäimist isikuandmetega, või abistada nende koostamisel
- Välja töötada teabe väljastamist, parandamist, kasutuse tõkestamist ja kustutamist käsitlevad nõuded, anda avalikkusele suunatud teavet, töötada läbi kodanikelt laekuv isikuandmetega seotud info ja esitatud küsimused
- Osaleda logifailide analüüsimises
- Osaleda isikuandmete töötlemisega seotud protseduuride juurutamises
- Osaleda infoturvet kajastavate reeglistike koostamises

Koolitamine ja koostöö

- Koolitada töötajaid andmekaitse alal ja võtta isikuandmetekaitse nõuete järgimiseks vajalikke meetmeid
- Anda juhtkonnale regulaarselt või vajaduse korral aru isikuandmete kaitse nõuete järgimise hetkeseisust ettevõttes või ametiasutuses
- Teha koostööd infoturbespetsialistiga
- Olla kontaktisikuks Andmekaitse Inspektsiooni ja teiste riiklike järelvalve asutustele. Vajadusel ka teiste asutuste või ettevõtete isikuandmete töötlemise eest vastutavale isikule

M 2.503 Isikuandmete kaitse kontseptsiooni aspektid

Algatamise eest vastutavad: infoturbespetsialist, i sikuandmete töötlemise eest vastutav isik

Rakendamise eest vastutavad: infoturbespetsialist, i sikuandmete töötlemise eest vastutav isik

Nii ettevõttes kui ka ametiasutuses tuleb kindlaks määrata ja dokumenteerida isikuandmete töötlemise nõuded ja nende täitmise tingimused. Sellega on võimalik käsitleda olukordi, kus üksikasjalikumad uuringud ja individuaalse isikuandmete kaitse kontseptsiooni väljatöötamine võivad osutuda teatud protseduuride jaoks liiga töömahukaks, ühe tervikuna. Lisaks luuakse sellega baas, mis kehtib üldjuhul kõikidele vanadele IT-süsteemidele ja mida saab kasutada ka uute IT-süsteemide jaoks, millele ei ole isikuandmete kaitse kontseptsiooni veel välja töötatud. Esmatähtis on muidugi kehtivate seaduste järgimine. Selles valdkonnas leidub aga ka palju üldisi aspekte, millega tuleb isikuandmete töötlemisel kindlasti arvestada. Allesitatud aspektide loetelu ei ole täielik, vaid üksnes viiteks konkreetsete isikuandmete kaitse kontseptsioonide koostamisel. Isikuandmete kaitse kontseptsiooni eesmärk on luua kokkuvõtlik õigusalaseid isikuandmete kaitse aspekte käsitlev dokumentatsioon ning seda kontseptsiooni saab kasutada õigusalaste isikuandme kaitse aspektide kontrollide jaoks. Aspektid, millega peab arvestama:

- Kõikide protseduuride loetelu
- Töödeldavate isikuandmete maht ja andmete kasutamine: kas andmetes kajastuvad viited isikutele on otsesed (nt aadress, maksuandmed) või kaudsed (auto registreerimisnumber, katastriüksus)?
- Andmetöötluse õiguslik alus
- Sihtotstarve
- Arvestamine eri liiki andmetega
- Andmete liigse kuhjumise ja mõttetute korduste vältimine
- Andmete kaitsevajadus: kaitsevajaduse väljaselgitamine turbeastmete kontseptsiooni alusel, võttes arvesse kasutusotstarvet (astmed: madal, keskmine, kõrge) ja ka õigusalaseid isikuandmete kaitse aspekte.
- Automaatsete päringuprotseduuride eripärad
- Automaatse analüüsi keeld
- Teabe saamise, korrigeerimise, kasutuse tõkestamise, vaidlustamise ja kahjunõude õigus
- Seaduserikkumiste ja nende tagajärgede vältimine
- Andmete kustutamine
- Logimine
- Eelkontrollid
- Isikuandmete kaitsega seotud töötajate vastutusalad (vt M 2.502 Isikuandmete kaitse vastutusalade kindlaksmääramine)
- Ametiasutuse või ettevõtte isikuandmete töötlemise eest vastutava isiku kaasamise protseduur ja selle dokumentatsioon

- Riikliku kontrolliinstitutsiooni või järelevalveasutuse kaasamise protseduur ja selle dokumentatsioon
- Isikuandmete töötlemisega seotud tellimistööde lepingusätted
- Isikuandmete töötlemise erinõuded, mis tulenevad koostööst kolmandate riikidega (muu hulgas *safe harbour* 'i reeglid)
- Teostuse hetkeolukorra võrdlemine eesmärgiga, revisjonid ja õigusalased isikuandmete kontrollid
- Isikuandmete töötlemise nõuete järgimise kohustus ja vastavad koolitused
- Kasutusse lubamise protseduurid
- Iga protseduuri metoodika kirjeldus
- Registrite teavitamine (vt M 2.510 Teabepäringuprotseduuride reeglid isikuandmete töötlemisel) Isikuandmete töötlemise eest vastutava isiku nimetamine ametisse ja tema tööülesanded (vt M 2.502 Isikuandmete kaitse vastutusalade kindlaksmääramine)
- Erinevate isikuandmete kaitse õigusvaldkonda puudutavate vastutusalade järgimine

Täiendavad kontrollküsimused:

- Kas kõiki töötajaid (sh uusi) teavitatakse isikuandmete kaitse kontseptsioonist ja kas neile tehakse selgeks, et selle järgimine on kohustuslik, ning kas nad saavad asjakohase väljaõppe?
- Kas isikuandmete kaitse kontseptsiooni uuendatakse regulaarselt?
- Kas töötajatele on antud isikuandmete kaitse kontseptsiooni järgimiseks vajalikud töövahendid?
- Kas ametisse on nimetatud isikuandmete töötlemise eest vastutav isik?
- Kas isikuandmete töötlemise eest vastutaval isikul on olemas kogu vajalik dokumentatsioon (nt protseduuride metoodika kirjeldused)?

M 2.504 Õigusalaste raamtingimuste kontrollimine ja isikuandmete töötlemise eelkontroll

Algatamise eest vastutavad: erialaspetsialist, infoturbespetsialist, isikuandmete töötlemise eest vastutav isik

Rakendamise eest vastutavad: erialaspetsialist, infoturbespetsialist, isikuandmete töötlemise eest vastutav isik

Isikuandmete kaitse seaduse kohaselt on isikuandmete töötlemine iga isikuandmetega tehtav toiming, sealhulgas andmete kogumine, salvestamine, korrastamine, säilitamine, muutmine ja avalikustamine, juurdepääsu võimaldamine isikuandmetele, päringute teostamine ja väljavõtete tegemine, isikuandmete kasutamine, edastamine, ristkasutamine, ühendamine, sulgemine, kustutamine või hävitamine, või mitu eelnimetatud toimingut, sõltumata toimingute teostamise viisist ja kasutatavatest vahenditest. Isikuandmete töötlemine on lubatud üksnes andmesubjekti nõusolekul, kui seadus ei sätesta teisiti.

Delikaatsete isikuandmete töötlemisel, kui isikuandmete töötleja ei ole määranud kindlaks isikuandmete kaitse seaduse §-s 30 sätestatud isikuandmete kaitse eest vastutavat isikut, on isikuandmete töötleja (vastutav töötleja) kohustatud registreerima delikaatsete isikuandmete töötlemise Andmekaitse Inspektsioonis. Kui isikuandmeid töötleb volitatud töötleja, esitab käesolevas peatükis sätestatud taotlusi vastutav töötleja ning kasutab selleks inspektsiooni kodulehel olevat elektroonilist lahendust DIAT.

Andmesubjektiks on isik, kelle isikuandmeid töödeldakse.

Isikuandmete töötlemine eeldab õigusalaste raamtingimuste kontrollimist ning selle käigus tuleb arvestada järgmiste aspektidega:

- andmetöötluse ja isikuandmete töötlemise seose kontrollimine;
- andmetöötlusprotsessi lubatavus;
- andmetöötlusprotsessi vajalikkus;
- andmete sihtotstarbeline kasutamine;
- andmete spetsiaalne sihtotstarbeline kasutamine;
- eelkontrolli tegemine.

Nende aspektide analüüsimisel tuleks võimalike keeruliste juriidiliste nüansside, eriti isikuandmetega seotud küsimuste korral konsulteerida juristidega.

Isikuandmete kaitse töötlusprotsessi lubatavus

Isikuandmeid võib koguda vaid ulatuses, mis on vajalik määratletud eesmärkide saavutamiseks ning koos andmete kvaliteedi (tõesuse) põhimõttega väljendab see, et isikuandmeid võib koguda üksnes ulatuses, mis on vältimatult vajalik andmetöötluse eesmärgi saavutamiseks. Isiku andmete töötluse lubatavuse kontrollimine peaks üldjuhul toimuma koostöös selle valdkonna eest vastutavate instantsidega.

Enne isikuandmete kogumist, töötlemist ja kasutamist tuleb kontrollida:

- kas selline tegevus on isikuandmete kaitse seaduse või mõne muu seadusesättega lubatud või kas on kehtestatud vastav kohustus;

Isikuandmete salvestamisel, muutmisel ja edastamisel kinnistes asutustes tuleb kontrollida:

- kas nimetatud andmetöötlusprotsessid põhinevad lepingulisel suhtel või mõnel muul sellisel asjasse puutuva poolega sõlmitud usaldusväärsel õigussuhtel;
- kas need protsessid on seotud vastutava asutuse õigustatud huviga ning kas on välistatud kahtlus, et isikuandmete kaitse põhimõte ei kaalu üles õigustatud huvi.

Vajalikkuse kontroll

Avalike asutuste töös kehtib põhimõte, et isikuandmeid tohib koguda vaid seaduse alusel (IKS) tööülesannete täitmiseks. See hõlmab olukordi, kus ilma isikuandmeteta oleks vajalike tööde tegemine kas võimatu või märkimisväärselt raskem. Isikuandmete kogumise vajalikkust tuleb iga juhtumi puhul eraldi kontrollida. Töötajad tohivad juurde pääseda ainult enda tööülesannete täitmiseks vajalikele isikuandmetele. Selle nõude järgimine osutub keeruliseks süsteemi haldajate puhul. Süsteemi haldajatel on enam levinud toodete korral täielik juurdepääs kõikidele andmetele s.h isikuandmetele. Ka süsteemi haldajate juurdepääsu andmetele tuleb teatud määral piirata, eriti kui tegu on salastatud andmetega, nt personaliaktidega. Selleks saab kasutada krüpteerimist, juurdepääsu piiramist, astmelisi volituskontseptsioone, menüüde juhtimist, süsteemiadministraatori töörollide jaotamist erinevate töötajate vahel ning süsteemi haldaja töö turvalist logimist. Tehnoloogia juurutamisel tuleks valida sellised protseduurid, mille puhul töödeldakse isikuandmeid võimalikult vähe. Isikuandmete töötluses tuleb vältida andmete liigset kuhjumist ja mõttetuid kordusi. Kui võimalik, tuleks protseduurid muuta anonüümseks või kasutada pseudonüüme. Teenuste osutamisel tuleb klientidele kindlasti pakkuda anonüümse protseduuri kasutamise võimalust.

Andmete sihtotstarbelise kasutamise kontroll

Enne isikuandmete salvestamist, muutmist ja kasutamist tuleb kontrollida, kas selline tegevus on kooskõlas nende andmete kogumisele kehtestatud eesmärkidega. Juhul kui isikuandmeid ei kogutud, tuleb jälgida, kas selline tegevus vastab eesmärkidele, milleks need andmed salvestati. Sihtotstarbelise kasutuse põhimõtte kõrval eksisteerib mitmeid, kohati väga kaugeleulatuvaid erandeid.

Isikuandmete spetsiaalse sihtotstarbelise kasutamise kontroll

Isikuandmete kaitse kontrollideks, varukoopiate tegemiseks või andmetöötlussüsteemi igapäevaste tööprotsesside tagamiseks salvestatavate isikuandmete puhul tuleb kontrollida, kas neid kasutatakse eranditult vaid nimetatud eesmärkidel.

Eelkontroll

Eelkontroll tehakse enne isikuandmeid töötlevate automaatprotseduuride esmakordset kasutust, et selgitada välja selle võimalikud ohud seoses inimeste andmealase enesemääratlusõigusega. Kui isikuandmete töötlemisega kaasnevad asjasse puutuvate isikute jaoks ohud, st kui see piirab nende õigusi ja vabadusi, nt kui töödeldakse delikaatseid isikuandmeid (teavet rassilise ja etnilise päritolu ning poliitiliste, usuliste ja filosoofiliste veendumuste, ametiühingusse kuulumise, tervise või seksuaalelu kohta) või kui eesmärk on hinnata kellegi isiksust ja tema

oskusi, võimekust või käitumist, tuleb enne isikuandmete töötlemisega alustamist teha eelkontroll. Eelkontrolli ei pea tegema järgmistel juhtudel: isikuandmete töötlus on seadusega ette nähtud, asjasse puutuvalt isikult on saadud selleks nõusolek, isikuandmete kogumine, töötlemine või kasutamine vastab lepingulise suhte sihtotstarbele või asjasse puutuva osapoolega on sõlmitud mõni muu usaldusväärne õigussuhe. Automatiseeritud protseduure tohib kasutada vaid juhul, kui ollakse veendunud, et nendega ei rikuta inimeste andmealast enesemääratlusõigust.

Siinkohal tuleb kontrollida järgmisi aspekte:

- sissepääsukontroll;
- juurdepääsukontroll;
- kasutuskontroll;
- edasiandmiskontroll;
- sisestamiskontroll;
- tellimuse kontroll;
- käideldavuskontroll;
- erinevatel eesmärkidel kogutud andmete töötlemine peab toimuma üksteisest lahutatult.

Võetavad meetmed peavad vastama tehnika tasemele ning nende võtmise kulud peavad tagama sellise turbeastme, mis vastab andmetöötlusega seotud ohtudele ja kaitstavate isikuandmete liigile. Kui isikuandmeid ei analüüsita automaatprotsessidega, tuleb võtta meetmeid, mis välistavad volitamata isikute juurdepääsu andmete töötlemisele, säilitamisele, transportimisele ja hävitamisele. Seepärast tuleb eelkontrolli tegemise otsus langetada iga juhtumi puhul eraldi.

M 2.505 Isikuandmete töötlemisega seotud tehniliste-töökorralduslike meetmete kindlaksmääramine vastavalt tehnika tasemele

Algatamise eest vastutab: asutuse/ettevõtte juhtkond, infoturbespetsialist, isikuandmete töötlemise eest vastutav isik

Rakendamise eest vastutavad: andmekaitsespetsialist, infoturbespetsialist, isikuandmete töötlemise eest vastutav isik

Üks väga oluline valdkond isikuandmete kaitse tagamisel on tehnilised ja töökorralduslikud meetmed, mida on tarvis inimeste andmealase enesemääratlusõiguse tagamiseks ning mis kaitsevad isikuandmeid väärkasutuse, vigade ja õnnetusjuhtumite eest. See, millised meetmed on vajalikud, ei olene mitte üksnes isikuandmete liigist ja nende kasutamise eesmärgist, vaid ka töökorralduslikest raamtingimustest, ruumioludest, personali arvukusest jms. Isikuandmete kaitse seaduse (IKS) kohaselt peavad meetmed olema järgmised:

- tõkestama volitamata isikute sissepääsu isikuandmeid töötlevate või neid kasutavate süsteemidega ruumidesse (sissepääsukontroll);
- tagama, et volitamata isikud ei saaks andmetöötlussüsteeme kasutada (juurdepääsu autentimine);
- tagama andmetöötlussüsteemide tööalaseks kasutamiseks volitatud isikute juurdepääsu ainult nende volitusastme kohastele andmetele ning tõkestama isikuandmete volitamata töötlemise, kasutamise ja salvestusjärgse volitamata lugemise, kopeerimise, muutmise ja eemaldamise (kasutuskontroll, rollipõhine juurdepääs - autentimine);
- tõkestama isikuandmete volitamata lugemise, kopeerimise, muutmise ja eemaldamise nende elektroonilisel edastamisel, transportimisel ja salvestamisel ning tagama kontrollimisvõimaluse, mille abil saab kindlaks teha isikuandmete edastamise lubatud sihtkohad (edasiandmiskontroll, rollipõhine juurdepääs – autentimine, logid);
- tagama tagantjärele rakendatava kontrollivõimaluse, millega saab kindlaks teha, kas andmetöötlussüsteemi on lisatud isikuandmeid, kas neid andmeid on muudetud või eemaldatud ning kes seda tegi (sisestamiskontroll, logid);
- tagama tellija nõuete täitmise lepingu alusel töödeldavate isikuandmete töötlemisel (tellimuse kontroll);
- kaitsma isikuandmeid juhusliku hävitamise või kaotamise eest (käideldavuskontroll);
- tagama erineval eesmärgil kogutud andmete töötlemise üksteisest lahutatult.

Tehniliste ja töökorralduslike meetmete puhul on määrav, et neid mõistetaks kui terviklikku koostoimivat kaitsesüsteemi. Selline kaitsesüsteem ei hoolitse mitte üksnes seadustega kehtestatud isikuandmete kaitse nõuete täpse järgimise eest, vaid tagab ka hästi reguleeritud ja toimivad tööprotsessid. Seetõttu on oluline, et isikuandmete kaitse kontseptsiooni arendataks ja kasutataks alati kooskõlas kõikide organisatsiooniüksuste erialavaldkondade kontseptsioonide ja muude turbekontseptsioonidega, nt infoturbekontseptsiooniga. Meetmete võtmisega seotud

tööde maht peaks olema mõistlikus suhtes soovitud turbeastmega (turbeastmete kohta vt standard ISKE turvameetmed). Mida raskemad on õiguste rikkumisega kaasnevad oletatavad tagajärjed ja mida suurem on kahju tekkimise tõenäosus, seda suurem võib olla mõistlik tööde maht. Eesmärk on valida võetavaid meetmeid, mitte muuta eesmärgiks seatud turbeastet. Vajalikuks tunnistatud meetmeid tuleb võtta ka siis, kui need peaksid IT-rakenduse arendamist ja kasutamist raskendama. Kui eesmärke ei ole võimalik ette nähtud meetmetega tagada, tuleb kas leppida töömahu suurenemisega või kaaluda mõne teise, väiksema töömahuga protseduuri rakendamist. Valitud meetmeid tuleb tehnika arenedes muuta, et need vastaksid alati tehnika tasemele. Samuti tuleb tagada, et institutsiooni infoturvet ja andmekaitset käsitlevad suunised vastaksid seadustes ette nähtud isikuandmete kaitse nõuetele.

Kui institutsioonis on loodud isikuandmete töötlemise eest vastutava isiku ametikoht, tuleks selliste üldiste suuniste, ringkirjade jms koostamisse, millega juhtkond reguleerib isikuandmetega ümberkäimist, kaasata ka isikuandmete töötlemise eest vastutav isik. Samuti tuleks isikuandmete töötlemise eest vastutav isik kaasata kõikidesse tööandja ja töötajate esinduse vahel isikuandmetega ümberkäimist reguleerivate kokkulepete sõlmimisse. Kehtestatud reeglite järgimist tuleb kontrollida.

Tehnilised-töökorralduslikud meetmed võivad olla näiteks järgmised:

- andmete füüsiline kustutamine (vt M 4.32 Andmekandjate füüsiline kustutamine enne ja pärast nende kasutamist);
- krüpteerimisprotseduuride kasutamine;
- organisatsioonisisesed IT- ja isikuandmete kaitse reeglid (vt M 2.1 IT kasutajate vastutuse ja reeglite kehtestamine);
- protseduuride logimine ja dokumenteerimine nende jälgitavuse tagamiseks (vt M 4.25 Logimine Unix-süsteemis).

M 2.506 Töötajate kohustamine ja koolitamine isikuandmete töötlemise alal

Algatamise eest vastutab: ametiasutuse/ettevõtte juhtkond

Rakendamise eest vastutavad: infoturbe juht, personaliosakond, juhtkond, isikuandmete töötlemise eest vastutav isik

Isikuandmete töötlemisega tegelevatele töötajatele kehtib konfidentsiaalsuskohustus, millest tuleb töötajaid teavitada. Konfidentsiaalsuse kohustus jääb kehtima ka pärast tööde lõpetamist. See kohustus tuleb töötajatele sobival moel teatavaks teha, dokumenteerida ning vajaduse korral seda protsessi ka korrata.

Teadmiseks

Ka siis, kui konfidentsiaalsuse hoidmiseks vajalik töötajate kohustamise või koolitamise nõue kehtib juba mõnel muul põhjusel, tuleks töötajaid siiski uuesti kohustada või koolitada, et suurendada nende teadlikkust isikuandmete kaitsest.

M 2.507 Töökorralduslikud meetmed osapoolte õiguste tagamiseks isikuandmete töötlemisel

Algatamise eest vastutavad: isikuandmete töötlemise eest vastutav isik, erialaspetsialist

Rakendamise eest vastutavad: isikuandmete töötlemise eest vastutav isik, erialaspetsialist

Osapoolte õiguste tagamiseks seoses teabe saamisega, andmete parandamisega, kasutuse tõkestamisega ning faili- ja protseduuriloendite lugemisega (kui sellised loendid on ette nähtud) tuleb välja töötada asjakohased tehnilised-töökorralduslikud protseduurid. Nimetatud protseduurid peavad osapooltel võimaldama oma õigusi rakendada kiiresti ja otstarbekohaselt.

Näited

- Isikuandmete töötlemisega seotud protseduur peab sisaldama kas analüüsiprogrammi või menüüpunkti, millega saab kõik asjasse puutuva isiku kohta salvestatud andmed täielikult välja printida.
- Protseduuriloend automatiseeritakse andmebaasiga nii, et teatud märksõnu kasutades saab lihtsalt juurde pääseda suurtele andmehulkadele ning koos sellega ka vastastikustele seostele.

M 2.508 Protseduuriloendite haldamine ja teavitamiskohustuste täitmine isikuandmete töötlemisel

Algatamise eest vastutavad: isikuandmete töötlemise eest vastutav isik , IT-juht

Rakendamise eest vastutavad: isikuandmete töötlemise eest vastutav isik , erialaspetsialist

Kui tsentraalse andmetöötluse puhul tuleb tagada ülevaade üksnes tsentraalsetest süsteemidest, siis detsentraalse andmetöötluse korral tuleb üles märkida kõik kasutatavad IT-süsteemid. Institutsioonil peab olema pidevalt ajakohastatav loend kogu kasutatava riist- ja tarkvara, rakendatavate protseduuride ning seni kogutud isikuandmete kohta. Osas isikuandmete kaitse-eeskirjades võiksid olla selliste loendite koostamiseks esitatud ka konkreetsed nõuded. Automaatsete andmetöötlusprotseduuride, st isikuandmete kogumise, töötlemise ja kasutamisega seotud protseduuride kohta peavad ülevaadet pidama (protseduuriloendit haldama) selle eest vastutavad organisatsiooniüksused.

Teatud tingimustel on ka kinnised asutused kohustatud enda peetavate registrite kohta, mis langevad suures osas kokku protseduuriloendiga, esitama teavet vastavale järelevalveasutusele. Teabe edastamise kohustus võib kehtida eelkõige kriminaaljälituse ja riskiennetuse valdkonnas. Selleks et institutsiooni isikuandmete töötlemise eest vastutaval isikul oleks võimalik enda kohustusi täita, peavad andmed olema täielikud ja võimalikult värsked. Siinkohal tuleb erilist tähelepanu pöörata sellele, et andmetöötluse õiguslik alus ja sihtotstarve oleksid esitatud piisavalt detailselt. See võimaldab hiljem selle sihtotstarvet muuta üksnes seadusega ette nähtud piirides.

M 2.509 Isikuandmete kaitse seadusele vastav kasutusse lubamine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, isikuandmete töötlemise eest vastutav isik
Rakendamise eest vastutavad: ametiasutuse/ettevõtte juhtkond

Tarkvara ja IT-protseduuride tööd tuleb katsetada süstemaatiliselt väljatöötatud andmetega (katsetusandmetega, mitte reaalsete isikuandmetega), võttes aluseks katsetusplaani, millest nähtub soovitud eesmärk (vt M 2.83 Tüüptarkvara testimine). Hulgikatsetusi saab vajaduse korral teha ka anonüümseks muudetud originaalandmetega, eeldusel et järelevalveametilt on saadud selleks luba ja protsessi käigus järgitakse järelevalveameti nõudeid. Järelevalveametilt saadud luba originaalandmete anonüümseks muutmise kohta ja kõikide testide tulemused tuleb dokumenteerida viisil, mis vastab revisjoninõuetele.

Üldjuhul originaalandmetega (reaalsete isikuandmetega) ei tohi teostada teste testkeskkonnas.

Testid anonüümseks muutmata originaalandmetega (reaalsete isikuandmetega) on lubatud vaid järgmistel juhtudel:

- testkeskkond vastab samadele turvanõuetele nagu toodangukeskkond (live);
- mõne muu õigusnormiga on antud selleks konkreetne luba;
- erandjuhud, kus vaatamata testkeskkonnas rakendatud originaalilähedastele andmetele on võimalik kasutatavates tööprotsessides esinevaid vigu tuvastada üksnes originaalandmetega või kui protseduuri turvet ei ole võimalik tagada mõnel muul viisil;
- kui anonüümseks muudetud originaalandmete kasutamine muudaks konkreetse testprotsessi töömahu ebamõistlikult suureks;
- kui testimisel ja testide tulemuste analüüsimisel suudetakse andmekaitse- ja infoturbenõudeid järgides tagada asjakohaste isikute isikuandmete piisav kaitse;
- kui on tagatud, et testide jaoks vajalikele andmetele pääsevad juurde üksnes töötajad, kellel on volitused teha testimisi ja parandada testimiste käigus esinevaid vigu;
- kui on tagatud, et andmetele on lubatud juurde pääseda vaid isikutel, kes on allutatud konfidentsiaalsuslepetele ja eriti andmekaitsenõuete tagamist puudutavatele ettekirjutustele.

Planeeritud testide läbiviimist tuleb piisavalt vara teavitada kas ettevõtte või ametiasutuse isikuandmete töötlemise eest vastutavat isikut või mõnda selle eest vastutavat üksust. Originaalandmetele tehtud pöördused, millega kaasneb kopeerimine, tuleb dokumenteerida. Pärast testimiste lõpetamist tuleb originaalandmete koopiatestkeskkonnast kas viivitamata kustutada või testkeskkonna sees anonüümseks muuta. Originaalandmete koopiate kasutamine tuleb revisjoninõuete kohaselt dokumenteerida. Selleks tuleb üles märkida nende kasutamise vajadus, põhjendus, andmete maht, kasutamise kestus ja võetavad turbemeetmed, samuti nendele katsetustele eelnenud katsetused testandmetega.

IT-protseduuride vastuvõtmine, kasutusse andmine, installimine ning paigaldami-

ne ja kasutamine peavad olema reguleeritud. Lisateavet leiate meetmest M 2.62 Tarkvara vastuvõtuprotseduurid ja moodulist B 1.10 Tüüptarkvara . Isikuandmetega seotud IT-protseduuride lubamiseks kasutusse on vaja ka kontrollida, kas need vastavad isikuandmete kaitse õigusnormidele.

M 2.510 Teabepäringuprotseduuride reeglid isikuandmete töötlemisel

Algatamise eest vastutavad: isikuandmete töötlemise eest vastutav isik, IT-juht

Rakendamise eest vastutavad: isikuandmete töötlemise eest vastutav isik, erialaspetsialist

Automaatsete teabepäringuprotseduuride korral tuleb pöörata erilist tähelepanu isikuandmete kaitse- ja andmevarundusaspektidele, sest pärast ühenduse loomist muutuvad päringu esitajale automaatselt, st ilma andmete väljastamise eest vastutava instantsi eraldi kontrollita, kättesaadavaks kas kõik isikuandmed või suur osa neist. Seetõttu näevad vastavad seadused ette, et teabepäringuprotseduuride korral kehtib kohustus järgida tehnilisi ja töökorralduslikke isikuandmete kaitse aspekte juba alates protseduuride planeerimisest. Automaatseid teabepäringuprotseduure defineeritakse seadustes kui andmetöötluse üht faasi, mille käigus avalikustatakse kas salvestatud või andmetöötluse tulemusel saadud isikuandmed kolmandatele osalistele viisil, mille korral seab andmetöötlusega tegelev osaline andmed kasutuseks valmis ning sellele järgnevad andmepäringud. Automaatse päringuprotseduuri näide on elektrooniline kinnistusraamat, mille puhul lubatakse volitatud kasutajatel seadusega reguleeritud korra kohaselt enda arvutist *online* -režiimis tutvuda kinnistusraamatu andmetega. Sellist teenust kasutavad eriti notarid, juristid, pangaasutused ja kindlustusseltsid ning riigiasutused, kes vajavad enda tööülesannete täitmiseks sageli kinnistusraamatu andmeid.

Iga päringu lubatavuse eest vastutab teabe saaja.

Järgnevalt kirjeldatakse automaatsete teabepäringuprotseduuride juurutamisele seaduste põhjal kehtivaid spetsiifilisi eeldusi. Lubatavuse kontrollimiseks tuleb kindlaks määrata ja dokumenteerida teabepäringuprotseduuri olulised üksikasjad. Üldised aspektid:

- Päringuprotseduuri juurutamise põhjus, eesmärk ja protseduuri osapooled
- Päringuprotseduuri kasutusvolituste kindlaksmääramine ja kontrollimine
- Päringute käigus avaldatavate andmete liik ja maht
- Andmekasutuse tõkestamise ja andmete kustutamise tähtajad
- Juhtumid, millal teabepäringu esitajad peavad teavitama andmeid väljastavat osapoolt

Volitamata päringute tõkestusmeetmed:

- Volitamata osapoolte teabepäringuid tuleb tõkestada sobivate meetmetega:
- Ebaõnnestunud katsete hulk, mille korral päringufunktsiooni kasutamine tõkestatakse
- Paroolide vahetamine regulaarsete ajavahemike möödudes: võimaluse korral tuleks paroolivahetus muuta vastavate programmidega kohustuslikuks
- Volitused eriliigiliste isikuandmete teabepäringute tegemiseks peavad olema seotud suurema turbeastmega (kasutaja vallatav vahend ja teadmised)
- Programmidega juhitavad kontrolliprotseduurid logifailide kontrollimiseks

- Logidesse salvestatavate andmete liik ja maht
- Juhuslikkuse põhimõttel tehtavad pistelised kontrollid või pidevlogimine
- Logimise asukoha kindlaksmääramine, st kas logitakse päringu esitaja või andmete väljastaja juures või mõlemas kohas
- Logimiskontseptsioon, mis võimaldaks tagantjärele kindlaks teha, kelle päringuvolitustega teabepäring esitati
- Päringu põhjuste logimine
- Andmepäringute korral tuleb logida, mis ühenduse ja millistesse lõppseadmetesse andmeid edastatakse.

Võrguühendus

Võrku ühendatud IT-süsteemide puhul tuleb kontrollida lõppsüsteemide võrguühendusi. Näiteks tuleb valimisühenduste puhul kontrollida nende jaoks ette nähtud turbemeetmeid, seevastu virtuaalsete püsiühenduste korral on vaja kontrollida, kas on sisse seatud suletud kasutajarühmad. Kohtvõrkudes peaksid kasutajarühmad olema sisse seatud selliselt, et iga rühm moodustaks omaette suletud organisatsiooniüksuse.

M 2.511 Isikuandmete töötlemise tellimustööde reeglid

Algatamise eest vastutavad: isikuandmete töötlemise eest vastutav isik, IT-juht

Rakendamise eest vastutavad: isikuandmete töötlemise eest vastutav isik, erialaspetsialist

Kui isikuandmeid töödeldakse tellimustööna (vastutav töötleja ja volitatud töötleja suhe), lasub isikuandmete kaitse seaduste ja -eeskirjade järgimise kohustus tööde tellijal. Tööde tellija (vastutav töötleja) peab hoolikalt valima, kellele ta selle töö usaldab. Tööde tellimus tuleb seadustes nimetatud tingimuste kohaselt esitada kirjalikult ning mis tahes alltöövõtud tuleb samuti kirjalikult fikseerida. Teatud valdkondade puhul võivad kehtida ka erinõuded. Olenevalt sellest, milline on tellimustööna töödeldavate andmete turbeaste, tuleb töö tegijale (volitatud töötleja) esitada ka vastavad lepingutingimused: mida suurem on turbeaste, seda piiravam ja täpsem peab olema tellimus. Eriti tundlike andmete töötlemisel võib juhtuda, et sellise töö väljasttellimine (nt jälitustoimikud) on keelatud.

Tööde tellijad peavad tagama, et andmetöötlusega seotud tellimustöid tehakse eranditult tellija nõuete kohaselt. Koostööpartner tohib ise allhanketööd kasutada üksnes tööde tellija nõusolekul. Kui tööde tellija ei ole avalik asutus, tuleb isikuandmeid töötlevatel isikutel lasta enne tööleasumist kirjalikult kinnitada, et nad järgivad tööd tehes andmesaladuse nõuet. Tööde tellijale ja vajaduse korral ka isikuandmete töötlemise eest vastutavale isikule peab olema tagatud alatine kontrollivõimalus.

M 2.512 Andmete seostamise ja kasutamise reeglid isikuandmete töötlemisel

Algatamise eest vastutavad: isikuandmete töötlemise eest vastutav isik, IT-juht
Rakendamise eest vastutavad: isikuandmete töötlemise eest vastutav isik, erialaspetsialist

Tüüpiliste IT-rakenduste puhul liigub kasutaja ekraanil nn maskide ja menüüde vahel. Et lihtsustada programmiga töötamist, kuvatakse kasutajale juba eeltäidetud küsimustikke ja palutakse tal valida sobivad vastused. Nii saab ta kasutada üksnes selliseid päringu- ja analüüsifunktsioone, mis on rakendusprogrammile ette nähtud ning mille isikuandmete kaitse aspektid on kontrollitud ja kasutusse lubatud. Kõik teised päringuvõimalused tõkestatakse. Seevastu andmebaasikeelte (nn vabade päringukeelte) ja moodsa office -tarkvara puhul on olukord hoopis teine. Viimased võimaldavad kasutajal ka ise andmekoosluse kohta esitatavaid päringuid sõnastada, selline kasutus väljub aga range menüüpõhise programmikasutuse piiridest. Nii saab teha tarbetuid ja seetõttu ka keelatud analüüse. Kuna tehnoloogia arenedes on praeguseks juba välja töötatud ka lahendused, millega saab n-ö vaba päringukeelega kaasnevaid isikuandmete kaitse ohte vähendada, võib põhjendatud üksikjuhtudel nn vabade päringukeelte kasutamist isegi piirangutega lubada. Sellest hoolimata tuleb välistada isikuvabaduste piiramine. Vastav kooskõlastus tuleb hankida ka töötajate esindusorganilt. Nn vabade päringukeelte ja office -funktsioonide kasutust tuleb võimalikult suures ulatuses piirata. Sellised andmeanalüüsi funktsioonid, mida läheb eeldatavasti kõige rohkem töös tarvis, tuleb kasutajatele kättesaadavaks teha kas menüüde või ekraanimaskidega. Nn vabade päringukeelte kasutamine peaks olema lubatud ainult erandkorras.

Enne nn vabade päringukeelte lubamist isikuandmete andmetöötluseks tuleb kontrollida, kas see on kooskõlas andmete kaitsevajadusega. Kui põhimõttelised vastuolud puuduvad, tuleks arvestada järgmiste nõuetega: süsteemil peab olema filtrisarnane tehniline piiranguvõimalus, mis tagab, et nn vaba päringukeelt saab kasutada üksnes piiratud mahus. Kasutuse mahtu saab piirata näiteks sellega, et töötajale võimaldatakse juurdepääs ainult kindlatele vähem tundlikele andmehulkadele. Filtrifunktsioonist möödahiilimist tuleb hoolikalt tõkestada, eriti programmi tehnoloogiaga. Andmeid, millele selliste päringukeeltega tohib juurde pääseda, ja lubatud päringuliike tuleb eelnevalt kontrollida. Siinkohal on olulised eelkõige järgmised kriteeriumid:

- õiguslik alus töö tegemiseks;
- tõendus selle kohta, et anonüümseks muudetud andmete analüüs ei täida vajalikku eesmärki;
- andmete tundlikkus nende jaoks ette nähtud rakenduses ja süsteemikeskkonnas;
- andmete kasutamise eesmärk ja kontekst.

Isikuandmete kaitse nõuete rikkumised on nn vabade päringukeelte kasutamisel välistatud vaid siis, kui analüüsi tulemused väljastatakse anonüümseks muu-

detud andmetena, st kui tulemusi ei ole võimalik seostada konkreetsete isikutega.

M 2.513 Isikuandmete kaitse nõuetele vastavuse dokumenteerimine

Algatamise eest vastutavad: isikuandmete töötlemise eest vastutav isik, IT-juht

Rakendamise eest vastutab: erialaspetsialist

Enne riist- või tarkvara kasutamist isikuandmete töötlemiseks tuleks kontrollida, kas sellise kasutamise eesmärk on kooskõlas isikuandmete kaitse nõuetega. Siinkohal esitatakse erinevatele IT-süsteemidele (nt võrguühenduseta arvutile või tsentraalsele arvutuskeskusele) väga erinevaid nõudeid. Kontrolli tulemus tuleb dokumenteerida. Selline dokumentatsioon on eriti oluline isikuandmete töötlemisega seotud kontrollide jaoks. Enne isikuandmete automaatset töötlemist rakendavate protseduuride kasutuselevõttu tuleb sellest võimalikult vara teavitada ka ametiasutuse või ettevõtte isikuandmete töötlemise eest vastutavat isikut. Isikuandmete töötlemise eest vastutava isiku ülesanne on valvata (nii olemasolevate kui ka uute) isikuandmete töötlemisse kaasatud andmetöötlusprogrammide kasutust. Seetõttu on soovitatav ametiasutuse või ettevõtte isikuandmete töötlemise eest vastutav isik protsessi kaasata alates esmasest planeerimisest. Nii saab juba planeerimisfaasis vältida isikuandmete kaitse nõuete vastu eksimist, mille tagajärgede hilisem kõrvaldamine võib olla kas väga ajamahukas või kulukas.

M 2.514 Isikuandmete kaitse tagamine igapäevatöös

Algatamise eest vastutab: ametiasutuse/ettevõtte juhtkond

Rakendamise eest vastutavad: isikuandmete töötlemise eest vastutav isik, infoturbespetsialist

IT-revisjoni eesmärk on kontrollida IT-turbekontseptsiooni rakendamist ja seeläbi veenduda andmetöötlusprotsessidele esitatud nõuete täitmises. Selle alla kuulub ennekõike dokumentatsiooni, protseduuride, protseduuride nõuetekohase kasutuse ja kõikide turbemeetmete kontrollimine. Seevastu organisatsioonisisese isikuandmete kaitse kontrolli puhul, mis kuulub enamasti isikuandmete töötlemise eest vastutava isiku vastutusalasse (vt M 2.502 Isikuandmete kaitse vastutusalade kindlaksmääramine), tuleb kontrollida isikuandmete kaitse seadustest tulenevate nõuete täitmist. Selle raames tuleb:

- kontrollida protseduuride vastavust õigusnormidele ja sihtotstarbele;
- teha kindlaks asjasse puutuvate isikute õigused, mis on seotud teabe saamise, andmete parandamise, kasutuse tõkestamise, kustutamise ja kahjunõudega;
- kohustada töötajaid järgima isikuandmete kaitse nõudeid ja tagama töötajate asjakohane väljaõpe;
- hallata faili- ja protsessiülevaateid ning seadmeloendeid;
- kontrollida seadustest tulenevate tehniliste-töökorralduslike ettekirjutuste järgimist sissepääsu-, juurdepääsu-, kasutus-, edasiandmis- ja sisestamiskontrolli, samuti tellimuse ja käideldavuse kontrolli valdkonnas ning töödelda erinevatel eesmärkidel kogutud andmeid üksteisest lahutatult.

IT-revisjoni ja isikuandmete kaitse kontrolli eest vastutavatel töötajatel oleks mõistlik omavahel koostööd teha ja üksteist täiendada. Logiandmete operatiivse analüüsimisega saavad nad näiteks kaasa aidata võimalike väärkasutuste kiirele avastamisele ning logiandmete säilitamise aja ja mahu vähendamisele. Nad võivad nõustada andmetöötlusega seotud organisatsiooniüksuste juhttöötajaid uute kontseptsioonide väljatöötamisel ja olemasolevate protseduuride edasiarendamisel ning täita kompetentse kontaktisiku rolli järelevalveametite ning riikliku või liidumaa isikuandmete kaitse voliniku kontrollivisiitidel. Mõlemat funktsiooni saab töötajatele panna ka lisakohustusena ning väikestes organisatsioonides võib need kaks ametikohta ka ühendada. Samas tuleb alati jälgida, et nimetatud tööülesannete puhul ei tekiks huvide konflikti (vt M 2.502 Isikuandmete kaitse vastutusalade kindlaksmääramine).

M 2.515 Isikuandmete kaitse nõuetele vastav kustutamine ja hävitamine

Algatamise eest vastutab: ametiasutuse/ettevõtte juhtkond

Rakendamise eest vastutavad: infoturbespetsialist, isikuandmete töötlemise eest vastutav isik

Andmete turvaline kustutamine magnetilistelt andmekandjatelt

Tundlike andmete kustutamisel magnetilistelt andmekandjatelt tuleb nii isikuandmete- kui ka infoturbenõuete järgimiseks tagada, et andmed kustutataks turvaliselt, st täielikult ja pöördumatult. Operatsioonisüsteemide tavalistest kustutusfunktsioonidest või ka andmekandja vormindamisest nende nõuete täitmiseks enamasti ei piisa, sest nende variantide puhul saab andmeid vabavaraliste tarkvaratööriistadega hõlpsalt taastada. Andmeid, mida soovitakse turvaliselt kustutada, tuleb töödelda kas füüsiliselt (mehaaniline või termiline hävitamine, andmekandja töötlemine magnetiga) või muuta mitmekordse ülekirjutamisega loetamatuks. Kustutamisel ja ülekirjutamisel tuleb võtta arvesse andmete haldamisele ja salvestamisele kehtivaid erinõudeid, nt andmetest varukoopiate tegemise nõuet, automaatselt süsteemiga või üksikute rakendustega koostatavate ajutiste failide või saalimisfailide nõuet või *journal* 'ite nõuet teatud failisüsteemide korral. Isikuandmete kaitse seisukohast tuleks siinkohal arvestada järgmiste soovitustega:

- Andmete turvaline kustutamine eeldab, et otsuseid langetavad isikud, administraatorid, infoturbespetsialist ja isikuandmete töötlemise eest vastutav isik ning kõik kasutajad oleksid selle teema osas kompetentsed. Selle saavutamiseks tuleb teha teavitustööd ja korraldada koolitusi.
- Asjakohaste vastutusalade piires tuleb kindlaks määrata ka andmete kustutamist reguleerivad tehnilised-töökorralduslikud meetmed. Need meetmed tuleb integreerida üleinstitutsioonilise isikuandmete- ja turbekontseptsiooniga. Eriti oluline on kindlaks määrata meetmed, mis reguleerivad andmekandjate väljastamist, kasutusest kõrvaldamist, tagastamist, parandamist ja hooldust.
- Meetmeid tuleb toetada konkreetsete tegutsemisjuhistega, mis õpetavad, kuidas turvaline kustutus peab aset leidma. Juhiste koostamisel tuleb arvestada kustutatavate andmete erineva turbevajadusega ning andmete võimaliku taastamise töömahu ja kulutustega.
- Kaitset vajavad andmed tuleks (võimaluse korral) andmekandjale salvestada krüpteeritud kujul. Selleks tuleks kasutada krüpteerivat failisüsteemi. Samuti tuleks krüpteerivat failisüsteemi kasutada ajutiste failide, saalimisfailide ja andmetest tehtud varukoopiate puhul, sest ka need võivad sisaldada kaitset vajavaid andmeid.
- Töökorras andmekandjatel olevate andmete kustutamiseks tuleb rakendada kas ühe- või mitmekordset täielikku ülekirjutamist juhuarvudega. Selleks sobivad spetsiaalsed tarkvaratööriistad. Kustutamisel ei ole soovitatav kasutada samasuguseid ülekirjutamisandmeid, sest need ei paku piisavalt kaitset põhjalike laborianalüüside vastu.
- Andmekandja ühekordset täielikku ülekirjutamist juhuarvudega tuleks rakendada kõikide andmeliikide puhul. Ülekirjutamist tuleks rakendada vähe-

malt kaks, veel parem kolm korda. Teise ülekirjutamise jaoks tuleks kasutada esimesele ülekirjutusele vastanduvat andmemustrit (bitijärjekorda). Kolmanda ülekirjutamise jaoks on soovitatav kasutada juhuandmeid. Nii saavutatakse parem kaitsetoime.

- Enne töökorras andmekandja müümist, väljaüürimist, kasutusest kõrvaldamist, tagastamist või kasutusvaldkonna muutmist tuleb kogu andmekandja mitu korda täielikult juhuarvudega üle kirjutada. Pärast sellise taaskasutusmeetme võtmist võib andmekandja uuesti kasutusele võtta (nt operatsioonisüsteemi uue installatsiooni jaoks).
- Seevastu üksikute failide selektiivse ülekirjutamisega kaasnevad väga sageli probleemid. Selline lahendus sobib vaid siis, kui on kindel, et nendest ülekirjutatud failidest ei ole üheski teises kohas rohkem koopiaid (nt ajutisi faile, saalimisfaile või andmete varukoopiaid) või kui sellised kohad on selgelt tuvastatavad, nii et koopiaid on võimalik turvaliselt ära kustutada. Lisaks tuleb tagada, et üle kirjutatakse ka kustutatud failide metaandmed, kui need peaksid sisaldama tundlikku teavet.
- Määrates kindlaks tehnilisi-töökorralduslikke meetmeid ja andmete turvalist kustutamist reguleerivaid tegevusjuhiseid, tuleb kriteeriumikataloogide põhjal välja valida ka kustutamiseks sobivad tarkvaratööriistad ning need kasutajatele valmis seada. Asjakohaste tarkvaratööriistade kasutust tuleb pisteliselt kontrollida.
- Defektsed andmekandjad, mille andmeid pole võimalik tarkvaratööriistadega üle kirjutada, tuleb kas mehaaniliselt või termiliselt hävitada (disketid, kõvakettad) või magnetitega kasutuskõlbmatuks muuta (disketid). Et protseduurid oleksid tõhusad, tuleb neid rakendada võimalikult korrektselt.
- Kui andmekandjaid on tarvis kellelegi edasi anda, ilma et neid saaks turvaliselt kustutada (nt toote saatmine parandusse või tagastamine tootjale garantiiaja jooksul), tuleb olenevalt andmekandjal hoitavate andmete kaitsevajadusest sõlmida selleks asjakohased lepingud ning vajaduse korral määratleda ka kahjunõue, et vältida andmete soovimatut lekkimist ja nende kasutamist rünnete eesmärgil. Kui tarvis, tuleb loobuda toote garantiiga seotud õigustest.

Paberdokumentide hävitamine

Kuna paberdokumente hävitatakse enamasti mitmes etapis, tuleb turbeaspektidega arvestada juba alates dokumentide vaheladustamisest paberikorvides ja kogumisanumates või alates dokumentide kogumisest töökohas ning jätkata sellega ka transportimisel ja tsentraalsel kogumisel kuni tegeliku hävitamisprotsessini välja.

Üldnõuded

Seaduste järgimiseks tuleb võtta tehnilisi ja töökorralduslikke meetmeid, mis tagavad andmete nõuetekohase töötlemise, st hävitamist käsitletakse siinkohal kui üht töötlemisetappi. Võtta tuleb üksnes selliseid meetmeid, millega kaasnev tööde maht vastab eesmärgiks seatud kaitsetoimele. Kui isikuandmeid töödeldakse failide kujul ilma automaatprotsessideta või kui töödeldakse paberdokumente kaustade kaupa, tuleb võtta meetmeid, mis välistaksid volitamata isikute juurdepääsu andmete töötlemisele, säilitamisele, transportimisele ja hävitamisele. Üldjuhul kehtib põhimõte, et andmeturbe eest vastutav organisatsiooniüksus vastutab dokumentides kajastuvate isikuandmete turbe eest seni, kuni need andmed on isikuandmete kaitse seaduste nõuete kohaselt kustutatud, st seni, kuni andmete

hävitamise protsess on lõpetatud. Selleks peab vastutaval üksusel säilima kõikide isikuandmeid sisaldavate dokumentide üle kuni nende hävitamiseni piiramatu käsutusõigus. Eriti oluline on vältida isikuandmeid sisaldavate dokumentide üleminekut kolmandate isikute omandisse, kui hävitamine ei ole veel lõpule viidud.

Kindlaks tuleb määrata seisund, mille saavutamisel võib andmeid lugeda hävitatuks.

Ka paberdokumentide hävitamisel kehtib nõue, et vastutav organisatsiooniüksus peab regulaarselt kontrollima, kas nõutud hävitusprotseduurid on nõuetekohaselt lõpule viidud. Selleks peab vastutav organisatsiooniüksus, eriti siis, kui hävitamise teenust ostetakse sisse, täpselt teadma nii hävitamise tehnilist protsessi kui ka hävitamise protseduuri. Dokumentide hävitamise kontrollikohustus tuleks kas vastava isiku või organisatsiooniüksuse jaoks fikseerida kirjalikult.

Dokumentide hävitamine ilma kõrvalise abita

Hävitamisel tuleb lähtuda põhimõttest, et andmed hävitataks võimalikult samades organisatsiooniüksustes, kus võetakse vastu andmete hävitamise otsus. Kõikvõimalikud vaheladustamised ja edasitoimetamised mitmete isikute vahendusel on alati väga veaaltid ning eeldavad ülitäpset reguleerimist ja kontrolli. Dokumentide hävitamine kohapeal organisatsiooni enda töötajate poolt on seega alati tõhus isikuandmete kaitse meede. Selleks tuleb kirjalikult reguleerida, kuidas töötajad peavad andmeid hävitama. Tööjuhiste kõrval tuleb kehtestada ka nõue, et andmeid hoitaks turvaliselt kuni nende hävitamiseni. Kui dokumente hävitatakse mõnes keskses kohas, tuleb kogu protseduur fikseerida kirjalikult. See kehtib nii erikaitset vajavate kogumispunktide kui ka transportimisprotsessi kohta, st andmete toimetamisele kesksesse kogumiskohta. Ka hävitatavate paberdokumentide turve tuleb tagada kuni nende toimetamiseni kogumispunkti. Kui dokumentide kokkukogumiseks kasutatakse mõnd tsentraalset teenust, tuleb hoolitseda, et ka selles etapis võetaks piisavalt turbemeetmeid. Dokumentide hävitamine tuleb sobival moel protokollida.

Paberdokumentide hävitamise teenuse kasutamine

Kui paberdokumendid hävitab mõni kolmas osaline andmetöötluse tellimustööna , tuleb kogu dokumentide käsitsemise protsessi kohta (alates dokumentide üleandmisest teenuseosutajale kuni dokumentide hävitamiseni) sõlmida kirjalik leping. Lepinguga tuleb kindlaks määrata dokumentide transportimine, võimalik vaheladustamine, hävitamise koht ja maksimaalne lubatud ajavahemik alates nende üleandmisest teenuseosutajale kuni hävitamisprotsessi lõpetamiseni. Lisaks tuleb täpselt fikseerida seisund, mille saavutamisel võib dokumendid lugeda hävitatuks. Teenuseosutaja peab tagama, et volitamata isikutele oleks juurdepääs dokumentides sisalduvatele andmetele tõkestatud. Dokumentide üleandmine teenuseosutajale tuleks kinnitada allkirjadega ja iga lõpule viidud hävitusprotsessi kohta tuleks teenuseosutajalt hankida kirjalik kinnitus. Üldjuhul kehtib põhimõte, et teenuseosutaja peab allhankeid võimaluse korral alati vältima. Hävitamise eest vastutaval organisatsiooniüksusel peab säilima kuni dokumentide lõpliku hävitamiseni dokumentide üle piiramatu käsutusõigus. Seetõttu peavad dokumendid jääma kuni hävitamise lõpuleviimiseni vastutava organisatsiooniüksuse omandisse. Selle alla kuulub ka nõue, et hävitatavaid dokumente ei tohi enne nende hävitamist kokku panna võõraste dokumentidega. Selleks tuleb teenuseosutajaga sõlmida leping, et tööde tellijal ja isikuandmete töötlemise eest vastutaval isikul on kuni hävitamise lõpuleviimiseni õigus hävitamisprotsessi kontrollida. Andmetöötlusega seotud tellimustööde kohta leiate lisateavet meetmest M 2.511 Isikuandmete töötlemise tellimustööde reeglid .

M 2.525 Salvestisüsteemide turvapoliitika väljatöötamine

Algatamise eest vastutavad: asutuse/ettevõtte juhtkond, infoturbespetsialist

Rakendamise eest vastutab: infoturbespetsialist

Kuna salvestilahendused on andmete salvestamiseks kasutatavad tsentraalselt toimivad tootelahendused, sõltuvad selle korrektsest toimimisest omakorda ka väga paljud muud asutuse tööprotsessid. Salvestilahenduse turvalist ja korrakohast käitamist saab tagada ainult siis, kui nende planeerimine, paigaldusasukohad, haldamine ja käitamine integreeritakse asutuses kehtivate turbenõuetega.

Olulised turbenõuded ja salvestilahenduse puhul nõutav turbeaste põhinevad asutuseülesel IT-turvapoliitikal. Vajalikud nõuded tuleks sõnastada salvestisüsteemide eraldi turvapoliitikana, et asutuse üldisi nõudeid saaks konkreetse valdkonna jaoks piisavalt täpsustada.

Turvapoliitikas kajastatavate nõuete sõnastamine eeldab kõikide salvestilahenduse abil salvestatavate andmete kaitsevajaduste dokumenteerimist (M 2.362 Sobiva salvestisüsteemi valik). Ainult vastava dokumentatsiooni abil on võimalik välja selgitada andmetele kehtivad erinevad käideldavus-, terviklus- ja konfidentsiaalsusnõuded ning tuvastada vajaminevate tehniliste ja töökorralduslike tööde maht.

Juhtudel kus asutuses hakatakse rakendama erinevaid salvestilahendusi,nt SAN, NAS, Object Storage) oleks vastutavatel töötajatel ilmselt mõttekas koostada iga kasutusvaldkonna jaoks eraldi turvapoliitika ja lähtuda sealjuures vastava valdkonna meetmetest).

Kuna SAN-lahenduste jaoks on tarvis luua eraldi võrk, tuleb SAN-lahenduste puhul täiendavalt arvestada meetmega M 2.279 Marsruuterite ja kommutaatorite turvapoliitika koostamine . Nimetatud meetmes tutvustatakse üldisi turbemeetmeid, mida võtta IT-komponentide puhul, mis võimaldavad sisevõrgus juurdepääsu andmetele või teistele süsteemidele. Seevastu NAS-lahenduste turvapoliitikat koostama hakates tuleks esmalt läbi töötada meede M 2.316 Serveri turvapoliitika kehtestamine . Nimetatud meetmes kirjeldatakse serverifunktsiooniga IT-süsteemide üldisi turbemeetmeid.

Täiendavad teemad, millele salvestilahenduse turvapoliitika väljatöötamisel tähelepanu pöörata, on järgmised:
Salvestisüsteemi planeerimist puudutavad ettekirjutused

- Asutus peab välja töötama ettekirjutused tehnilise taristu tarbeks, mille raa-

mes vastavad salvestikomponendid üles seatakse. Ruumide taristu, kuhu salvestilahenduse komponendid paigaldatakse, peab olema piisav, et tagada salvestilahenduse käideldavusnõuete täitmine (elektrivarustus, võrguühendus, kliimaseade). Samuti peab sissepääs nendesse ruumidesse olema piisavalt kaitstud.

- Asutusevälistele töötajatele tuleb kehtestada sisenemisreeglid (nt hoolduse eesmärgil). Kuna teenuseosutajatega sõlmitavates salvestikomponentide seire- ja hoolduslepingutes nõutakse tihti salvestisüsteemi otsest ühendust kas tootja või teenuseosutaja seiresüsteemiga, tuleb selliste pöörduste jaoks kehtestada ka asjakohased kontrollimis- ja logimisnõuded.
- Väga suurte käideldavusnõuete korral tuleks nõuda avariikindlate SAN-lahenduste kasutamist. Selles kontekstis võiks analüüsida ka salvestilahenduse nõrku lülisid (Single Points of Failures, SPoFs), mille võimalik tõrge halvab terve salvestilahenduse töö. Seevastu väga suurte käideldavusnõuete korral on SPoFs-ide analüüsimine kindlasti kohustuslik. Juhtudel, kus kõrge käideldavusega SAN-lahendusse soovitakse juurutada uusi komponente, tuleb nende tõrkevaba integreerimist kontrollida eelnevalt spetsiaalsetes katsetussüsteemides.

Administraatorite töökorraldus

- Dokumenteerida tuleb põhimõtted, millise skeemi alusel antakse administraatoritele salvestilahenduse ja terviksüsteemi haldamisõigused. Selleks on soovitatav koostada eraldi töörollide kontseptsioon.
- Määratleda tuleks administraatorite erinevad töörollid, millele antakse vastavalt nende tööülesannetele ka vajalikud õigused. Siinkohal on eriti oluline, et rutiinsete süsteemihaldusülesannetega seotud õigused (nt backup) oleks piiratud miinimumini. Administraatorite kasutajanimed seotakse seejärel konkreetsete rollidega. Võimalike vigade vähendamiseks tohib administraatori kasutajanime alt töid teha vaid siis, kui see on ilmtingimata vajalik.
- Administraatorite juurdepääsusid tuleb kaitsta vähemalt tugevate paroolidega, vajaduse korral ka spetsiaalsete, kasutajate autentimist võimaldavate turbemeetmetega.
- Salvestiressursside haldamiseks ja kontrollimiseks tuleks nii administraatoritele kui ka revidentidele võimaldada juurdepääsu salvestisüsteemile kas ainult kohapeal läbi otseühendusega konsooli, läbi eraldi haldusvõrgu või läbi krüpteeritud ühenduse. Juurdepääsusid salvestiressurssidele tuleb piirata, määrates kindlaks ligipääsetavad süsteemid ja kontrollides seda nt turvalüüsidega.
- IT-süsteeme, mida rakendatakse halduskonsoolidena või revisjonide tarbeks, tuleb kaitsta parimal võimalikul moel viiruste ja pahavara eest.
- Tööülesannete jaotamisega, ettekirjutuse ja kasutusreeglitega ning kõikide salvestikomponentide konfiguratsioonide dokumentatsiooni pideva täiendamisega tuleb tagada, et administraatoritel ei oleks võimalik salvestisüsteemides algatada protsesse või teha selliseid seadistusi, mille tagajärjel võiksid tekkida kas ebakõlad, avariid või andmekaod. Olulised muudatused tuleb dokumenteerida. Selleks on soovitatav juurutada muudatuste haldamise

protseduur, mis võib põhineda nt ITIL-i dokumendikogul (IT Infrastructure Library).
- Asutus peab määrama kindlaks muudatuste valdkonnad, mille puhul tuleb rakendada nelja silma põhimõtet.

Salvestisüsteemi installeerimine ja konfigureerimine

- Dokumenteerida tuleb esmakordse installeerimise protseduur. Kuna paljudel juhtudel teeb esmapaigalduse kas tootjafirma või tarnija, tuleb lasta endale saata vastav dokumentatsioon.
- Pärast installeerimist tuleb kontrollida, kas default-seadistustes esineb võimalikke turvariske, samuti tuleb desaktiveerida võrgukomponentide ja salvestiseadmete ebaturvalised teenused ning muuta ära standardsed kasutajanimed ja paroolid.
- Süsteemikonsoolide juurdepääsusid salvestikomponentidele tohiks läbi LAN-i lubada üksnes juhul, kui selleks kasutatakse krüpteeritud ühendusi. Selliste seadmete pääsuõiguseid omavate kasutajate ring tuleks hoida võimalikult väike. Konsooli kasutamise ja konfigureerimisnõuded ja juurdepääsuliikide piirangud tuleb dokumenteerida.
- Asutus peab välja töötama nõuded, mis sätestavad dokumentatsiooni korrakohase koostamise, hooldamise ja dokumentatsiooni vormi (nt protseduurireeglid administratiivsete ülesannetega seotud kasutajatunnuste loomiseks, kasutusjuhendid igapäevatöös vajalikele töö- ja kontrolliprotseduuridele).
- SAN-i sees tuleks rakendada spetsiifilisi segmenteerimismeetodeid (vt M 5.130 Salvestisvõrgu (SAN-i) kaitse segmenteerimise abil). Sellega saavutatakse SAN-süsteemi parem kaitse, st sellega suurendatakse nii konfidentsiaalsust, käideldavust kui ka SAN-konfiguratsiooni terviklust.

Turvalise käitamise nõuded

- Salvestisüsteemi haldus tuleb muuta turvaliseks seeläbi, et haldamiseks vajalikud juurdepääsud suunatakse läbi spetsiaalsete ühenduste (st läbi eraldi haldusvõrgu või olenevalt olukorrast ka läbi salvestivõrgu enda).
- Vajaduse korral tuleb leida sobivad tarkvaratööriistad, mis võimaldaksid salvestikomponente käitada, hooldada ja integreerida olemasoleva võrguhaldussüsteemiga. Nimetatud tööriistade jaoks tuleb välja töötada turvalise konfiguratsiooni nõuded. Võimaluse korral tuleks kasutada ainult krüpteeritud ühendusi ning mittevajalike liideste ja teenuste kasutamine tuleks desaktiveerida.
- Juhul kui soovitakse kasutada tootja pakutavaid kaughoolduse või kaugseire võimalusi, tuleb välja töötada ettekirjutused, mis sätestavad selleks vajalike juurdepääsude turbenõuded. Näiteks tuleb nõuda, et ühenduste jaoks kasutatakse VPN-i või eksklusiivseid, st ainult selleks otstarbeks ette nähtud ühendusi, samuti tuleb nõuda, et asutusele saadetaks selliste tegevus-

te kohta ka arusaadavad logiandmed. Lisateavet leiate meetmest M 4.80 Kaug-võrguhalduse turvalised pääsumehhanismid .

- Asutus peab kehtestama täpsed reeglid, kellel on õigus installeerida tarkvaravärskendusi ja muuta konfiguratsiooni. Vastavate protseduuride teostusviis tuleb samuti dokumenteerida. Niipea kui on teada, et käideldavusnõuded on väga suured, tuleb nõuda, et muudatusi ja värskendusi kontrollitaks enne igapäevatöös kasutatavasse süsteemi installeerimist alati eelnevalt asjakohases katsetussüsteemis.
- Salvestilahenduse käitamise raames tuleb logida kõik haldamisega seotud tegevused. Selleks tuleb koostada salvestisüsteemide haldamise ja seire kontseptsioon. Lisateavet leiate meetmest M 2.359 Salvestisüsteemide seire ja haldamine .
- Olenevalt kaitsevajadusest (nt suur või väga suur), käitamismudelist (nt asutuseväline käitamine), paigaldusasukohast (nt salvestilahenduse või selle üksikute komponentide paigaldamine teenuseosutaja juurde) või olenevalt teenusetarbijate turvalisest lahutamisest simultaanteeninduses võib tarvis minna krüpteerimist. Lisateavet leiate meetmest M 4.448 Krüpteeringu kasutamine salvestisüsteemides .
- Salvestilahenduse andmevarunduse valdkond tuleb ühelt poolt kooskõlastada asutuse üldise andmevarunduspoliitikaga (vt moodul B 1.4 Andmevarunduspoliitika) ja teisalt salvestilahenduse enda turbenõuetega. Spetsiaalsete konfidentsiaalsusnõuete puhul tuleb varukoopiate tegemise suhtes rakendada kasutajaõiguste haldust.
- Kuna salvestilahendus on terve asutuse jaoks väga oluline, tuleb see kaasata asutuse hädaolukordade planeerimisse (vt ka M 6.98 Salvestisüsteemide hädaolukordadeks ettevalmistamine ja reageerimine hädaolukorras).
- Asutus peab määrama, kes vastutab revisjonide ja auditite tegemise ees ja kehtestama nõuded, kuidas neid teha. Salvestilahenduste revisjon tuleb integreerida asutuseülesesse revisjoni kontseptsiooni.

Kontrollküsimused

- Kas salvestilahenduste kasutamise käitamise jaoks on koostatud vastav turvapoliitika?
- Kas turvapoliitikas on sõnastatud ka turbeaste?
- Kas turvapoliitikas käsitletakse salvestilahenduse planeerimist, haldamist, installeerimist, konfigureerimist ja käitamist?
- Millal toimus viimati turvapoliitika värskendamine?
- Kas salvestilahenduste turvapoliitika on integreeritud asutuseülesesse revisjonide ja auditite kontseptsiooni ja kas asutus on määratlenud kokkupuutepunktid hädaolukordade haldusega?

M 2.526 Salvestisüsteemi käitamise planeerimine

Algatamise eest vastutavad: asutuse/ettevõtte juhtkond, infoturbespetsialist

Rakendamise eest vastutavad: infoturbespetsialist, IT-juht

Salvestilahenduse pikaajaline turvaline käitamine eeldab head planeerimist. Käitamisel järgitava kontseptsiooni ja salvestilahenduse paigalduskoha valimise kõrval tuleb tegelda ka salvestilahenduse käitamise töökorralduse ja salvestilahenduse dokumenteerimisega. Käitamise lihtsustamiseks tuleks sisse seada käitamisraamat, mida hakatakse regulaarselt värskendama.

Alljärgnevalt kirjeldatakse lähemalt salvestilahenduse planeerimise puhul olulisi teemasid.

Käitamiskontseptsiooni valimine

Salvestisüsteemi käitamise kontseptsioon tuleb üldjuhul kindlaks määrata juba salvestilahenduse planeerimisel. Selleks tuleb salvestisüsteemi kohta kokku koguda täpsemad andmed, nt selle kohta, kes vastutab käitamise eest ja kes on kontaktisikud. Seega peab asutus dokumenteerima, kas salvestilahendust hakkavad käitama asutuse enda töötajad või hoopis teenuseosutaja ja kas teenuseosutaja hakkab ka käitamise eest ise vastutama või mitte. Dokumenteerida tuleb muu hulgas ka väljavalitud teenuseosutaja, teenuseosutaja vastutavad kontaktisikud ja salvestilahenduse võimalikud eripärad, nt kas asutus hakkab rakendama teenusepõhist talletusmudelit (Storage as a Service).

Salvestilahenduse paigaldus

Salvestilahenduse paigaldusele tuleks samuti pöörata tähelepanu juba salvestilahenduse planeerimisel. Paigaldusmeetmed on enamasti tihedalt seotud välja valitud käitamiskontseptsiooniga. Otsus, kas seadmed paigaldatakse asutuse või hoopis teenuseosutaja ruumidesse, tuleb dokumenteerida. Salvestilahenduste käitamiseks vajaliku taristu kohta leiate lisateavet meetmest M 2.351 Salvestisüsteemide planeerimine . Salvestilahendust planeerides tuleks analüüsida, kas see vastab eelnevalt mainitud meetmes kajastatud nõuetele, arvestades seejuures täiendavalt ka salvestilahenduse paigalduskoha ja salvestilahenduse võimalike eritingimustega. Salvestisüsteemi paigaldust kajastav dokumentatsioon ei tohi minna vastuollu meetmega M 1.59 Arhiivisüsteemide asjakohane rajamine .

Käitamisraamatu sisseseadmine ja pidev värskendamine

Salvestilahenduste käitamisel on oluline, et võetaks kasutusele käitamisraamat, kuhu kantakse kõikvõimalik käitamist puudutav oluline teave. Salvestilahenduse arhitektuuri ja liideste ülevaate kõrval peaks käitamisraamatus kajastuma ka teave, kuidas salvestilahendust installeerida ja igapäevatöös kasutusele võtta. Samuti tuleb käitamisraamatu puhul tagada, et seda kontrollitaks pidevalt, kas see kajastab piisavas mahul olulist teavet, kuidas salvestisüsteemi töös hoida, kuidas selle tööd katkestada ning kuidas korraldada süsteemi seiret, arhiveerimist ja andmete kustutamist. Puuduvad ja valed andmed tuleb vastavalt lisada või kustutada. Asutus peab kehtestama nõude, et käitamisraamatu pidev täitmine on administraatoritele kohustuslik ning peab reguleerima ka kõikvõimalikud kõrvalekalded. Käitamisraamatut tuleb regulaarselt, vähemalt kord aastas, värskendada. IT etalonturbe abivahendite alt leiate ka salvestilahenduse käitamisraamatu koostamise näidise.

Vastutusalade määratlemine ja piiritlemine

Olenevalt valitud käitamiskontseptsioonist tuleb dokumenteerida ka lisateave salvestilahenduse funktsioonide või jõudluse kohta. Funktsioonidest lähtuvalt tuleb määratleda ka asjakohased vastutusalad. Asutus peab nt määrama, kes vastutab käitamises esinevate tõrgete lahendamise eest, kuidas toimub alarmeerimine ja millised on lubatud reaktsiooniajad. Kõik vastutavad administraatorid peavad olema kontaktisikutega kursis, ning vastav teave peab olema tehtud administraatoritele kättesaadavaks. Neid andmeid tuleb kindlasti värskendada mitte ainult kord aastas, vaid sagedamini. Lisateavet leiate ka meetmetest M 2.356 Lepingud SAN teenusepakkujatega ja M 6.98 Salvestisüsteemide hädaolukordadeks ettevalmistamine ja reageerimine hädaolukorras . Dokumentatsiooni puhul tuleb jälgida, et määratlused ja piiritlused ei läheks omavahel vastuollu.

Teenusetarbijate lahutamine simultaanteeninduses

Teenusetarbijate turvalist lahutamist simultaanteeninduse puhul käsitletakse lähemalt meetmes M 2.528z Teenusetarbijate turvaline lahutamine salvestisüsteemides . Salvestilahenduse käitamise planeerimise raames on oluline, et asutus dokumenteeriks konkreetsed töökorralduslikud ja tehnilised meetmed, millega tagatakse teenusetarbijate turvaline lahutamine. Selleks on oluline üles märkida, kas teenusetarbijate lahutamist rakendatakse üksnes võrgu tasandil või ka täiendavate tootepõhiste funktsioonidega nagu virtuaalne failiserver (tuntud ka mitmete tootjapõhiste nimetustega nagu filer, virtual data mover jms). Samuti on tarvis fikseerida töötajate töörollid ja nende juurde kuuluvad õigused. Regulaarselt tuleb ka kontrollida, kas andmed on värsked.

Salvestilahenduse integreerimine olemasoleva keskkonnaga

Asutus peab dokumenteerima, kuidas tuleb salvestilahendus olemasoleva IT-keskkonnaga integreerida. Selleks peab asutus esmalt looma ülevaate vajaminevatest liidestest. Liideste kõrval tuleb dokumenteerida ka nõuded, mis esitatakse süsteemide laiendamiseks või väljavahetamiseks vajalikele komponentidele ja süsteemide kohandamisprotsessile. Salvestilahenduse käitamise planeerimise raames tuleb täpselt sõnastada, mil määral töötajate senised tööülesanded muutuvad ning vastav teave vastutavatele isikutele ka õigel ajal edastada. Vajalikke nõudeid välja töötades arvestage kindlasti ka meetmega M 3.54 Salvestisüsteemide administraatorite koolitus .

Salvestilahenduse katsetused ja kasutuselevõtt

Asutus peab kehtestama tingimused, kuidas salvestisüsteemi ja selle juhttarkvara katsetatakse ja kuidas nende komponente kasutusse lubatakse. Selleks tuleb muu hulgas reguleerida vajalik hooldustööde intervall ja arvestada kõikvõimalike lepinguliste suhetega. Asutus peab määratlema, mis tingimustel on katsetuskeskkonna rakendamine kohustuslik ja millised eeldused peavad olema täidetud selleks, et süsteemi võiks lõplikult kasutusse lubada. Juhtudel, kus salvestilahenduse käitamine on jäetud teenuseosutaja hoolde, tuleb täiendavalt arvestada ka meetmega M 2.356 Lepingud SAN teenusepakkujatega .

Krüpteerimise kasutamine

Salvestilahenduse käitamise jaoks tuleb määratleda administraatorite tööülesanded seoses krüpteeringu kasutamisega. Siia alla kuuluvad nt võtmete halda-

mine, andmetest varukoopiate tegemine ja kindlasti ka krüpteeritud andmete dekrüpteerimine. Teabe krüpteerimisel järgige moodulit B 1.7 Krüptokontseptsioon ja M 4.448z Krüpteeringu kasutamine salvestisüsteemides .

Kontrollküsimused:

- Kas salvestilahenduse käitamiseks vajalikud nõuded, töökorraldused ja seadistused on dokumenteeritud?
- Millal värskendati viimati salvestilahenduse käitamise dokumentatsiooni?
- Kas käitamismudeli valik ja sellega seonduvate otsuste põhjendused on kõigile arusaadavalt dokumenteeritud?

M 2.527 Turvaline kustutamine SAN-keskkonnas

Algatamise eest vastutavad: asutuse/ettevõtte juhtkond, infoturbespetsialist

Rakendamise eest vastutavad: administraator, infoturbespetsialist

Salvestilahenduses hoitavad andmed, mida enam ei vajata, tuleb turvaliselt kustutada. Andemete turvalist kustutamist käsitletakse moodulis B 1.15 Andmete kustutamine ja hävitamine . Seevastu andmete selektiivse kustutamisega seotud probleeme, millega puututakse kokku ka tänapäevastes salvestisüsteemides, kirjeldatakse meetmes M 2.431 Korrakohased protseduurid informatsiooni kustutamiseks või hävitamiseks .

SAN-keskkonnas muudab andmete turvalise kustutamise keeruliseks eelkõige asjaolu, et SAN-keskkondadega on seotud palju teenusetarbijaid. Seetõttu tuleb võtta täiendavaid meetmeid.

SAN-keskkondadele kehtivaid turvalise kustutuse meetmeid tuleb järgida ka salvestisüsteemide hädaolukorra katsete ja õppuste planeerimisel (vt ka meede M 6.98 Salvestisüsteemide valmisolek hädaolukorraks). Selliste katsete ja õppuste käigus genereeritakse paljudes ja vajaduse korral erineva kaitsevajadusega LUN-ides suured andmehulgad, mis tuleb pärast katsete lõpetamist ka ära kustutada. Samad nõuded kehtivad olukorras, kus pärast avarii likvideerimist on LUN-idest olemas mitu koopiat.

Enamatel juhtudel saab SAN-keskkonnas hoitavate andmete kustutamiseks kasutada järgmisi võimalusi:

- **Loogilise kõvaketta kustutamine salvestisüsteemis (LUN):**
  LUN-i kustutamisel, murtakse selle juurde kuuluvate kõvaketaste, RAID-rühmade või kõvakettakogumike (pools) loogiline struktuur lahti, et kustutatud LUN-i ressurss muutuks taas kasutatavaks. Füüsilisi plokke selle käigus ei „nullita”, st neid plokke ei kirjutata andmemustritega (patterns) üle. Selle tagajärjel ei pääse rakenduse poolt vaadatuna enam LUN-i andmetele juurde, sest kustutatud LUN-i ei ole võimalik salvestisüsteemi enda vahenditega taastada. Pärast LUN-i kustutamist pole enam võimalik aru saada, millised salvestusüksused või kõvaketta sektorid olid LUN-iga millisel kujul seotud, mistõttu pääseb ka potentsiaalne ründaja ligi üksnes biti või baidi tasandile, mitte aga kokkukuuluvatele andmehulkadele. LUN-i andmete taastamine on ülimalt tülikas ja eeldab füüsilist juurdepääsu salvestuskandjatele. Ründajad võivad selleks otstarbeks kasutada digitaaljuurdluse tööriistu, mille abil on võimalik loogilisest struktuurist läbi murda.

- **LUN-i andmete mitmekordne ülekirjutamine:**
  Lähtudes selle juurde kuuluvast serverist kirjutatakse LUN-i andmed (mitu korda) üle kas kindlaksmääratud andmete või juhuandmete mustritega. Olenevalt asutuses kehtivatest andmekustutuse nõuetest on võimalik rakendada ka sertifitseeritut kustutamist, mis vastab USA standardile DoD 5220-22.M. Selleks saavad asutused hankida endale vastava tarkvara. Iseseisva tegevuse asemel saab sertifitseeritud kustutamist salvestilahenduse tootja käest ka teenusena sisse osta. Sel moel ülekirjutatud andmeid ei ole hiljem enam võimalik taastada. Siiski tuleb arvestada, et andmete sertifitseeritud kustutamine on LUN-ide puhul võimalik üksnes serverites, sest salvestisüsteemides sellised võimalused puuduvad. Sellisel moel andmeid kustutades tekib salvestilahenduse vastavates osades, mida kasutavad ka teised teenusetarbijad, tavapärasest suurem hulk kirjutamisprotsesse. Seetõttu tuleb kustutustöid tehes arvestada, et kustutamine ei kahjustaks teiste teenusetarbijate andmeid ja et teiste teenusetarbijate teenuse kvaliteet säiliks nõutud tasemel. Seevastu SAN-keskkondades tuleks arvestada, et sama kustutamisprotseduuri kasutamine ei pruugi õnnestuda, nt põhjusel, et kettad töötavad erinevate kasutusrežiimidega. Näiteks juhtudel, kus LUN paikneb nt väikse kirjutusvõimsusega alas ning seda asutakse mitu korda üle kirjutama, st tekitatakse suur kirjutuskoormus, kopeerib SAN vastava LUN-i ümber suure kirjutusvõimsusega alasse. Sellisel juhul kirjutatakse üle ainult uus ümberkopeeritud LUN, kuid väiksema kirjutusvõimsusega valdkondade andmed jäävad üle kirjutamata.

- **Salvestisüsteemi andmete kustutamine:**
  Kui terve salvestisüsteemi andmeid soovitakse kustutada mõne sertifitseeritud protseduuriga, rakendades selleks andmete ülekirjutamist, saab tihti kasutada salvestilahenduste tootjate pakutavaid teenuseid.

- **Disc retention:**
  Juhul kui hooldusle pingutes nähakse ette disc retention, jäävad kõvakettad võimalike defektide korral asutuse kätte, mitte ei tagastata tootjale. Sellisel juhul vastutab kõvaketta sisu turvalise kustutamise eest mitte tootja, vaid asutus. Defektsete kõvaketaste puhul eelistavad asutused enamasti füüsilist hävitamist. Vaatamata asjaolule, et disc retention toob endaga sageli kaasa kulude suurenemise, tuleks seda siiski kaaluda isegi tavapäraste konfidentsiaalsusnõuete korral.

Eelpool kirjeldatud salvestisüsteemi andmete turvalised kustutamismeetodid on väga mitmetahulised ja komplekssed. Seetõttu peab asutuse vastutav töötaja endale teadvustama, et andmete turvaline kustutamine eeldab tavapärasest suuremat tähelepanu.

Tavapäraste kaitsevajaduste rahuldamiseks piisab praeguste arusaamade kohaselt LUN-i kustutamisest, sest lähtuvalt SAN-keskkondade tööpõhimõttest muutub kustutatud andmete taastamine ülimalt keeruliseks.

Seevastu tavapärasest suuremate konfidentsiaalsusnõuete puhul võiks kaaluda LUN-i ülekirjutamist nõnda, et sellesse oleks kaasatud ka kõik juurdekuuluvad salvestisüsteemid.

Salvestisüsteemide kasutuselt kõrvaldamisel järgige meedet M 2.361 Salvestisüsteemide kasutuselt kõrvaldamine .

Kontrollküsimused

- Kas salvestisüsteemi jaoks on kindlaks määratud, milliseid andmeid milliste protseduuridega kustutatakse?
- Kas simultaanteenindust võimaldavates salvestilahendustes on tagatud, et konkreetsete teenusetarbijatega seotud LUN-e on võimalik kustutada?
- Kas suure kaitsevajadusega andmete kustutamiseks kirjutatakse LUN-i vastavad segmendid mitu korda üle?

M 2.528z Teenusetarbijate turvaline lahutamine salvestisüsteemides

Algatamise eest vastutavad: IT-juht, infoturbespetsialist
Rakendamise eest vastutavad: infoturbespetsialist, IT-juht

Salvestilahenduste peamine eelis seisneb paljude asutuste jaoks peamiselt selle simultaanteeninduse funktsioonis. Juhtudel, kus salvestisüsteemidele on kehtestatud teenusetarbijate lahutamise nõue, peab asutus võtma meetmeid, mis tagavad, et lahutamine toimub turvaliselt.

Salvestisüsteemide planeerimisel tuleb analüüsida, millisel kujul ja millises ulatuses on simultaanteenindus (multitenancy) erinevate tootjate poolt pakutavates salvestilahendustes juba olemas. Paljud salvestilahenduste tootjad kasutavad simultaanteenindust reklaamiargumendina. Kahjuks ei lange asutuste ettekujutus simultaanteeninduse funktsioonidest alati kokku tootjate ettekujutusega.

Nii nt eeldavad asutused nn tüüpiliste teenuseosutaja keskkondades toimivate salvestilahenduste puhul, et erinevad teenusetarbijad oleksid üksteisest turvaliselt lahutatud mitte üksnes rakenduse, vaid ka muudel tasanditel.

Seetõttu peavad asutused kontrollima, kas tootja suudab enda poolt pakutava simultaanteeninduse tehnilises teostuses pakkuda vähemalt alljärgnevalt kirjeldatud variante.

- Block-storage-keskkonnas tuleb teenusetarbijad lahutada LUN-masking-funktsiooniga. Selleks peab salvestilahenduse halduskomponent sisaldama asjakohaseid konfigureerimisvõimalusi.
- Fileservice-keskkondades peab olema võimalus kasutada virtuaalseid failiservereid (tuntud ka mitmete tootjapõhiste nimetustega nagu filer, data mover jt). Need võimaldavad iga teenusetarbijaga siduda selle isikliku failiteenuse. Virtuaalseid failiservereid saab hallata kapseldatud keskkondadena. Suure käideldavusega keskkondades kasutamiseks saab virtuaalseid failiservereid koos kõikide nende omadustega ühest arvutuskeskusest teise peegeldada. Nõnda saab teenusetarbija turvalise lahutamise tagada siis, kui salvestilahenduses või selle üksikkomponendis peaks tekkima tõrge.
- Tavapärasest suurema kaitsevajaduse korral peaks teenusetarbijatele, st sise- või väliskasutajatele, olema võimalik pakkuda juurdepääsu erinevate salvestikogumike (storage pool) ressurssidele. Salvestikogumikud kujutavad endast erinevate üksteisest füüsiliselt lahutatud salvestuskandjate kokkuliitmist üheks salvestikogumikuks. Seejuures tohib iga salvestuskandja olla seotud ainult ühe kindla salvestikogumikuga. Seetõttu tohib ka iga loogiline kõvaketas (LUN), mis genereeritakse ühest sellisest salvestikogumikust, olla

seotud üksnes ühe konkreetse teenusetarbijaga. Nõnda välistatakse teiste teenusetarbijate juurdepääs teenusetarbijaga seotud salvestuskandjatele.

Sellise teenusetarbijate lahutamise kõrval ja lisaks funktsioonidele, mis võimaldavad salvestilahendusele ka otsejuurdepääsu, saab teenusetarbijaid üksteisest turvaliselt lahutada ka võrgu tasandil. Teenusetarbijate võrgupõhist lahutamist ehk segmenteerimist saab teha IP, iSCSI ja FC-SAN-i abil.

- IP- ja iSCSI-keskkonnas saab seda tagada võrkude füüsilise lahutamisega või ka sellega, et võetakse kasutusele VLAN. Lisateavet leiate selle kohta meetmetest M 5.77 Alamvõrkude rajamine ja M 5.62 Sobiv loogiline segmenteerimine .
- Seevastu FC-keskkonnas kasutatakse enamasti ainult ühte tsentraalset liiasusega võrku. Võrkude füüsilist lahutamist rakendatakse siin üksnes erandkordadel. Eraldamiseks võetakse sageli appi VSAN ja soft zoning. Seevastu hard-zoning-tüüpi ressursijaotust kasutatakse täna üha vähem, sest suurem turve, mis saavutatakse salvestuskandjate sidumisel konkreetse võrguga, hakkab piirama SAN-keskkonna vajalikku paindlikkust. Lisateavet leiate meetmetest M 5.130 Salvestisvõrgu (SAN-i) kaitse segmenteerimise abil ja M 4.447 SAN-Fabricu tervikluse tagamine .

Täiendavad meetmed suure kaitsevajaduse korral:

- suure kaitsevajaduse, eelkõige suurte käideldavusnõuete korral on soovitatav kaaluda krüpteerimise ja sellega kokku käiva võtmehalduse juurutamist. Krüpteerimist saab rakendada väga erinevatel tasanditel. Lisateavet leiate muu hulgas meetmest M 4.448 Krüpteeringu kasutamine salvestisüsteemides .

Kontrollküsimused

- Kas teenusetarbijate lahutamisele esitatavad nõuded on arusaadavalt dokumenteeritud?
- Kas teenusetarbijate lahutamiseks rakendatavad meetodid vastavad dokumenteeritud nõuetele?
- Kas block-storage-keskkonnas kasutatakse teenusetarbijate lahutamiseks LUN-maskimist?
- Kas virtuaalsete failiserverite puhul seotakse iga teenusetarbija ühe konkreetse failiteenusega?
- Kas IP, iSCSI ja FC-SAN-i kasutamisel tagatakse teenusetarbijate lahutamine võrgu segmenteerimisega?

M 2.529w Salvestisüsteemide modelleerimine

Algatamise eest vastutavad: IT-juht, infoturbespetsialist

Rakendamise eest vastutavad: administraator, IT-juht

IT-süsteemide vastuvõetava turbeastme saavutamiseks tuleb salvestilahendus koos kõikide selle salvestisüsteemidega asutuse turbekontseptsiooni süstemaatiliselt sisse töötada. IT etalonturbe metoodika kontekstis tähendab see eelkõige seda, et kõiki salvestilahendusi tuleb kajastada nii struktuurianalüüsis kui ka modelleerimises.

Modelleerimise all peetakse IT etalonturbe metoodika puhul silmas olemasolevate sihtobjektide (IT-süsteemide, rakenduste, tööruumide jmt) analüüsimist, et selgitada välja neile kehtivad moodulid. Salvestilahenduste modelleerimisel tuleks enamatel juhtudel järgida IT etalonturbe kataloogide peatükki 2.2. IT etalonturbe kohalduvate moodulite leidmisel tuleks esmajoones lähtuda analüüsitava IT-süsteemi funktsioonist (server, klient jms), seejärel kasutatavast operatsioonisüsteemist (Unix, Windows jms) ja seejärel süsteemis käitatavatest rakendustest (andmebaas, veebiserver jms).

Kuna tänapäevased salvestilahendused on väga kompleksse ülesehitusega, toome järgnevalt teieni mõned täiendavad modelleerimisjuhised, mis käsitlevad konkreetseid juhtumeid.

Network Attached Storage'i (NAS) modelleerimine

Network Attached Storage (NAS) võimaldab salvestisüsteeme kasutada protokollidega NFS (Network File System) ja CIFS (Common Internet File System). NAS-i peamine kasutusvaldkond on failiserveri teenuste osutamine. Seetõttu kasutavad teenuseosutajad nende süsteemide puhul ka terminit filer. Seetõttu tuleb NAS-lahenduste puhul rakendada täiendavalt ka moodulit B 3.101 Server .

Storage Area Network'i (SAN) modelleerimine

Storage Area Network'i (SAN) lahenduse puhul luuakse serverite ja lõppseadmete vahele eraldi salvestivõrk. SAN-süsteemid töötati välja suurte andmehulkade pidevaks ja kiireks jadaandmeedastuseks. Täna kujutavad need endast suure käideldavuse ja suure jõudlusega installatsioone, mis kasutavad kas Fibre-Channel- või IP-protokolli (iSCSI). Seetõttu tuleb SAN-lahenduste puhul rakendada ka moodulit B 4.1 Heterogeensed võrgud . Seevastu SAN-lahenduste võrgukomponente (nt Fibre-Channelkommutaatoreid) tuleb täiendavalt kaitsta mooduliga B 3.302 Marsruuterid ja kommutaatorid .

Hybrid-Storage- või Unified-Storage-lahenduste modelleerimine

Salvestilahendusi, mis kujutavad endast NAS-i ja SAN-i kombinatsiooni, nimetatakse sageli Hybrid-Storage-salvestisüsteemideks või ka kombineeritud salvestisüsteemideks (Unified Storage). Teenuste osutamisel võib neid käitada nii NAS- kui ka SAN-süsteemina. Kombineeritud käitamine on võimalik tänu vastavatele süsteemikomponentidele ja nende konfiguratsioonile. Nii on võimalik, et üks ja sama salvestisüsteem suudab juurdepääsu teatud rakendustele pakkuda läbi Ethernet-ühenduse, töötades nn filer-ina ja osutada seeläbi failiteenuseid CIFS- ja NFS-protokolliga ja pakkuda läbi Fibre Channel'i või iSCSI teistele serveritele ka salvestimahtusid. Seetõttu tuleb NAS-i ja SAN-i kombinatsioonide puhul rakendada mooduleid B 3.101 Server ja B 4.1 Heterogeensed võrgud . SAN-i võrgukom-

ponente (nt Fibre-Channel-kommutaatoreid) tuleb täiendavalt kaitsta mooduliga B 3.202 Autonoomne IT-süsteem .

Salvestisüsteemide virtualiseerimise modelleerimine

Salvestilahenduste virtualiseerimise korral lisatakse salvestivõrku uus virtuaalne kiht, mis seob salvestiruumi osutamise lahti füüsilistest oludest. Salvesti virtualiseerimine põhineb virtualiseerimisseadmel (appliance). See võimaldab kõiki salvestivaldkondi tsentraalselt hallata. Seetõttu tuleb salvestilahenduste virtualiseerimiskomponentidele rakendada täiendavalt mooduleid B 3.101 Server ja B 3.304 Virtualiseerimine .

Object Storage'i modelleerimine

Object Storage (sageli ka Object based Storage) võimaldab traditsiooniliste ploki- ja failipõhiste juurdepääsude kõrval rakendada andmete suhtes ka objektipõhist juurdepääsu. Objektikesksed salvestilahendused salvestavad andmeid salvestisüsteemi keskkonda koos nende juurde kuuluvate metaandmetega mitte failide, vaid objektidena. Objekti saab eksimatult identifitseerida objekti ID (räsiväärtus) põhjal, mis sisaldab muu hulgas ka objekti metaandmeid. Juurdepääs objektipõhisele mälule toimub läbi juhtiva rakenduse. Rakendus pääseb objektipõhisesse salvestisüsteemi kas spetsiaalse API ja selle võimalike käskudega või otse IP-ga. Juhtudel, kus juurdepääsuks kasutatakse API-d, peab vastav rakendus toetama objektipõhise salvestisüsteemi tootjapõhist API-d.

Andmevarundus

Salvestisüsteemi külge ühendatud andmevarundusseadmete puhul tuleb arvestada mooduliga B 1.12 Arhiveerimine . Andmetest varukoopiate tegemise kontseptsiooni kohta leiate lisateavet moodulist B 1.4 Andmevarunduspoliitika .

Salvestilahenduste haldamine

Salvestilahenduste Element Manager'id ja nende komponendid kujutavad endast tsentraalseid haldustööriistu, mis kasutavad salvestilahenduse ja selle komponentide haldamiseks ja juhtimiseks erinevaid protokolle. Seevastu Element Manager'ide enda funktsioon ja ülesehitus on tegelikult väga sarnane paljude teiste haldussüsteemidega. Seetõttu saab nende halduslahenduste jaoks kasutada IT etalonturbe kataloogides leiduvaid mooduleid. Eriti nt moodulit B 4.2 Võrgu- ja süsteemihaldus ja süsteemipõhiseid mooduleid nagu nt B 3.101 Server , B 3.102 Server Unixi all , B 5.7 Andmebaasid ja B 5.21 Veebirakendused .

M 2.530 Üleviimiste planeerimine ja ettevalmistus

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: administraator, vastutav spetsialist

IT-taristute üleviimine on enamasti väga kompleksne ülesanne, mida mõjutavad väga paljud tegurid ja millega on seotud suur hulk potentsiaalseid veaallikaid. Üleviimised kulgevad edukalt sageli üksnes siis, kui neid on piisavalt hoolikalt planeeritud ja ette valmistatud.

Parema ülevaatlikkuse säilimiseks on soovitatav valida mõni tunnustatud protsessimudel. Praktikas ei ole end lõplikult tõestanud ei top-down-mudel, mis näeb ette ühekordse täiemahulise üleviimise, ega ka spetsialistide rakendatav tegevuspunktide põhine bottom-up-mudel. Parima tulemuse annab hoopis kesktee, mille puhul toimub tööprotsesside ja IT-mudelite pidev kooskõlastamine. Korduvate kooskõlastuste vajadust võivad aidata välja selgitada küpsusmudelid.

Pärast seda, kui asutus on määratlenud üleviimisprotsessi järgmise etapi eesmärgid ja tuvastanud üleviidavad teenused, tuleb järgneva planeerimistöö käigus lähtuvalt asutuse eesmärkidest välja töötada IT-le esitatavad nõuded (k.a turbenõuded). Üleviimise etapp hõlmab nende nõuete tehnilist teostust rakenduste ja süsteemide näol, mida hakatakse käitama. Seda tsüklit korratakse seni, kuni saavutatakse sobiv küpsusaste. Iga korduse puhul tuleb analüüsida, milliseid muudatusi tuleb teha (vanades) rakendustes ja liidestes.

Pärast seda, kui üleviimisprotsessi ajalised piirid ja tööde ulatus on kindlaks määratud, tuleb planeerida vajaliku tehnilise taristu teostus. Siin on eelkõige oluline dimensioneerimine, sest veebirakenduste käitamiskeskkonnad on vajalike ressursside parameetrite poolest olemasolevatest keskkondadest sageli väga erinevad. Mõistlik oleks teha koormuskatsed või vähemalt kaasata spetsialistid, kes oskavad ressursse planeerida.

Üleviimise planeerimisel tuleb täpselt paika panna, milliseid süsteeme millal üle viiakse, kas üleviimiseks on tarvis seisakuaegasid ja kas planeeritud seisakuajad on vastuvõetavad. Ootamatute sündmuste jaoks tuleb ette näha ka üleviimise katkestamisnõuded ja eelnenud olukorra taastamise protseduurid, mis võimaldavad vastava keskkonna uuesti kasutuskõlblikuks muuta.

Siinkohal on eriti oluline, et planeerimise etapis arvestataks kõikvõimalike sõltuvussuhetega, mis puudutavad tootjaid ja standardeid. Standardid tuleks välja valida väga hoolikalt ja asutus peaks end pidevalt kursis hoidma nende võimalike

arengute ja avastatud turvaaukudega.

Juhtudel, kus võetakse kasutusele spetsiaalsed süsteemid, mida seni ei ole tarvis läinud, nt XML-tulemüür, mida kasutatakse Application Level Gateway funktsioonides, tuleb neid enne kasutuselevõttu põhjalikult katsetada ja nende kasutamine turbekontseptsiooni sisse kirjutada.

Juhtudel, kus üleviimine loob võimaluse pakkuda tsentraalselt toimivaid teenuseid nagu identiteedihaldust ja PKI-d standardiseeritult, tuleb eraldi tähelepanu pöörata ka nende teenuste turbele. Võimalikku mõju turbele tuleb väga täpselt kontrollida eriti siis, kui planeeritakse single sign-on-lahendusi, vt ka M 4.456 Autentimine veebiteenustes , M 4.455 Volitamine veebiteenustes ja M 4.453 Pääsmikuteenuse (Security Token Service) kasutamine .

Üleviimisega seotud spetsiifilised ohud on ühelt poolt seotud muudatustega süsteemi arhitektuuris. Seetõttu tuleb eesmärgiks seatud arhitektuuri kaitseks vajalikud turbemeetmed tuvastada juba võimalikult vara, et nendega saaks algusest peale piisavalt arvestada (meetmed tuleb leida kas asjakohastest moodulitest, täiendava turvaanalüüsi või vajaduse korral ka riskianalüüsiga). Üleviimise puhul tuleb arvestada, et üleviimine võib tekitada uusi sõltuvussuheteid, mis võivad oluliselt suurendada seniseid käideldavusnõudeid. Teisalt võib ka üleviimise protsess ise tuua kaasa uusi riske nagu kulutuste ootamatu suurenemine ja üleviimisprotsessi venimajäämine. Mõlemad nimetatud ohud tuleks üleviimise planeerimisel läbi analüüsida ja dokumenteerida.

Suuremahulise üleviimise ja arhitektuuri süvamuudatuste korral on tungivalt soovitatav koostada eraldi turbekontseptsioon ja töötada üleviimise lõpptulemus sisse olemasolevasse turbekontseptsiooni.

Eriti kehtib see neil juhtudel, kus üleviimiseks kasutatakse mõnda tsentraalselt toimivat hooldusliidest (servicebus) (sageli ESB, Enterprise Service Bus). Kuna hooldusliides on tsentraalne komponent, mille tõrge mõjutab ka kõike muud, tuleb sellega hädaolukordade planeerimisel piisavalt arvestada ka juhul, kui SOA käideldavusele on esitatud asjakohased nõuded.

Alahinnata ei tohiks ka vajaminevaid teadmisi. Kuna arhitektuuri muudetakse oluliselt, peavad nii administraatorid kui ka valdkonna eest vastutavad spetsialistid muudatustega harjuma, st tuleb arvestada, et ümberharjumine võtab aega ning

et inimesi on tarvis koolitada.

Üleviimine on kõikidel juhtudel pikaajaline ja strateegiline protsess, mille õnnestumiseks peab juhtkond seda piisavalt juhtima ja toetama ning kasutajad peavad sellele kogu protsessi vältel elu sisse puhuma.

Kontrollküsimused

- Kas üleviimise jaoks on valitud sobiv protsessimudel?
- Kas üleviidavad teenused on tuvastatud ja kas nende nõuded, k.a turbenõuded on teada ja dokumenteeritud?
- Kas vajamineva taristu ja vajalike süsteemide jõudlusnäitajad on tuvastatud ekspertiisi või realistlike koormuskatsetega?
- Kas üleviimiseks vajalikud seisakuajad on välja selgitatud, planeeritud ja kooskõlastatud?
- Kas üleviimise jaoks on koostatud eelnenud olukorra taastamise stsenaarium ja üleviimise katkestamisnõuded?
- Kas üleviimise spetsiifilised ohud on tuvastatud ja dokumenteeritud?
- Kas vastutavatele spetsialistidele ja süsteemi käitajatele on tagatud piisavad teadmised?
- Kas juhtkond tegeleb üleviimise strateegiaga ja juhib üleviimist aktiivselt?

M 2.531 Veebiteenuste turvapoliitika väljatöötamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht
Rakendamise eest vastutavad: administraator, arendaja

Veebiteenuse vajaliku turbeastme tagamiseks tuleb otsustada, kuidas vajalikke turbefunktsioone rakendada ja kes selle eest vastutab. Auditeeritavuse tagamiseks peavad sellised otsused olema arusaadavalt dokumenteeritud. Dokumenteerimiseks on kõige parem kasutada infoturbepoliitikat, sest see moodustab kindla osa asutuse turbealastest ettekirjutustest vt ka M 2.338 Sihtrühmakohase infoturbepoliitika koostamine).

Infoturbepoliitika peaks kajastama vähemalt järgmisi teemasid. Teemade puhul, mida kajastatakse kohustuslikus korras hoopis teistes dokumentides, piisab asjakohasest viitest teistele dokumentidele.

Arhitektuur ja platvormid
Veebiteenuste osatähtsus üldises IT-strateegias
Rakendatava (teenusepõhise) arhitektuuri määratlemine

Arhitektuuri komponentide kirjeldus:

- kaasatud süsteemid,
- kaasatud tarkvarakomponendid,
- kataloogide (registries/repositories) kasutamine,
- Enterprise Service Bus'i kasutamine,
- turvakomponentide (XML-tulemüüride, logiserverite jms) kasutamine, kolmandate osapoolte turbeteenuste kaasamine,
- identifitseerimis- ja autentimis- või volitusteenuste kasutamine.

Otsus, et asutus võtab kasutusele järgmised:

- tooted,
- programmeerimiskeeled ja käigukeskkonnad,
- XML-skeemid,
- standardid,
- protokollid.

Veebiteenustele esitatavad turbenõuded

Veebiteenuse kasutusotstarve asutuse jaoks

- veebiteenustele kehtivad konfidentsiaalsus-, käideldavus- ja terviklusnõuded,
- vajaduse korral kaitsevajadusest olenevate erinevate turvaklasside määratlused,
- võimalikud kolmandate osapoolte turbenõuded (nt veebiteenuste välistarbijad, vt M 2.532 Veebiteenuste osutamine kolmandatele isikutele).

Konkreetsete nõuete tuletamine ja nõuete täpsustamine

- autentimine (autentimisprotseduurid, kolmandate osapoolte kaasamine, liidendus),
- volitamine,
- andmetalletus ja andmete terviklus,
- liideste teostus (backend-süsteemide ühendamine, Enterprise Service Bus'i kasutamine, rakendatavad protokollid),
- side / XML-teadete ja andmetalletuse krüpteerimine,
- side / XML-teadete ja andmete tervikluse tagamine,
- võtmete ja sertifikaatide haldus (ühendamine PKI-ga, kolmandate osapoolte sertifikaatide kasutamine, krüptovõtmete andmevarundus),
- veebiteenuste orkestreerimine ja koreograafia seoses asutuseüleste funktsioonide käitamisega,
- varukoopiate tegemine,
- mastabeeritavus,
- tõrkekindlus,
- logimine,
- dokumenteerimine.

Veebiteenuste haldamine

- aredustöödele esitatavad nõuded,
- katsetus- ja kasutuselevõtu protseduurid,
- elutsükli haldamine,
- kõikide veebiteenuste ja kõikide süsteemide eest vastutavate konkreetsete isikute nimetamine, vastutusalade täpne piiritlemine, kui vastutus jaotub eri valdkondade või isikute vahel (nt arendamine ja käitamine, platvorm ja veebiteenus),
- kasutajate ja õiguste haldamine (protsessid, vastutusalad, dokumentatsioon),
- personali koolitused ja täiendõpe (arendajad, administraatorid), samuti turbealast teadlikkust suurendavate meetmete võtmine,
- turvet puudutavate sündmuste analüüsimine,
- regulaarsete auditite tegemine,
- veebiteenuste hädaolukordade planeerimine (vt ka M 6.154 Veebiteenuste hädaolukordade haldamine).

Turvapoliitika tuleb kõikide asutuse sees sellest puudutatud osapooltega kooskõlastada ja muuta seejärel asutuse vastava instantsi poolt kehtivaks. Kõik puudutatud töötajad peavad kehtiva turvapoliitikaga kursis olema ja see peab olema

neile lihtsalt ligipääsetav. Sobivate protsesside ja töötajate vastustusalade määratlemisega tuleb tagada, et turvapoliitikat täiendataks ja ajakohastataks vajadust mööda.

Turvapoliitika nõuete täitmist tuleb regulaarselt kontrollida, nt revisjonidega.

Kontrollküsimused

- Kas selles meetmes loetletud valdkonnad on asutuse sobivas dokumendis reguleeritud?
- Kas ajakohaste nõuete järgimine on asutuses kohustuslik (nõuete kehtestamine)?
- Kas nõuete ajakohastamine ja edasikirjutamine on tagatud sobivate intervallidega?
- Kas kehtestatud nõuete järgimist kontrollitakse regulaarselt?

M 2.532 Veebiteenuste osutamine kolmandatele isikutele

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond
Rakendamise eest vastutavad: müügiosakond, lepingute haldajad

Veebiteenuseid saab osutada mitmel moel. Neid saab müüa nt valmis lahendusena (teenust käitab teenuse tarbija) või ka teenusena (teenust käitab teenuse osutaja). Teenuseosutamise puhul tuleb veebiteenuse tarbijaga kokku leppida kõik olulised lepingutingimused ja vormistada need teenusetasemeleppena (SLA), milles määratletakse nt kontaktisikud, reaktsiooniajad, kontroll andmete üle, teenused, võetavad turbemeetmed jms (vt ka M 2.533 Veebiteenuste osutamise lepingutingimuste koostamine).

Veebiteenuste osutamisel kolmandatele osapooltele tuleks pöörata tähelepanu järgmistele teguritele:

Ümbrus

Veebiteenuste osutamiseks saab rakendada teenuseosutaja enda IT-taristut, teenuse tarbija IT-taristut või ka mõnda kolmanda osapoole IT-taristut. Olenevalt sellest, millist taristut teenuse osutamiseks kasutatakse, vastutab taristu turbe, aga ka nt varukoopiate tegemise ja hädaolukorra õppuste korraldamise eest erinev osapool. Seetõttu tuleb lepingupartnerite vahel täpselt paika panna, kes milliste komponentide ja tööprotsesside eest vastutab ja vastavad kokkulepped tuleb ka kõigile arusaadavalt dokumenteerida.

Kontaktisikud

Kõik lepingupartnerid (veebiteenuse osutaja ja tarbija) peavad nimetama enda kontaktisikud vähemalt järgmistes valdkondades:

- lepinguküsimused,
- sisulised/valdkonnapõhised küsimused,
- tõrgetest teavitamine, tõrgete likvideerimine ja hädaolukordadest teavitamine,
- turvaintsidentidest teavitamine ja nende likvideerimine,
- kokkulepitud aruannete esitamine jõudlusnäitajate, turvet puudutavate sündmuste ning süsteemide ja teenuste muudatuste kohta.

Kõikide kontaktisikute jaoks tuleb planeerida ja määrata ka asendajad.

Kasutajate ja õiguste haldamine

See lepingupartner, kes tegeleb veebiteenuste kasutaja- ja õigustuseprofiilide haldamisega, peab juurutama ka asjakohased haldus-, side- ja dokumenteerimisprotseduurid. Kasutajakontode loomine ja õiguste haldamine võib toimuda nii teenuseosutaja kui ka teenuse tarbija vastutusel. Mõeldavad on ka mitmeastmelised teenusemudelid, mille puhul teenuseosutaja loob tarbija jaoks administraatori kasutajakontod, mille abil tarbija loob iseseisvalt vajalikud asutusesisesed kasutajakontod. Keerulisema struktuuriga keskkondades võib kasutajate tuvastamine, autentimine ja volitamine olla ka kolmanda osapoole hallata ja sel juhul kasutatakse loetletud teenuste osutamiseks omakorda ka veebiteenust.

Hooldus

Hooldustööd, eriti nt veebiteenuste või neid käitavate süsteemide turvapaikade ja värskenduste installeerimine, võivad otseselt mõjutada teenuse tarbijat. Hooldustööde tagajärjel võivad nt muutuda tarbijale pakutavad funktsioonid ning veebiteenuse käideldavus võib olla lühiajaliselt piiratud. Seetõttu tuleb juurutada asjakohased protseduurid, mis tagavad, et vajalikud hooldustööd saaksid teenuse tarbijaga kooskõlastatud võimalikult vara, nt saab kokku leppida kindla hooldusgraafiku.

Aruandlus- ja teavitamiskohustused

Veebiteenuste osutaja peab juurutama protseduurid, mis võimaldavad tal täita tarbijaga kokku lepitud aruandlus- ja teavitamiskohustust. Siia kuuluvad ka aruandluse vormiline pool ja aruandluse esitamiskanalid.

Turvaintsidentide lahendamine

Turvavintside lahendamise protsessi puhul tuleb arvestada, et turvaintsidentide käsitlemiseks võib minna tarvis teenuseosutaja ja teenuse tarbija vahelist väga laialdast koostööd. Koostöö tagamiseks tuleb kindlaks määrata vajalikud suhtluskanalid, kontaktisikud ning alarmeerimis- ja dokumenteerimisprotsessid.

Hädaolukorraks valmisoleku planeerimine

Ka hädaolukorraks valmisoleku planeerimine eeldab veebiteenuse osutaja ja tarbija vahelist koordineeritud koostööd. Veebiteenuse hädaolukorraks valmisoleku planeerimisel tuleb pöörata erilist tähelepanu tarbija vajadustele. Samas tuleb täpselt kooskõlastada ka hädaolukordade ennetamiseks vajalikud meetmed, nt ühiste hädaolukorra õppuste korraldamine.

Kontrollküsimused

- Kas käitamiskeskkonda puudutavad vastutusalad on kindlaks määratud ja kirjalikult fikseeritud?
- Kas kõik partnerid on nimetanud enda kontaktsikud ja need teistele teatavaks teinud?

- Kas kasutajate ja õiguste haldamiseks on olemas asjakohased haldusprotseduurid?
- Kas veebiteenuste ja nende käitamiskeskkonna hooldamiseks ja edasiarendamiseks on juurutatud protseduurid?
- Kas aruandlus- ja teavituskohustuse täitmiseks on juurutatud asjakohased protseduurid, aruandlusvormid ja määratletud suhtluskanalid?
- Kas turvaintsidentide lahendamise puhul on arvestatud vajaliku koostööga teenuseosutaja ja selle tarbija vahel?
- Kas veebiteenuse osutaja on enda hädaolukordade halduse protsessides arvestanud tarbija nõuetega ja kas hädaolukordade ennetamise meetmed on omavahel kooskõlastatud?

M 2.533 Veebiteenuste osutamise lepingutingimuste koostamine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond

Rakendamise eest vastutavad: müügiosakond, lepingute haldajad

Olukorras, kus veebiteenuseid osutatakse kolmandatele osapooltele, peavad veebiteenuse osutaja ja veebiteenuse tellija sõlmima omavahel kirjalikud kokkulepped, mis reguleerivad teenuse turvet ja ka teisi teenuseosutamise tingimusi.

Konkreetsed tingimused sõltuvad veebiteenust kasutavate rakenduste ja tööprotsesside turbest. Tingimuste poolest on sageli kesksel kohal veebiteenuse käideldavus, sest veebiteenuse tõrge võib omakorda pärssida teiste sellest sõltuvate veebiteenuste ja rakenduste tööd, st ühe veebiteenuse tõrge võib häirida korraga paljusid tööprotsesse.

Veebiteenuste osutaja ja nende tellija vahel sõlmitavate lepingute sõlmimisel tuleks olenevalt kaitsevajadusest pöörata tähelepanu järgmistele teguritele.

Lepingu üldteemad

Valdkonnapõhised lepingupunktid

- tellija poolt tarbitavate veebiteenuste tüüp ja maht, kasutusvaldkond,
- veebiteenuste osutaja poolt tellijale pakutav valdkonnapõhine nõustamis- ja tugiteenus,
- koolitused ja dokumentatsioon,
- kliendiandmed / seadusandluse muutumine.

Tehnilised jõudlusnäitajad

- käideldavus (käideldavuse keskmine näitaja, hooldustähtpäevad, maksimaalne seisakuaeg),
- jõudlus (tehingukiirus, samaaegsete pöörduste arv, ühenduse ribalaius),
- andmetalletus (salvestuskohad, krüpteerimine, varukoopiate tegemine).

Töökorralduse tingimused

- kommunikatsioonikanalite ja kontaktisikute määramine,
- protsesside, tööprotsesside ja vastutusalade kindaksmääramine,
- probleemide lahendamisprotseduurid, vajalike volitustega kontaktisikute nimetamine,
- regulaarsed kooskõlastused,
- andmekogumite arhiveerimine ja kustutamine (eriti lepinguliste suhte lõpetamisel),
- veebiteenuste teenuseosutaja personali sissepääsuõigused ja pääsuõigused seoses tellija ruumide ja IT-süsteemidega,
- arveldusmudel ja arvelduspõhimõtted.

Personal

- töötajate omavahelise asenduskorra kehtestamine ja kooskõlastamine.

Valmisolek hädaolukorraks ja reageerimine hädaolukorras

- vigade ja häirete liigitamise kategooriad lähtuvalt nende tüübist, raskusastmest ja pakilisusest,
- vajalikud tegevused tõrkeolukorras,
- alarmeerimisprotsessi kontaktisikud koos kontaktandmete ja asendajatega,
- reageerimisajad ja eskalatsiooniastmed,
- tellija osaluskohustus hädaolukordade lahendamisel,
- regulaarsete ja adekvaatsete hädaolukordade õppuste liigid ja nende toimumise ajaline järjestus,
- andmevarunduse tüüp ja maht,
- kokkulepe, kas ja millised süsteemid peavad olema liiasusega,
- vääramatu jõuga seotud kahjud,
- lepingu lõpetamise tingimused seoses maksejõuetusega ning veebiteenuste osutaja või tellija tegevuse lõpetamisega, kaasa arvatud sätted, mis reguleerivad, kuidas käiakse ümber teenuseosutaja poolt salvestatud andmetega.

Turbekontseptsioon

Turbekontseptsiooni ja selle juurde kuuluva hädaolukorraks valmisoleku kontseptsiooni olemasolu on tarvis tõestada, samuti tuleb võtta kõik andmete kaitseks ette nähtud turbemeetmed ja need ka dokumenteerida. Võetud meetmete, eriti aga teenuse tellija andmetöötlusega seotud tehniliste ja töökorralduslike meetmete kohta, peab veebiteenuse osutaja pidama ise sobivat ülevaadet. Veebiteenuse osutaja peab tellijale kinnitama, et järgib kõiki olulisi asjakohaseid ettekirjutusi ja seadusi ning eelkõige andmekaitseseadust.

Veebiteenuste arendamine ja laiendamine

Veebiteenuste efektiivse arendustöö tagamiseks tuleb kokku leppida tingimused, mis on kõikidele lepingupartneritele kohustuslikud. Eesmärk on tuvastada võimalikult kiiresti kõik potentsiaalsed kontseptsiooni- ja programmeerimisvead ja vältida vigu. Arendustöödel tuleks järgida mõnda sobivat töömudelit, nt V-mudelit XT (extreme tailoring).

Muudatuste ja paikade haldus

- Välja tuleb töötada tingimused, mis võimaldaksid veebiteenuse tellijal kohandada sisseostetavat teenust enda muutunud nõuetega. Tuleb kehtestada reeglid, kuidas peab teenuseosutaja reageerima teenuse tellija nõuete muutumisele.
- Tuleb määratleda vigade kõrvaldamiseks lubatud aeg.
- Kokku tuleb leppida uue riist- ja tarkvara katsetusprotseduurides. Siinkohal tuleks kaasata järgmised punktid:
  - vastastikune teavitamiskohustus ja
  - vastastikused kooskõlastused enne süsteemis tehtavaid olulisi muudatusi.

Kontrollid

- Teenuseosutaja ja teenuse tellija peavad kokku leppima, kui kaugele ulatuvad teenuste tellija õigused teha teenuseosutaja süsteemidele auditeid. Juhtudel, kus teenuseosutajal on ette näidata turbealased sertifikaadid, tuleks kokku leppida, et tarbijale esitatakse auditite aruanded (või vähemalt väljavõtted tarbija jaoks olulistest lõikudest).
- Lepingu pooled peavad kokku leppima logimisele ja logifailide analüüsile kehtestatavad nõuded.
- Lepingupartneritele peab olema selge, milline on tarbija õigus nõuda logiandmete esitamist või nendega tutvumist ja millist lisateavet ja milliseid juurdepääse võimaldatakse tarbijale seoses turvaintsidentide lahendamisega.

Eelnevalt loetletud punktide kohta saavutatud kokkulepped tuleb lepingu poolte vahel ka jõustada, st need peavad moodustama lepingulises suhtes kindla osa nii teenuste osutamisel kui ka nende tarbimisel.

Kontrollküsimused

- Kas kõik kokkulepped on kirjalikult fikseeritud?
- Kas leping sisaldab kõiki konkreetse teenuseosutaja ja tarbija vahelise lepingulise suhte jaoks olulisi punkte?
- Kas veebiteenuse osutaja ja tarbija vahelised kokkulepped on sõlmitud õiguslikult siduvalt?

M 2.534 Pilvteenuse kasutamisstrateegia koostamine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond

Rakendamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, spetsialist

Pilvteenuse kasutamise otsuses on alati teatud kokkupuude strateegiaga ja seda ka siis, kui pilvteenuseid hakatakse kasutama üksnes väikses mahus. Teenuse väike maht võib luua olukorra, kus vastava väljasttellimise võimalikke tagajärgi hakatakse kas eitama või alahindama. Pilvteenuste väljasttellimine erineb teistest IT-väljasttellimistest nii teenuste mahu, lepingu kestuse kui ka teenuste tarbimise poolest. Kõigele vaatamata jääb pilvteenuste kasutamine olemuselt siiski väljasttellimiseks (vähemalt juhul, kui asutus tellib teenuse asutusevälise teenuseosutaja käest) ning on seetõttu seotud strateegiliste otsustega. Strateegiline otsus eeldab majanduslike, tehnoloogiliste, töökorralduslike ja turbealaste raamtingimuste põhjalikku analüüsi.

Selles meetmes ei käsitleta konkreetsete pilvteenuste valimise protsessi ega ka pilvteenustele esitatavate nõuete määratlemist. Nimetatud tegevuste juurde tuleb asuda alles pärast pilvteenuse kasutamisstrateegia koostamist. Pilvteenuse kasutamisstrateegia koostamisel tuleks arvestada järgmiste punktidega, mis tuleb ka dokumenteerida.

Integreerimine asutuse üldstrateegiaga. Asutus peab endale selgeks tegema, millised on pilvteenuste kasutamise strateegilised lähtepunktid. Tuleb luua ülevaade, millised pilvteenused asutuse jaoks üldse kõne alla tulevad. Tuleb määratleda, mis põhjusel hakatakse pilvteenust kasutama ja milline on pilvteenuste kasutamise eesmärk, samuti see, kui teenusepõhiseks tahetakse valdkonda arendada, st mil määral soovitakse seniseid nn klassikalisi IT-lahendusi asendada pilvteenustega. Sõnastatud eesmärgid tuleks kaasata ka asutuse üldstrateegiasse.

Teostatavuse uuring ja raamtingimuste koostamine. Vastav analüüs tuleks vormistada teostatavuse uuringuna, millest nähtub, kas asutusel on mõtet analüüsitud pilvteenust juurutada või mitte.

Majanduslikud tegurid ja esmane tulude ja kulude analüüs. Tulude ja kulude esmane analüüsimine peaks looma üldise ettekujutuse, kas pilvteenuste juurutamisega kaasneb majanduslikke eeliseid. Kulude poolel tuleb arvestada pilvteenuse käitamiskulude, üleviimisega seotud kulude, töötajate ja administraatorite koolituskulude ning võimaliku uue riistavara soetamise ja võrgu jõudlusnäitajate suurendamise kuludega.

Teenuste ja teenusemudeli valimine. Strateegiliste otsuste raames tuleb dokumenteerida, milliseid konkreetseid teenuseid hakatakse tulevikus pilvteenuse osutajate käest soetama. Teenusevaliku kõrval tuleb teenuste jaoks tuvastatud nõuete järgi otsustada ka see, millist teenusemudelit hakatakse tarbima (nt kas privaat-, avalik või hübriidpilv).

Turbeaspektidega arvestamine juba algusest peale. Asutus peab tagama, et kõiki olulisi ja üldkehtivaid tehnilisi ning töökorralduslikke turbenõudeid järgitaks piisavalt juba pilvteenuste kasutamise planeerimise etapis. Oluline on välja selgitada, mil määral on pilvteenuste kasutamist kajastatud asutuse infoturbepoliitikas.

Asutuse vastutavad töötajad peaksid olema kursis eelkõige järgmiste pilvtehnoloogia eripäradega:

- pilvteenuse osutajal võib olenevalt teenusemudelist tekkida juurdepääs asutuse andmetele. See juurdepääs võib hõlmata ka suure kaitsevajadusega andmeid;

- pilvteenuste kasutamise tehniline teostus eeldab teenuseosutaja ja asutuse vahelist andmeedastust. Sellega kaasneb tavapärasest suurem ohupotentsiaal, mille tagajärgi peab asutus analüüsima ja hindama;
- pilvteenuste kasutuselevõtt eeldab asutuselt ka uute tööprotsesside väljatöötamist, juurutamist ja tööshoidmist. Asutus peab välja selgitama, kui palju tuleb selle jaoks teha ümberkorraldusi.

Samuti peaks asutus enda jaoks välja selgitama, analüüsima ja dokumenteerima kõik pilvteenuste kasutamise eelised ja puudused, mis seonduvad asutuse infoturbega.

Turvaanalüüsi koostamine. Pilvteenuse kasutamisstrateegia koostamiseks peab asutus tegema planeeritava pilvteenuse kohta turvaanalüüsi/riskianalüüsi. ISKE rakendusjuhend näeb ette täiendava turvaanalüüsi ehk tegeliku turvaolukorra kontrolli (ISKE rakendamise samm 10). Selline turvaanalüüs võib viia täiendavate turvameetmete rakendamiseni või välistada mingit tüüpi tegevused (nt teatavate andmete hoidmise pilves või andmete saatmise üle avaliku interneti).

Pilvtöötluse puhul tuleks täiendav turvaanalüüs läbi viia juba pilvtöötluse kavandamisel, sealhulgas meetmete planeerimise juures (ISKE rakendamise samm 8). Kui turvaanalüüsi tulemusena otsustatakse tugevdada olemasolevaid ISKE meetmeid või lisada uusi meetmeid, siis võib see otsus kaasa tuua täiendavaid kulutusi. Turvaanalüüsi tegemisel tuleb lähtuda ISKE rakendusjuhendis toodust ja riskianalüüsi parimatest praktikatest. Nii on võimalik tuvastada, kuidas olemasolevaid tööprotsesse ja IT-kooslusi piirata ja teistest lahutada, et teatud osa nendest saaks hakata kasutama pilvteenusena. Pärast turvaanalüüsi saab otsustada, kas ja kuidas tuleks edasi tegutseda. Analüüs peaks muu hulgas kajastama ka pilvteenuste kasutamisega seotud jääkriske. Turvaanalüüsi tulemused peaksid kajastuma ka kulude ja tulude analüüsis, mida tuleb vajaduse korral (olenevalt turvaanalüüsi tulemustest) muuta.

Tegevuskava koostamine. Pärast strateegilisi otsuseid ja turvet kajastavate tegurite analüüsimist tuleks hakata mõtlema tehnilisele teostusele. Juhtudel, kus asutus soovib korraga kasutusele võtta mitu pilvteenust, on abiks olnud tegevuskava (cloud road map) koostamine. Tegevuskavas tuleks paika panna pilvteenuste juurutamise ajagraafik ja kirjeldada asjakohase etapimudeliga juurutamiseks vajalikke tööetappe. Tegevuskava suurendab muu hulgas kasutajate vastuvõtlikkust pilvteenuste rakendamise suhtes ja aitab tuvastada võimalikke juurutamisega kaasnevaid tehnilisi probleeme.

Kontrollküsimused:

- Kas asutus on koostanud pilvteenuse kasutamisstrateegia?
- Kas asutus on enda jaoks analüüsinud pilvteenuste kasutamisega seotud seadusandlikke ja töökorralduslikke raamtingimusi ja tehnilisi nõudeid?
- Kas asutus on välja selgitanud, kuidas mõjutab pilvteenuste kasutamine asutuse tehnoloogia ja tööprotsesside turvet?
- Kas pilvteenuste jaoks on ette nähtud individuaalne turvaanalüüs?
- Kas asutus on dokumenteerinud, milliseid teenuseid ja teenusemudeleid hakatakse tulevikus pilvteenuste osutaja kaudu tarbima?
- Kas asutusel on koostatud pilvteenuste juurutamise tegevuskava?

M 2.535 Pilvteenuse kasutamise turvapoliitika koostamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: erialaspetsialist, infoturbespetsialist

Pilvteenuste kasutamist reguleeriva turvapoliitika koostamisel saab aluseks võtta eelnevalt koostatud strateegia, kui see on piisavalt detailne (vt M 2.534 Pilvteenuse kasutamisstrateegia koostamine). Strateegias sõnastatud nõudeid tuleb turvapoliitika jaoks täpsustada nõnda, et need kirjeldaksid pilvteenust võimalikult laialdaselt (vt ka meede M 2.536 Tarbitavate pilvteenuste määratlemine teenuste tarbija poolt) ja et nende põhjal saaks valida ka sobiva pilvteenuste osutaja (vt M 2.540 Pilvteenuste osutaja hoolikas valimine).

Turvapoliitikas tuleks kajastada kõiki liideste, tööprotsesside korralduse ning tehnoloogia ja seadusandlusega seotud raamtingimusi. Turvapoliitika peab tehnoloogia ning selle juurde kuuluvate sidekanalite ja -teenuste kõrval sisaldama ka andmekaitse aspekte, nt asutusest väljapoole suunatud andmete liigitamist eri turbeklassidesse. Erilist rõhku tuleb pöörata andmete konfidentsiaalsusele ja tervikusele. Samuti peaks turvapoliitika kajastama asutuse töökorraldust puudutavaid meetmeid, nagu kasutajate ja administraatorite koolitamine.

Pilvteenuse kasutamise turvapoliitikas tuleb muu hulgas kajastada järgmisi valdkondi:

Vastutus

Andmete omanik vastutab vastutava töötlejana oma andmete turvalisuse eest ka pilvteenuste kasutamisel. Andmete omanik ehk teenuse tellija peab pilvteenuse tellimisel veenduma, et teenuse osutaja rakendaks piisavaid turbemeetmeid. Kolmandate osapoolte pakutava pilvteenuse kasutamisel ei ole andmete omanikul teatud juhtudel võimalik kontrollida pilvteenuse osutaja rakendatavaid meetmeid, vaid ta peab usaldama teenuseosutaja tellitud auditeid ja vastavuse kontrolle. Seda olulisem on pöörata rõhku pilvteenuse pakkuja valimisele ja kohustuste reguleerimisele lepingus.

Pilvteenuste osutajatele kehtestatavad turbenõuded

Asutusel peaksid olema selged nõuded soetatava teenuse käideldavusele ja pilvteenuste osutaja tegevuskohale. Samuti peaks asutus kehtestama pilvteenuse osutajale töökorraldust käsitlevad nõuded (nt kahemehereegli järgimise kohustus haldustöödel) ja võõra personali rakendamise reeglid (vt M 2.226 Asutusevälise personali kasutamise protseduurid). Turbenõuetes tuleb sätestada konkreetsed eeskirjad andmete talletamisele, töötlemisele ja kustutamisele. Turvapoliitikas tuleks dokumenteerida ka teenuseosutajalt nõutavad sertifikaadid (eelistatavalt IT etalonturbe sertifikaadid).

Avaliku pilve kasutamisel sõltuvad turbemeetmed pilves töödeldavate andmete turbe vajadusest, erilist tähelepanu tuleb pöörata andmete konfidentsiaalsuse ja tervikluse tagamisele ning hinnata selle kohaselt kriitiliselt pilvtöötluse asukohta, omandust ja transpordikanaleid.

Teenuseosutamise seadusandlikud piirangud

Euroopa Liidus asuvas ja EMP-s või samaväärse andmekaitsetasemega riigis tegutsevas avalikus pilves tohib andmeid töödelda kuni turvaklassini K2T1S1 k.a. Käideldavus on piiratud klassiga K2, terviklus klassiga T1 ja konfidentsiaalsus klassiga S1. Piirangud on tingitud andmete avalikus pilves töötlemisega kaasnevatest täiendavatest ohtudest, mille tingivad osapoolte paljusus, vastutuse jagunemine, turvameetmete rakendatuse kontrollimise keerukus ja läbipaistmatus, teenusepakkuja usaldatavus, seadusandlikud erisused, pilveressursi jagamine teiste klientidega jne.

Ka Eestis paikneva kolmanda osapoole pakutava pilvteenuse kasutamisel tuleb eelnevalt teostada põhjalik riskianalüüs, sh hinnata andmete pilves töötlemise ja väljasttellimisega kaasnevaid riske ning järgida muu hulgas ISKE teenuse väljasttellimise ja andmete pilves töötlemise nõudeid. Eesti territooriumil servereid majutava ja ISKE auditi läbinud pilvteenuse osutaja puhul viiakse läbi lihtsustatud riskianalüüs, mis ei pea käsitlema pilvteenuse osutaja valimisega kaasnevaid riske.

Kui asutus hakkab kasutama Eestis paiknevates serverites majutatavat ja ISKE nõuetekohaselt auditeeritud avalikku pilvteenust, tuleb muu hulgas kindlaks määrata teenuse soetaja poolt teenuse osutajale antavad õigused (nt õigus juurdepääsule, õigus süsteemide ja andmete pääsuõigustele).

Seadustest ja ettekirjutustest tulenevad turbenõuded

Pilvteenuste osutajatele, kes tegutsevad riikideüleselt või rahvusvaheliselt, tuleks pöörata erilist tähelepanu, sest neile võivad jurisdiktsioonist tulenevalt kehtida tavapärasest erinevad kohustuslikud nõuded ja ettekirjutused. Asutusesisesed turbenõuded tuleb sõnastada turbekontseptsioonina, nagu on kirjeldatud meetmes M 2.539 Pilvteenuste kasutamise turbekontseptsiooni koostamine . Turbekontseptsiooni koostamisel on asutusel valida, kas võtta kasutusele mitu eraldi kontseptsiooni iga spetsiifilise kasutusvaldkonna jaoks või koostada üldine kontseptsioon, mis katab kõiki või mitut kasutusvaldkonda.

Kontrollküsimused:

- Kas pilvteenuse kasutamise turvapoliitika sisaldab konkreetseid ja piisavalt detailseid juhiseid, kuidas seda poliitikat asutuses rakendada?
- Kas pilvteenuste osutajale esitatavad spetsiifilised turbenõuded on dokumenteeritud?
- Kas pilvteenustele kehtivad konfidentsiaalsus-, terviklus- ja käideldavusnõuded on dokumenteeritud?
- Kas asutusele on teada, millised seadustest tulenevad nõuded kehtivad nii riigisisestele kui ka rahvusvaheliselt tegutsevatele pilvteenuste osutajatele.

M 2.536 Tarbitavate pilvteenuste määratlemine teenuste tarbija poolt

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: erialaspetsialist, infoturbespetsialist

Asutus, kes soovib kasutusele võtta pilvteenused, peab need esmalt enda jaoks määratlema. Information Technology Infrastructure Library (ITIL) määratleb teenust kui võimalust, mis peaks teenuse tellijale looma lisaväärtuse. Selleks peab teenus kas lihtsustama või soodustama mõne eesmärgi saavutamist. Seevastu teenuse tellija ise ei vastuta kõikide kulude ega ka riskide eest.

Pilvteenuste kontekstis tähendab see seda, et teenuseosutaja saab luua lisaväärtust üksnes juhul, kui asutus teab, millised on tema pilvteenuste kasutamise eesmärgid ja on need ka sobivalt dokumenteerinud. Pilvteenutse kasutamisega seotud eesmärgid määratletakse asutuse erinevate nõuete baasil, nagu on kirjeldatud meetmetes M 2.534 Pilvteenuse kasutamisstrateegia koostamine ja M 2.535 Pilvteenuse kasutamise turvapoliitika koostamine . Määratlemisel on soovitatav kasutada ühtse struktuuriga loetelu, mis kajastaks kõiki planeeritavaid pilvteenuseid võimalikult ülevaatlikult.

Selleks võib kasutada nt ITIL-i koostatud teenusenäidiseid (service templates). Loetelu võiks kajastada järgmisi teemasid:

- teenuse lühend ja teenuse nimi,
- lühikirjeldus,
- kategooria,
- alam- ja sekundaarteenused,
- variandid,
- tehnilised parameetrid,
- teenuseparameetrid/SLA-d
- SLA-de mõõtmine,
- teenuste kehtivus (ajavahemik),
- teenuse üleandmine,
- kuluarvestuse metoodikad,
- hind/arveldamine,
- teenuse kontaktisikud,
- õigustatud isikud ja taotlejad,
- eeldused.

Tarbitavate pilvteenuste määratlemisel peaks asutus pöörama erilist tähelepanu järgmistele valdkondadele.

Liidesed ja töötajate vastutusalad

Teenuseid tarbima hakkav asutus peaks tuvastama enda jaoks kõik olulised liidesed ja nendega seotud vastutusalad ning need dokumenteerima.

Pilvteenuste kasutamise olulise komponendi ja liidese moodustab klienttarkvara (nt täiendava ajamisüsteemi integreerimiseks, et kasutada onlain-salvestusteenuseid). Seetõttu tuleb pilvteenuste määratlemisel pöörata suurt tähelepanu selliste komponentide ja liideste valikule.

Kuna siin tuleb arvestada erinevate teguritega, võiks asutus sobiva valiku tegemiseks leida esmalt vastused järgmistele küsimustele.

- Kas juhtudeks, kus klienttarkvaras peaks tekkima tõrge, on välja töötatud selged asendustasandid?
- Kas seni kasutatava IT-taristu kontekstis võib eeldada sõltuvus- või ühilduvusprobleeme?
- Kas klienttarkvara saab muudatuste haldamise protsessi kaasata ilma probleemideta või tuleb tarkvara kohandada? Lisateavet leiate artiklitest M 2.221 Muudatuste haldus , B 1.14 Turvapaikade ja muudatuste haldus .
- Kas klienttarkvara vastab asutuses kehtivate katsetus- ja kasutusse lubamise protseduuride nõuetele?

Turvaliste autentimismeetodite valimine ja täiendavate turbeaspektidega arvestamine

Pilvteenuste juurutamist planeerides tuleks valida võimalikult turvalised autentimismehhanismid, nt kahefaktoriline autentimine pilvteenuste haldamisel ja kasutamisel.

VPN lahendus pilvteenuste kasutamisel läbi interneti – teenusemääratlus peab sisaldama ka asjakohaseid krüpteerimisnõudeid ja varukoopiate tegemist asutuse töötajate poolt.

OLA ja SLA defineerimine

Pilvteenuste jaoks tuleb välja töötada konkreetsed asutusesisesed nõuded ja koos nendega sõnastada ka kasutajate vajadustega arvestav teenusetase. Asutusesisesed nõuded, mida nimetatakse ka OLA-ks (operational level agreement) võetakse hiljem lähtematerjaliks, mille baasil töötatakse välja välise teenuseosutajaga sõlmitav SLA (service level agreement).

Pärast seda, kui tarbitav pilvteenus on määratletud, tuleb selle kasutamiseks välja valida sobiv teenuseosutaja (vt ka M 2.540 Pilvteenuste osutaja hoolikas valimine). Määratletud pilvteenuse lõplikud tegelikud nõuded tuleb vormistada teenuse tellija ja pilvteenuse osutaja vahel sõlmitavas lepingus (vt ka M M 2.541 Pilvteenuseosutajaga sõlmitava lepingu koostamine).

Kontrollküsimused:

- Kas asutus on määratlenud tarbitava pilvteenuse sisu?
- Kas asutusel on loetelu, mis kajastab kõiki planeeritavaid ja kasutatavaid pilvteenuseid?
- Kas kõik pilvteenuse kasutamiseks vajalikud liidesed ja töötajate vastutusalad on määratletud ja dokumenteeritud?
- Kas asutus on määratlenud turvaliste autentimismeetodite valimise nõuded?
- Kas tarbitavate pilvteenuste jaoks on välja töötatud konkreetsed asutusesisesed nõuded?
- Kas asutus on välja töötanud pilvteenuste krüpteerimise nõuded?

M 2.537 Teenuste pilvteenusteks üleviimise turbe planeerimine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: erialaspetsialist, infoturbespetsialist

Asutus, kes otsustab juurutada pilvteenused, peab pöörama tähelepanu üleviimisprotsessi ja pilvteenuste juurutamise turbele. Terminiga üleviimine (ka migratsioon) tähistatakse nii tehnoloogilist üleminekut ühe süsteemi kasutamiselt teisele kui ka pilvteenuse osutaja vahetamist.

Pilvteenuste turvalise juurutamise planeerimine (vt M 2.538 Pilvteenuste juurutamise turbe planeerimine) puudutab erinevaid tegureid, mis väljuvad üleviimisprotsessi planeerimise raamidest. Teenuste pilvteenusteks üleviimise turbe planeerimisel peab asutus koostama üleviimise kontseptsiooni, mis tuleb vormistada pilvteenuste kasutamise turbekontseptsiooni ühe osana (vt M 2.539 Pilvteenuste kasutamise turbekontseptsiooni koostamine). Nende tööde käigus tuleb arvestada mitmete pilvtehnoloogia eripärade ja eeldustega ning kaasata need üleviimise kontseptsiooni.

Pilvteenuste juurutamise planeerimine asutuses

Pilvteenuste juurutamine toimub enamasti etapikaupa ja see erineb n-ö klassikalisest väljasttellimise protseduurist. Enamatel juhtudel puudub vajadus nn tegeliku ülemineku (transition) järele. Ülemineku all peetakse silmas ühe käitamismudeli asendamist teisega, nt iseseisva käitamise asendamist väljasttellimisega.

Planeerimistööde algusetapis tuleks paika panna kõik töökorraldust puudutavad muudatused, nagu töörollide hierarhiline struktuur, töörollide sisu, jaotumine ja töötajate vastutusalad, samuti asjakohased katsetus- ja üleminekuprotseduurid, et tagada tõrkevaba üleviimine ning käitamise pidev turve. Lisaks on soovitatav välja töötada täiendavad lepingutingimused, mida asutus hakkab kasutama pilvteenuse osutaja ja võimalike väliste üleviimisteenust osutavate partneritega sõlmitavates lepingutes. Asutus peaks selgelt defineerima, millisest ajahetkest on asutusel õigus nõuda teenuse vastamist kokkulepitud teenusetasemele.

Asutuse IT-süsteemidega arvestamine

Pilvteenuste tõrkevaba kasutamise tagamiseks tuleb üleviidavad teenused siduda asutuse IT-süsteemidega, analüüsida asutuse IT-keskkonda ja tuvastada kõik senised liidesed ja võimalikud tulevikus vajatavad liidesed ning mõelda, kuidas neid muutuvate nõuetega kohandada.

Mõju tööprotsessidele

Senised tööprotsessid tuleb kohandada pilvteenuste kasutamisele vastavaks. Vajaduse korral peab asutus sõnastama uued tööülesanded, määratlema vastutusalad ja korraldama vajalikud koolitused.

Kontrollküsimused:

- Kas paneeritavate pilvteenuste jaoks on koostatud üleviimise kontseptsioon, mis on osa pilvteenuste kasutamise turbekontseptsioonist?
- Kas üleviimisega seotud töökorralduse muutused on reguleeritud?
- Kas asutuse senised tööprotsessid on pilvteenuste kasutamise kontekstis läbi analüüsitud ja kas need on kohandatud?

- Kas üleviimise protsessi puhul on piisavalt arvestatud asutuse seniste IT-süsteemidega?
- Kas asutus on välja selgitanud töötajate koolitamisvajadused?

M 2.538 Pilvteenuste juurutamise turbe planeerimine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator, infoturbespetsialist

Siin pööratakse tähelepanu sellele, kuidas viia teenuseid turvaliselt üle pilvteenusteks ja kuidas neid võimalikult turvaliselt juba olemasoleva IT-keskkonnaga integreerida.

Pilvteenuse kasutamisele esitatud nõuete alusel (vt M 2.534 Pilvteenuse kasutamisstrateegia koostamine) peab asutus analüüsima, kas ja kui suur on vajadus kohandada vähemalt alljärgnevalt kirjeldatud valdkondi. Analüüsi tulemused tuleb dokumenteerida ja kui nõuded muutuvad, tuleb analüüsi muudatustega kohandada. Dokumenteerida tuleb ka kõik valdkonnad, mis eeldavad aktiivset tegutsemist, et nendega saaks arvestada täiendavate meetmete võtmisel.

Liidesesüsteemide kohandamine

Analüüsida järgmisi liidesesüsteeme: koormusejaoturid, proksid, marsruuterid, turvalüüsid, liIT-süsteemid (federation systems).

Küsimused kohandamisevajaduste ja uute toodete soetamise vajaduse väljaselgitamiseks:

- Kas asutusel on tarvis uusi liidesesüsteeme?
- Kas kõik senised liidesesüsteemid toetavad planeeritava pilvteenuse kasutamist?
- Kas senised liidesesüsteemid suudavad planeeritavaid pilvteenuseid teenindada kõikides valdkondades? Näiteks kas kasutatav proksi suudab tagada rakendusserveri piisava ülevaatuse?
- Millised on liidesesüsteemidele esitatavad jõudlusnõuded ehk andmete läbilaskenõuded?
- Kas liidesesüsteemid tuleb rajada liiasusega. Kui jah, siis kuidas seda tehakse?

Juhtudel, kus pilvteenuste juurutamiseks kasutatakse liidest (application programming interface, API), tuleb täiendavalt arvestada ka mooduli B 5.24 Veebiteenused .

Võrguühenduse kohandamine

Küsimused seni kasutatud võrguühenduse sobivuse tuvastamiseks:

- Kas võrguühenduse senine ribalaius on pilvteenuste kasutamiseks piisav või tuleb seda pilvteenuste vajadustega kohandada?
- Kas planeeritavad pilvteenused seavad erilisi nõudeid võrguühenduse latentsusajale?
- Kas pilvteenuste ühendused tuleb rajada liiasusega? Kuidas sellisel juhul ühenduste liiasus tagatakse?
- Kas erinevat tüüpi võrgusidele on tarvis kehtestada erinevaid prioriteete (quality of service, QoS), nt selleks, et videote ja kõnede andmeside kvaliteet oleks hea?
- Milliseid meetmeid on võetud võrguühenduse tõrkekindluse tagamiseks? Kas sellega seoses on tarvis võtta täiendavaid meeteid?

Haldusmudeli kohandamine

Küsimused haldusmudeli kohandamisvajaduste väljaselgitamiseks:

- Kas pilvteenuste haldamise protsess on hoolikalt planeeritud?
- Kas asutusel on olemas töörollide ja õiguste kontseptsioon, mis näeb ette, et pilvteenuste administraatorite (customer cloud service administrators, sageli ka lihtsalt service administrators) ja kasutajate kasutajakontod on lahutatud?

Andmehalduse mudeli kohandamine

Olenevalt valitud teenuseosutamise mudelist ei pruugi asutuse andmete haldamine kuuluda enam eranditult asutuse kompetentsi. Seetõttu tuleb planeerida, mil moel muutuvad pilvteenuste juurutamisega senised varukoopiate tegemise strateegiad ja andmete säilitamise strateegiad.

Kontrollküsimused:

- Kas asutuse erinevad kohandamisvajadused, mis on seotud pilvteenuste juurutamisega, on dokumenteeritud?
- Kas uute liidesesüsteemide juurutamise vajadust on analüüsitud?
- Kas pilvteenuste kasutamiseks on olemas haldusmudel (töörollide ja õiguste kontseptsioon)?
- Kas asutus on analüüsinud varukoopiate tegemise strateegia ja andmete säilitamise strateegia kohandamise vajadust?

M 2.539 Pilvteenuste kasutamise turbekontseptsiooni koostamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator, infoturbespetsialist, IT-juht

Asutus, kes otsustab kasutusele võtta pilvteenused, peab selle jaoks koostama turbekontseptsiooni. Turbekontseptsiooni koostamisel tuleks võimalikult täpselt järgida IT etalonturbe metoodikat.

Turbekontseptsioonis tuleb arvestada kõigi pilvteenuste kasutamise protsessi osapooltega, kes on enamasti järgmised:

- Pilvteenuse klient (kasutaja, cloud consumer) on pilvteenuse osutajaga ärisuhtes ning kasutab selle teenuseid;
- Pilvteenuse osutaja (cloud provider) vastutab kliendile pakutavate teenuste eest. Selles moodulis pilvteenuse osutajale seatud nõuded kehtivad ka käsitletava teenuse allhanketarnijate kohta;
- Pilvtöötluse maakler (cloud broker) haldab pilvteenuste kasutamist, jõudlust ja tarnet ning lepib kokku suhted pilvteenuse osutaja ja kliendi vahel. Selles moodulis pilvteenuse maaklerile seatud nõuded kehtivad ka käsitletava teenuse allhanketarnijate kohta;
- Pilvtöötluse operaator (kandja, cloud carrier) vahendab ühendust ning teenuste transporti pilvteenuse osutaja ja kliendi vahel. Selles moodulis pilvteenuse operaatorile seatud nõuded kehtivad ka käsitletava teenuse allhanketarnijate kohta.

Kõik loetletud osapooled peavad koostama enda turbekontseptsiooni.

Teenust tarbiv asutus peab tagama endale õiguse pilvteenuse osutaja turbekontseptsiooni kontrollimiseks kas audititega või kolmandate sõltumatute osapoolte kontrollidega.

Pilvteenuse puhul tuleb tagada, et pilvtöötluse, sealhulgas teenuse transpordi osapoolte asukohad, omanikud, jurisdiktsioon ning allhanketarnijad on kasutajale teada, on lepingute tasemel sätestatud ning kaasnevad riskid on analüüsitud ja aktsepteeritud.

Turbekontseptsiooni koostamise eesmärk on muu hulgas pilvteenuste kasutamiseks vajalike turbemeetmete dokumenteerimine. Dokumenteerimisel tuleb lähtuda pilvteenuste kasutamiseks koostatud turvapoliitikast (vt M 2.535 Pilvteenuse kasutamise turvapoliitika koostamine), mida tuleb kohandada konkreetse kasutusvaldkonna või konkreetse pilvteenuse eripäradega.

Andmete konfidentsiaalsuse ja tervikluse tagamise kohustus (turvaosaklass S1, T1) ning vajadus tagada andmete terviklus enam kui viie aasta jooksul seab pilve kasutamisele kitsendused. Sellisel juhul võivad välisel teenuseosutajal olla mitmesugused võimalused andmete manipuleerimiseks, lisaks võib tervikluse tagamiseks vajalike krüptoalgoritmide usaldusväärsuse ajahorisonti hinnata viiele aastale. Riskide maandamiseks tuleb kaaluda andmekogu kannete, tulemüüri konfiguratsioonimuudatuste, süsteemi tegevuslogide, serverilogi jm kriitilise info krüptoaheldamist juba turvaosaklassi T1 puhul (ISKE meetmed HT.10, HT.13, HT.14, HT.16 jt).

Pilvteenuste kasutamise turbekontseptsiooni koostamisel tuleks lähtuda IT-teenustele kehtivatest n-ö klassikalistest turbenõuetest ja -meetmetest ning erilist rõhku tuleb pöörata pilvteenuse spetsiifiliste ohtude maandamisele.

Peamised pilvteenuse spetsiifilised ohud on järgmised:

- teenuselepingu enneaegne või sunnitud lõpetamine;
- välise teenuseosutaja poolne tervikluse häirimine;
- välise teenuseosutaja poolne konfidentsiaalsuse häirimine;
- volitamata juurdepääs andmetele, nt pilvteenuse osutaja administraatorid või kolmandad pooled;
- turvameetmete ebapiisav järelevalve;
- andmete puuduv porditavus (eriti tarkvara teenusena tootelahendused) ja süsteemide puuduv porditavus (eriti platvorm teenusena tootelahendused) olukorras, kus valitud pilvteenus ei vasta enam levinud standarditele;
- sõltuvus pilvteenuse osutajast, st teenuseosutaja vahetamisvõimaluse puudumine (vendor lock-in);
- spetsiifiliste tootjapõhiste andmevormingute kasutamine (võib seada ohtu andmete tervikluse säilimise ja raskendada teenuseosutaja vahetamist);
- pilvtaristu paralleelne kasutamine mitme asutuse poolt (simultaanteenindus);
- puudulikud teadmised andmete salvestuskohast;
- teabe suur mobiilsus;
- ebapiisav rollide ja pääsuõiguste kontseptsioon;
- puudulik nõuete haldus pilvtöötluse kasutamisel;
- pilvtöötluse teenuseosutaja puudulik auditeerimine.

Pilvteenuste spetsiifiliste ohtude põhjal tuleb iga konkreetse pilvteenuse kasutamisele kehtestada selged turbemeetmed. Turbemeetmete kohustuslik järgimine tuleb kindlasti sisse kirjutada ka pilvteenuse osutajaga sõlmitavasse lepingusse.

Siin tuleks ennekõike arvestada järgmiste punktidega:

- pilvteenuse turvalise haldamise nõuded (nt rakendada kriitiliste haldustegevuste, nagu andmehulkade või süsteemide kopeerimise puhul kahemehereeglit);
- tööprotsesside ja turbehalduse nõuded (nt milliseid liideseid kasutatakse muudatuste, turvaintsidentide ja riskide haldamiseks);
- teenuseosutamise ja aruandluse nõuded;
- andmete kasutuse ja administraatorite tegevuste logimine ja logide krüptoaheldamine;
- andmete krüpteerimine;
- õiguste andmine ja tagasivõtmine;
- varukoopiate tegemine nii pilvteenuste osutaja kui ka asutuse enda töötajate poolt.

Kontrollküsimused:

- Kas pilvteenuste kasutamise jaoks on tuvastatud turbenõuete põhjal koostatud turbekontseptsioon?
- Kas asutus on võrguteenuste osutajaga kokku leppinud, et võrguteenuste osutaja peab koostama turbekontseptsiooni?

- Kas asutus kontrollib turbekontseptsiooni olemasolu ja rakendamist pilvteenuste osutaja ja teiste osapoolte juures ise või laseb seda teha sõltumatul kolmandal osapoolel?

M 2.540 Pilvteenuste osutaja hoolikas valimine

Algatamise eest vastutavad: infoturbespetsialist, asutuse/ettevõtte juhtkond, IT-juht

Rakendamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, infoturbespetsialist, IT-juht

Pärast planeerimistöid ja kontseptsiooni koostamist tuleb asutusel valida enda sõnastatud pilvteenuste kasutamiseks sobiv teenuseosutaja. Selleks koostab asutus nõuetekataloogi, mis sisaldab teavet järgmistest meetmetest: M 2.535 Pilvteenuse kasutamise turvapoliitika koostamine , M 2.536 Tarbitavate pilvteenuste määratlemine teenuste tarbija poolt ja M 2.539 Pilvteenuste kasutamise turbekontseptsiooni koostamine . Koostatud nõuetekataloogi põhjal saab asutus korraldada hankeid ja võrrelda pilvteenuste osutajate võimalikke standardseid lepingupakkumusi.

Nõuded pilvteenuse osutajale ja teenusele

- Teenuse osutaja peab asuma EL-is, tegutsema EMP-s või samaväärse andmekaitsetasemega riigis (nimekiri riikidest: http://ec.europa.eu/justice/dataprotection/international-transfers/adequacy/index_en.htm)
- Teenus peab vastama standarditele PCI DSS, ISO 27001 ja soovitatavalt kas ISO 27017, NIST SP 800-53r4 või NIST 800-171 standardile.

Lisateabe hankimine ja analüüsimine

Pilvteenusele seatud tingimuste täitmise kõrval tuleb pilvteenuste osutaja valimisel arvestada ka lisateguritega. Hindamismeetodina on praktikas palju abi erinevatest punktiskaaladest (nt tasakaalus tulemuskaart).

Alljärgnevalt antakse ülevaade erinevatest aspektidest, millega tuleks arvestada sobiva pilvteenuste osutaja valimisel.

- Pilvteenuse osutaja ja pilvtöötluse maakleri usaldusväärsus, sh vajaduse korral omandus kõrgel usaldusväärsuse tasemel.
- Pilvtöötluse operaatori ehk andmeedastusteenuse pakkuja paindlikkus ja usaldusväärsus, sh vajaduse korral transport kõrgel usaldusväärsuse tasemel.
- Teenuseosutaja põhitegevusala ja kogemus pilvteenuste osutamise vallas.
- Teenuseosutaja kohta avaldatud hinnangud ja turuanalüüsid.
- Due diligence riskianalüüs (nt turbeaspektid, kasutatav tehnoloogia, liidesed, protsessid jmt).
- Pilvteenuste osutaja tegevuskohad ja jurisdiktsioon. Olenevalt teenuseosutaja tegevuskohast võivad sellele kehtida erinevad riiklikud avalikustamis- ja teabekohustused. Välistatud ei ole ka salvestatud andmete kontrollikohustus, millest teenuseosutaja ei saa keelduda või ka kolmandate osapoolte õigus nõuda andmetega tutvumist kohtu loa alusel. Vajaduse korral asukoht kõrgel usaldusväärsuse tasemel.
- Teenuseosutamisse kaasatud alltöövõtjad.
- Lepingutingimuste analüüsimine.

Kulude ja tulude analüüsimine

Sageli selgub, et pilvteenuste defineerimise käigus muutuvad pilvteenuste kasutamist reguleerivad nõuded. Tulude ja kulude analüüs aitab asutusel välja selgitada, milline on tingimuste muutmisega kaasnev täiendav kasu või turvalisus ja kui palju see maksma läheb.

Kulude analüüsimisel tuleks eristada investeerimiskulusid (Capex – capital expenditure) ja tegevuskulusid (Opex – operational expenditure). Pilvteenuste kasutuselevõtt toob endaga alguses kaasa täiendavaid kulusid, sest üleminek pilvteenustele ei hakka kohe asendama varasemaid teenused ega vabasta nende jaoks vajalikku taristut.

Kontrollküsimused:

- Kas soovitud pilvteenuse määratluse baasil on koostatud pilvteenuse nõuetekataloog?
- Kas pilvteenuse osutaja valimisel arvestati ka täiendava teabega (nt turuanalüüsid, lepingutingimused või tegevuskoht)?
- Kas teenuseosutaja teenuste kohta avaldatud kirjeldusi (SLA-d, lepingu tüüptingimused) analüüsiti hoolikalt?

M 2.541 Pilvteenuseosutajaga sõlmitava lepingu koostamine

Algatamise eest vastutavad: infoturbespetsialist, ametiasutuse/ettevõtte juhtkond, IT-juht

Rakendamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, infoturbespetsialist, IT-juht

Kui sobiv pilvteenuste osutaja on välja valitud, tuleb kõik kavandatava pilve kasutamise tingimused fikseerida ja sätestada teenusetasemeleppes. Lepinguliste sätete liik, ulatus ja täpsusaste peab vastama pilvteenuste kasutamisega seotud andmete ja rakenduste kaitsevajadusele.

Teenusetasemeleppe koostamisel peab arvestama järgmiste nõuetega:

Pilvteenuseosutaja teenuse osutamise koht

Teenuse osutaja peab asuma EL-is, tegutsema EMP-s või samaväärse andmekaitsetasemega riigis (nimekiri riikidest: http://ec.europa.eu/justice/dataprotection/international-transfers/adequacy/index_en.htm). Fikseerida tuleb, millised on pilvteenuseosutajalt tellitud pilvteenuste osutamise asukohad (nt riiklikult, EL-i piires jne). Vajaduse korral tuleb täpselt kindlaks määrata ka konkreetsed arvutuskeskused. Konfidentsiaalsete andmete puhul peab olema tagatud asukoht kõrgel usaldusväärsuse tasemel.

Teenuse omanik ja teenuse osutamisel osalevad allhankefirmad või muud kolmandad isikud

Konfidentsiaalsete andmete puhul peab olema tagatud omandus kõrgel usaldusväärsuse tasemel, nõue rakendub ka allhankijate ja kolmandate isikute puhul. Kui teenuse osutamisel osalevad allhankefirmad või kui pilvteenus põhineb muudel pilvteenustel, tuleb see lepingus fikseerida osaleva kolmanda isiku nimetamisega. Muudatustest tuleb teavitada pilvteenuse kasutajat ja kriitiliste teenuste korral tuleb anda ka erakorraline tühistamisõigus.

Andmete transport pilvteenuse osutaja ja kliendi vahel

Pilvteenuseosutajad annavad avalikud liidesed pilvteenuste kasutajate käsutusse. Sageli toimub see veebiliideste kaudu. Nende liideste kaudu toimub pilvteenuste kasutajate keskne juurdepääs pilvteenuseosutajate pakutavatele pilvteenustele. Siinjuures tuleb kasutada turvalisi liideseid ja logisid, mis võimaldavad pilvteenuseosutaja ja pilvteenuste kasutaja vahel krüpteeritud suhtlust. Suhtluse kaitsmiseks tuleb kasutada tunnustatud tehnika eeskirjadele vastavaid piisava krüpteeringu ja autentimisega turvalisi logisid.

Pilvteenuseosutaja taristu eeskirjad

Eeskirjades tuleb muu hulgas järgida olemasoleva taristu turvalisuse tagamise nõudeid ja tõrkekindluse tagamiseks rakendatavaid meetmeid pilvteenuseosutaja juures. Ka nõuded simultaanteeninduse taristu rakendamisele pilvteenuseosutaja poolt peavad olema lepinguliselt sätestatud ja sertifikaatidega tõendatud.

Pilvteenuseosutaja töötajatega seotud eeskirjad

Kui teenust kasutav asutus esitab erinõudeid pilvteenuseosutaja töötajate oskuste tasemele, pädevusele, erilubade olemasolule ja sertifikaatidele, tuleb see

lepinguliselt fikseerida. Muu hulgas tuleb arvestada järgmiste aspektidega:

- eeskirjad pilvteenuste pakkuja tegevuse jaoks IT-administraatorite või muude kliendiandmetele juurdepääsuõigustega töötajate töölevõtmisel. Lepingupartnerite korral, kes asuvad erinevates riikides, tuleb kindlaks määrata, et olenemata töötaja töökohast, on talle seatud samad kriteeriumid.
- nõuded töötajate infoturbealaseks koolitamiseks pilvteenusepakkuja poolt;
- vajaduse korral võib töötajatelt nõuda turvakontrolli tõendit;
- nõuded töötajate korrapäraseks hindamiseks.

Eeskirjad sidekanalite ja kontaktisikute kohta

Asutuse ja pilvteenuseosutaja vahel tuleb määratleda selged vastutusalad, eskaleerimistasemed ja sidekanalid. Kindlaks tuleb määrata suhtluskeel. Eriti tuleb tähelepanu pöörata sellele, et kontaktisikuid puudutavad eeskirjad hõlmaksid hädaolukorda, turvaintsidentide haldust ja vigade kõrvaldamist. Tellija nõudmiste kohaselt tuleb esitada täpsed telefoninumbrid, kontaktisikud ja kättesaadavuse ajad.

Protsesside, töökorralduse ja vastutusalade eeskirjad

Lepinguliselt tuleb sätestada:

- nõuded korrapäraste turbeseiretegevuste läbiviimiseks;
- nõuded turvaintsidentide käsitlemiseks;
- nõuded korrapäraste kooskõlastuste läbiviimiseks;
- nõuded pilvteenuseosutaja muudatuste haldusele;
- nõuded pilvteenuseosutaja kaugpöörduse juhistele;
- rakendatavad meetmed kaitseks kahjurvaraprogrammide eest;
- varundus-ja taastusprotsessi üksikasjalik dokumentatsioon;
- teenust tarbivale asutusele oma andmevarunduse õiguse andmine (kui see on pakutava teenuse puhul võimalik);
- krüpteeritud transpordikanalite olemasolu;
- pilvteenuste kasutaja osaluskohustused.

Erilist tähelepanu tuleb pöörata pilvteenuse kasutaja ligipääsule andmete kasutuse logidele. Erinevad pilvetehnoloogia mudelid (IaaS, PaaS, SaaS) sisaldavad erinevaid teenuseid ning seetõttu ei ole ühest lahendust, kuidas tagatakse kliendile ligipääs andmete kasutust puudutavatele logidele. IaaS mudeli korral on pilvteenuse kliendil kõige enam tehnilisi võimalusi loomaks andmete kasutuse logimiseks lahendused, mis on võimelised rakenduma alates operatsioonisüsteemi kihist. PaaS mudeli korral tuleb andmete kasutuse logimine lahendada tarkvara arendamise käigus. Ilma sellise arenduseta võib öelda, et andmete logimise lahendust ei ole võimalik saavutada. SaaS-i korral tarnitakse pilvteenuse kliendile valmislahendus ning andmete kasutuse logimise funktsionaalsus sõltub teenusepakkuja rakenduse funktsionaalsusest.

Lisaks andmete kasutust puudutavatele logidele on hea praktika töötada välja ühtne logide haldamise süsteem tervele platvormile, mis aitaks probleemide korral nii klienti kui ka arendajat ning vähendaks probleemide otsimiseks kuluvat aega. Logid võivad sisaldada delikaatseid andmeid, mistõttu tuleb nende töötlemisel arvestada ISKE turvaklassiga ning muude õigusaktides sätestatud nõuetega.

Lepingulise suhte lõpetamise eeskirjad

Muu hulgas tuleb käsitleda ka andmete tagastamist. Täiendav teave rakendatavate meetmete kohta juhul, kui lepinguline suhe lõpetatakse, on toodud meetmes M 2.307 Väljasttellimissuhte nõuetekohane lõpetamine .

Andmete kustutamise tagamine pilvteenuseosutaja poolt

Kokku tuleb leppida, mida mõistetakse andmete kustutamise all ja mida hõlmab andmete täielik kustutamine. Kõikide andmete all tuleb silmas pidada toodangusüsteeme, testkeskkondi, muid keskkondade kloone, kõiki varukoopiaid ning andmebaasisüsteeme ja -teenuseid. Vahet tuleb teha märgendite eemaldamise ja andmete (mitmekordse) ülekirjutamise vahel. Samuti tuleb selgelt eristada standardites (nt DoD 5220.22-M ja NIST 800-88) käsitletavaid termineid tavakustutamine (clear), millega muudetakse andmed tavakasutuses kättesaamatuks (andmed jäävad füüsiliselt siiski kettale alles, kuid viited andmete asukohale failisüsteemis eemaldatakse), ning täiskustutamisel (purge), millega muudetakse andmed loetamatuks ka erivahendeid kasutades.

Teenusepakkujad tagavad sageli neist esimese variandi – tavakustutamise –, mis tähendab, et viited asukohale failisüsteemis kustutatakse, kuid andmed on kettal siiski alles seni, kuni järgmine klient need üle kirjutab. Lisaks tuleb kokku leppida selles, millist turbeastet eeldatakse pilvteenuseosutajalt andmete kustutamisel ja kas tuleb teha vahet andmete kustutamisel korrapärase kasutamise korral ning lepingu lõppemisel. Konfidentsiaalsete andmete puhul tuleb rakendada täiskustutamist (purge), et andmete taastamine professionaalsete taastustööriistade abil ei oleks võimalik. Kui andmete turbevajadus nõuab andmete täielikku kustutamist ja näiteks andmekandjate hävitamist standardi DIN 66399 kohaselt, tuleb kohe alguses teha selgeks, kas pilvteenuste osutaja seda nõuet ka täidab (vt M 2.540 Pilvteenuste osutaja hoolikas valimine). Turvalise kustutamise probleeme on vaadeldud mooduli B 3.303 Salvestisüsteemid ja salvestivõrgud meetmes M 2.527 Turvaline kustutamine SAN-keskkonnas . Siit võivad eesmärgiks seatud turbeastme puhul abi leida nii kasutaja kui ka pilvteenuste osutaja.

Juurdepääsuõiguste eeskirjad

Kui asutuse eelnevatest tähelepanekutest tuleneb selline nõue, on siin mõeldav juurdepääsuvolituste piiramine ainult sertifitseeritud töötajatele. Lisaks tuleb kinni pidada pilvteenuse osutaja arvutuskeskustes rakendatavatest turvameetmetest.

Hädaolukordadeks valmisoleku eeskirjad

Lepingus peab olema kirjas, et pilvteenuste osutajal on olemas hädaolukorra kavad ja need on pilvteenuse kasutajale kontrollimiseks kättesaadavad. Olenevalt kasutaja kättesaadavuse nõuetest tuleb kindlaks määrata hädaolukorra astmed, kokku leppida tagatud reaktsiooniajad hädaolukorras ning nõuda hädaolukordade õppuste läbiviimist pilvteenuste osutaja poolt.

Seadusandlusega seotud raamtingimuste eeskirjad

Vaadelda tuleb järgmisi teemasid:

- pilvteenuste osutaja kohustus pidada kinni kehtivatest õigusaktidest olenevalt tema asukohast ja asjakohasest tegevusvaldkonnast;
- kolmandate isikute kaasamise eeskirjad. Pilvteenuste osutaja peab olema kohustatud tagama teenuste läbipaistvuse. Avalikustada tuleb teenused, mis puudutavad teenuste osutamise tarneketti (service delivery supply chain), ohustavad turvalisust ja mida pakutakse allhankefirmade kaudu. Tuleb tagada, et pilvteenuste pakkujaga sõlmitavas teenusetasemeleppes kajastuvad turbenõuded kehtiksid samas mahus ka allhankijatele ja kolmandatele isikutele. Pilvteenuste osutaja peab suutma kontrollitavalt tagada oma allhankefirmade tegelikku turbenõuete täitmist ja teenusetaset. Lepinguliselt tuleb reguleerida kolmandate isikute kohustused, vastutus ja kontrolli teostamine;
- nõuded pilvteenuste kasutamise lõpetamiseks, nt tühistamise eeskirjad;
- konfidentsiaalsuslepingud;
- lepingutrahvide kokkulepped;
- poolte vastutuse kindlaks määramine;
- kohtupädevus ja kohaldatav õigus ka kehtivate andmekaitsenõuete puhul.

Muudatuste halduse ja katsetusprotseduuride kindlaks määramine

Muudatuste halduse ja katsetusprotseduuride rakendamise puhul tuleb kindlaks määrata, millisel määral on olemas paindlikud kohaldamisvõimalused. See on eriti oluline juhul, kui esinevad vastuolud seadusest tulenevate muudatustega või kasvanud nõuete puhul.

Kontrollide läbiviimise eeskirjad

Teenust tarbiv asutus peaks lepinguliselt jätma endale õiguse viia läbi auditeid pilvteenuste osutaja juures. Samuti tuleb kirjalikult kinnitada auditi aktsepteerimine kolmanda isiku poolt ja penetratsioonitestide läbiviimine. Sellega seoses tuleb fikseerida, kes kannab kulud auditi läbiviimise eest. Lisaks tuleb kindlaks määrata, kuidas käsitleda pilvteenuste osutaja auditi logisid.

Käsitleda tuleks järgmisi teemasid:

- nõuded logiandmete säilitamistähtaegadele;
- tõhus kontroll logide kaitsmise üle volitamata juurdepääsude eest;
- auditi logide tervikluse kontrollimise ja tagamise meetodid;
- auditi logide ülevaatuse läbiviimine;
- nõuded kellale, mida kasutatakse süsteemide sünkroniseerimiseks ja täpse ajatempli panemiseks auditi logidele.

Lisaks tuleks lepinguliselt reguleerida, milliseid mõõtmisi teostatakse teenusetasemelepete täitmiseks. Tagatud peab olema ka seotud muudatuste korrapärane aruandlus pilvteenuste osutaja poolt (nt funktsioonide ulatuse, allhankefirmade ja kõikide leppega seotud sündmuste kohta).

Erinõuete järgimine

Vajaduse korral võivad asutused esitada pilvteenusele erinõudeid. Neid tuleb järgida sarnaselt lepinguliste sätetega.

Võimalikud on näiteks järgmised nõuded:

- ainult kindlate, eelnevalt määratletud arvutuskeskuste kasutamise tagamine;
- eeskirjad andmete importimiseks ja eksportimiseks, samuti vajalikele liidestele muudel teenustel ja süsteemidel;
- konkreetsete konfiguratsiooniparameetrite kindlaks määramine määratletud koostalitlusvõime nõuete puhul;
- õiguse andmine oma andmevarunduste läbiviimiseks ning vajalike liideste ja parameetrite koostamiseks.

Kontrollküsimused:

- Kas lepinguliste eeskirjade liik, ulatus ja täpsusaste on sobitatud pilvteenuste kasutamisega seotud andmete ja rakenduste kaitsevajadusega?
- Kas on sätestatud, millises asukohas osutab pilvteenuste osutaja oma teenuseid?
- Kas teenust tarbiva asutuse ja pilvteenuste osutaja vahel on määratletud selged vastutusalad, eskaleerimistasemed ja sidekanalid?
- Kas on olemas kokkulepped andmete turvaliseks kustutamiseks pilvteenuste osutaja poolt?
- Kas tühistamise eeskirjad on fikseeritud kirjalikult?

M 2.542 Teenuste turvaline üleviimine pilvteenusteks

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator, spetsialist, infoturbespetsialist, IT-juht

Kui pilvteenuste osutaja on välja valitud, tuleb üleviimise rakendamisel järgida erinevaid turvalisusega seotud aspekte. Turvalise üleviimise nõudeid tuleb rakendada ka siis, kui pilvteenus tuuakse tagasi oma asutusse või see edastatakse teisele teenuseosutajale.

Põhiaspekte turvalisemaks pilvteenusteks üleviimise planeerimiseks kirjeldatakse põhjalikult meetmes M 2.537 Teenuste pilvteenusteks üleviimise turbe planeerimine . Seejuures tuleb tähele panna, et pilvteenuse taristu valmistab ette pilvteenuste osutaja. Seetõttu ei käsitleta seda üleviimise rakendamise raames.

Üleviimise teostamine

Üleviimine toimub üleviimise kontseptsiooni alusel, mis on koostatud juba planeerimisetapis ning mis sisaldab üleviimise tehnilisi ja korralduslikke eeldusi. Seetõttu kirjeldatakse siin kindlaid nõudeid üleviimise protsessiks, nagu katsetus- või piltootetapi teostamine.

Üleviimise raames tuleb üleviimise kontseptsiooni ja pilvteenuste kasutamise turbekontseptsiooni nõudeid kohandada tegelikkusega. Kõrvalekallete puhul tuleb need registreerida ja dokumenteerida ja vajaduse korral rakendada täiendavaid meetmeid.

Erilist tähelepanu tuleb pöörata järgmiste, turvalisusega seotud aspektide kooskõlastamisele:

- Andmete üleviimiseks asutusest pilvteenuste osutajale on vajalikud privilegeeritud juurdepääsuõigused. Taotletava turbeastme tagamiseks tuleb kindlaks teha, kuidas toimub juurdepääsuõiguste üleandmine ja kas need võetakse pärast üleviimise lõpetamist ära.
- Kui üleviimist planeerib ja teostab kõrvaline kolmas isik ja kui üleviimise planeerimisele on esitatud erilised nõuded, tuleb kontrollida nendest kinnipidamist.
- Valesti teostatud või katkenud üleviimise puhul tuleb tagada, et pilvteenuste osutaja võtab vajalikud meetmed juba edastatud andmete kustutamiseks.

Enne esimeste andmete edastamist asutuselt pilvteenuste osutajale tuleb lisaks kontrollida kõiki hädaolukorraks valmisoleku meetmeid ning intsidentide lahendamise ja haldamise protsesse, kas need on täielikud ja ajakohased. Vajaduse korral tuleb neile kohandada ka varustrateegiaid, et hädaolukorras oleks võimalik andmeid pilvest tagasi tuua. Eeskirjad, kuidas asutused peavad käituma andmeedastuse katkemise korral, tuleb üle kontrollida seoses nende rakendatavuse ja nendest kinnipidamisega. Ka siis, kui üks osa andmeid on juba üle viidud ja on loodud kõik vajalikud eeldused pilvteenuste kasutamiseks, peab kasutaja andmekogu pidevalt varundama. Andmevarunduse korrakohast läbiviimist tuleb seetõttu üleviimise ajal regulaarselt kontrollida.

Üleviimise teostamine proovikäitamise raames

Selleks, et tagada võimalikult sujuv üleminek pilvteenuste kasutamisele ilma igapäevatööd kahjustamata, tuleb üleviimise rakendatavust kõigepealt kontrollida testandmetega proovikäitamise raames. Samuti kontrollitakse, kas üleviimise ja turbekontseptsiooni nõuded on põhimõtteliselt teostatavad. Proovikäitamise raames peaks mõõtma jõudlust ja tegema kindlaks, kas planeeritav üleviimiskanal on põhimõtteliselt rakendatav. Lisaks saadakse teadmisi, kas plaanitav ribalaius on piisav ja kas kindlaksmääratud andmehulkade samaaegne rakendamine on plaanikohaselt teostatav.

Üleviimise teostamine proovikasutuse etapis

Olenevalt pilvteenuse kasutamise ulatusest soovitatakse pärast edukalt lõppenud proovikäitust üle minna proovikasutuse etappi. See annab kasutajapoolsetele teenuse administraatoritele võimaluse tutvuda uue teenusega ja saab kontrollida, kas pilvteenuste osutaja peab kinni kõikidest oma lubadustest ja lepingulistest kohustustest.

Üleminek töörežiimile

Kui proovikäitus ja üleminek proovikasutuse etapile on edukalt läbitud, järgneb pilvteenuste üleviimine töörežiimi. Sellega seoses tuleb tähelepanu pöörata kasutaja, pilvteenuste osutaja ja vajaduse korral väliste üleviimise teenuse osutajate vahel sõlmitud üleandmisprotsesside eeskirjadele.

Kontrollküsimused:

- Kas turbekontseptsiooni nõuetele vastavust ja kohandatust on üleviimise rakendamise ja sellega seotud eeskirjade raames kontrollitud?
- Kas üleviimise rakendamise käigus kontrolliti kõigi hädaolukorraks valmisoleku meetmete täielikkust ja ajakohasust?
- Kas enne proovikäitust kontrolliti pilvteenuse toimimist?
- Kas toimus tootmise ühtlustamine asutuse pilvteenuse jaoks määratletud nõuetega?

M 2.543 Pilvteenuste infoturbe tagamine igapäevatöös

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator, infoturbespetsialist, IT-juht

Pärast teenuse üleviimist pilvteenustele tuleb tagada infoturbe säilitamine igapäevatöös., milleks peab olema tagatud dokumentide ja juhiste korrapärane uuendamine. Tuleb tagada korrapäraste kontrollide läbiviimine, mis hõlmavad võimalikult paljusid pilvteenuste valdkondi. Järgida tuleb vähemalt järgmisi aspekte ja kaasata neid korrapärastes kontrollides.

Pilvteenuste korrakohase haldamise tagamine

Meetme M 3.11 Hooldus- ja halduspersonali väljaõpe kohaselt tuleb tagada asutuse pilvteenuste administraatorite erialane koolitus ning olukord, kus kõik pilvteenuste administraatorid tunnevad nõudeid ja on võimelised neid täitma. Korrapäraselt tuleb üle vaadata administraatoritele antud volitused ja kui turbekontseptsioon seda ette näeb, siis ka kahemehereegli järgimine.

Teenuste osutamise regulaarne kontrollimine

Lisaks teenusetasemeleppe täitmisele tuleb kontrollida ka teenuse osutamiseks vältimatuid parameetreid, nagu näiteks võrguühenduse ja -ühenduste jõudlus.

Pilvteenuste osutaja ja kasutaja vahelised regulaarsed teenuseülevaated

Tuleb teostada korrapäraseid teenuseülevaatuseid pilvteenuste osutaja ja asutuse vahel. Teenuseülevaatus peab sisaldama kokkulepitud ja tegelikult saavutatud teenusetaset ning erandolukordade, nagu näiteks laiaulatuslik rünne või globaalne võrgurike, käsitlemist.

Pilvteenuste koostalitlusvõime tagamine

Paljude pilvteenuste kasutamisel tuleb nende koostalitlusvõime tagamiseks testida nende koostalitlusvõimet.

Turvalisusega seotud tõendite esitamine pilvteenuste osutaja poolt

Asutus peab pilvteenuste osutajalt nõudma korrapäraselt teenuse osutamisega seotud dokumentatsiooni, näiteks muudatuste ja intsidentide haldust puudutavad ajakohased andmed. Samuti peab pilvteenuste osutaja olema võimeline esitama tõendeid oma protsesside ja teenuste sisemiste kontrollisüsteemide sertifitseerimise kohta, kui see on lepinguliselt kokku lepitud.

Andmevarunduse korrakohane läbiviimine

- Ettenähtud ja kokkulepitud protsesside järgimise tagamine.
- Lubamatute teenuste takistamiseks mõeldud tehniliste meetmete kontrollimine, näiteks prokside kasutamisega.
- Auditite, turvakontrollide, penetratsioonitestide või turvaaukude analüüside läbiviimine.

Kõik teenuse osutamist puudutavad muudatused peavad olema tellijaga kooskõlastatud. Sinna alla käivad muu hulgas muudatuste planeerimine ja pilvteenuste osutaja töötajate olukorda puudutavad muudatused.

Turbe säilitamiseks ja täiendamisvajaduste väljaselgitamiseks tuleb korraliselt planeerida ja viia läbi harjutusi ja teste. Eelkõige tuleb kontrollida reageerimist

süsteemikatkestustele (testkatkestus ja täielik katkestus), keskendudes asutuse ja pilvteenuste osutaja vahelisele suhtlusele. Lisaks tuleb teostada ja dokumenteerida andmevarunduste põhjal teenuse taastamist ja selle planeerimist. Tuleb testida pilvteenuste kasutamisel esineda võivate turvaintsidentide lahendamist ja haldamist.

Kontrollküsimused:

- Kas dokumente ja juhiseid (nt käsiraamatuid ja kasutusjuhendeid) uuendatakse korrapäraselt?
- Kas teenuste osutamist kontrollitakse regulaarselt?
- Kas pilvteenuste osutaja esitas turvalisusega seotud tõendeid?
- Kas pilvteenuste osutaja ja teenust tarbiva asutuse vahel viiakse läbi korrapäraseid kooskõlastusringe?
- Kas planeeritakse ja viiakse läbi harjutusi ja teste, et kontrollida intsidentidele reageerimist ning intsidentide lahendamist?

M 2.544 Pilvteenuste kasutamise auditeerimine

Algatamise eest vastutavad: IT-juht, infoturbespetsialist

Rakendamise eest vastutab: infoturbespetsialist

Auditite läbiviimist vaadeldakse pilvteenuste kasutamisel kui vajalikku meedet. Praktilised kogemused on näidanud, et teenust tarbival asutusel on üksnes teenuse auditeerimisega võimalik tuvastada lepingusätetest kõrvalekaldumist, nt seda, et teenuse tase ei vasta kokkulepitud tingimustele või et teenuseosutaja ei järgi kokkulepitud turbenõudeid.

Kuna pilvteenuse kasutamise keskkonnas on auditeerimine nii oluline, tuleks auditeid käsitleda pilvteenuse kasutamise erinevates etappides:

- teenuseosutaja valimisel, pidades silmas auditi-õiguse üldist võimaldamist;
- lepingu koostamisel pilvteenuseosutajaga, pidades silmas auditi-õiguse teostamist;
- korrapäraste auditite läbiviimise meetmete kindlaksmääramisel pilvteenuste kasutamisel.

Teenust tarbiv asutus peaks pilvteenuste osutajaga kokkulepitud turvameetmete rakendamist regulaarselt kontrollima. Selleks otstarbeks pakutakse auditi läbiviimiseks ka spetsiaalselt väljatöötatud küsimustikke.

Pilvteenuste osutaja auditite läbiviimine

Andmete omanik peab kehtiva regulatsiooni kohaselt tellima korralisi ISKE auditeid. Osas, mida pilvteenuse olemusest tulenevalt ei ole võimalik ISKE järgi auditeerida, aktsepteeritakse teenuse osutaja tellitud ja kolmandate sõltumatute osapoolte läbiviidud vastavusauditeid. Eelistada tuleks sertifitseerimist Saksa Infoturbeagentuuri (Bundesamt für Sicherheit in der Informationstechnik) väljaantud ISO 27001 IT Grundschutzi baasil, mis vastab ISKE aluseks olevale IT Grundschutzi metoodikale.

Täiendavalt on võimalik aktsepteerida ka järgmiste standardite vastavusauditeid:

- PCI DSS, ISO 27001, ISO 27017, NIST SP 800-53r4 või NIST 800-171.

Pilvteenuste osutaja auditeerimise formaat võib sõltuda pilvteenuse liigist.

- Asutuse pilv – enda hallatavat ja oma teenuste kasutamiseks loodud pilvelahendust auditeeritakse tavapärase ISKE auditi käigus.
- Eesti riigipilv– riigipilves pakutava kogukonnapilve teenuse puhul on tegemist jagatud vastutusega, kus andmekogu turvalisuse tagamisel on tegevad kaks või kolm osalist: andmete omanik (vastutav töötleja, volitatud töötleja) ja pilvteenuse pakkuja. Riigipilve teenuse pakkuja allub eesti jurisdiktsioonile, rakendab ISKE-st tulenevaid nõudeid ja peab teostama korralisi ISKE auditeid.
- Eestis paiknev avalik kommertspilv, mille serverid asuvad füüsiliselt Eesti territooriumil, mis vastab kindlustavate süsteemide, sh ISKE nõuetele. Teenusepakkuja allub eesti jurisdiktsioonile, rakendab ISKE-st tulenevaid nõudeid ja peab teostama korralisi ISKE auditeid.

- Avalik pilv ELi piires – andmete konfidentsiaalsuse tagamine on oluliselt raskendatud. Osapoolte paljususe tõttu on otsene auditeerimine oluliselt raskendatud või võimatu. Turbemeetmete rakendatuse taseme hindamiseks tuleks aktsepteerida ja hinnata teenuse osutaja tellitud ja kolmanda osapoole läbiviidud sertifitseerimisi ja auditeid. Eelistada tuleb sertifitseerimist Saksa Infoturbeagentuuri (Bundesamt für Sicherheit in der Informationstechnik) väljaantud ISO 27001 IT Grundschutzi baasil, mis vastab ISKE aluseks olevale IT Grundschutzi metoodikale.
- Avalik pilv kolmandates riikides – andmete konfidentsiaalsus ei ole tagatav. Osapoolte paljususe tõttu on otsene auditeerimine sisuliselt võimatu. Turbemeetmete rakendatuse taseme hindamiseks tuleks aktsepteerida ja hinnata teenuse osutaja tellitud ja kolmanda osapoole läbiviidud sertifitseerimisi ja auditeid.

Pilvteenuste erinevaid teenusemudeleid auditeeritakse erinevas mahus.

Pilvteenuste kasutamisel tootelahendusena taristu teenusena (infrastructure as a service, IaaS) tuleb peamiselt auditeerida arvutuskeskust ja sinna juurde kuuluvat taristut, pilvteenuste kasutamisel tootelahendusena platvorm teenusena (platform as a service, PaaS) lisandub operatsioonisüsteemide ja vahevara (nt veebiserverid, andmebaasid, muud rakendused sinna juurdekuuluvate liidestega) auditeerimine. Tootelahenduse tarkvara teenusena (software as a service, SaaS) kasutamisel kaasatakse ka rakendustasand.

Kolmanda osapoole auditi puhul peab arvestama järgmist:

- auditile peab eelnema riskianalüüs;
- auditi puhul tuleb arvestada, milliseid pilvtöötluse aspekte katab kolmanda osapoole sertifitseerimine ja rakendada ülejäänud aspektidele otsest auditit;
- ISKE põhineb IT Grundschutzi raamistikul ning seetõttu tuleb eelistada sertifitseerimist Saksa Infoturbeagentuuri (Bundesamt für Sicherheit in der Informationstechnik) väljaantud ISO 27001 IT Grundschutzi baasil, mis vastab ISKE aluseks olevale IT Grundschutzi metoodikale;
- täiendavalt on võimalik aktsepteerida ka järgmiste standardite vastavusauditeid:
- PCI DSS, ISO 27001, ISO 27017, NIST SP 800-53r4 või NIST 800-171. Sellisel juhul tuleb luua vastavustabel kasutatava raamistiku ja IT Grundschutzi vahel, kusjuures sellest vastavustabelist peab järelduma, et kõik IT Grundschutzi põhise auditeerimise aspektid on kasutatava raamistiku puhul kaetud;
- eelmisest sertifitseerimisest ei tohi olla möödunud rohkem aega kui kehtestab ISKE-põhine andmekogude auditeerimise kohustus.

Audiitor peab lisaks sellele alati arvesse võtma ka teabe kaitsevajadust ja sõltuvust muudest valdkondadest, nagu taristu, süsteemid, rakendused või teenused, mis moodustavad koguteenuse.

Kontrollküsimused:

- Kas asutus peab auditi läbiviimise õiguse tagama lepinguliselt?

- Kas pilvteenuste osutajaga on lepinguliselt fikseeritud turvameetmete rakendamise kontrollimine korrapäraste auditite teostamise kaudu?
- Kas auditite kavandamisel ja läbiviimisel võetakse arvesse teenusemudelite IaaS, PaaS ja SaaS eripärasid?
- Kui soovitakse rakendada kolmanda osapoole auditit, kas siis on arvestatud ülaltoodud kitsendusi?

M 2.546 Uute rakenduste nõuete analüüs

Algatamise eest vastutab: vastutav spetsialist

Rakendamise eest vastutavad: vastutav spetsialist, infoturbespetsialist, asutuse juht

Enne kui planeeritakse ja projekteeritakse uut rakendust, peaksid olema selgeks tehtud kasutamise raamtingimused, näiteks

- milliseid tööprotsesse peab see mil moel toetama,
- millise kaitsevajadusega millist teavet peab sellega töötlema,
- kes peab ja kes võib millistele rakenduse osadele juurde pääseda,
- millistest õiguslikest raamtingimustest tuleb kinni pidada (vt M 2.547 Rakendustele kehtivate õigusnormide väljaselgitamine ja dokumenteerimine),
- kuidas näeb välja infokooslus, millesse see paigaldatakse, näiteks, kuidas näevad välja võrgustruktuurid ja
- milliseid IT-komponente vajatakse rakenduse kasutamiseks, nt riistvara platvorm, operatsioonisüsteemid, andmebaasid.

Juba algsel planeerimisel soovitatakse arutleda ohtude ja riskide üle, mis võivad esineda rakenduse kasutamisel. Siinjuures tuleks läbi viia ka esimene analüüs, et tuvastada varakult võimalikke ründeid ja muid rakenduse usaldusväärsust, terviklust ja kättesaadavust puudutavaid riske. Turvalisusega seotud riskide dokumenteeritud tulemused leiavad seejärel koha üksikasjalikus riskianalüüsis, mis viiakse läbi nõuetekogumiku koostamise käigus (vt M 2.548 Nõuetekogumiku koostamine). Ka projekti hilisemas etapis peaksid nii vastutav spetsialist kui ka arendaja arvestama pidevalt võimalike ohtudega, et oleksid järgitud kõik turvalisusega seotud nõuded. Selle põhjal saab tuletada sobivad turvameetmed ja testimisnõuded, mis lisatakse turvastruktuuri.

Kui raamtingimused rakenduse kasutamise ajal oluliselt muutuvad, näiteks installeeritakse uued serveri platvormid, tuleb turvameetmeid uuesti hinnata.

Seetõttu tuleb turvahalduse raames luua protsesse, et arendada, installeerida, kasutada, kontrollida ja hooldada turvaliselt rakendusi ning koolitada administraatoreid ja kasutajaid neid turvaliselt käsitlema.

Nende protsesside raames tuleb kindlaks määrata vastava rakenduse rollid, vastutusalad ja ülesanded kontseptsiooni, ülesehitamise ja kasutamise jaoks. Selle põhjal saab asjakohaselt kindlaks määrata volitused rakenduse erinevates kasutusaja etappides. Lisaks sellele tuleb rollikontseptsiooni raames kindlaks teha, millised pädevused on vajalikud rolli omandamiseks. Nii saab kindlaks teha ka võimaliku koolitusvajaduse ja teavitada eesmärgipäraselt vastavaid rolliomanikke nende turvalisusega seotud vastutuse osas.

Kontrollküsimused

- Kas raamtingimused käsitletud rakenduste kasutamiseks on selgeks tehtud?

M 2.547 Rakendustele kehtivate õigusnormide väljaselgitamine ja dokumenteerimine

Algatamise eest vastutavad: asutuse juht, infoturbespetsialist
Rakendamise eest vastutab: vastutav spetsialist

Selleks, et kindlaks teha, kas töö- või haldusprotsessid, mis peavad rakendusi toetama, töötavad kooskõlas seadusandlusega, on vaja planeerimise (ja hiljem ka auditeerimise ja kontrollimise) eesmärgil täielikku ülevaadet asjakohastest õigusaktidest (vt B 1.16 Nõuete haldus). Kui asutuses on olemas õigusosakond, võib see aidata nimetatud kogumiku koostamisel. Õigusnormid tuleb koondada ühte ülevaatesse, mida saab kasutada dokumendina nõuetekogumiku, andmekaitsekontseptsiooni ja turbekontseptsiooni jaoks.

Vastavatele asutustele kehtivatest õigusnormidest võivad tuleneda konkreetsed nõuded teabeturbele, näiteks

- kaitsevajaduseks (valdkonnapõhised ametisaladused nagu maksu- ja sotsiaalsaladus jne);
- nõuded turvameetmete sisulisele suunale ja teostusele. Eriti isikuandmete töötlemisel tuleb järgida seadustest tulenevaid nõudeid nagu vastavus sihtotstarbele (mõjutab näiteks nõudeid väliste liideste ja aruannete struktuurile ja turvalisuse tagamisele) või andmehulga minimeerimisele ning andmete kokkuhoiule (mõjutab näiteks nõuet kustutustähtaegade määramisele);
- konkreetseid turvameetmeid puudutavad nõuded, nagu näiteks peegelandmebaaside, kvalifitseeritud elektroonilise allkirja kasutamine, töödeldavate andmete puhul pseudonüümide kasutamine või nende anonüümseks jätmine või protokollimise kujundamine;
- nõuded salvestamise või arhiveerimise tähtaegadele.

Kontrollküsimused

- Kas andmete rakendustega töötlemiseks on olemas ülevaade õigusnormidest?

M 2.548 Nõuetekogumiku koostamine

Algatamise eest vastutab: vastutav spetsialist

Rakendamise eest vastutavad: vastutav spetsialist, infoturbespetsialist, IT-juht

Nõuetekogumik kirjeldab nõudeid, mida rakendus peab vaadeldava töö- või halldusprotsessi raames täitma. Seejuures ei käsitleta üksnes rakenduse erialaseid (funktsionaalseid) nõudeid, vaid ka mittefunktsionaalseid.

Erialaste ja infotehnoloogiliste nõuete kõrval käsitletakse ka turbenõudeid. Ka nende puhul tuleb vahet teha funktsionaalsete ja mittefunktsionaalsete turbenõuete vahel. Funktsionaalsed turbenõuded katavad rakenduse konkreetseid funktsioone nagu näiteks:

- identiteedi ja volituste haldus,
- paroolide haldus,
- andmete krüptograafiline kaitse.

Turbenõuete liik ja vorm nagu näiteks kahefaktorilise autentimise integreerimine, PKI ülesehitus, SAML-i või WS-Security kasutamine sõltuvad suurel määral rakenduse vastavast kaitsevajadusest.

Kirjeldades mittefunktsionaalseid turbefunktsioone, räägitakse sellest, millised kvaliteediomadused peavad rakendusel olema. Siia kuuluvad aspektid nagu tarkvara kvaliteet, usaldusväärsus, veataluvus, hooldamine ja loomulikult konfidentsiaalsuse, tervikluse ja kättesaadavuse tagamine. Mittefunktsionaalse nõude näide on muuta rakendus vastupidavaks teatud rünnete suhtes.

Nõuetekogumiku puhul on tegemist üldkontseptsiooniga tellija seisukohast lähtudes, mis jätab rakendamise viisi paljudes osades veel lahtiseks. Nõuetekogumik on oluline alus arendusprojekti käivitamiseks, samuti nagu see on nõuete kataloogiga standardtarkvara korral (vt M 2.80 Tüüptarkvara nõuete kataloogi koostamine).

Nõuetekogumiku koostamisel tuleb arvestada järgmiste aspektidega:

- töö- või halldusprotsessis töödeldava teabe (andmete) kaitsevajadus;
- õigusnormid, millele tuleb kasutamisel tähelepanu pöörata ja seega ka juba rakenduse kontseptsiooni juures (vt M 2.547 Rakendustele kehtivate õigusnormide väljaselgitamine ja dokumenteerimine);

- nõuded, standardid ja kriteeriumid, mida tuleb arvesse võtta. Olenevalt rakendusalast võivad siia kuuluda ka turvalisusega seotud kriteeriumisüsteemid,
- tehnilised juhised või arhitektuurisoovitused ning ka juurdepääsetavusega seotud nõuded.

Selliste nõuete ja kriteeriumide näited on järgmised:

- Common Criteria for Information Technology Security Evaluation (ISO 15408), eriti 2. osa „Security functional requirements”,
- eGovernment'i standardid ja arhitektuurid (SAGA),
- kontrollikodade miinimumnõuded kasutamiseks info- ja kommunikatsioonitehnoloogias.

Nõuetekogumiku ettevalmistamisel, eriti vajalike turbefunktsioonide tuletamisel ja loomise, on asjakohane viia vajaduse korral (st eriti kõrge ja väga kõrge kaitsevajaduse korral) läbi juba esimene riskianalüüs, näiteks BSI-standardis 100-3 kirjeldatud meetodi põhjal. Seda riskianalüüsi esimest versiooni tuleb seejärel täiendada kohustuslike tööde loetelu koostamise käigus (vt M 2.552 Kohustuslike tööde loetelu koostamine), rakenduse lõpuleviimisel ja ühiskasutusse andmise ettevalmistamisel. Selles riskianalüüsi esimeses ringis võib muidugi ka ainult uurida, millistele ohtudele peab rakendus vastu pidama ja kehtestada esimesed turbenõuded. Konkreetsed turvameetmed saab kindlaks määrata alles kohustuslike tööde loetelus.

Nõuetekogumik peab nii üksikasjalikult, kui see on selles etapis võimalik, sisaldama lisaks funktsionaalsetele (erialastele) nõuetele seisukohti ka järgmiste mittefunktsionaalsete aspektide kohta:

- kvaliteedinõuded (nt kasutajasõbralikkus, usaldusväärsus, jõudlus);
- nõuded, mis puudutavad arhitektuuri ja IT-taristut, mille jaoks rakendus on loodud (vt M 2.214 IT-kasutuse kontseptsioon). Igal asutusel peab olema selgelt esitatud nõue, kuidas IT-d asutuses kasutatakse ja kuidas see muude valdkondadega kokku sobib. See võib olla kindlaks määratud nt IT-raamistikus ja arhitektuurikontseptsioonis. Uute IT-komponentide ja rakenduste planeerimisel tuleb kindlaks teha, et need sobivad taristusse ja üldistesse projektidesse;
- tehnilised lisanõuded (nt rakenduse arhitektuur, programmikeel, operatsioonisüsteem, laiendamisvõimalus);
- nõuded dokumentidele (nt UML-i modelleerimine);
- nõuded planeeritud juurutamiseks. Siin tuleb vahet teha, kas tegemist on üleviimisega, mille korral võetakse andmed ja töötlusprotsessid üle olemasolevast rakendusest, või täielikult uue arendusega. Oluline võib olla ka see, kas uue rakenduse juurutamine on planeeritud tähtaja muudatusega või etapiviisiliselt. Väärtuslikud juhised protsessi planeerimiseks rakenduste üleviimisel on esitatud föderaalvalitsuse infotehnoloogia voliniku üleviimise juhendite etapimudelis;
- üleandmise nõuded (üleandmise põhimõtted ja pilootkäitus);

- nõuded vajalikele turbefunktsioonidele.

Need turbefunktsioonid võivad muu hulgas hõlmata järgmisi nõudeid:

- nõuded protseduuri kättesaadavusele (talutavad seisakuajad, taastusajad jne);
- teenusetarbijate eraldamise nõuded (vt M 2.549 Simultaanteeninduse kontseptsiooni koostamine);
- andmevarunduse (vt M 6.33 Andmevarunduskontseptsiooni loomine) ja vajaduse korral arhiveerimise nõuded;
- nõuded välistele liidestele ja nende turvalisuse tagamisele;
- nõuded andmetalletuse ja andmete edastamise krüpteerimisele (vt M 2.161 Krüptokontseptsiooni väljatöötamine);
- nõuded autentimisele ja autoriseerimisele;
- nõuded andmetalletusele ja andmete struktureerimisele;
- nõuded andmete edukale ja tõhusale kustutamisele.

Nõuetekogumik peaks rakendusele esitatavaid nõudeid kirjeldama niivõrd piisavalt, et selle alusel ülesehitatav rakendus koostatakse nii, et on võimalik rakendada nõutavaid turvameetmeid ja saavutatakse kaitsevajadusele vastav üldine turvalisus.

Kontrollküsimused

- Kas nõuetekogumiku koostamisel võeti piisavalt arvesse erialaseid nõudeid, mis puudutavad arhitektuuri ja IT-taristut, rakenduste juurutamise nõudeid ja vajalikke turbefunktsioone?

M 2.549 Simultaanteeninduse kontseptsiooni koostamine

Algatamise eest vastutavad: infoturbespetsialist

Rakendamise eest vastutavad: vastutav spetsialist, infoturbespetsialist, IT-juht

Sageli kasutavad paljud asutused ühe teenuseosutaja keskseid IT-taristuid või teenuseid koos. Seejuures võidakse kasutada koos ka rakendusi, mille puhul andmetalletus ja andmetöötlus peab toimuma nt seadustest tulenevate nõuete või ärisaladuste alusel eraldi. Sellistel juhtudel räägitakse sageli simultaanteeninduse rakendustest, kus igale teenust tarbivale asutusele eraldatakse omaette kliendikeskkond, lühidalt klient.

Sellekohane näide on avaliku halduse registrirakendused nagu näiteks e-rahvastikuregister, milles paljud kohalikud omavalitsused kui iseseisvad andmeid töötlevad asutused säilitavad ja haldavad oma rahvastikuregistri andmeid.

Kõigil nendel juhtudel tuleb sobiva simultaanteeninduse kontseptsiooniga tagada, et rakendusi kasutatakse simultaanteeninduse kohaselt. Siia juurde kuulub veel, et iga andmeid töötlev asutus võib oma valdkonna, st oma kliendisüsteemi piires muuta oma erialaseid nõudeid (nt mis puudutavad protokollimise ulatust ja säilitamise aega) või järgida oma kontrollikohustusi. Simultaanteeninduse kontseptsioon tuleb koostada simultaanteeninduse rakenduse kasutajate kaudu ja anda teenust tarbivate asutuste käsutusse. Need peavad enne sellise süsteemi või teenuse koos teiste kasutajatega kasutama asumist veenduma, et simultaanteeninduse kontseptsioon tagab nende kaitsevajadusele sobiva turvalisuse. Simultaanteeninduse kontseptsioon on seega turbekontseptsiooni osa, mis on vajalik väljasttellimise protseduuri jaoks (vt B 1.11 Väljasttellimine (Outsourcing) , eriti M 2.254 Väljast tellitud projektile infoturbekontseptsiooni loomine).

Ka andmekaitse aspektide alusel tuleb arvesse võtta nõudeid teenusetarbijate eraldamiseks. Juhised selle jaoks leiate föderatsiooni ja liidumaade andmekaitseametnike tehnoloogia töörühma „Simultaanteeninduse juhendist”.

Kui muretsetakse või koostatakse uus rakendus või kui seda muudetakse oluliselt, tuleb kõigepealt põhimõtteliselt selgeks teha, kas see rakendus on võimeline kliente puhtalt eraldama (vt M 2.552 Kohustuslike tööde loetelu koostamine).

Simultaanteeninduse kontseptsioon peaks arvesse võtma vähemalt järgmisi punkte:

- nõuetekohased õigusnormid: seadustest tulenevad nõuded ei tohi olla vastuolus ühiste, simultaanteeninduse rakendusmeetoditega. Lisaks tuleb ta-

gada, et klientide eraldamise tehniline teostus vastab iga kliendi andmete kaitsevajadusele;
- tehingute lõpetatus: andmetöötluse etapid, mida üks klient läbi viib, ei tohi kaasa tuua seda, et andmeid muudetakse teiste klientide juures või et nad pääsevad ligi neid andmeid lugema;
- klientide omavaheline konfigureerimist puudutav sõltumatus: olemas peab olema vähemalt kaks administratiivset tasandit. Esimene tasand on mõeldud teenustarbija haldamiseks: siia paigaldatakse simultaanteeninduse süsteemid ja kustutakse need, viiakse läbi simultaanteenindust hõlmavaid konfigureerimisega seotud seadistusi, antakse rollid simultaanteeninduse administraatoritele, toimub simultaanteenindust hõlmav protokollimine ja viiakse läbi selle audit. Teine tasand on mõeldud simultaanteeninduse süsteemi haldamiseks: siin antakse volitused simultaanteeninduse süsteemi jaoks, viiakse läbi simultaanteeninduse siseseid konfigureerimisi, konfigureeritakse simultaanteeninduse sisest protokollimist ja viiakse läbi protokolli audit;
- volituste kontekstide eraldamine: igal kliendil on oma suletud volituste kontekst. Ühe simultaanteeninduse süsteemi volitused ei tohi mõjutada teist simultaanteeninduse süsteemi. Volituste andmine või muutmine vastava kliendi administraatorite kaudu ei tohi mõjutada teiste klientide volitusi;
- teenuseosutajal peab olema administratiivne tasand klientide haldamiseks, millel ei ole aga volitusi kliendisiseste andmete töötlemiseks;
- protokollimise kontekstide eraldamine: simultaanteeninduse süsteemi protokolli audiitoritel ei tohi olla juurdepääsu teiste simultaanteeninduste süsteemide protokolliandmetele. Näiteks võivad klientidel olla oma logiandmed. Teine võimalus võiks olla, et asutus pääseb oma kliendi protokolliandmetele ligi teenuseosutaja poolt vastavalt paigaldatud filtrite või aruande generaatorite kaudu;
- simultaanteenindust hõlmava andmetöötluse piirang: simultaanteeninduse haldamise tasand ei tohiks põhimõtteliselt lubada andmete töötlemist simultaanteeninduse sees väljaspool kliendi haldust. Andmevahetus kliendiga peaks toimuma määratletud ja nõuetekohaselt turvatud liideste kaudu (vt liideste kontseptsiooni).

Nende nõuete rakendamine võib toimuda mitmel moel. Silmapaistvat rolli mängib seejuures asjakohane rollide ja volituste kontseptsioon rakenduste sees. Sellest tulenevalt võib rakendada taristu ja teenuste tasemele nt virtualiseerimistehnikaid nagu

- erinevate andmebaaside kasutamine (nimetatakse ka instantsideks) ühises andmebaaside haldussüsteemis (DBMS);
- VPD (Virtual Private Database) andmebaaside teenuste tasemel;
- teenusetarbija atribuudiga varustatud andmehulkade salvestamine ühises andmebaasis ja ühistes tabelites, nii et teenusetarbijate eraldamine toimub rakenduse kaudu;
- virtuaalsed masinad süsteemitasandil;
- VLAN (Virtual LAN), VRF (Virtual Routing and Forwarding), VPN (Virtual Private Network) võrgutaristus (vt ka M 5.62 Sobiv loogiline segmenteerimine).

Tellija peaks kontrollima, kas teenuseosutaja poolt valitud klientide eraldamise lahendus on tõhus.

Kontrollküsimused

- Kas kontseptuaalselt on võetud arvesse, et erinevate teenust tarbivate asutuste rakendus- ja andmekontekstid on eraldatud puhtalt?
- Kas teenuseosutaja on klientide eraldamiseks rakendanud piisavalt vajalikke mehhanisme?
- Kas on olemas asjakohane väljasttellimise protseduuri turbekontseptsioon?

M 2.550 Rakenduse arendamistööde nõuetekohane juhtimine

Algatamise eest vastutab: asutuse juht
Rakendamise eest vastutavad: üksikute rakenduste eest vastutavad töötajad

Kui teatud kasutuse eesmärgil ei ole võimalik soetada standardtarkvara, on vajalik individuaalse tarkvara arendamine. See võib toimuda asutuses endas või väliste teenuseosutajate abil.

Lisaks majanduslikele aspektidele on rakenduse arendamistööde nõuetekohane juhtimine oluline ka turvaaspektide seiskohalt, sest see aitab vältida vigu rakenduses ja turvaauke. Mida varem vead ja turvariskid avastatakse, seda lihtsam on neid kõrvaldada.

Arendamise juhtimiseks ja projektihalduseks tuleks kindlaks määrata nõuetekohane juhtimis- ja projektihaldusmudel, mis võtab arvesse asutuse eripärasid ja seal kasutatavaid tarkvaraarendusprojektide meetodeid. See peaks arvesse võtma järgmisi aspekte:

- arendamiseks ettenähtud töötajatel peaks olema vajalik pädevus;
- tarkvara loomiseks ja juhtimiseks ning rakenduste hooldamiseks tuleb juurutada protsess, mis katab kasutusaja kõiki etappe (Application Lifecycle Management, ALM). Seejuures tuleks arvesse võtta tarkvaraarenduse nõuetekohaseid etappe, et vastavalt ära jaotada ning käsitleda vajalikke tegevusi (tööprotsessi modelleerimine, nõuete analüüs, tarkvaralahendus, rakendamine, testimine, tarnimine jne). Protsessi edukaks juurutamiseks on end eriti oluliseks osutunud vajalike rollide ja funktsioonide kandjate hoolikas kirjeldus ja piiritlemine;
- rakendusprojekti korrapäraseks läbiviimiseks tuleb luua vajalikud eeldused. Need hõlmavad projektijuhi tellimist, kirjeldatud protsessi rollide jaotust ja protsessimudeli valikut arenduse jaoks, mis sobib antud asutusele ning tarkvaraprojekti tüübile ja suurusele. See võib näiteks ette näha etappide järjestikuse läbimise (koskmudel) või järkjärgulise läbimise (spiraalmudel);
- hinnata ja käsitleda tuleb tarkvaraarenduse riske. Siinjuures tuleb arvestada spetsiifiliste turvariskidega, mis turbefunktsioonide rakendamisega tavaliselt vähenevad, ning riske arendusprotsessis endas, nagu ebapiisav dokumentatsioon, mitteküllaldased kvaliteedi tagamise meetmed, ajakava ületamine jms. Rakenduse turvalisust võivad vahetult mõjutada ka riskid arendusprotsessis, eriti kui ajahädas olles rakendatakse turbefunktsioone ebapiisavalt või ei rakendata neid üldse;
- piisavalt tuleb arvesse võtta arendusprotsessi kvaliteediaspekte, mis on olulised ka üldise turvalisuse jaoks. Nii ei võimalda näiteks hästi dokumenteeritud ja struktureeritud kood mitte üksnes hõlpsamalt hooldada, vaid ka turvalisusega seotud probleeme on võimalik tuvastada kiiremini.

Tarkvara arendamisel on end õigustanud rida protsessimudeleid ja parimaid tavasid. Need võib üldistades jagada kahte kategooriasse:

- rasked protsessimudelid: neil on formaalne iseloom, järgivad pigem eelnevalt kindlaks määratud plaani ja pööravad suurt tähelepanu lepingutele ja dokumentatsioonile. Need sobivad eelkõige suurtele projektimeeskondadele või väga formaalse suhte korral tellija ja teenuseosutaja vahel ning eelistavad projekti alguseks laiaulatuslikku nõuete selgitamist. Tuntud esindajad on V-mudel XT ja Rational Unified Process (RUP);
- kerged, liikuvad protsessimudelid: need pööravad suuremat tähelepanu projektiosaliste omavahelisele suhtlemisele ja vähem tähelepanu formaalsele teostusele ning sobivad väiksematele projektidele või tellija intensiivse osalusega projektidele. Need pakuvad võimalust täpsustada ebaselgeid nõudeid projekti teostamise jooksul või reageerida paindlikult nõuete muudatustele. Liikuvate protsessimudelite näited on Scrum, Kanban, Crystal Clear.

Protsessimudeleid on võimalik kombineerida. Kasutada võib näiteks töömeetodeid Scrum'i eXtreme Programming'ist (Pair Programming). V-mudeli XT-projekti sees võib luua väikseid arendustsükleid kui Scrum-Sprint'e.

Tarkvaraarenduse jaoks sobivaid alavaldkondi ja protsesse kirjeldatakse järgmistes väljaannetes:

- IEEE Software Body of Knowledge (SWEBOK) ja
- ISO/IEC 12207 „Systems and software engineering – Software life cycle processes".

Ka tarkvara arendusprotsessi kvaliteedi tagamiseks on olemas erinevad protsessimudelid ja -meetodid. Siia kuuluvad muu hulgas CMMI (Capability Maturity Model Integration) ja SPICE (Software Process Improvement and Capability Determination) ning ISO/IEC 15504 „Information technology - Process assessment".

Selles valdkonnas on asjakohane ka standardisari ISO 250xx. Standard ISO/EC 25000 „Software-Engineering – tarkvaratoodete kvaliteedikriteeriumid ja hindamine (SQuaRE) – SquaRE juhised" annab ülevaate selle sarja põhimõistetest ja põhimõtetest.

Tuleb kindlaks määrata, milliseid kvaliteedi tagamise meetodeid ja millist konkreetset lahendust asutuses või vastava projekti jaoks kasutatakse. Majanduslikel põhjustel ei ole tavaliselt igat liiki kontrollimised kõikvõimalikes sügavustes võimalikud. Seetõttu tuleb otsustada, milliseid neist on milliseks ajahetkeks ja millise rakenduse osa jaoks mõistlik rakendada. Seejuures tuleb tagada, et turbenõuded on piisavalt kaetud.

Kontrollküsimused

- Kas arendusprotsessi jaoks määrati kindlaks nõuetekohane juhtimismudel?
- Kas arendusprotsessi jaoks kasutati kvaliteedi tagamise meetodit, mille korral järgiti piisavalt ka turvalisusega seotud aspekte?

M 2.551z Nõuetekohase ja seadustele vastava hankemenetluse korraldamine

Algatamise eest vastutab: asutuse juht
Rakendamise eest vastutab: vastutav spetsialist

Hankemenetlusele, mis viiakse läbi standard- või individuaalse tarkvara soetamiseks, võib olla esitatud rida nõudeid, mida tuleb järgida.

Iga asutus peab enne vahendite soetamist selgitama, millised seadustest tulenevad ja muud raamtingimused on seejuures aluseks. Vahendite soetamise ja hankelepingute jaoks peavad asutuses olema määratletud protsessid ja kindlaks määratud kontaktisikud (vt M 2.547 Rakendustele kehtivate õigusnormide väljaselgitamine ja dokumenteerimine).

Igal juhul on mõistlik varakult selgeks teha, milline tähtsus on hankeotsuse tegemisel sertifikaatidel. Siia kuuluvad sertifikaadid, mis hindavad toodete turvalisust nagu Common Criteria ehk sellised, mis hindavad haldussüsteeme nagu sertifikaat „ISO 27001 IT-etalonkaitse baasil", ja ka isikusertifikaadid (vt M 2.66 Sertifikaatidega arvestamine IT soetamisel).

Kontrollküsimused

- Kas hankemenetluse planeerimine ja läbiviimine vastab kehtivatele nõuetele?

M 2.552 Kohustuslike tööde loetelu koostamine

Algatamise eest vastutavad: asutuse juht, vastutav spetsialist
Rakendamise eest vastutab: vastutav spetsialist

Kohustuslike tööde loeteluga kirjeldatakse, kuidas tuleks nõuetekogumikku tehniliselt rakendada. Tavaliselt esitab tellija, nt vastutav erialaosakond nõuetekogumiku. Selle põhjal töötab (sisemine või väline) arendusosakond, kes peab rakenduse looma, välja kohustuslike tööde loetelu, milles formuleeritakse nõuetekogumiku nõuete tehniline rakendamine. Tellija peab kontrollima kohustuslike tööde loetelu selles osas, kas kajastatud on kõik nõuetekogumiku nõuded, et on võimalik saavutada taotletavad arenduseesmärgid. Mõistlik on sellega siduda turbehaldus, et tagada ka formuleeritud turbe-eesmärkide saavutamine.

Seejuures tuleb järgida vähemalt järgmisi aspekte.

Valdkonnaga seotud nõuete kirjeldus

Üksikasjalikult tuleb kirjeldada, kuidas tuleb rakendada valdkonnaga seotud nõudeid (nt töövood, dialoogid, töötlemismaskid, andmestruktuurid).

Sidumine infokooslusega

Kohustuslike tööde loetelus peab olema välja töötatud, kuidas sobitada rakendust infokooslusesse ja millised kohandused tuleb läbi viia. Siinjuures tuleb näiteks selgitada, milliseid ja kui palju käitamiskeskkondi (arendus, testimine, kvaliteedi tagamine, tootmine jne) vajatakse ja kuidas tuleks neid taristuliselt rakendada (nt virtuaalsete masinate (VM) või terminaliserveri teenuste kasutamisega).

Rakenduse juurutamise planeerimine

Uue rakenduse juurutamist tuleb planeerida. Siinjuures tuleb kohustuslike tööde loetelus järgida muu hulgas järgmisi punkte.

- Enne rakenduse tavatöö režiimi ülevõtmist tuleb seda testida ja see kasutusse lubada. Kohustuslike tööde loetelus tuleb nimetada testide ja väljastamise plaanitud protsessid ja kriteeriumid. Otstarbekaks on osutunud, et kohustuslike tööde loetelus kirjeldatakse eduka väljastamise kriitilisi testimisolukordi (vt test ja väljastamine, M 2.83 Tüüptarkvara testimine ja M 2.62 Tarkvara vastuvõtuprotseduurid).
- Üleviimine. Kui uue rakenduse kasutusele võtmisega lõpetatakse olemasoleva rakenduse kasutamine, tuleb tööprotsessid ja IT-keskkond sellega kohandada, ning andmekogud uude rakendusse üle viia. Üleviimise etapp on kogemuste põhjal turbe seisukohast alati eriti kriitiline ning seda tuleb hoolikalt ette valmistada ja läbi viia. Enne üleviimise etapi lõppemist tuleb ka sinna juurde kuuluvad andmed uude rakendusse ja seal kasutatavasse andmevormingusse üle kanda. Täiendavad suunised leiduvad ka meetmes M 2.319 Serveri üleviimine . Väärtuslikud juhised protsessi planeerimiseks rakenduste üleviimisel annab föderaalvalitsuse infotehnoloogia voliniku juhis üleviimise kohta.

Rakenduse turbefunktsioonid

Kindlaks tuleb määrata, millised turbefunktsioonid peavad rakenduses sisalduma ja kuidas need tuleb teostada (vt ka M 4.42 Turvafunktsioonide rakendamine IT-rakenduses). Need võivad sisaldada järgmist:

- kättesaadavuse kontseptsioon ja liiasuse kontseptsioon (vt M 6.157 Rakenduste liiasuse kontseptsiooni koostamine)
- teenusetarbijate eraldamine:
  kohustuslike tööde loetelus tuleb formuleerida, kuidas rakendus tagab teenusetarbijate puhta eraldamise (vt M 2.549 Simultaanteeninduse kontseptsiooni koostamine)
  krüpteerimise, kontrollsummade ja muude krüptograafiliste meetodite rakendamise planeerimine ja dokumentatsioon. Krüptograafiat võib nõuetekohase kasutuse kontseptsiooni korral kasutada, et kaitsta andmeid edastamisel rakenduse sees, edastamisel väliste liideste kaudu või rakenduse sees volitamata juurdepääsu eest.
  Sobiliku krüptograafilise meetodi planeerimine ja kasutamine on keeruline ülesanne. Seetõttu soovitatakse nõuded ja ideed koondada krüptokontseptsiooni, vt M 2.161 Krüptokontseptsiooni väljatöötamine .
- Andmevarunduse kontseptsioon (vt M 6.33 Andmevarunduskontseptsiooni loomine)
- Arhiveerimiskontseptsioon (vt M 2.243 Arhiveerimiskontseptsiooni väljatöötamine):
  Arhiveerimisel tuleb tähelepanu pöörata sellele, et arhiveeritud saaksid kõik rakenduse komponendid, mida on vaja tööprotsessi võimalikuks uueks kasutusele võtmiseks, st näiteks tarkvara, konfigureerimisandmed ja sisulised andmed. Teatud juhtudel võib olla mõistlik arhiveerida ka riistvara komponendid, nt autentimise andmekandjad. Arhiveerimiskontseptsioon peaks sisaldama rollide kontseptsiooni (vt M 2.5 Vastutuse ja ülesannete jaotamine), autentimiskontseptsiooni (vt M 2.555 Rakenduste autentimiskontseptsiooni koostamine), tarkvara hoolduse kontseptsiooni (vt M 2.553 Rakenduste hoolduskontseptsiooni koostamine) ja väliste liideste kasutamise ja kaitsmise kontseptsiooni.

Lisaks tuleb formuleerida nõuded vormile, keelele, sügavusele ja vajaduse korral ka lähtekoodi dokumentatsiooni tarnimise tähtajad, samuti käsiraamatute ülesehitus, sisu ja formaat (paber, pdf-dokument, online-abi).

Siinjuures tuleb kirjeldada, millised uue rakenduse juurutamisel osalevad asutused (tellijad, teenuseosutajad jne) võtavad millised kirjeldatud ülesanded.

Lisaks sellele tuleb koostada protokollimise kontseptsioon, milles määratakse kindlaks, milliseid rakenduse sündmusi ja millisel moel protokollida tuleb ja kuidas tuleb käsitleda protokolliandmeid (vt M 2.500 IT-süsteemide logimine). Seejuures tuleb järgida vähemalt järgmisi aspekte.

- Kuidas ja milliseid sündmusi tuleb logida?
- Kuidas toimub mittevajalike logiandmete kustutamine?
- Kuidas tuleb kaitsta juurdepääsu logiandmetele?

- Kas on vajalik revisjonikindel logimine?
- Kas hindamise kaitseks tuleb kasutada standardseid aruandeid?
- Kas teatud logitud sündmuste korral peaksid rakenduses käivituma muud sündmused (Security Incident'i ja Event Monitoring'u kasutamine)?

Seoses sellega, et logimine puudutab alati ka isikuandmeid, tuleb siinjuures arvestada andmekaitse nõuetega (vt ka M 2.110 Andmeprivaatsuse suunised logimisprotseduurides).

Kontrollküsimused

- Kas kohustuslike tööde loetelu koostamisel võeti piisavalt arvesse valdkonnaga seotud nõudeid, mis puudutavad arhitektuuri ja IT-taristut, rakenduste juurutamise nõudeid ja vajalikke turbefunktsioone?

M 2.553 Rakenduste hoolduskontseptsiooni koostamine

Algatamise eest vastutab: IT-juht

Rakendamise eest vastutavad: administraator, infoturbespetsialist, IT-juht

Kui kasutatakse individuaalselt arendatud rakendust, vajatakse käitamiseks hoolduskontseptsiooni, et tagada rakenduse töövõime ja turvalisus jooksvas tööprotsessis (vt ka M 4.107 Tootja ressursside kasutamine). See peaks arvesse võtma järgmisi aspekte, mis tuleb siduda asutuse muudatuste haldusega (vt B 1.14 Turvapaikade ja muudatuste haldus):

- Rakenduses peab aegsasti kasutama uusi või muudetud erialaseid nõudeid.
- Jooksva kasutamise käigus ilmnevad funktsionaalsed vead (nt valed arvutused ootamatute olukordade korral) tuleb tähtaja piires kõrvaldada.
- Tagada tuleb ühilduvus rakendatud käitamiskeskkondade, nagu nt operatsioonisüsteemid ja vahevara komponendid nagu teegid, raamistikud (nt NET) ja Runtime Environment'id (nt Java Runtime Environment, JRE) paikade ja uuendustega. Ideaaljuhul saab nende komponentide paikasid paigaldada sõltumatult ja eraldi rakenduse tarkvarast. Kui nende komponentide paikamine on võimalik üksnes koos rakendusega, tuleb kindlaks teha, kas rakenduse tarkvara tootja annab aegsasti vastavad paigad kõikide seotud komponentide jaoks. Tähelepanu tuleb pöörata sellele, et kõikidel rakenduse piires kasutatavatel tarkvara komponentidel on vastava tootja paikamise tugi. Komponendid, mille kasutamine vastava tootja poolt katkestatakse, tuleb kiiresti välja vahetada.
- Kavandada tuleb turvaaukude kiire kõrvaldamine tarkvaras endas.
- Kindlaks tuleb määrata, kuidas kasutada protsesse vigade analüüsimiseks või optimeerimiseks. Selleks võib kasutada spetsiaalseid liideseid või lubada juurdepääsu kaitstud andmetele.

Testide nõuetekohaseks ettevalmistamiseks (vt M 2.83 Tüüptarkvara testimine) ja muudatuste tegemiseks rakendustes on osutunud otstarbekaks teha vahet turvapaikade ja funktsionaalsete muudatuste (muud paigad ja uuendused) vahel. Turvapaigad on mõeldud üksnes turvaaukude sulgemiseks ja ei ole tavaliselt seotud funktsionaalsete muudatustega rakenduses (vrdl ka M 3.66 Turvapaikade ja muudatuste halduse põhimõisted). Seetõttu võib turvapaikade teste ja väljastamist teha lihtsustatud meetoditega (nt astmelise Roll-Out'i raames esimeses etapis pilootkasutajale ja üldiselt väljastatud ühiskasutuste kaudu andmekaitse ja turvaaspektidega).

Hoolduskontseptsiooni koostamisel tuleks ka selgitada, milliste kanalite kaudu saab kasutada andmeid turvaaukude, uuenduste ja paikade kohta, nt tootjate meililistid, Computer Emergency Response Teams (CERT-id) (vt ka M 2.35 Teabe hankimine turvaaukude kohta) ja kuidas neid oma paikade ja muudatuste protsessis (vt moodulit B 1.14 Turvapaikade ja muudatuste haldus) töödeldakse.

Kontrollküsimused

- Kas rakenduse hooldus on nõuetekohaselt reguleeritud või lepinguliselt kokku lepitud?
- Kas funktsionaalsete muudatuste kõrval võeti nõuetekohaselt arvesse ka rakenduse turvapaikasid ja rakendatud vahevara komponente?

M 2.554z Rakenduste ostu-, arendamis- ja käitamislepingute koostamine

Algatamise eest vastutab: asutuse juht

Rakendamise eest vastutab: vastutav spetsialist

Rakenduse ostmisel, arendamisel või käitamisel võib asutus toetuda ühele või mitmele teenuseosutajale. Need võivad olla sisemised või välised teenuseosutajad. Tavaliselt võib eristada vähemalt kolme osapoolt: hilisemad kasutajad, arendajad ja rakenduse käitajad. Kui rakenduse arendab või seda käitab kolmas isik, tuleb koostada nõuetekohased lepingulised raamtingimused.

Nõuetekogumikus ja kohustuslike tööde loetelus, samuti osakontseptsioonides antud ja rakenduse turvatehniliste omaduste kasutamine tuleb osaleva asutuse ja teenuseosutajate vahel lepinguliselt kokku leppida.

Seejuures tuleb turvaaspektide puhul eriti järgida vähemalt järgmisi aspekte:

- nõuetekohaselt tuleb kirjeldada tarne või teenuse ulatust (funktsioonide ulatus, kaasa arvatud turbefunktsioonid, käitusvorming, litsentsi liik, dokumentatsioon, käsiraamatud jms);
- sõlmida tuleb tarkvarahoolduse kokkulepped (vt M 2.552 Kohustuslike tööde loetelu koostamine). Tellitavate arenduste korral tuleb kokku leppida nõuetekohased kasutusõigused genereeritava lähtekoodi ja sellele juurdepääsu osas (vt ka HK.37 Usaldusele toetuv deponeerimine (Escrow)).

Rakenduse käitamisel teenuseosutaja kaudu tuleb arvesse võtta mooduli B 1.11 Väljasttellimine (Outsourcing) .

Kontrollküsimused

- Kas lepingute koostamisel väliste teenuseosutajatega on rakenduste ostmise, arendamise ja käitamislepingute osas loetletud ja lepinguliselt arvesse võetud kõik olulised aspektid ja kas neid on hinnatud?

M 2.555 Rakenduste autentimiskontseptsiooni koostamine

Algatamise eest vastutavad: IT-juht, vastutav spetsialist, infoturbespetsialist

Rakendamise eest vastutavad: vastutav spetsialist, infoturbespetsialist, IT-juht

Uue rakenduse kasutamise kontseptsioonis tuleks selgitada, kuidas autentida kasutajaid enne juurdepääsu rakendusega töödeldavatele andmetele. Autentimiskontseptsioonis tuleb selgitada, kas rakendusel peavad üldse olema autentimismehhanismid (kontori suhtlustarkvara korral ei ole see nt tavaks, sest volitusi reguleeritakse töödeldavate dokumentide tasandil). Kui see on ette nähtud, tuleb selgitada, kas rakendusel on iseseisev kasutajahaldus või peab autentimine toimuma keskse kataloogiteenuse (vt moodulit B 5.15 Üldine kataloogiteenus) kaudu. Kui kasutatakse kataloogiteenust, tuleb selgitada, kas ette on nähtud ainulogimisega pöördus (single sign-on, SSO).

Põhimõtteliselt peaks eelistama ise loodud autentimise ühendamist kataloogiteenuse või SSO-teenusega. Kui see ei ole võimalik, tuleks igal juhul kindlustada, et autentimisandmed (identsustõendid, paroolid jne) sisestatakse varjatult ja neid ei salvestata kaitsmata kujul (st krüpteerimata) andmekandjatele, nagu kõvakettad, või ei edastata suhtlusvõrkude kaudu (vt M 2.11 Paroolide kasutamise reeglid).

Lisaks võib kontseptsioonis käsitleda järgmisi aspekte:

- nõuded logimisteatele: näiteks on logimisel mõistlik kuvada viimast logimisaega ja kasutusjuhiseid. Teisest küljest ei tohiks logimisteated sisaldada liiga palju teavet, eelkõige sellist, mis võiks ründe toimepanijale anda lähtepunkte, nt võrguaadressid või kasutatud tarkvara liik ja versioon;
- kasutaja rakenduse paralleelsete sessioonide käsitlemine (kui jah, kui mitu on lubatud);
- autentimisandmete kaitsmine: tuleb kindlaks määrata, kuidas kaitstakse krüptograafiliselt autentimisandmete salvestamist ja edastamist;
- aegjuhtimisega sundlahutamine kasutaja tegevusetuse korral ja nõuetekohane teave (juhiste aken) täielikul automaatsel lahutamisel ja väljalogimisel.

Lisaks sellele tuleks kirjeldada autentimismehhanismide ettenähtud liiki ja tugevust. **Siinjuures tuleb eriti järgida meetmes M 4.133z Sobivate autentimismehhanismide valimine nimetatud kriteeriume:**

- kasutatavate tehnoloogiate liik ja kombinatsioon või autentimise tegurid (teadmised, omand, biomeetrilised tunnused);
- rakendatavate tegurite tugevus (teadmiste tegurite kohta vt ka M 2.11 Paroolide kasutamise reeglid).

Kontrollküsimused:

- Kas autentimise funktsiooni ja turvalisuse nõudeid rakendati nõuetekohaselt?
- Kas autentimisandmete salvestamine ja edastamine on krüptograafiliselt piisavalt kaitstud?

M 2.556 Rakenduste katsetamine ja kasutusloa väljastamine

Algatamise eest vastutavad: infoturbeametnik, vastutav spetsialist
Rakendamise eest vastutab: vastutav spetsialist

Rakenduse käituse korrakohaseks üleminekuks ja oluliste muudatuste korral tuleb viia läbi vajalikud testid ja väljastada kasutusluba. Testide planeerimisel ja rakendamisel ning nendel põhineva kasutusloa väljastamisel tuleb tavaliselt arvesse võtta nelja tasandit, kuhu tuleb kaasata teised erialaste teadmistega ametiisikud:

- erialane tasand (esindavad vastutavad spetsialistid),
- IT-süsteemide tasand (esindab IT-juht),
- teabeturbe tasand (esindab infoturbeametnik),
- andmekaitse tasand (esindab andmekaitseametnik).

Vastavalt rakenduse liigile ja keerukusele võib vaja minna veel teisigi ametiisikuid, nt töötajate esindajaid.

Kõikide nimetatud tasemete jaoks tuleb luua testimis- ja kontrollimiskorrad ning kasutusloa väljastamise kriteeriumid. Siinjuures tuleb arvestada järgmist:

- erialasel tasandil tuleb rakendada meetmeid M 2.62 Tarkvara vastuvõtuprotseduurid ja M 2.83 Tüüptarkvara testimine (see meede on rakendatav ka individuaaltarkvara korral), mis kirjeldavad testide, vastuvõtmise ja kasutusloa väljastamise protseduure;
- IT-osakond peaks kindlaks tegema, kas rakendust on võimalik integreerida IT-taristusse ja IT-tööprotsessidesse;
- rakenduse kontseptsioon ja selle kasutamine peavad vastama reeglistikule (juhised, juhendid), kontseptsioonidele (nt krüptokontseptsioon) ja teabeturbe headele tavadele (nt OWASP). Eriti tuleb silmas pidada seda, et rakendatakse vajalikke turbefunktsioone ja et need töötavad laitmatult;
- vajaduse korral tuleb planeerida andmekaitseõigusega seotud kasutusloa väljastamine (vt M 2.509 Isikuandmete kaitse seadusele vastav kasutusse lubamine).

Testide ja kontrollimiste tulemused tuleb dokumenteerida ning neid tuleb hinnata. Kõrvalekalded ja vead võib nende kriitilisust arvestades jaotada kolme kategooriasse (nt madal, keskmine, kõrge). Selle hindamise alusel teeb vastutav kasutusloa väljastamise ametnik otsuse kasutusloa väljastamise kohta. Kasutusloa väljastamise eest vastutab tavaliselt ettevõtte juhtkond või viimase poolt määratud ametiisik. Kasutusloa väljastamine tuleb nõuetekohaselt dokumenteerida, eriti tuleb arvestada seadusest tulenevaid nõudeid, nt kirjalik vorm (vt ka M 2.85 Tüüptarkvara kinnitamine).

Kontrollküsimused

- Kas kasutusloa väljastamiseks läbi viidud testid on dokumenteeritud ja tulemused hinnatud?

M 2.557 Infoturbealase koolitusprogrammi kontseptsioon

Algatamise eest vastutavad: personalijuht, infoturbeametnik, ametiasutuse/ettevõtte juhtkond

Rakendamise eest vastutavad: infoturbeametnik, ülemused

Selleks, et viia asutuses sisse turbekontseptsioon, peavad töötajad seda aktsepteerima, järgima ning pidevalt kasutama. Olulised asjaolud edu tagamiseks on asutuse eripära arvestavad ja juhtkonna poolt nähtavalt toetatavad programmid infoturbealase teadlikkuse tõstmiseks ja koolituseks. Esmajoones tähendab infoturbealase teadlikkuse tõstmine seda, et kõiki töötajaid teavitatakse töökeskkonnas esinevatest ohtudest ja antakse juhiseid, kuidas nimetatud olukordades käituda, et ennetada kahjusid või neid parimal võimalikul viisil piirata (vt M 2.312 Infoturbealase koolitus- ja teavitusprogrammi kavandamine). Koolitustel vahendatakse töötajatele täiendavalt kõiki vajalikke teadmisi ja oskusi, et nimetatud käitumisviise õigesti ellu viia. Koolituse mõiste hõlmab kõiki planeeritud ja kontrollitud teadmiste edastamise vorme, nt kontaktkoolitused, veebikeskkonnas asuvad õppeprogrammid, juhendamine vastutavate töötajate poolt või vastavate reeglite ja kohustuste teatavaksvõtmine.

Teadlikkuse tõstmine ja koolitus täiendavad üksteist ning neid peaks arendama üksteisega sobitatult. Olemas peaks olema koolitusprogramm, kuhu kaasatakse kõik asutuse töötajad, mis on jaotatud sihtrühmadesse ja võtab arvesse ka töötajate karjääri (nt tööülesannete, osakondade või asukohavahetust). Juhtkond peab koolitusprogrammi ilmtingimata toetama, et oleks selge selle eriline tähtsus ning et oleksid olemas vajalikud ressursid planeerimiseks, rakendamiseks ja järjepidevuseks (vt M 3.96 Juhatuse tugi teavitusele ja koolitusele).

Alljärgnevalt kirjeldatakse olulisi samme, et luua ettekujutus infoturbealasest koolitusprogrammist.

1. Koolituseesmärkide määratlemine

Koolitusprogramm peab kinnistama infoturbe eesmärgid ja sellest tulenevad meetmed kõikidele asutuse töötajatele. Seetõttu peab koolituse eesmärgid tuletama infoturbe eesmärkidest.

Selliste koolitusmeetmete tavalised eesmärgid võivad olla järgmised:

- saavutada infoturbega seonduv tähelepanelikkus ja huvi,
- vahendada infoturbealaseid põhiteadmisi,
- edastada spetsiaalseid infoturbealaseid teadmisi, mida töötajad vajavad oma erialaste ülesannete täitmiseks,
- vahendada praktilisi teadmisi, et töötajad oleksid suutelised turbe seisukohast kriitilistele juhtumitele õigesti reageerima,
- saavutada järjepidev käitumismallide muutmine, et töötajad saaksid aru ja aktsepteeriksid, et infoturbealased juhendid ja meetmed on vajalikud ning et nad integreeriksid need oma igapäevatöösse.

Lisaks sellele tuleb määratleda koolitusprogrammi edukriteeriumid, et oleks võimalik hinnata selle mõju.

2. Sihtrühmade analüüs

Infoturbe poolest võrreldavate nõudmiste ja ülesannetega töötajad tuleb kindlaks määrata sihtrühma analüüsi põhjal, et arendada koolitusmeetmeid võimalikult vajaduspõhiselt ja kompaktselt. Täpsemaid soovitusi sihtrühma analüüsiks leiate meetmest M 3.93 Teavitus- ja koolitusprogrammide sihtrühmade analüüs .

3. Sihtrühmade koolitusvajaduse määratlus

Sihipäraste koolituste jaoks tuleb eelnevalt analüüsida iga sihtrühma koolitusvajadust. Kindlaks tuleb teha, kes millises olukorras milliseid teadmisi vajab. Selleks, et hinnata sihtrühmade tegelikku teadmiste taset, võib kasutada näiteks enesehinnangu küsimustikke.

Kindlasti tuleb arvesse võtta järgmisi valdkondi:

- põhiteadmised kõikidele töötajatele,
- juhtkonna infoturbega seonduv eeskuju,
- uute töötajate juhendamine,
- eriteadmised kindlate rühmade jaoks, nagu nt administraatorid ja kaugtöötajad,
- lisateadmised sihtrühmadevahelistel vahetamistel.

4. Koolituste sisu täpsustamine

Kõik töötajad peavad tundma sisemisi infoturbe reeglistikke, kontseptsioone ja protseduure, mis on nende tööga seotud, ning teadma, kus need asuvad.

Oluline on, et infoturbe dokumentatsioon oleks lihtne, ülevaatlik ja üldiselt arusaadav.

- Koolitusmeetmete sisulist loomist kirjeldatakse lisaks ka meetmes M 3.45 IT-turbealaste koolituste sisu kavandamine .
- Infoturbe alused on kindlaks määratud meetmetes M 3.5 Turvameetmete koolitus ja M 3.26 Personali juhendamine IT-vahendite turvalise kasutamise kohta .
- Spetsiifilisemate teemade kohta leiate teavet meetmetest M 3.45 IT-turbealaste koolituste sisu kavandamine ja M 3.49 Koolitus etalonturbe protseduuride alal .

Nimetatud meetmeid võib kasutada ka siis, kui koolitusi viivad läbi töötajad väljastpoolt oma asutust, sest vastavate kontrollnimekirjade abil saab luua ülevaate, kas eelnevalt kokku pandud seminarides käsitletakse kõiki vajalikke teemasid.

Oskuste vahendamise hulka kuuluvad ka praktilised ülesanded, kuidas järgida kindlaid turbenõudeid igapäevatöös. Eesmärk on, et need muutuksid üha enam iseenesestmõistetavaks, selle asemel, et seda võetaks pidevalt kui ebameeldivat lisakoormust.

Infoturbelased koolitusmeetmed tuleb ühildada asutuse muude koolitusmeetmetega. Kus vähegi võimalik, tuleks infoturvet puudutavad teemad lisada olemasolevatesse koolitustesse, et edendada ka seda, et töötajad võtaksid teemat iseenesestmõistetavalt. Vajaduse korral tuleb seniseid koolitajaid selle jaoks täienda-

valt kvalifitseerida. Lisaks peab infoturbe aspektidele võimaldama koolituse raames piisavalt aega.

5. Koolitusmoodulite arendamine

Selle etapi eesmärk on koondada võimalikult hästi koolituse sisud, kaasa arvatud nõuetekohased vahendid ja metoodika. Selleks tuleb loodavate koolituse sisude abil kindlaks määrata vastavad moodulid.

Lisaks tuleb määratleda, kuidas mooduleid realiseeritakse (vt ka M 3.48z Koolitajate või koolitusfirmade valimine), näiteks:

- oma töötajate läbiviidud koolituste kaudu,
- asutuseväliste õppejõudude läbiviidud koolituste kaudu, mis on kas spetsiaalselt asutuse vajadustele kohandatud (tavaliselt asutuse sees) või mis toimuvad seminariteenuste osutajate pakkumiste raames (vajaduse korral asutuse sees),
- juba olemasolevate koolitustega sidumise kaudu või
- koolitusmaterjalide loomise kaudu iseseisvaks õppimiseks.

Võimalikud vahendid ja meetodid on järgmised:

- klassikaline kontaktkoolitus,
- infoturbega seotud teabekogu, blogi või uudised intranetis, töötajate ajaleht,
- infoturbeteemalised ajakirjad,
- organisatsioonisisesed teabeüritused,
- organisatsioonivälised seminarid, messid ja konverentsid,
- spetsiifilisi infoturbe teemasid kajastavad videomaterjalid,
- e-õppeprogrammid, arvutipõhine koolitus, meelelahutuslik teave, veebiseminarid ja
- infoturvet kajastavate situatsioonide läbimängimine (vt M 3.47z IT-turbealased tegevus- ja rollimängud).

Kõik asutuses olemasolevad koolitusprogrammid ja -materjalid tuleks läbi vaadata, et välja selgitada, millised neist on osutunud edukaks, et need üle võtta ning samuti tuleks uurida, kas turvet kajastavaid teemasid oleks võimalik lisada ka ülejäänud koolitusprogrammide kavadesse.

E-õppeprogrammide valikul tuleks arvesse võtta, et need ei mõjutaks negatiivselt infoturvet rakendatud IT-keskkonnas. Kui e-õppeprogramme soovitakse lisaks intraneti keskkonnale rakendada ka interneti vahendusel, tuleb kasutusest kõrvale jätta nt aktiivsisu (Java, Javascript, ActiveX jne). E-õppe rakendusi nagu ka kõiki teisi rakendusi tuleks üldjuhul enne kasutamist testida ja anda neile kasutusluba ainult siis, kui need ei kujuta endast ohtu turbele (vt B 5.25 Rakendused).

6. Koolitusplaanide kindlaks määramine

Erinevate sihtrühmade jaoks tuleb kindlaks määrata koolitusplaanid ja lisaks sellele ka tsüklid või määratletud ajad töötajate karjääri jooksul, millal teatud moodulid läbitakse. Koolitusmooduleid tuleks täiendada vastava aja- ja ressursside kavaga ning juurutada see sündmusena. See annab vastutavatele juhtivtöötajatele võimaluse planeerida töötajate infoturbekoolitusi.

7. Õpitulemuste edukuse kontrollimine

Infoturbe koolitusmeetmete korral tuleb tagada, et osavõtjad saavutavad kavandatud koolituseesmärgid. Vastasel korral tuleb ette näha vastavad parandusmeetmed. Mõned õpitulemuste edukuse kontrollid tuleks läbi viia nii koolituse ajal pärast tähtsaid koolitusetappe (nt ühiste kokkuvõtete ja koolitajate küsimustega) kui ka koolituse lõpus ning veelkord mõne nädala pärast (vt ka M 3.94 Õpitulemuste edukuse mõõtmine ja hindamine). Asutusel peaks olema ajakohane ja täielik ülevaade oma töötajate turbealastest teadmistest, näiteks koolitustõendite ja isikusertifikaatide kaudu.

8. Õppematerjali kinnistamine ja ajakohastamine

Kord omandatud teadmisi tuleb pidevalt värskendada. Kui kiiresti ja intensiivselt see peab toimuma, sõltub omandatud teadmiste teemade ja praktilise kasutuse astme dünaamikast. Uute tehnoloogiate, aga ka uute ohtude, turvaaukude ja võimalike kaitsemeetmete tõttu tuleb infoturbealaseid teadmisi pidevalt värskendada ja täiendada. Koolitusprogramm peab seda asjaolu reeglipäraste töötajate täienduskoolituste näol arvesse võtma. Lisaks on oluline kogu programmi regulaarselt uuendada ja vajaduse korral uute asjaoludega kohandada (vt ka M 2.198 Personali teavitamine infoturbe küsimustest ja M 3.95z Õppematerjali kinnistamine).

Kontrollküsimused:

- Kas infoturbealaste koolitusmeetmete puhul on läbi viidud sihtrühmade ja koolitusvajaduse analüüs?
- Kas infoturbealaste koolitusprogrammide korral arvestatakse asutuse kõigi töötajatega nende ülesannete ja teadmiste kohaselt?
- Kas infoturbealaste koolitusmeetmete sisud kohandatakse muude koolitusmeetmetega?
- Kas infoturbealaseid koolitusprogramme uuendatakse regulaarselt?

M 2.558 Töötajate mobiil- ja nutitelefonide ning tahvel- ja pihuarvutite infoturbe teadlikkuse suurendamine

Algatamise eest vastutavad: personalijuht, infoturbeametnik

Rakendamise eest vastutavad: personaliosakond, ülemused

Lisaks üldisele koolitusele ja infoturbe teadlikkuse tõstmisele (vt M 2.198 Personali teavitamine infoturbe küsimustest ja M 3.5 Turvameetmete koolitus) peavad töötajad, kes kasutavad mobiil- ja nutitelefone, tahvel- ja pihuarvuteid, olema kursis nende seadmete infoturbe aspektidega. Seetõttu tuleb töötajaid, kes neid seadmeid kasutavad, kaasata eraldi koolituse ja teadlikkuse tõstmise planeerimisse ning neid tuleb koolitada ja teavitada selle plaani järgi.

Mobiil- ja nutitelefonide, tahvel- ja pihuarvutite puhul on nende väikese suuruse ja suhteliselt kõrge hinna tõttu eriti suur oht, et neid kaotatakse või varastatakse.

Pointsec'i tõus aastal 2005 suurimaks, 900 taksoga Chicago taksoettevõtteks tõi kaasa selle, et kuue kuu jooksul jäeti taksodesse 85 619 mobiiltelefoni ja 21 460 pihuarvutit. Seega tuleb töötajate tähelepanu juhtida eriti sellele, et neid esemeid ei tohi jätta järelevalveta ning kaotuse korral võtta ise või lasta IT-osakonnal võtta viivitamata kohased meetmed nagu positsioneerimine, andmete kustutamine ja seadmete lukustamine.

Kui puuduvad täiendavad turvameetmed, kaovad koos seadme kaotusega ka seadmes olevad andmed. Tänapäevased seadmed võivad salvestada andmeid kahekohalises gigabaitide mahus, mis võimaldab piisavalt ruumi konfidentsiaalsetele äriandmetele, hinnakalkulatsioonidele, aadressiraamatutele ja e-kirjadele. Seetõttu tuleb rakendada turvameetmeid nagu nt kõikide seadmel olevate andmete täielik krüpteerimine ja seadme lukustamine parooliga pärast seda, kui seda ei ole mõned minutid kasutatud. Kogemuste põhjal vaatavad töötajad nendele vajalikele meetmetele kriitiliselt, sest seadme kasutamine nõuab rohkem vaeva. Seetõttu tuleb töötajaid teavitada siin esitatud infoturbe ohtude osas ja koolitada täiendavate turvameetmete osas.

Mobiil- ja nutitelefonid ning tahvelarvutid pääsevad tavaliselt ligi internetile ja e-kirjadele. Töötajad peavad teadma sellega seotud ohtusid: seade võib nakatuda kahjurvaraga. Kaitset vajavad andmed võidakse seadmest varastada või seadet võidakse kasutada ruumisiseste kõnede (vt G 5.95 Pealtkuulamine ruumis mobiiltelefonidega) ja telefonikõnede pealtkuulamiseks. Seetõttu tuleb seadmeid kaitsta kahjurvara eest näiteks kohase kaitsetarkvara installeerimisega. Lisaks tuleb kaaluda võimalust, et suunata kogu mobiil- ja nutitelefonide andmeliiklus üle VPN-i asutuse serveri kaudu, et tõrjuda juba seal kahjurvara ja ründeid. Ka nende ohtude ja nendest tulenevate piirangute osas tuleb töötajaid vastavalt teavitada.

Kuna sidevaldkonna pealtkuulamisohuga käiakse tihti ümber liigagi kergekäeliselt, peaksid asutused kontrollima, kas senine töötajate teavitamine sidevaldkonnaga seotud ohtudest on olnud piisav. Olenevalt vajadusest tuleb töötajatele võib-olla koguni regulaarselt pealtkuulamisohtu meelde tuletada ja neid selle suhtes tähelepanelikumaks muuta.

Töötajatele tuleb selgitada, et konfidentsiaalset infot ei tohi niisama telefoni teel lihtsalt edasi anda. Eriti oluline on sidepartneri täpse identiteedi väljaselgitamine juhtudel, kui on plaanis edastada detailset infot (vt G 3.45 Sidepartnerite puudulik autentimine). Mobiiltelefonide kasutamise puhul tuleks jälgida ka seda, et konfidentsiaalset juttu ei aetaks avalikus kohas. See kehtib eriti lühisõnumite puhul, mis on saadetud oletatavalt tuntud numbrilt (vt G 5.192 Helistaja või SMS-i saatja telefoninumbri võltsimine). Kui lühisõnumites või vestlustes küsitakse konfidentsiaalset teavet, tuleks alati tagasihelistamisega kontrollida, kas küsimus pärineb tõesti antud suhtluspartnerilt. Seda kontrolli tuleb teostada ka siis, kui tuttavalt numbrilt saadetakse ootamatult manus või link.

Ikka ja jälle liiguvad ringi tähelepanuväärsed, kuid valed hoiatused (vt G 5.80 Pettemeilid). Selleks, et kallist tööaega ei raisataks liigselt niisuguste teadete tõepõhja kontrollimiseks, tuleks kõiki töötajaid võimalikult kiiresti teavitada, kui mõni uus pettemeil jälle liikvele on läinud. Vastavasisuliste hoiatuste edastamiseks saab kasutada erinevaid teavitusteenuseid.

Need turvameetmed piiravad tavaliselt seadmete kasutusmugavust. Nii toob täielik krüpteerimine kaasa pikema ooteaja seadme sisselülitamisel, vastuvõetava parooli jooksvat sisestamist peetakse segavaks ja kogu andmeliikluse suunamine üle VPN-i asutuse serveri kaudu pikendab ooteaega internetis surfamisel. Lisaks suurendab iga täiendav kaitseprogramm voolutarbimist ja lühendab seega aku kasutamise aega. Need piirangud võivad viia selleni, et töötajad üritavad turvameetmeid vältida, mille tõttu tuleb töötajate teavitamise käigus eriti rõhutada infoturbe ohtusid, mis tekivad seadmete nagu mobiil- ja nutitelefonid või tahvelarvutid kasutamisel, et meetmed oleksid alati tõhusad.

Kontrollküsimused:

- Kas töötajaid teavitatakse erilistest infoturbega seotud ohtudest seoses mobiil- ja nutitelefonide, tahvel- ja pihuarvutitega?
- Kas teavitamise kavandamisel võetakse eriti arvesse töötajate rühma, kellel on mobiil- ja nutitelefonid, tahvel- ja pihuarvutid?

M 2.559 Windows 8 soetamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: varumisosakond

Varasemate Windowsi versioonidega võrreldes suurenenud nõudmiste ja Windows 8 süsteemidel kasutatava riistvara soovituste põhjal, nt UEFI (Unified Extensible Firmware Interface) või Secure Boot, tuleb nii riist- kui ka tarkvara soetamise eel planeerida täpselt kasutamise eesmärk ja kasutamise variant.

Ametlikud Windows Hardware Certification'i nõudmised, varem tuntud kui Windows Logo nõudmised, määravad kindlaks nõudmised arvutile või komponentidele, mis tahavad kanda ametlikku Windowsi logo. Nende nõudmiste raames eristatakse ARM-i ja x86 platvorme.

Kui ARM-platvormidel on kohustuslik kasutada UEFI-d ja Secure Boot'i, peavad x86-l põhineva riistvara tootjad võimaldama Secure Boot'i inaktiveerimist. Sobiva riistvara valikul tuleb arvesse võtta selle eelduse rakendamist Microsofti kaudu. Lisaks tuleks riist- ja tarkvara valimisel silmas pidada, mil määral võtavad vastava riist- ja tarkvaratootjad arvesse riikliku võtmetähtsusega küsimuste dokumendis antud soovitusi seoses Trusted Computing'i ja Secure Boot'iga (vt ka M 4.471 Windows 8 uute turbefunktsioonide ülevaade).

Kui kasutatakse vastava redaktsiooni 64-bitist versiooni, tuleb rakendatavat riistvara ja installeeritavaid rakendusi kontrollida 64-bitise ühilduvuse suhtes. Põhiliselt on kasutada neli Windows 8 redaktsiooni. Kaks organisatsioonides kõige sagedamini kasutatavat redaktsiooni on Pro ja Enterprise.

Windows 8 redaktsioonid	Kokkuvõte
Windows RT 8.1	Windows 8 RT-versiooni pakutakse hetkel ARM-protsessorite jaoks. See on eelinstalleer
Windows 8.1	Windows 8 tüüpversioon nn kodukasutajate jaoks.
Windows 8.1 Pro	Tüüpversiooni funktsioonide kõrval sisaldab see redaktsioon mh funktsioone nagu liitum
Windows 8.1 Enterprise	Lisaks Pro-redaktsiooni funktsioonidele on sellesse redaktsiooni integreeritud funktsioon Enterprise-versioone saab üksnes hulgilitsentsidega.

Välja arvatud Windows RT, on kõik redaktsioonid kasutatavad 32- ja 64-bitiste protsessorite jaoks.

Seetõttu võivad Euroopa majandusruumi ja Šveitsi kasutajad või asutused omandada nn N-redaktsiooni. See redaktsioon võimaldab valida rakendusi nt DVD-de või digitaalsete meediafailide esitamiseks ja haldamiseks. See vastab muul juhul vastavate aluseks olevate versioonide funktsioonide ulatusele.

Hulgilitsentsiga soetamise korral tuleb arvesse võtta ka süsteemi aktiveeri-

miseks vajalikku taristut. See kehtib eelkõige hiljuti lisandunud aktiveerimisvariandi ADBA (Active Directory Based Activation) kohta, mis on mõeldud Windows 8 süsteemide mahu aktiveerimiseks.

Arvesse tuleb võtta, et vanemad süsteemid, nagu Windows 7 või Windows Server 2008 R2, on endiselt suunatud KMS-teenusele. ADBA aktiveerimise ainuke kasutusvõimalus on seetõttu üksnes puhtas Windows-8- ja Windows-Server-2012-keskkonnas (vt M 4.336 Hulgilitsentslepinguga Windows süsteemide aktiveerimine alates Windows Vistast või Windows Server 2008-st).

Kontrollküsimused:

- Kas enne Windows 8 süsteemi soetamist kontrolliti, millised redaktsioonid on kasutamise eesmärgi jaoks vajalikud?
- Kas kontrolliti, kas rakendused, mis töötavad Windowsi 64-bitise rakendusega, on võimelised töötama 64 bitiga?
- Kas kasutusele võetavad riistvara platvormid vastavad Windows Hardware Certification'i nõudmistele?
- Kas kasutatakse sobivaid protseduure süsteemide litsentseerimiseks, aktiveerimiseks või uuesti aktiveerimiseks?

M 2.560 SOA-l põhineva need-to-share-kontseptsiooni integreerimine turbehaldusesse

Algatamise eest vastutavad: IT juht

Rakendamise eest vastutavad: IT juht, organisatsiooni juht

Kui asutus juurutab teenusele suunatud struktuuril (SOA) põhineva need-toshare-kontseptsiooni, tuleb sisse viia turvakultuur, mida iseloomustab turbega seotud kõrge teadlikkus uue tehnoloogia ja mõtlemisviisi suhtes. Need-toshare-kontseptsioonist tulenevalt antakse suhtlemises osalejatele põhimõtteliselt rohkem teavet.

Töötajad peavad olema teadlikud oma vastutusest ja neil peab olema piisavalt teadmisi võimalikest riskidest, näiteks volitamata teabe väljavoolust. Selleks tuleb luua turbega seotud teadlikkus ja seda vahendada. Sama kehtib ka siis, kui olemasolevat need-to-know-kontseptsiooni laiendatakse need-to-share-kontseptsioonina infodomeeni kõikidele osalistele. Kõigil osalistel peab ka siin olema juurdunud turbega seotud teadlikkus, et nad käituksid asjakohaselt ja väldiksid riske. Peale selle ei tohi need-to-share-kontseptsiooni laiendada vahetult kõikidele need-to-know-dokumentidele.

Kontrollküsimused:

- Kas IT-süsteemi turbevahendid kaitsevad need-to-share-kontseptsiooni?
- Kas rakendatakse protsesse, mis aitavad kaasa need-to-sharekontseptsiooni sisseviimise ja need-to-know-kontseptsiooni laiendamise jaoks vajaliku turbega seotud teadlikkuse suurendamisele?

M 2.561 Standardikohaste SOA-rakenduste ja konfiguratsioonide loomine

Algatamise eest vastutavad: IT juht

Rakendamise eest vastutavad: administraator, IT-juht

Teenusele suunatud struktuuride (SOA) rakendused ja konfiguratsioonid peavad vastama standarditele (nt WS-Security). See tuleb tagada tehniliste abivahendite ja töökorralduslike protsessidega (nt nelja silma põhimõte). Lisaks tuleb vältida järeleproovimata või vähemlevinud standardeid ja raamistikke. Kuna just teenusele suunatud struktuuride valdkonnas areneb tehnoloogia kiiresti, on pidev standardeid, protokolle, struktuurirakendusi ja tehnoloogiaid puudutav täiendõpe hädavajalik.

Asutused peaksid rakendama võimalikult standardiseeritud võrguprotokolle, mis on välja töötatud vastava kasutuseesmärgi jaoks, ja omama integreeritud turvamehhanisme.

Kui struktuuris kasutatakse protokolle, millel puuduvad asjakohased kaitsemehhanismid, tuleks kasutada täiendavaid tehnoloogiaid ja alternatiivseid protokolle, et tagada asjakohane turbeaste. Just vanemad võrguprotokollid ei ole sageli rünnete vastu piisavalt kaitstud. Nii ei ole näiteks FTP-l (File Transfer Protocol) sõnumite autentsust, terviklust või konfidentsiaalsust puudutavaid kaitsemehhanisme. Need funktsioonid tuleb tagada muul moel.

Tähelepanu tuleb pöörata ka sellele, et kasutataks ainult selliseid võtmepikkusi ja krüptograafilisi meetodeid, mis pakuvad piisaval määral turvalisust, nt SOAP koos SHA-512-ga ja AES-256-ga (vt M 2.164 Sobiva krüptoprotseduuri valimine).

M 2.562 Integreeritud süsteemide kasutamise eeskirjad

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond

Rakendamise eest vastutavad: infoturbespetsialist

Ka integreeritud süsteemide jooksva kasutuse käigus tuleb arvestada terve rea turvanõuetega. Vastavad süsteemid peavad olema tehnilise ja organisatoorse kasutuskeskkonnaga adekvaatselt seotud. Selleks tuleb kehtestada järgmised organisatoorsed eeskirjad.

Kindlaks tuleb määrata personali koolitust, kasutajatuge, töötajate asendamise korda, kohustusi ja tööjaotust puudutavad vajalikud meetmed ja need ka ellu viia. Kasutajaid tuleb integreeritud süsteemide ja integreeritud süsteemidega seadmete kasutamisega seonduvatel teemadel regulaarselt koolitada. Käsiraamatuid peab olema vajalikus koguses ja need peavad olema ajakohases versioonis. Nimetada tuleb isikud, kes vastutavad püsivara uuendamiste, hooldus- ja remonditööde, logiandmete analüüsi ning turvaintsidentidele ja talitlushäiretele reageerimise eest. Tõrgete, talitlushäirete ja turvaintsidentide korral tuleb selgelt määratleda, mida nende puhul ette võtta. Kõiki töötajaid tuleb teavitada vastavatest käitumisreeglitest ja teavitamise protseduuridest. Kindlaks tuleb määrata eeskirjad tervikluse ja töökindluse katsetamiseks. Seejuures tuleb anda teavet nt intervallide, tööprotsessidega sobivuse ja vastutavate isikute kohta. Kindlaks tuleb määrata nõuded füüsikalise kasutuskeskkonna kohta, nagu nt õhuniiskuse ja temperatuurivahemik ning toite tagamine. Vajaduse korral tuleb taristus võtta selleks täiendavaid meetmeid. Kasutajate jaoks peavad integreeritud süsteemid olema valmistaja või administraatori poolt eelnevalt nii konfigureeritud, et oleks võimalik saavutada asjakohane turvalisus ja funktsioonid. Integreeritud süsteemide konfiguratsioon peab olema dokumenteeritud, et seda saaks pärast väljavahetamist, uuendamist või süsteemi taastamiseks rakendada kättesaadavuse nõuete kohaselt. Krüptograafiliste osadega integreeritud süsteemide kohta tuleb krüptokontseptsioonis kindlaks määrata täiendavad eeskirjad.

Kontrollküsimused:

- Kas integreeritud süsteemi toimimise eest vastutavad isikud on kindlaks määratud?
- Kas kasutajaid ja administraatoreid on integreeritud süsteemi või sellist süsteemi sisaldava seadme kasutamiseks piisavalt koolitatud?
- Kas kõiki kasutajaid ja administraatoreid on teavitatud käitumiseeskirjadest ja teavitamise protseduuridest tõrgete, talitlushäirete või turvaintsidendi kahtluse korral?
- Kas eeskirjad tervikluse ja töökindluse katsetamiseks on kindlaks määratud?
- Kas nõuded füüsikalisele kasutuskeskkonnale on kindlaks määratud?
- Kas integreeritud süsteem on eelnevalt turvaliselt konfigureeritud ja kas see on dokumenteeritud?

M 2.563 Usaldusväärse tarne- ja logistikaketi ning pädeva tootja valimine integreeritud süsteemide jaoks

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond
Rakendamise eest vastutavad: hankija

Lülituste ja kiipide funktsionaalsed kirjeldused ja füüsiline tootmine pärinevad tihtilugu erinevatelt ettevõtetelt. Nii mitmedki tuntud kiibitootjad kui ka spetsialiseeritud väikeettevõtted on nn „fabless companies". Need ettevõtted arendavad välja lülitusi ja kiipe, kuid ise neid ei tooda. Valmistamine toimub sellele tegevusele spetsialiseerunud ettevõtetes (nn „silicon foundries") üle kogu maailma, enamasti väljaspool Euroopat. Valmistatud kiibid tarnitakse sealt otse klientidele või hulgikaupmeestele. Ka tuntud edasimüüjad on üle maailma laiali. Süsteemitootja peab seetõttu veenduma, et valmistatud koostisosad vastavad igati täpselt standardile, ei sisalda peidetud lisafunktsioone ja vastavad kõikidele kvaliteedinõuetele. Ladustamise, vahendamise ja transportimise ajal ei tohi olla võimalik programmeeritavate loogikamoodulite kahjustamine või koostisosade vahetamine. Sellest tulenevalt tuleb logistikaketis teha tõhusaid pistelisi kontrolle. Tootja ja logistikaettevõte peavad olema sertifitseeritud tunnustatud standardite kohaselt.

Suurema kaitsevajaduse korral tuleb kvalifitseerida tootjad ja nende alltöövõtjad, kas nad toodavad riist- ja tarkvara konfidentsiaalselt. Atesteerimine tuleb dokumenteerida. Tootja kvalifitseerimist tuleb regulaarselt uuendada. Ükski arenduse ja remondiga seotud ettevõte ei tohi integreeritud süsteemi kaudu kaitstavale teabele ega süsteemis olevatele andmetele ligi pääseda. Selleks tuleb välja töötada ja rakendada IT-turbekontseptsioon. Töötajaid tuleb asjakohaselt koolitada ja teavitada. Teabe edastamiseks peavad olema kehtestatud kindlad eeskirjad. Juhtumitest tuleb teada anda ja need liigitada. Pärast juhtumit tuleb eeskirjad üle kontrollida ja lünkade või liiga paindlike nõuete korral neid vastavalt kohandada. Tellija peab veenduma, et teised ettevõtted rakendavad turvakontseptsiooni nõudeid.

Kontrollküsimused:

- Kas on tagatud, et integreeritud süsteem ei sisalda kahjustatud, võltsitud või vahetatud koostisosi?
- Kas on tagatud, et integreeritud süsteem vastab standardile ja et valmistamisel ei ole rakendatud peidetud funktsioone?
- Kas on tagatud, et volitamata isikud ei pääse integreeritud süsteemi kaudu ligi konfidentsiaalsele teabele?
- Kas osalevad ettevõtted on tõendatult kvalifitseeritud?

M 2.564 Integreeritud süsteemide soetamise kriteeriumid

Algatamise eest vastutavad: ametiasutuse / ettevõtte juhtkond, IT-juht

Rakendamise eest vastutavad: infoturbespetsialist, soetaja

Integreeritud süsteemid soetatakse üldiste süsteemide väljatöötamise käigus või on need osa soetatavatest üldistest süsteemidest. Koos puhta riist- ja püsivaraga võidakse soetada ka täiendavaid komponente ja teenuseid.

Kui integreeritud süsteemi soetamisel tehakse vigu, võib see mõjutada negatiivselt üldise süsteemi turvalist toimimist või rakenduse või tööülesande turvalist teostamist. Seetõttu tuleb enne integreeritud süsteemi soetamist koostada nõuete nimekiri, mille alusel oleks võimalik kõne alla tulevaid süsteeme või komponente hinnata. Hindamisele toetudes saab toote soetamisel kindel olla, et integreeritud süsteem vastab ka reaalselt oma töös kõigile turvanõuetele. Nõuete nimekiri peaks hõlmama peamiselt alljärgnevalt esitatud turvalisusega seotud valdkondi ja kriteeriume.

Töökorralduslikud raamtingimused

Soetamisel tuleks arvestada järgmiste aspektidega:

- kas on võimalik luua tõhus protsess turvalisusega seotud püsivara uuendustega varustamiseks?
- Kas tootja teavitab turvaaukude leidmise korral puudutatud osapooli?
- Kas tootja pakub ka tehnilist klienditeenindust, mis oleks võimeline vastuvõetava aja jooksul pakkuma teavet või kõrvaldama talitlushäireid?
- Kas tootja pakub integreeritud süsteemi turvalisuseks koolitusi ja käsiraamatuid?

Nõuded rakendusalalt

Integreeritud süsteem peab vastama konkreetsel rakendusalal kehtivatele standarditele ja normidele ning täitma vajaduse korral tootepõhise kasutusloa kriteeriume. Sellised kasutusload on tavalised nt lennu-, maanteeliikluse ja meditsiinitehnika valdkonnas.

Füüsiline turvalisus

Kui integreeritud süsteemi kasutatakse ebasoodsates keskkonnatingimustes, nagu niiskus, äärmuslikud temperatuurid, mehhaanilised koormused ja tolmune keskkond, peab see olema füüsikaliselt vastupidav. Pistikühendusi ei tohi kasutada või tohib kasutada üksnes mõnda usaldusväärset pistikühendust. Tundlikud komponendid peavad olema spetsiaalselt kapseldatud ja varustatud summutusseadmetega. Kui võimalik, tuleb loobuda liikuvate komponentidega osadest.

Tõrke- ja töökindlus

Olenevalt nõutavast käideldavusest tuleb integreeritud süsteemile esitada nõuded tõrkekindluse, elektromagnetilise ühilduvuse, sisemiste kontrolli- ja käivitustestimehhanismide ning taaskäivitamise suhtes.

Protsessori arhitektuur

Protsessori arhitektuuride ribalaius on väga suur. Erinevalt arvuti- või serverivaldkonnast kasutatakse uusarenduste kõrval sageli ka vanemaid arhitektuure.

Seda põhjustavad madalamad kulutused protsessorile endale ja võimalus kasutada uuesti rakenduse projekti, programmikoodi ja arendustööriistu ning silumistööriistu. Tuleb arvestada sellega, et valitud protsessori arhitektuur oleks sobiv vajalike turbefunktsioonide elluviimiseks.

Püsivara salvesti

Püsivara võib asuda ROM-il, EPROM-il, EEPROM-il või välkmälus. Välkmälu korral võib püsivara uuendada ilma kiipi välja vahetamata. ROM-i korral tuleb enamasti kogu kiip välja vahetada, mõnikord ka kogu lülitus. Püsivara salvesti tuleb luua nii, et koos plaanitud hooldusprotsessiga oleks võimalik ka turvaline uuendamine.

Operatsioonisüsteem ja rakendustarkvara

Kui integreeritud süsteem soetatakse koos operatsioonisüsteemide ja/või rakendustarkvaraga, tuleb kindlaks määrata, millised turvalisusega seotud omadused neil olema peavad, nt seoses järgmiste teemadega:

- turvaline buutimisprotsess
- turvaliste suhtlusprotokollide kasutamine
- turvaline installeerimine ja uuendamine
- pääsuõiguste kaitse
- kasutajate ja õiguste haldamine
- protokollimine
- hoiatamine
- tervikluse kaitse.

Arenduskeskkond

Kui koos integreeritud süsteemiga soetatakse ka arenduskeskkond, tuleb arvestada, et lisaks nõutavatele tööfunktsioonidele peavad sellel olema ka vajalikud turbefunktsioonid. Näiteks ei tohi koodiloomise etappide ajal tekkida tahtmatuid funktsioone ega tagauksi ning arenduskeskkonnal peavad olema mehhanismid, et suuta end kahjustamise vastu ise kaitsta. Võimaluse korral tuleks soetada sertifitseeritud tööriistad.

Kriteeriumid, mis ei ole otseselt turvalisusega seotud.

Kriteeriumidel, nagu nt

- voolu tarbimine
- integratsiooniaste
- signaali liikumise ajad
- reaalaja nõuete täitmine
- ruumivajadus ja
- kulud

puudub otsene mõju infoturbele. Samas tuleb siiski silmas pidada, et turvalisusega seotud kriteeriume tuleb teatud juhtudel vaadelda teisiti, kui eespool nimetatud kriteeriumid on optimeeritud.

Kinnitused ja sertifikaadid

Integreeritud süsteemide ja elektrooniliste komponentide jaoks on olemas mitmed kinnitused ja sertifikaadid. Kui soetamiskriteeriumidele lisanduvad nõuded, tuleb arvestada, et ka need võivad olla võltsitud, halva kvaliteediga ja eksitavad.

Kontrollküsimused:

- Kas integreeritud süsteemi soetamisel arvestatakse piisavalt füüsilise turvalisuse aspektidega?
- Kas integreeritud süsteemi soetamisel arvestatakse piisavalt riistvara turbefunktsioonide nõuetega?
- Kas integreeritud süsteemi soetamisel arvestatakse piisavalt tarkvara turbefunktsioonide nõuetega?
- Kas integreeritud süsteemi soetamisel arvestatakse piisavalt arenduskeskkonna turvalisuse aspektidega?
- Kas integreeritud süsteemi soetamisel arvestatakse piisavalt töökorralduslike turvalisuse aspektidega?

M 2.565 Turbega seotud sündmuste protokollimine integreeritud süsteemides

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator

Integreeritud süsteemide kasutamisel tuleb turbega seotud sündmused dokumenteerida.

Tehnilised võimalused võivad integreeritud süsteemide erinevate liikide ja nende keskkonna puhul suures ulatuses varieeruda.

Võimalikud teostused, funktsioonid ja parameetrid on järgmised:

- protokollimine püsimällu, kumulatiivselt erinevate protsesside kaudu,
- andmete salvestamine lihtsatesse, vormindatud tekstifailidesse, nt CSV või XML,
- protsessiandmete salvestamine andmelogide kaudu ajastuse, sündmuste või muudatuste järgi,
- sündmuste struktureeritud salvestamine andmebaasisüsteemis,
- kontroll reaalajas koos kasutaja teabe ja töö käigus sekkumise võimalusega,
- kõikide või konfigureeritavate oleku- ja üleminekumuudatuste protokollimine,
- muutujate kulu jälgimine, nt Audit Trails,
- statistiline hindamine aruandevormis või graafiliselt ja
- korrelatsioon, hindamine.

Kui vähegi võimalik, tuleks integreeritud süsteemide puhul protokollida vähemalt turvaintsidente, nagu volitamata juurdepääsu katse või teostamine. Eriti tuleb jälgida privileegidega kasutajate, nt tehnikute ja administraatorite tegevusi. Sellega ei ole küll võimalik ära hoida õiguste väärkasutust, kuid see on eeldus, et sulgeda sihipäraselt turvaauke. Peale selle mõjub protokollimine vähemalt avastamise riski suhtes võimalikele pahategijatele hirmutavalt.

Kui elektrooniline protokollimine ei ole kontseptsiooni piirangute tõttu piiratud vahenditega võimalik või on teostatav piirangutega, tuleks luua töökorralduslikud eeskirjad. Ühelt poolt tuleks kõikide integreeritud süsteemide juures tehtavate tööde korral fikseerida logiraamatus nimetatud tööde kohta, aega ja teostajat, samuti tegevuse liiki ning põhjust puudutavad andmed. Teiselt poolt peaksid logiraamatus olema dokumenteeritud tõrked, ilmsed pääsuõiguste rikkumised ja muud kõrvalekalded. Sissekandeid tuleb hinnata regulaarselt ja juhtumite kaupa.

Nii automaatselt koostatud protokolle kui ka töötajate ülestähendusi tuleb kaitsta hilisema volitamata muutmise eest. Protokollidele tohivad ligi pääseda üksnes eraldi volitatud isikud. Kui see on tehniliselt võimalik, tuleb võtta meetmed, et ka privileegidega kasutajad ei kustutaks ega muudaks protokolliandmeid, nt salvestamisega mitteülekirjutatavatele andmekandjatele või elektroonilise allkirja abil. Protokolliandmetega andmekandjaid tuleb säilitada turvaliselt ja osalevatele isikutele tuleb õpetada nende andmete õiget kasutamist.

Kontrollküsimused:

- Kas turbega seotud sündmusi protokollitakse automaatselt?
- Kas protokollid sisaldavad vajalikku teavet sobivas hinnatavas vormis?
- Kas protokolle on võimalik vajaduse korral mõistlikus ulatuses (käsitsi) hinnata?
- Kas protokollimise jaoks on olemas töökorralduslikud eeskirjad?
- Kas protokolle hinnatakse mõistlikus ulatuses?
- Kas protokollid on kaitstud volitamata juurdepääsu ja kahjustamise vastu?

M 2.566 Integreeritud süsteemi turvaline kasutusest kõrvaldamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator

Enne integreeritud süsteemi kasutusest kõrvaldamist tuleb kõik andmekandjatel olevad ja alaliselt salvestatud andmed niimoodi kustutada, et need ei oleks tagantjärele ka spetsiaalsete tarkvarade abil loetavalt taastatavad ja et neid ei saaks väärkasutada. Kui andmeid ei ole võimalik turvaliselt kustutada, tuleb sellised andmekandjad turvaliselt hävitada. Põhimõtteliselt kehtivad moodulite B 1.9 Riist- ja tarkvara haldus , B 1.15 Andmete kustutamine ja hävitamine ja M 2.167 Andmete kustutamiseks või hävitamiseks sobivate lahenduste valik soovitused.

Magnetiliste kõvaketaste korral tuleb kogu andmekandja juhuandmetega üle kirjutada ja protseduuri kontrollida.

Pooljuht-muutmälude, nt SRAM-i või DRAM-i korral tuleb kustutamiseks elektritoide välja lülitada ja eemaldada varutoite aku, kui see on olemas.

Väga kõrge kaitsevajadusega pooljuht-muutmälude, nt SRAM-i või DRAM-i korral tuleb mälu enne elektritoite väljalülitamist juhuandmetega üks kord üle kirjutada. Pooljuht-püsimälude, nt EPROM-i, EEPROM-i või välkmälu puhul tuleb kõrge kaitsevajaduse korral kogu mäluruum sobiva tarkvaraga kolm korda üle kirjutada.

Olenevalt integreeritud süsteemi liigist ja salvestatud andmete kaitsevajadusest on vajalikud järgmised tegevused:

- Kõvakettad tuleb kaitsevajaduse jaoks lubatud meetodiga kustutada või füüsiliselt hävitada.
- Pooljuhtmäludega, SSD- või hübriidkõvakettad tuleb füüsiliselt hävitada.

Kui arhitektuur või osaliselt riistvaraliselt lahendatud programmeerimine sisaldab kaitsmist vajavat teavet, tuleb komponendid füüsiliselt hävitada.

Kiipkaardid tuleb hävitada füüsiliselt. Selleks võib need tükeldada või sulatada.

Täpsemaid nõudeid teabekandjate hävitamisseadmete kohta võib leida standardist DIN 66399 „Büroo- ja andmetehnoloogia: andmekandjate hävitamine”. See standard eristab hävitamisel seitset turbeastet ja võtab kehtestamisel arvesse teabe kaitseastet, teabekandjate füüsikalisi omadusi ja kasutatavaid tehnilisi meetodeid.

Integreeritud süsteemid, millele on salvestatud tundlikke andmeid, peaks kõrge kaitsevajaduse korral olema kustutamisvõimalus hädaolukorras. Kui see funktsioon käivitatakse, kustutatakse kõik konfidentsiaalseks liigitatud andmed usaldusväärselt. Juhul kui selleks tuleb süsteem füüsiliselt hävitada, võib, nagu

on kirjeldatud meetmes M 4.487z Urkimiskaitse (tuvastamine, takistamine, tõrje) integreeritud süsteemides .

Kui on olemas ümbritseva keskkonna tsentraalselt käivitatav, automaatne hädaolukorras kustutamise protseduur, nt Central Clear, Crash Clear, peab integreeritud süsteemi hädaolukorras kustutamise funktsioon olema integreeritav. Selleks on ette nähtud vastavad liidesed.

Vajaduse korral võib rakendada ka automaatset hädaolukorras kustutamise funktsiooni, mis kustutab või hävitab kõik tundlikud andmed.

Kui kasutusest kõrvaldatud integreeritud süsteemide andmekandjad kustutatakse või hävitatakse ja kui riistvara hävitatakse, tuleb see dokumenteerida.

Kontrollküsimused:

- Kas kõik integreeritud süsteemi andmed kustutatakse enne kasutuselt kõrvaldamist turvaliselt?
- Kas integreeritud süsteemi riistvara hävitatakse enne kasutuselt kõrvaldamist turvaliselt?
- Kas süsteemil on asjakohane hädaolukorras kustutamise funktsioon?
- Kas kustutamine või hävitamine dokumenteeritakse?

M 2.567 Usaldusväärsete arendustööriistade valik

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: soetaja, arendaja

Kui süsteemide jaoks arendatakse riist- või tarkvara, kasutatakse tavaliselt tervet rida tööriistu. Seejuures on sageli tegemist võimsate, graafikal põhinevate arendustööriistadega. Need on kõrgintegreeritud ja ühendavad nõuete halduse, graafilise projekti ja koodiloomise. Lisaks kasutatakse nende andmebaasi automaatsete katsete põhjana. Protsessi etappide kõrge automatiseerimise astmega ideest koodini jäetakse tööriistale või tööriistadele võimalikult kõrge autonoomsuse aste. Seetõttu peavad arendustööriistad olema vigadeta ja neid ei tohi olla võimalik kahjustada, sest muidu on ohustatud ka sihtsüsteemi riist- ja tarkvara.

Arendustööriistu ei tohi väärkasutada selle jaoks, et lisada peidetud tagauksi või turvaauke. Süsteemitootja arendustööriistad peavad olema kvalifitseeritud arendatava funktsiooni ja sellega töödeldava teabe kaitsevajaduse kohaselt. Selle jaoks peab tootja esitama tellijale tööriista-suunise, mis sisaldab tööriista olulisi turbenõudeid, ettenähtud tööriistakeskkonda, ostupoliitikat ja kvalifitseerimise meetmeid. Tellija peab soetatud tööriistade korral tööriista-suunist eraldi kontrollima.

Kompilaatoriga tõlgitud koodid muudavad kirjakeele koodi vahekoodiks või masinakoodiks. Assemblerit võib samuti vaadelda kompilaatorina, sest see tõlgib riistvarapõhise keele masinakoodi ümber. Tavaliselt kasutatakse ristkompilaatoreid, sest tõlgitava süsteemi arvutiarhitektuur ei ole sama nagu integreeritud süsteemi oma. Seejuures ei tööta kompilaator mitte sihtsüsteemis, vaid näiteks tavaarvutis, ja loob seal koodi, mis laaditakse sihtsüsteemi.

Praegu (versioon 2015) on tarkvaraarenduses üha suurenev roll programmeerimiskeelel Java. Javas kirjutatud programmid tõlgitakse kõigepealt masinast sõltumatusse baitkoodi. Seejärel tõlgendab tõlgendaja seda konkreetsel riistvaral. Moodsad tõlgendajad on optimeeritud suurele täitmiskiirusele. Mudelil põhineva arenduse korral määratakse süsteemi omadused ja käitumine kindlaks modelleerimiskeelte või graafiliste mudelite abil. Nendest genereeritakse seejärel kirjakeeles olev kood. Silurite ja ristsiluritega leitakse riist- ja tarkvaras vead, kusjuures silumiseks kasutatakse ka täiendavat riist- ja -tarkvara. Mõned tootjad pakuvad oma mikrokontrollerite jaoks täielikke süsteemiarenduse pakette, nn System Design Kits'e. Need koosnevad enamasti prototüüpsest riistvarast plaadi, mikrokontrolleri, liideste ja lisaseadmetega ning Software Development Kit'ist, millega saab luua tarkvara selle mikrokontrolleri jaoks. Software Development Kit töötab tavaliselt laiatarbearvutis, mis ühendatakse silumise liidese, nt IEEEstandardi 1149.1 kohaselt prototüüp-plaadiga.

Kontrollküsimused:

- Kas süsteemi arendamiseks kasutatakse üksnes tõestatud turbefunktsioonidega tööriistu?
- Kas on kindlaks tehtud, et tööriistu ei ole võimalik kahjustada?
- Kas riist- või tarkvara tootjale esitatakse piisavad turbenõuded?

M 2.568 Tarkvara testimisprotseduurid

Algatamise eest vastutavad: ametiasutuse / ettevõtte juhtkond, IT-juht

Rakendamise eest vastutavad: testija

Tarkvara kvaliteedi tagamiseks on olemas staatilised meetodid, mille puhul programm ei tööta, ja dünaamilised meetodid käitamise ajal.

Staatilised meetodid

Staatiliste meetoditega kinnitatakse programmikood. Olulised staatilised meetodid on koodi ülevaatused ja automaatne staatiline koodianalüüs.

Koodi ülevaatused

Süsteemi arendamisel peaksid toimuma koodi ülevaatused, sest on olemas riistvarast sõltuvad vead, mida saab mõistlike kuludega üksnes nii üles leida.

Kulutused peaksid olema orienteeritud kaitsevajaduse ja kulude-tulude suhte järgi. Lihtne ja vähem formaalne variant on nn walkthrough, mille korral esitleb autor oma tööd sammhaaval ja osalised annavad tagasisidet. Kõrgemate turbenõuete korral tuleks läbi viia formaalne koodi kontrollimine. Mõlemaid liike võib teostada ka kolleegläbivaatustena. Sel puhul osaleb autori kõrval ainult üks, ametiredelil samal positsioonil olev töötaja. Kolleegläbivaatused vähendavad kulusid ning toovad sageli kaasa üksnes mõistliku turbe languse.

Ülevaatused peaksid orienteeruma kontrollnimekirjale, mis võib sisaldada nt järgmisi küsimusi:

- Kas välja indeksid võivad üle täituda?
- Kas kõik muutujad on määratletud õiges kontekstis?
- Kas muutujate bitilaius on piisav?
- Kas tuvastatakse aritmeetilised ületäited ja kas neid käsitletakse?
- Kas välditakse tuntud vigaseid struktuure?

Automaatne staatiline koodianalüüs

Automaatse staatilise koodianalüüsi jaoks turul olevate tööriistade hinnaskaala on lai. On nii soodsaid kui ka kallihinnalisi tööriistu. Soodsatel tööriistadel võivad olla paljud analüüsimeetodid ja need võivad analüüsida nt käsu- ja andmevoogu, otsida mitteinitsialiseeritud muutujaid ja tuvastada numbrilisi väärtusi. Täiendavate analüüsivõimaluste kõrval peituvad kallihinnaliste süsteemide eelised selles, et neid on kergem kasutada ja need toodavad vähem valepositiivseid tulemusi. Koodi kvaliteedi kohta võivad anda teavet ka koodi indikaatorid, nt pesastussügavused, dünaamiliselt loodud objektide arv või kommentaaritihendus.

Dünaamiline meetod

Dünaamilise meetodi korral valideeritakse valmis programm või selle osad. Seejuures käitatakse testitavat tarkvara süstemaatiliselt kindlaksmääratud testiandmetega. Testiandmed koosnevad eel- ja järeltingimustest ning moodustavad koos testitava funktsiooniga testijuhtumi. Testimisel tuleb eelkõige tuvastada programmivead, mis ilmnevad olenevalt dünaamilistest käitamisparameetritest, nt anduri andmetest või kasutaja sekkumistest.

Testimisel on etapid üldiselt jaotatud alljärgnevalt:

- testijuhtumi eelduste loomine,
- programmi või testi osafunktsiooni teostamine,
- oodatava väärtuse võrdlemine tegelikult saadud väärtusega ja järeltingimuste kontrollimine,
- testi lõpetamine.

Seejuures võib tarkvaraprojekti arendamise ajal alustada paralleelselt testiprojektiga. Nii saab testimisetappi lühendada ja on võimalik tuvastada testijuhtumid, mille jaoks vajatakse spetsiaalset testimise riistvara. Dünaamiliste testidega võib alustada, kui esimesed tarkvara moodulid on valmis. Selle asemel, et määrata testijuhtumid kindlaks alles protsessi lõpus, võib testidega alustada ka enne rakendamist ja juhtida sel moel arendamist olulisel määral. Seda meetodit nimetatakse testidel põhinevaks arenduseks (inglise keeles: Test-Driven-Development, TDD).

Teste võib tuletada erinevate moodustega. Põhilised kategooriad on:

- standarditele orienteeritud meetodid, nn Black-Box-testid ja
- struktuurile orienteeritud meetodid, nn White-Box-testid.

Testidel on erinevad täpsuse tasemed ja teostamise järjekord. Tavaline tarkvara testimise järjekord on järgmine:

- komponentide test,
- integreerimistest,
- süsteemitest.

Seejuures on komponentide test kõige vähem üksikasjalik ja süsteemitest kõige põhjalikum. Samuti peavad olema lõpetatud kõik need komponentide testid, millel integreerimistest põhineb. Sama kehtib süsteemitesti kohta. Järgmine oluline aspekt on, kuidas testid läbi viiakse.

Black-Box-test

Black-Box-testi korral testitakse testi objekti selle projektis kindlaks määratud eesmärgi suhtes. Peale oodatavate funktsioonide tuleb testida käitumist ebatavaliste sisestuste korral. Kuna peaaegu kunagi ei ole võimalik testida kõiki võimalikke sisestusi ja väljastusi, tuleb moodustada vastavusklassid. Need peavad olema liigitatud nii, et testija lähtub sellest, et ühe vastavusklassi sisestused käituvad ühtemoodi. Teste viiakse läbi tugevdatuna vastavusklassi piirväärtustega, seega nt kõige suurema ja väiksema ulatusega negatiivsete ja positiivsete väärtustega. Testida tuleb ka nullväärtust ja selle ümbruses olevaid väärtusi.

White-Box-test

White-Box-testi korral määratakse testijuhtumid tarkvara lähtekoodi põhjal. Need võib üldiselt jaotada keerulisteks, praktikas mitte eriti laialt levinud andmevoole orienteeritud meetoditeks ja käsuvoole orienteeritud meetoditeks. Viimaste korral sõltub täpsus testi katvusest. See määratletakse protsentuaalse osana üksustest, nt juba testid läbinud tarkvara määrangud ja harud. Testi katvuse erinev

aste saavutatakse kattuvustestidega, mis sobivad testiobjektide väiksema suuruse tõttu eriti komponentide testide jaoks.

Suureneva ranguse järgi liigitatuna on kõige rohkem kasutatavad indikaatorid järgmised:

- määrangu katvus (statement coverage): testi katvuse kõige lihtsama indikaatoriga kontrollitakse, milline osa programmimäärangutest teostati. 100%
- määrangute katvus on suhteliselt halb tõestus ja on piisav üksnes vähese kaitsevajadusega süsteemide korral.
- harude katvus (branch coverage): kontrollitakse, kas iga haru korral on iga funktsiooni vähemalt üks kord läbitud.
- otsuste ja tingimuste katvus (decision and condition coverage): lisaks harude katvusele on nõutav loogikaavaldise iga osatingimuse muutmine.
- tingimuste/otsuste katvuse modifitseeritud test (modified decision and condition coverage): iga osatingimus, mis võib mõjutada haru, peab näitama, et see võib olenemata muudest tingimustest määrata programmikulgu.

Komponentide test

Komponentide testid puudutavad kõige väiksemaid kasulikult eraldi testitavaid üksusi. Neid võib läbi viia Black-box- ja/või White-Box-testidena. Komponentide testid peavad toimuma sihtsüsteemil, sest ainult siis on võimalik leida ühilduvusvigu ja tuvastada võimalikke tõlgendusvabadusi, mis võivad kaasa tuua erinevaid tulemusi hostil või sihtsüsteemil. Nii ei ole nt C-kompilaatorite puhul negatiivse täisarvulise väärtuse paremale nihutamise tulemus täpselt määratletud või võivad andmelaius ja baitide järjekord olla hostil ja sihtsüsteemil erinevad.

Integratsioonitestid

Integratsioonitestidega kontrollitakse, kas tarkvarakomponentide koostoime omavahel ja riistvarakomponentidega on õige. Seejuures teostatakse testid Black-Box-testidena. Tüüpilised tarkvara/tarkvara-integratsioonitestid on Bottom-Up-komponenttestid, struktureeritud integratsioonitestid ja alamprogrammide käivituste testi katvuse mõõtmine. Igal meetodil on oma tugevused ja nõrkused. Bottom-Up-komponentteste on mõistlik kasutada väikeste projektide korral, kus ei ole tegemist komponentide tsükliliste sõltuvustega. Struktureeritud integratsioonitestid ja alamprogrammide käivituste testide katvuse mõõtmine on problemaatilised, kui kasutatakse globaalseid muutujaid. Viimati nimetatud strateegia üks puudus on ka see, et integreerimisel tuvastatakse vead suhteliselt hilja.

Riistvara/tarkvara-integratsioonitestide eesmärk on kontrollida riist- ja tarkvara koostoimet. Kui sihtkeskkond on algusest peale kasutatav, võivad Bottom-Upkomponenttestid toimuda pidevalt seal. Regressioonimeetodi korral kapseldatakse juurdepääsud riistvarale abstraktsioonikihi abil. Kui süsteemil on kõrge kaitsevajadus, tuleb analüüsimisel arvesse võtta ka kõiki mõeldavaid veaolukordi ja tulemused täpselt dokumenteerida. Ideaaljuhul on iga funktsionaalse omaduse ja vale käitumise jaoks olemas tõestatav test.

Võimalike piiratud ressursside korral on mõnede süsteemide puhul oluline läbi viia ka ressursitestid. Nendega kontrollitakse, kas CPU ja olemasolev mälu on ettenähtud tarkvara jaoks piisava jõudlusega ja piisavalt dimensioneeritud.

Süsteemitestid

Black-Box-testidega kontrollitakse, kas süsteem tervikuna täidab kindlaks määratud nõudeid. Samaaegselt tuleks Traceability-tabelite abil jälgida, millist nõuet millise testiga kontrollitakse. Testiandmed luuakse vastavusklasside moodustamise abil kehtivate ja kehtetute sisestusandmete kaudu. Ühe testijuhtumi kohta tohib ühest kehtetute väärtustega vastavusklassist võtta ainult ühe väärtuse.

Testide teostamisviisid

Testid võivad toimuda manuaalselt, poolautomaatselt või automaatselt. Testi automatiseerimise kõrge aste annab eelise teostada korduvaid teste kiiresti ja lihtsalt. See sobib eriti nt regressioonitestidele, seega testidele, mis viiakse läbi pärast vigade kõrvaldamist, et olla kindel, et seeläbi ei teki vead mõnes teises kohas. See võimaldab ökonoomselt läbi viia ka manuaalselt üksnes raskustega teostatavaid teste, nt koormusteste. Testimisel tuleb vajaduse korral arvesse võtta ka vajalikke manuaalseid sekkumisi, nt integreeritud süsteemide testimisel.

Kontrollküsimused:

- Kas teostatakse koodi ülevaatused ja automaatne staatiline koodianalüüs?
- Kas komponentide testide korral moodustatakse kasulikud vastavusklassid ja testitakse kõiki kriitilisi piirväärtusi?
- Kas testi katvuse jaoks valitud indikaatorid vastavad kaitsevajadusele ja kas komponentide testid viiakse läbi sihtsüsteemil?
- Kas viiakse läbi kaitsevajadusele vastavad integratsiooni- ja süsteemitestid?
- Kas testitakse, et CPU ja olemasolev mälu on ettenähtud tarkvara jaoks piisava jõudlusega ja piisavalt dimensioneeritud?

M 2.569 Rollide ja vastutuse määratlemine tarkvaraarenduses

Algatamise eest vastutavad: IT juht, organisatsiooni juht

Rakendamise eest vastutavad: IT juht, organisatsiooni juht

Tarkvaraarenduses peavad rollid ja vastutused olema üheselt määratud, erilist tähelepanu tuleb seejuures pöörata asjakohastele funktsioonidele. Kõik projekti juures töötavad isikud peavad teadma, millised on tema vastutusala ülesanded ja kes on kontaktisik väljaspool tema ülesannete vastutusala. Nimetada tuleb isik, kellel lasub koguvastutus tarkvaraarendusprotsessis vajaliku turbe eest, kes määrab kindlaks kõik turvameetmed ja kes neid kontrollib ning kes on lisaks ka kontaktisik seoses meetmeid puudutavate küsimustega.

Üldise vastutusega isikul peab olema:

- selge arusaam oma rollist
- piisavad oskused
- küllaldaselt aeg
- sobivad vahendid ja volitused
- juurdepääs asutusesisele ja -välisele infoturbe ekspertiisile
- dokumenteeritud meetodid rutiinsete turvameetmete jaoks ja
- ajakohane teave infoturbe kohta. Infoturbe olekut tuleb igas projektis koos arenduse eest vastutava isiku ja pädevate osakondadega regulaarsete ajavahemike järel kontrollida. Peale selle tuleb iga järgmise võtmetegevuse jaoks määrata vastutav isik:
- arendussuuniste järgimine
- nõuete analüüs
- riskianalüüs
- projekt ja teostus
- testimine ja roll-out.

Kui meeskonna suurus seda võimaldab, peaksid kõik rollid olema jaotatud erinevate isikute vahel. Arendust, testimis- ja tootmisprotsessi peaksid läbi viima erinevad isikud.

Kontrollküsimused:

- Kas tarkvaraarenduse projekti jaoks määrati üldiselt vastutav isik?
- Kas kõikidele võtmetegevustele määrati rollid ja vastutused?

M 2.570 Protsessimudeli valik tarkvaraarenduse jaoks

Algatamise eest vastutavad: arendusjuht

Rakendamise eest vastutavad: arendusjuht

Tagamaks kogu arendusprotsessi reguleeritud kulgu, on elementaarne valida tarkvaraarenduse jaoks välja sobiv protsessimudel. Kõik protsessis osalevad isikud saavad paremini orienteeruda ja oma tegevust koordineerida, kui rakendatakse ranget metoodikat.

Olenevalt arendatava tarkvara nõuete ulatusest tuleb välja valida protsessimudel, mis arvestab piisaval määral kõigi arendusprotsessi aspektidega. Näiteks tuleks koskmudelile eelistada spiraalmudelit, kui juba protsessi alguses on selge, et arendamise ajal muudetakse veel sageli tarkvara funktsionaalseid nõudeid. Mõned protsessimudelid pakuvad pigem jäika raamistikku ja sobivad üksnes projektidele, mille nõuded on selgelt kindlaks määratud ja projekti jooksul tõenäoliselt oluliselt ei muutu. Teised protsessimudelid toetavad dünaamilist ja liikuvat tarkvaraarendust ning võimaldavad mitmekordsete iteratsioonidega kohandada projekti kõigi arendusetappide käigus paindlikult muutunud nõuetele vastavaks.

Tarkvaraarenduse väljakujunenud protsessimudelid on näiteks järgmised:

- koskmudel
- Arendus jaotatakse siin selgelt määratletud etappideks, mis läbitakse üksteise järel. See algab nõuete analüüsiga, millele järgneb süsteemi projekt. Seejärel programmeeritakse tegelik tarkvara ja testitakse seda modulaarselt. Lõpuks järgneb integratsiooni- ja süsteemitestile tarkvara väljastamine ja hooldus tootmissüsteemi jaoks.
- spiraalmudel
- See üldine protsessimudel on koskmudeli edasiarendus ja vaatleb tarkvaraarendust iteratiivse protsessina, mille tsükleid läbitakse mitu korda. Iga tsükkel on jaotatud neljaks sektoriks. Kõigepealt määratakse kindlaks eesmärgid ja raamtingimused. Seejärel hinnatakse alternatiive ja riske. Edasi realiseeritakse kindlaksmääratud vahe-eesmärk ja kontrollitakse seda. Lõpuks kavandatakse jätkamiseks järgmine tsükkel.
- üldine V-mudel
- V-mudel põhineb koskmudelil ja määratleb tarkvara arendusprotsessi ja kvaliteedi tagamise etappide kaupa, kusjuures iga projektietappi võrreldakse testietapiga. Etappide arv ja tähistamine on siinjuures paindlik.
- V-mudel XT
- Võttes aluseks V-mudeli, on V-mudel XT määratletud Saksa Liitvabariigi avalikus halduses arendusstandardina. V-mudel XT-s määratakse kindlaks tegevused ja tulemused, mille ajaline järjekord on paindlik. Tegevusi võib luua ka näiteks koskmudelil.
- prototyping
- Prototyping'u korral keskendub tarkvaraarendus sellele, et anda kiiresti prototüübid, mille funktsioonid määratletakse ja optimeeritakse seejärel täpsemalt etappide kaupa koostöös teenuseosutaja ja tellijaga.
- MDSD (ingl Model-Driven Software Development)

- Mudelile orienteeritud arenduse korral toodetakse tarkvara automaatselt formaalsetest mudelitest, mis luuakse mudelikeelte või graafiliste mudelitööriistadega. Soovitud süsteemi funktsioonid saab seejuures määratleda abstraktsel tasemel.
- TDD (Test-Driven Development)
- Selles protsessimudelis koostatakse enne tegeliku tarkvara loomist alati kõigepealt tarkvaratest. Kui testid (nn grey-box-testid) on lõpetatud, luuakse võimalikult väheste kulutustega tegelik programmikood ja kohandatakse see vajaduse korral testidega. Teste võib siinjuures luua nii üksikute moodulite (unit-testid) kui ka kogu süsteemi (süsteemitest) jaoks.

Tarkvaraarenduseks on olemas veel mitmesugused muud protsessimudelid.

Peale selle tegeletakse ISO-standardites 12207 ja 13407 arusaamaga tarkvaraarendusest ning prototüüpse kasutajale suunatud tarkvara toodanguga. Protsessimudeli üle otsustamine tuleb dokumenteerida ja koostada projekti jaoks vastav protseduuriskeem, mis hõlmab kõiki rakendusetappe ja vastavaid vastutavaid isikuid.

Valitud protsessimudeli põhjal tuleb koostada asutusesisene suunis tarkvaraarenduseks. Peale selle tuleb kindlaks määrata:

- kuidas tuleb süsteemiarenduse ajal arvesse võtta asutust hõlmavat turvasuunist, seadusest tulenevaid nõudeid ning
- kuidas teostada konkreetses arendusetapis nõuete analüüs, projekt ja rakendamine, testimine ja roll-out, arvestades turvalisusega.

Töötajaid tuleks koolitada valitud protsessimudeli metoodika suhtes. Tarkvaraarenduse suunist tuleks regulaarselt kontrollida ja hoida kõige värskemal kujul. Suunisest kinnipidamist tuleb kontrollida kõikide tarkvaraarenduse võtmepunktide juures.

Kui ükskord valitud protsessimudeli metoodika vahetatakse teise protseduuri vastu, võib see muudatuse etapis suurendada arendusega seotud kulutusi. Sel põhjusel tuleb protsessimudeli valik läbi viia võimalikult hoolikalt.

Kontrollküsimused:

- Kas tarkvaraarenduse jaoks määrati kindlaks sobiv protsessimudel?
- Kas valitud protsessimudeli alusel koostati protseduuriskeem tarkvaraarenduse jaoks ja dokumenteeriti turbenõuded?
- Kas arvesse võeti asutust hõlmavaid turvasuuniseid, seadusest tulenevaid nõudeid ja konkreetseid turvanõudeid?
- Kas töötajaid koolitati valitud protsessimudeli metoodika suhtes?

- Kas tarkvaraarenduse suunist kontrollitakse regulaarselt ja muudetakse vajadusest lähtudes?

M 2.571 Vastavusnõuete järgimine tarkvaraarenduse jaoks

Algatamise eest vastutavad: nõuete haldur

Rakendamise eest vastutavad: arendaja, nõuete haldur

Tarkvara arendamise ja välja töötatud tarkvara rakendamise korral tuleb arvestada sellega, et ei kahjustata seadusest ja normatiividest tulenevaid tingimusi. Kui autoriõigusega kaitstud programmiosi, raamatukogusid või tabeleid kasutatakse mõtlematult, võivad sellel olla tõsised õiguslikud ja materiaalsed tagajärjed.

Nii kasutatavate arendustööriistade kui ka välja töötatud tarkvaratoote suhtes tuleb kontrollida vähemalt järgmisi aspekte:

- seaduste või lepingute täitmine
- standarditest kinnipidamine
- kasutatava tarkvara litsentsitingimuste täitmine
- patendiõiguste järgimine
- disainilahenduste jäljendamine
- isikuõigused.

Kõikidel töötajatel peavad olema teadmised selleks, et saada vastavusnõuete rikkumisest õigeaegselt aru. Lisaks tuleb kindlaks teha, et kõiki rikkumisi oleks võimalik kindlaks teha juba arendusfaasis ja et need ei jõuaks tootmissüsteemi. Rikkumiste ilmsikstuleku korral tuleb kohe võtta meetmeid ja kohandada tarkvaraarendus kehtivatele tingimustele.

Kontrollküsimused:

- Kas tarkvaraarenduses järgitakse kõiki vastavusnõudeid?

M 2.572z Tööriistade soetamine tarkvaraarenduse jaoks

Algatamise eest vastutavad: hankejuht, arendusjuht

Rakendamise eest vastutavad: hankija

Arenduskeskkonna kõrval võib tarkvaraarenduse jaoks vaja olla veel ka täiendavaid tööriistu, näiteks graafikaprogramme või haldustööriistu. Samuti võib olla vaja lisaseadmeid, näiteks kiipkaardilugejaid või digitaallaudu.

Tööriistad, mis on tarkvaraarenduse aktiivsed komponendid, tuleks soetada standardiseeritud ja dokumenteeritud protseduuride kohaselt, mis määratlevad muuhulgas järgmist:

- suunised riist- ja tarkvara valimiseks
- meetodid, et tuvastada soetatud riist- ja tarkvara turvalisusega seotud puudused ja neid käsitleda
- nõuded tarkvara vastuvõetavatele litsentsitingimustele
- ülevaatuse ja väljastamisprotseduurid soetatud riist- ja tarkvara jaoks.

Soetamisel tuleks kontrollida pakkujaid ja arvesse võtta vastava kasutuseesmärgi kehtivaid turbenõudeid. Kättesaadavus on eelkõige spetsiaalse riistvara korral oluline valikukriteerium.

Lisaks tuleb arvesse võtta, kas soetatud riist- ja tarkvara tohib kasutada tarkvaraarenduseks ja kas sellega loodud või töödeldud andmete edastamine ei tekita konflikti tootja litsentsitingimustega.

Asutusevälised riist- ja tarkvara turvakontrollid ja -sertifitseerimised vähendavad turvalisusega seotud puuduste tõenäosust. Soetamise otsuse kvaliteedi tagamist peaksid kontrollima töötajad, kes tunnevad turbenõudeid ja oskavad otsustada, kas need on täidetud.

Kontrollküsimused:

- Kas tööriistade soetamine tarkvaraarenduseks toimub standardiseeritud ja dokumenteeritud protseduuride kohaselt?

M 2.573 Kinnipidamine turvalisest protseduurist tarkvaraarenduses

Algatamise eest vastutavad: arendusjuht

Rakendamise eest vastutavad: arendaja, arendusjuht

Rakendamise protsess peab olema tarkvaraarenduses turvaliselt kujundatud, et tuvastada ja vältida näiteks olukorda, kus tarkvara muudetakse kogemata või kahjustatakse tahtlikult. Tagamaks arendatava tarkvara infoturvet, peavad mitu arendajat nt nelja silma põhimõtte range rakendamisega kontrollima ja testima arendamise ajal ennekõike turvalisusega seotud tarkvarakomponente, nt autentimissüsteeme. Tagada tuleb arendatava tarkvara versioonikontroll. Eriti on nõutav versioonide erinevuste dokumenteerimine ja võimalus naasmiseks varasemate versioonide juurde (vt M 6.32 Regulaarne andmevarundus).

Selleks, et tarkvara terviklus ei saaks kahjustatud, on nõutavad regulaarsed koodi ülevaatused. Neid peavad läbi viima sõltumatud kolmandad osapooled või äärmisel juhul arendajad, kes ei ole ise koodi kirjutanud. Seejuures tuleb kontrollida, kas programmikood sisaldab kõiki soovitud funktsioone ning et see ei sisaldaks samal ajal täiendavaid või soovimatuid funktsioone. Kui arenduskeskkonda on lisatud väliseid raamatukogusid või koode asutusevälistest allikatest, tuleb neid kontrollida turvaaukude ja võimalike konfliktide suhtes muude, juba kasutatavate komponentidega. See peaks toimuma asutuseväliste teabeallikate (nt veebikataloogid, mis sisaldavad tuntud veateateid ja turvaauke) ja asutuse enda testidega, mis on kooskõlastatud arenduse eest vastutava isikuga.

Kontrollküsimused:

- Kas arendatava tarkvara suhtes rakendatakse versioonikontrolli?
- Kas viiakse läbi regulaarseid sõltumatuid koodi ülevaatusi?

M 2.574 Tarkvaraarenduse põhjalik dokumenteerimine

Algatamise eest vastutavad: spetsialistide osakonna juhataja

Rakendamise eest vastutavad: IT juht, spetsialistide osakonna juhataja

Tarkvaraarendus peab olema tõestatavalt dokumenteeritud, et oleks võimalik tuvastada turvalisusega seotud aspekte ja et tarkvara saaks hooldada. Dokumentatsioonis saab eristada projekti dokumentatsiooni, teavet tarkvaraarenduse projektijuhtimise kohta ja süsteemiarenduse dokumentatsiooni (süsteemi dokumentatsioon).

Projekti dokumentatsioon peaks sisaldama põhjalikult vähemalt järgmisi andmeid:

- nõuded arendatavale süsteemile: nõuete kataloogi või kohustuslike tööde loetelu kujul
- otsuste alus organisatsioonisiseseks arenduseks või tellimustöö jaoks: otsuste alus, sh riskianalüüs, mis tõi kaasa hankelepingu, organisatsioonisisese arenduse või muu arendusvormi, peab olema küllaldaselt dokumenteeritud.
- hankeprotsessi dokumentatsioon: nii avalikele kui ka enamikule eraettevõtetest on ette nähtud hankelepingu kontrollitavus vähemalt sisekontrolli poolt.
- leping: kõikidest teenustest, tingimustest ja kokkulepetest tellija ja teenuseosutaja vahel tuleb kirjalikult kinni pidada.
- projekti protsessi dokumenteerimine: selleks, et lahendada mitte üksnes käimasoleva projekti raames, vaid ka hiljem tekkivaid küsimusi, on oluline dokumenteerida projekti protsess kontrollitavalt. See hõlmab vastutusalade, protokollide, projekti kohta tehtud otsuste, verstapostide, vastuvõtu ja kasutuslubade fikseerimist.

Süsteemi dokumentatsioon sisaldab arendusprotsessi dokumentatsiooni, sh

- süsteemi standard
- süsteemi arhitektuur ja projekt (protseduuriskeemid)
- liideste määratlused (sh asutusesiseselt kasutatud raamatukogud, arenduskeskkonnad ja muu tarkvara)
- kodeerimissuunised (nt nimeandmise põhimõtted, struktureerimissuunised jne)
- koodi kommentaarid
- konfiguratsiooni dokumendid
- muudatuste dokumendid
- kvaliteedi tagamise ja testide dokumendid (vt ka M 2.568 Tarkvara testimisprotseduurid)
- paigalduse ja kasutuselevõtu dokumendid, juhendid administraatoritele
- kasutusjuhendid kasutajatele.

Eriti siis, kui tahetakse süsteemi sertifitseerida (nt Common Criteria järgi), on soovitatav teha dokumentatsioonile sertifitseerimiseks esitatavad nõuded õige-

aegselt teatatavaks ja nendest kinni pidada. Hilisemad dokumendid võivad olla väga kulukad või sisaldada vigu.

Kontrollküsimused:

- Kas on olemas piisav projekti ja süsteemi dokumentatsioon?

M 2.575 Tarkvara arenduskeskkonna korrapärane turvaaudit

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: arendaja, arendusjuht

Töötajad või teenuseosutajad, kes ei kuulu arendusmeeskonda, peaksid läbi viima regulaarseid arenduskeskkonna ja ka testimiskeskkonna turvaauditeid. Seejuures tuleks kontrollida turbega seotud tegevusi arendusprojektide ja turvalise rakendamise oleku suhtes arenduskeskkonnas. Turvaaudit peaks põhinema määratletud ja dokumenteeritud eeskirjadel ja nendest kinnipidamist tuleb kontrollida. Kõik töötajad peaksid olema teadlikud turvalisusest, mis tugevdab infoturbe meetmete vajalikkust ja teeb selgeks, miks neid on vaja kasutada.

Auditi raames testitakse arenduskeskkonna turvalisust ja kontrollida tuleks vähemalt järgmisi aspekte:

- arendus- ja testimiskeskkonna ajakohasus (versioon, turvapaigad, uuendused, viirusetõrje ja tuntud turvaaugud)
- arendus- ja turvakeskkonna funktsioonid (nt konfiguratsioon ja kasutustingimused)
- juurdepääsupiirangud arendus- ja testimiskeskkonnale (volitatud ja volitamata kasutajad)
- juurdepääsupiirangud arendus- ja testimisandmetele (nt kood, asutusevälised lisatud raamatukogud ja kompileeritud tarkvaramoodulid)
- juurdepääsupiirangud muudele arenduse ja testimisega seotud andmetele, eriti kõrgendatud kaitsevajaduse korral (nt liideste dokumentatsioon või salajased funktsioonid).

Kontrollküsimused:

- Kas toimuvad tarkvara arenduskeskkonna regulaarsed turvaauditid?
- Kas toimuvad tarkvara testimiskeskkonna regulaarsed turvaauditid?

M 2.576 Turvapoliitika koostamine kohalike võrkude kasutamisele

Algatamise eest vastutavad: asutuse/ettevõtte juhtkond, infoturbeametnik

Rakendamise eest vastutavad: infoturbeametnik, asutuse/ettevõtte juhtkond

Kohalike võrkude kasutuselevõtu üks olulisemaid organisatoorseid ülesandeid on asjakohase turvapoliitika kavandamine ja sõnastamine. Kõnealune turvapoliitika peab kindlaks määrama kõik LAN-ide kasutamisele kehtestatavad turvasuunised.

LAN-ide turvaline ja nõuetekohane käitamine on tagatud üksnes siis, kui kavandamine, kontseptsioon ja käitamine on integreeritud olemasolevatesse turvatehnilistesse nõuetesse.

Olulised turbenõuded ja salvestilahenduse puhul nõutav turbeaste põhinevad asutuseülesel IT turvapoliitikal. Vajalikud nõuded tuleks sõnastada LAN-ide eraldi turvapoliitikana, et asutuse üldisi nõudeid saaks konkreetse valdkonna jaoks piisavalt täpsustada.

Turvapoliitikaks vajalike asjakohaste nõuete määratlemisel tuleb aluseks võtta kõikide LAN-is töödeldavate, edastatavate ja salvestatavate andmete kaitsevajadusi kajastav dokumentatsioon. Ainult vastava dokumentatsiooni abil on võimalik välja selgitada andmetele kehtivad erinevad kättesaadavus-, terviklus- ja konfidentsiaalsusnõuded ning tuvastada vajaminevate tehniliste ja töökorralduslike tööde maht.

Kuna LAN koosneb mitmesugustest IT-süsteemidest, tuleb LAN-i puhul arvesse võtta ka teisi turvapoliitikaid ja eeskirju ning kooskõlastada need kohalike võrkude turvapoliitikaga. Nimetada võib näiteks järgmisi:

- marsruuterite ja kommutaatorite turvapoliitika (vt M 2.279 Marsruuterite ja kommutaatorite turvapoliitika koostamine),
- turvalüüside turvapoliitika (vt M 2.299 Turvalüüsi (tulemüüri) turvapoliitika koostamine),
- VPNi kasutamise turvapoliitika (M 2.418 VPNi kasutamise turvapoliitika koostamine),
- jne.

Esimese asjana tuleks otsustada, kas konfigureerimise ja halduse üldstrateegia lähtub printsiibist „liberaalne” või „piirav”, kuna kõik edasised otsused sõltuvad suurel määral sellest valikust.

Alamvõrkude puhul, mis salvestavad ja töötlevad andmeid ainult tavalises turbeastmes, võib valida suhteliselt liberaalse üldstrateegia, mis lihtsustab paljudel juhtudel nende konfigureerimist ja haldamist. Siiski on ka niisugustel kasutusjuhtudel soovitatav, et strateegia oleks „ainult nii liberaalne kui parasjagu vajalik".

Kõrge kaitsevajadusega alamvõrkude puhul soovitatakse enamasti valida piirav strateegia.

Alljärgnevalt on esitatud mõned punktid, mida tuleb LAN-ide turvapoliitika puhul järgida. Aspektide puhul, mida kajastatakse kohustuslikus korras muudes dokumentides (nt turvapoliitikas), piisab asjakohasest viitest nendele dokumentidele.

LAN-ide planeerimist puudutavad ettekirjutused

Välja tuleb töötada ettekirjutused taristu jaoks, milles seatakse üles LANkomponendid (nt marsruuter ja kommutaatorid, turvalüüs, mälukomponendid, server). Ruumide taristu, milles LAN-komponente kasutatakse, peab olema sobiv, et tagada LAN-ide käideldavusnõuete täitmine (elektrivarustus ja kliimaseade). Samuti peab sissepääs nendesse ruumidesse olema piisavalt kaitstud. Asutusevälistele töötajatele tuleb kehtestada LAN-ile juurdepääsu (nt hoolduse eesmärgil) eeskirjad. Siinjuures tuleb kindlaks määrata, kuidas selliseid juurdepääse kontrollitakse ja protokollitakse.

Seevastu LAN-ide väga suurte käideldavusnõuete korral on kindlasti kohustuslik Single-Points-of-Failure (SPoFs) analüüsimine. Juhtudel, kus kõrge käideldavusega LAN-i soovitakse juurutada uusi komponente, tuleb nende tõrkevaba integreerimist kontrollida eelnevalt spetsiaalsetes katsetussüsteemides.

Administraatorite töökorraldus

Dokumenteerida tuleb põhimõtted, mille alusel antakse administraatoritele LANide üksikute komponentide haldamisvolitused. Selleks on soovitatav koostada eraldi töörollide kontseptsioon.

Määratleda tuleks administraatorite erinevad töörollid, millele antakse vastavalt nende tööülesannetele ka vajalikud õigused. Siinkohal on eriti oluline, et rutiinsete süsteemihaldusülesannetega seotud õigused (nt backup) oleks piiratud miinimumini.

Administraatorite kasutajanimed seotakse seejärel konkreetsete rollidega. Võimalike vigade vähendamiseks tohib administraatori kasutajanime alt töid teha vaid siis, kui see on ilmtingimata vajalik.

Administratiivseid juurdepääse tuleb kaitsta vähemalt tugevate paroolide (vt M 2.11 Paroolide kasutamise reeglid), või veel parem, mitmefaktorilise autentimise kasutamisega.

LAN-ressursside haldamine ja kontrollimine administraatorite kaudu on lubatud kas ainult kohapeal läbi otseühendusega konsooli, läbi eraldi haldusvõrgu või läbi krüpteeritud ühenduse. Administratiivsed juurdepääsud peaksid olema piiratud määratletud süsteemidega ja neid tuleks kontrollida nt turvalüüside kaudu. Eriti tuleb tugevdada IT-süsteeme, mida kasutatakse halduskonsoolidena või revisjoni jaoks (vt B 3.201 Klient).

Tööülesannete jaotamisega, ettekirjutuste ja eeskirjadega ning kõikide LAN-komponentide konfiguratsioonide dokumentatsiooni pideva täiendamisega tuleb tagada, et administraatoritel ei oleks võimalik algatada üksikute LANkomponentide juures protsesse või teha selliseid seadistusi, mille tagajärjel võiksid tekkida kas ebakõlad, tõrked või andmekaod. Olulised muudatused tuleb dokumenteerida. Seetõttu on soovitatav kasutada muudatuste haldamise protseduuri (vt B 1.14 Turvapaikade ja muudatuste haldus). Tuleb kindlaks määrata, kas teatud turvalisusega seotud muudatuste korral tuleb rakendada nelja silma põhimõtet.

LAN-komponentide installeerimise ja konfigureerimise nõuded

LAN-komponentide esmakordse installeerimise protseduur tuleb dokumenteerida. Pärast installeerimist tuleb kontrollida vaikesätteid turvariskide suhtes, inaktiveerida LAN-komponentide ebaturvalised teenused ning muuta ära standardsed kasutajanimed ja paroolid.

Süsteemikonsoolide juurdepääse üksikutele LAN-komponentidele tuleks lubada üksnes krüpteeritud ühenduste kaudu. Seadmetele juurdepääsuõigust omavate isikute ringi tuleb hoida võimalikult väiksena. Konsooli kasutamise ja konfigureerimise eeskirjad ning juurdepääsuliikide piirangud tuleb dokumenteerida. Tuleb reguleerida, kuidas koostada dokumendid (nt protseduurireeglid administratiivsete ülesannetega seotud kasutajatunnuste loomiseks, kasutusjuhendid igapäevatöös vajalikele töö- ja kontrolliprotseduuridele) ja kuidas neid hooldada ning millises vormis peaksid dokumendid olema. LAN-id tuleb sobivalt segmenteerida (vt M 5.61 Sobiv füüsiline segmenteerimine . M 5.62z Sobiv loogiline segmenteerimine ja M 5.77z Alamvõrkude rajamine).

Turvalise käitamise nõuded

LAN-süsteemi haldus tuleb muuta turvaliseks seeläbi, et haldamiseks vajalikud juurdepääsud leiavad aset üksnes spetsiaalsete ühenduste (eraldiseisev haldusvõrk) kaudu. Vajaduse korral tuleb leida sobivad tarkvaratööriistad, millega kasutada, hooldada ja integreerida LAN-komponente olemasolevas võrguhaldussüsteemis (vt B 4.2 Võrgu- ja süsteemihaldus). Nimetatud tööriistade jaoks tuleb välja töötada turvalise konfiguratsiooni nõuded. Võimaluse korral tuleks kasutada ainult krüpteeritud ühendusi ning inaktiveerida või keelata mittevajalikud liidesed ja teenused. Juhul kui soovitakse kasutada tootja pakutavaid kaughoolduse või kaugseire võimalusi, tuleb välja töötada nõuded juurdepääsude kaitseks. Ühenduse võib teostada näiteks VPN-i või eksklusiivsete, ainult selleks otstarbeks kasutatavate ühenduste kaudu. Peale selle tuleb kaugpöördused asutuse jaoks

kontrollitavalt protokollida. Lisateavet leiate meetmest M 4.80 Kaug-võrguhalduse turvalised pääsumehhanismid .

Asutus peab täpselt kindlaks määrama, kes on vastutav tarkvaravärskenduste käivitamise ja konfiguratsiooni muutmise eest. Protseduur tuleb dokumenteerida. Kui käideldavusnõuded on väga suured, tuleb muudatusi ja värskendusi pidevalt enne igapäevatöös kasutamist testida ja hinnata identses testimissüsteemis.

LAN-ide käitamise raames tuleb logida kõik haldamisega seotud tegevused.
Kui kaitsevajadus seda nõuab, peab andmete transportimine ja salvestamine toimuma krüpteeritult.

Eeskirjad andmevarunduseks LAN-is tuleb kooskõlastada asutuse üldise andmevarunduspoliitikaga (vt B 1.4 Andmevarunduspoliitika). Spetsiaalsete konfidentsiaalsusnõuete puhul tuleb varukoopiate tegemise suhtes rakendada kasutajaõiguste haldust.

LAN-i keskse tähenduse tõttu tuleb koostada hädaolukorra plaanid ning lisada need organisatsiooniülesele hädaolukorra haldusele. Kirjeldada tuleb revisjoni ja auditi vastutusi ja protseduure. LAN-ide revisjon tuleb integreerida asutuseülesesse revisjoni kontseptsiooni.

Kontrollküsimused:

- Kas kohalike võrkude kasutamise jaoks on koostatud vastav turvapoliitika?
- Kas turvapoliitikas käsitletakse LAN-ide planeerimise ja kontseptsiooni ning käitamise nõudeid?
- Millal toimus viimati turvapoliitika värskendamine?
- Kas LAN-ide turvapoliitika on integreeritud asutuseülesesse revisjonide ja auditite süsteemi ja kas asutus on määratlenud kokkupuutepunktid hädaolukordade haldusega?

M 2.577 Sobiva krüpteerimismeetodi valik võrkudele

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator

Kommunikatsioonivõrgud transpordivad andmeid erinevate IT-süsteemide vahel.

Andmete edastamine ühelt sidepartnerit teisele toimub väga harva eraldiseisva ja ainult selleks otstarbeks kasutatava sideühenduse vahendusel. Enamasti suunatakse andmed nende teekonnal läbi paljude vahepunktide. Selleks, et volitamata kolmandad isikud ei saaks edastatavaid andmeid pealt kuulata, kahjustada ega tehniliste vigade kaudu muuta, tuleb andmete kaitseks nende transportimisel või edastamisel kasutada sobivat krüptograafilist meetodit. Teabe tegeliku kaitse kõrval on oluline ka süsteemide omavaheline tuvastamine ja autentimine, kasutajate tuvastamine ja autentimine süsteemide poolt ja süsteemide tuvastamine ja autentimine kasutajate poolt.

Võrgupõhine andmete krüptograafiline kaitsmine võib toimuda OSI-etalonmudeli erinevatel kihtidel. Näiteks Layer 2-l võib teostada asukohapõhise võrgule juurdepääsu kontrolli LAN-i ja WLAN-i jaoks. Enne kui IT-süsteem (klient) saab juurdepääsu võrgule, peab see end registreerima autenturi juures (nt kommutaator, marsruuter või WLAN Access Point). Autentur kontrollib edastatud autentimisandmeid autentimisserveri abil ja annab olenevalt tulemusest võrgu-juurdepääsu.

Layer 3-l toimub andmete krüptograafiline kaitse tavaliselt IPSec-i ja IKE-ga.

IPSec pakub funktsioone krüpteerimiseks ja tervikluse kaitseks IP-suhtluse jaoks.

Kombineerides seda IKE-protseduuriga (Internet Key Exchange) saab rakendada ka automaatset võtmevahetust ja tunnelduse lõpp-punktide autentimist. Ka käsitsi võtmevahetust saab kaitsta IPSec-iga. Kasutajate autentimiseks tuleb seevastu kasutada teisi protseduure.

OSI-mudeli Layer 5–7-l toimub teabe krüptograafiline kaitsmine sageli SSL-i/TLSi, PGP, S/MIME-ga jne.

Olenemata valitud protseduurist, tuleb andmete kaitsmisel pöörata tähelepanu krüptograafilise protseduuri valimisele vastava kasutuseesmärgi jaoks, mis vastab tehnika tasemele ja millel ei ole teadaolevaid turvaauke (vt ka M 2.164 Sobiva krüptoprotseduuri valimine). Lisaks tuleb järgida nõudeid, mis on kirjas meetmetes M 2.46 Krüpteerimise õige korraldus ja M 5.68z Krüpteerimisprotseduuride kasutamine võrgusuhtluses .

Kontrollküsimused:

- Kas andmete kaitseks kasutatakse krüptograafilisi protseduure, mis vastavad tehnika tasemele?

M 2.578 Kohaliku võrgu paigaldamine, konfigureerimine ja hooldamine kolmandate isikute poolt

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: infoturbeametnik, IT-juht

Kui LAN-i paigaldab, seda konfigureerib ja hooldab asutuseväline teenuseosutaja, tuleb lisaks moodulis B 1.11 Väljasttellimine (Outsourcing) antud soovitustele võtta arvesse järgmisi punkte:

- kontrollida alati, et LAN-i installeerimine ei toimuks iseseisvalt. Selle jaoks tuleb läbi viia teostatavuse ja kulude kontroll.
- LAN-i turvapoliitika tuleb alati ise koostada ja seda ei tee kolmas osapool.

Sellega välditakse olukorda, kus asutuses ei tegelegi keegi põhjalikult LAN-i turvaaspektidega ja võimalust, et vajalikud turvameetmed unustatakse ära. Kui aga ei ole olemas asutusesiseseid ressursse, on mõistlik LAN-i turvapoliitika koostamiseks kasutada kolmanda osapoole nõustamist ja abi.

Kohaliku võrgu installeerimise, konfigureerimise ja hooldamise hanke korral tuleb kaasata infoturbespetsialist. Koostada tuleb üksikasjalik kohustuslike tööde loetelu. Seal tuleb määratleda kõik minimaalsed nõuded LAN-i komponentidele.

Teenuseosutajale tuleb esitada LAN-i turvapoliitika. Teenuseosutajat tuleb lepinguliselt kohustada turvapoliitikast kinni pidama ja seda rakendama. Tuvastamaks juba eos võimalikke probleeme, tuleb seda lepinguliselt kokkulepitud teenuste kasutamise korral ka regulaarselt kontrollida. Turvapoliitika peab olema kohustuslike tööde loetelu kindel osa.

Teenuseosutajal peaksid olema ulatuslikud ja soovitatavalt pikaajalised kogemused LAN-i ülesehitamisel ja kaitsmisel. Teenuseosutaja peab esitama vastavad soovitused ja neid tuleb vähemalt pisteliselt kontrollida.

Teenuseosutajale tuleb panna lepinguline kohustus, mille järgi tal pole õigust LAN-komponentide konfiguratsiooni, samuti paroole, ühendusevõtmeid, juurdepääsutunnuseid ega -mehhanisme volitamata isikutele edasi anda. Samuti tuleb teenuseosutajale panna kohustus, mille järgi tal puudub LAN-i ülesehitamisel võimalikult teatavaks saadud teabe ja andmete ajutise salvestamise ja volitamata isikutele edasi andmise õigus.

Enne LAN-i installeerimist teenuseosutaja poolt tuleb teostada vastavad testimissätted.Seejuures tuleb põhjalikult testida kõiki kavandatavaid turvaseadistusi.

Kui kohalikku võrku installeerib, konfigureerib või hooldab teenuseosutaja, tuleks tähelepanu pöörata sellele, et teenuseosutaja ei lisaks LAN-ile tagauksi. Teenuseosutaja peab kõik seadistused ja konfiguratsioonid täpselt dokumenteerima ja installeerimise lõpetamise järel täielikult tellijale üle andma.

Pärast LAN-i installeerimise lõpetamist tuleks teenuste nimekirja alusel teostada vastuvõtmine. Lisaks võib hindamise aluseks võtta kohustuslike tööde nimekirjas pärast üleandmist koostatud täitedokumendid, sest siin võib näiteks kindlaks määrata vastuvõtumõõtmiste protseduuri.

LAN-paigaldise vastuvõtmine peaks toimuma sõltumatu eksperdi abil, et lasta täpselt kontrollida ka tehnilisi üksikasju. Siia tuleb kaasata ka infoturbespetsialist.

Vastuvõtul tuleks keskenduda dokumentide täielikkuse ja võimalike ebakõlade kontrollimisele.

Kui LAN-i hooldab ka pärast installeerimist asutuseväline teenuseosutaja, tuleb ka siinjuures kohustada teenuseosutajat lepinguliselt mitte edastama teatavaks saanud andmeid, nagu paroole, tundlikke andmeid, konfigureerimissätteid jms volitamata isikutele. Samuti tuleks koos teenuseosutajaga koostada hädaolukorra ennetamise plaan (vt ka M 6.165 Hädaolukorra plaani koostamine kohaliku võrgu tõrke puhuks). Siinjuures tuleks iga võimaliku LAN-is tekkiva probleemi puhul täpselt kindlaks määrata selle raskusaste, reaktsiooniaeg, vastavad tööetapid ja isikud, keda hädaolukorra puhul teavitada.

Kontrollküsimused:

- Kas teenusosutajad on kohustatud kohaliku võrgu installeerimisel, konfigureerimisel või hooldamisel järgima LAN-i turvapoliitikat?
- Kas teenuseosutajaga koostati hädaolukorra ennetamise plaan probleemide puhuks LAN-is?

M 2.579 Kohaliku võrgu regulaarsed auditid

Algatamise eest vastutavad: asutuse/ettevõtte juhtkond, infoturbeametnik

Rakendamise eest vastutavad: infoturbeametnik, asutuse/ettevõtte juhtkond

LAN-i taristu kõikide komponentide puhul tuleb regulaarselt kontrollida, kas kõik määratletud turvameetmed on rakendatud ja õigesti konfigureeritud. Seejuures tuleks kõikidele osapooltele selgeks teha, et auditid on alati mõeldud kontrollimiseks, mitte süüdistuste esitamiseks.

Auditi tulemuste kajastamiseks võib koostada ka lihtsa võrdlustabeli, kus kõrvutatakse kehtestatud nõudeid ja hetkeolukorda. Aruanne peaks asjakohaselt ja lühidalt välja tooma eeskirjad (nt turvapoliitikast tulenevad nõuded) ja loetlema iga eeskirja kohta auditite käigus tehtud järeldused. Kui kehtestatud nõuetest leitakse kõrvalekaldeid ja abinõud on teada, tuleks need raportisse sisse viia.

Audiitorite sõltumatus

Auditeid peaksid läbi viima sõltumatud audiitorid, st töötav personal ei tohiks ennast ja oma tööd ise auditeerida. Audiitorid vajavad oma töö tegemiseks põhjalikke teadmisi LAN-i kohta ka siis, kui salvestisüsteemi administraatorid on neile auditeerimise käigus toeks. Vastavaid teadmisi tuleb regulaarselt asjakohaste koolitustega omandada ja täiendada. Audiitorid ei tohi teha võrgus muudatusi, seetõttu vajavad nad üksnes lugemisõigusi.

Neil juhtudel, kui asutus ei ole omalt poolt kehtestanud konkreetseid eeskirju, tuleks auditi käigus kontrollida vähemalt alljärgnevaid valdkondi:

- LAN-i tehnilise varustuse ja töökorralduslike reeglite kohta peab olema koostatud asjakohane turvakontseptsioon.
- Salvestatud andmete kaitsevajadusega kaasnevad nõuded käideldavusele ja konfidentsiaalsusele peavad olema kindlaks määratud ja dokumenteeritud, lähtudes kasutajate andmetest.
- Kasutuselevõtmisel asendatakse kõikide LAN-komponentide (server, marsruuter ja kommutaatorid, turvalüüsid, salvestilahendused, halduseks kasutatavad arvutid jne) standardsed paroolid.
- LAN-komponendid (server, marsruuter ja kommutaatorid, turvalüüsid, salvestilahendused jne) on üles seatud sobiva taristuga (elektritoide, kliimaseade) juurdepääsukaitsega ruumidesse.
- Administratiivsed juurdepääsud LAN-komponentidele toimuvad üksnes krüpteeritult või eraldi haldusvõrgu kaudu
- Haldusvõrk peab olema kaitstud tulemüüri, viirusetõrjetarkvara ning vajaduse korral ka IDS-iga.
- Haldamiseks tohib kasutada ainult turvalisi ühendusi (nt HTTPS, SSH).
- Andmeid edastatakse krüpteeritult ja salvestatult, kui see on kaitsevajaduse alusel nõutav.

- Logi peab olema korraldatud selliselt, et logis kajastuksid andmed veasituatsioonide ja väärkasutamise katsete kohta. Logiandmeid tuleb regulaarselt kontrollida.
- Aluskonfiguratsioon ja olulised hilisemad muudatused selle konfiguratsioonis peavad olema dokumenteeritud. Nii LAN-i loogilise kui ka füüsilise topoloogia kirjeldus on olemas ja ajakohane. Nimetatud dokumentatsioon peab olema kättesaadav ka hädaolukorras.
- Pärast võimalike muudatuste sisseviimist kontrollitakse vastavate LANkomponentide turvalisust puudutavad seadistused veelkord üle.
- Regulaarselt tuleb kontrollida, kas andmevarundusega seotud protsessid toimivad rikkevabalt ning kas salvestusvahendid on töökorras.

Kontrollküsimused:

- Kas LAN-i taristu kõikide komponentide puhul tuleb regulaarselt kontrollida, kas kõik määratletud turvameetmed on rakendatud ja kas LANkomponendid on õigesti konfigureeritud?

M 2.580 Võrgukomponentide kasutuselt kõrvaldamine

Algatamise eest vastutavad: infoturbametnik, IT-juht

Rakendamise eest vastutavad: infoturbeametnik, IT-juht

Kui LAN-i võrgukomponendid, nagu nt marsruuter või kommutaatorid, kõrvaldatakse kasutuselt või asendatakse, tuleb andmed, mida veel vajatakse, kas varundada või arhiveerida välisele andmekandjale või kanda need asendussüsteemile.

Pärast andemete varundamist tuleb kontrollida, kas kõik andmed on korrektselt varundatud. Lisateavet selle valdkonna kohta leiate moodulitest B 1.4 Andmevarunduspoliitika ja B 1.12 Arhiveerimine . Seetõttu tuleb kõik turvalisusega seotud andmed kustutada. Eriti kehtib see siis, kui komponendid satuvad pärast kasutusest kõrvaldamist kolmandate osapoolte kätte (nt müüakse edasi), kui seade vahetatakse garantiikorras välja või kui see toimetatakse kas tootjafirma või teenusepakkuja parandustöökotta ning isegi juhul, kui seadmeid kasutatakse mujal asutuse sees edasi või kui need saadetakse utiliseerimisele.

Olenevalt võrgukomponentide kasutusalast võivad need sisaldada nt järgmist teavet ja andmeid:

- konfigureerimisfailid, millest võib välja lugeda teavet asutuse võrgustruktuuri kohta,
- paroolifailid,
- logifailid, mis võivad sisaldada turbega seotud infot või isikuandmeid,
- sertifikaadid ja krüptograafilised võtmed (näiteks juurdepääsuks muudele IT-süsteemidele).

IT-süsteemide puhul tuleks kõvaketastel olevad andmed kustutada mõne sobiva rakenduse abil selliselt, et neid poleks enam võimalik taastada. Selleks ei piisa kõvaketaste uuesti vormindamisest, vaid need tuleb vähemalt üks kord täielikult üle kirjutada. Täiendavaid suuniseid leiate meetmetest M 2.13 Tundlike ressursside jäljetu hävitamine , M 2.167 Andmete kustutamiseks või hävitamiseks sobivate lahenduste valik ja M 2.433w Ülevaade meetoditest andmete kustutamiseks ja hävitamiseks .

Kui IT-süsteemi puhul on tegemist seadmega, võib kustutamine kujuneda raskemaks. Seadmete puhul sõltub protseduur sellest, kus ja kuidas andmed salvestatakse, kas näiteks sisseehitatud kõvakettale või püsimälusse. Paljud seadmed on varustatud tehaseseadete taastamisfunktsiooniga, mille abil on võimalik kõik konfiguratsiooni puudutavad seadistused lähtestada väärtustele, mis on seadmel tehasest väljudes. Pärast tehaseseadete taastamisfunktsiooni kasutamist tuleb siiski üle kontrollida, kas andmed on tõepoolest kustutatud ehk tarneseisundisse tagasi muudetud või on teatud andmed või failid siiski alles jäänud.

Võrgukomponentide puhul, kuhu on salvestatud eriti tundlikku turvalisusega seotud teavet, mille puhul ei ole piisavalt kindel, kas andmed tõesti turvaliselt kustutati, tuleb kõvakettad ja mälukiibid füüsiliselt vajaduse korral hävitada või muuta need kasutuskõlbmatuks.

Lisaks võrgukomponentidele salvestatud andmetele tuleb kontrollida, et tundlikke andmeid ei leiduks ka varukoopiate andmekandjatel. Kui pärast seadme kasutuselt kõrvaldamist ei ole tarvis varukoopiate andmekandjaid alles hoida, (säilitamisnõuded võivad tuleneda arhiveerimisvajadusest või seadustest), tuleks kustutada ka varukoopiate andmekandjad.

Sageli on võrgukomponentidele paigaldatud tähistused IP-aadresside, hosti nimede või muu tehnilise teabega. Ka need tähistused tuleb enne seadme kõrvaldamist eemaldada.

Eespool välja toodud soovituste alusel on soovitatav koostada kontrollnimekiri, mis tuleks kasutuselt kõrvaldamise protsessi käigus samm-sammult läbi töötada.

Selle abil saab vältida ka üksikute vajalike etappide unustamist.

Kontrollküsimused:

- Kas on tagatud, et enne võrgukomponentide kasutusest kõrvaldamist või väljavahetamist on salvestatud andmed varundatud või välistele andmekandjatele arhiveeritud või asendussüsteemile üle kantud?
- Kas on tagatud, et enne võrgukomponentide kasutusest kõrvaldamist või väljavahetamist on salvestatud andmed turvaliselt kustutatud?
- Kas on tagatud võrgukomponentide täielik füüsiline hävitamine, kui nendel salvestatud andmete turvaline kustutamine ei ole võimalik?
- Kui võrgukomponentide varukoopiate andmekandjad ei ole enam vajalikud, siis kas tundlikud andmed kustutatakse varukoopiate andmekandjatel turvaliselt?
- Kas võimalikud võrgukomponentidel olevad tähistused on enne kasutusest kõrvaldamist eemaldatud?

M 2.581 Haldusvõrgu ehitus võrguhalduse jaoks

Algatamise eest vastutavad: infoturbametnik, IT-juht

Rakendamise eest vastutavad: infoturbeametnik, IT-juht

Kõrgete turvanõuetega võrgusiseste ressursside haldamine ja seire peab olema piisavalt ette valmistatud. Võrgusiseseid ressursse tuleb vastavalt hallata ja jälgida, eelkõige kõrgema kaitsevajadusega süsteemide, nt aktiivsete võrgukomponentide puhul. Selleks kasutatav võrguhalduse süsteem peab olema asjakohaselt kaitstud.

Vajalike nõuete täitmiseks on tihti kõige ülevaatlikum, tõhusam ja majanduslikult soodsam lahendus, kui võrguhalduseks luuakse eraldiseisev LAN, mida kasutatakse eranditult üksnes haldusülesannete täitmiseks. Nimetatud haldusvõrku ühendatakse PC-d, mida kasutatakse ainult kriitilise tähtsusega komponentide haldamiseks.

Nimetatud võrgus tuleks haldamiseks kasutada ainult turvalisi protokolle (SSH-d Telneti ja HTTPS-i HTTP asemel). Kui haldusvõrgud eraldatakse tootmisvõrkudest vähemalt loogiliselt, veel parem, kui füüsiliselt, on mõeldav ka ebaturvaliste protokollide, eriti paljudes tootmiskeskkondades ikka veel peaaegu vältimatu SNMP versiooni 1 kasutamine.

Kontseptsioon/planeerimine

- Kõige lihtsam viis, kuidas hakata haldusvõrku üles ehitama, on võtta kasutusele eraldi kommutaator.
- Kõik administraatorite kliendid seotakse nende võrguliideste abil haldusvõrguga.
- Kõik kõrgema kaitsevajadusega serverid ja süsteemid (aktiivsed võrgukomponendid) varustatakse täiendava võrguühendusega, mis liidab need haldusvõrguga.
- Käitamistarkvara ja rakenduste haldusjuurdepääs seotakse serverites seal kus võimalik alati eraldi haldusvõrgu võrguaadressiga.

Haldusvõrgus tuleks kasutada privaatseid aadresse, nagu on sätestatud RFCstandardis 1918. Selliste aadresside marsruutimist „ametlikes" võrkudes ei toimu, mistõttu tuleb ühendust ametliku võrguga, juhul kui selle rakendamine on vajalik, kaitsta alati NAT (Network Address Translation) ja muude tulemüüri kasutamist nõudvate kaitsemeetmetega.

Haldusvõrgus peab kõikidel IT-komponentidel NTP serveri kasutamise või rakendamise kaudu olema tagatud ühtne kellaaeg (vt M 4.227 Lokaalse NTP

-serveri kasutamine aja sünkroniseerimiseks). Seeläbi kergendatakse logide analüüsimist ja võimaldatakse anda hinnanguid sündmustele, mille mõjusid on täheldatud mitmel erineval komponendil.

Tarvis on luua ülevaade saadaolevatest ressurssidest, mida on võimalik kasutada haldussüsteemi ülesehitamiseks. Siia alla kuuluvad nii personaliressursid, mis on vajalikud kontseptsiooni loomiseks ja elluviimiseks ning võrgu käitamiseks, kui ka selleks vajalikud rahalised vahendid. Tulemused tuleb sobilikul moel kirja panna.

Peale selle tuleb kontrollida, kas haldusvõrgus on tarvis rakendada täiendavaid seiremeetmeid. Näiteks on võrgu-ID-dega võimalik luua täiendav ülevaade sellest, kas võrgus leiab aset keelatud tegevusi või mitte.

Samuti võiks haldusvõrgus kasutada tsentraalset logimist, kus üks konkreetne instants toimib tsentraalse logiserverina ja haldab kõikide võrguga ühendatud komponentide logiandmeid. Esmalt tuleks välja selgitada, millisel kujul on tootmisvõrku ning selles asuvaid statsionaarseid servereid ja muid seadmeid (nt aktiivseid võrgukomponente, salvestisüsteeme) võimalik haldusvõrgu võrra laiendada.

Haldusvõrgu ehitamiseks tuleks läbi töötada meetmed M 2.139 Olemasoleva võrgukeskkonna läbivaatus ja M 2.140z Võrgu hetkeolukorra analüüsimine . Seejärel tuleks välja selgitada loodava haldusvõrgu nõuded seoses võrgus asetleidva kommunikatsiooniga ning määrata kindlaks tulevase võrgu kaitsevajadus.

Teostus

Proovikäitamise raames tuleb läbi viia kontroll, mille käigus testitakse rakendatavaid turvameetmeid ja luuakse alus vastava võrgu käitamiseks vajaliku dokumentatsiooni väljatöötamiseks. Tüüpilised kontrollküsimused on järgmised:

- Kas haldusvõrk on tootmisvõrgust läbivalt eraldatud?
- Kas kõikjal kasutatakse võimalikult turvalisi teenuseid (secure shell'i, httpsi)? Kas nende teenuste ebaturvalised variandid (telnet, http) on hallatavates seadmetes inaktiveeritud?
- Kas valdkondade kohta, kus ebaturvaliste teenuste kasutamisest ei ole võimalik loobuda, on olemas ülevaade ja asjakohane dokumentatsioon?
- Kas kõikide süsteemide, nagu serverite ja aktiivsete võrgukomponentide vaikimisi kasutajatunnused ja paroolid on muudetud?

Seejärel võib lahenduse tootmissüsteemis kasutusele võtta.

Kasutamine

Võrgu jooksva kasutamise ajal tuleb tähelepanu pöörata sellele, et võrgu, selle komponentide või õiguste juures tehtavate muudatustega ei kahjustataks haldusvõrgu turvalisust. Loodud logifaile tuleb regulaarselt analüüsida. Seetõttu tuleb ka kasutamise ajal kontrollida regulaarselt haldusvõrgu turvalisust (vt M 5.8 Võrgu regulaarne turvakontroll).

Kasutusest kõrvaldamine

Võrgukomponentide või muu riistvara väljavahetamisel, või isegi siis, kui need eemaldatakse haldusvõrgust parandustöödeks ainult lühikeseks ajaks, tuleb tagada, et sinna ei oleks salvestatud siseinfot (paroole, logiandmeid, sisedokumente jms).

Valmisolek hädaolukorraks

Hädaolukordadeks peab olema ette valmistatud plaan, mis tagab tootmisvõrgu jätkuva töö ka siis, kui haldusvõrgus peaks tekkima avarii.

Kontrollküsimused:

- Kas rakendatakse kaitstud haldusvõrku?
- Kas kõikidele haldusvõrgu komponentidele on tagatud ühtne kellaaeg?
- Kas haldusvõrgu proovikäitamise raames testitakse turbemeetmeid ning kas testimine ja tulemused dokumenteeritakse?
- Kas on olemas hädaolukorra plaan, et haldusvõrgu rikke korral saaks tootmisvõrk edasi töötada?

M 2.582 Võimalused haldusvõrgu loomiseks

Algatamise eest vastutavad: IT-turvaspetsialist, IT-juht

Rakendamise eest vastutavad: administraator

Haldusvõrk annab kasutada sideühendused võrgu ja süsteemihalduse süsteemi ning hallatavate komponentide vahel.

Selleks on olemas mitmesugused võimalused:

- Out-of-Band: ehitatakse eraldi füüsikaline haldusvõrk, mida kasutatakse üksnes võrgu- või süsteemikomponentide halduseks. See tähendab, et need ühendatakse täiendava võrguliidese kaudu haldusvõrguga.
- In-Band: võrgu- ja süsteemikomponente hallatakse olemasoleva (andme-)võrgu kaudu.
- Lokaalne: võrgu- või süsteemikomponente hooldatakse lokaalselt, nt konsooli kaudu.
- Segatud haldusvõrk: kriitilised võrgu- või süsteemikomponendid on ühendatud Out-Of-Band-haldusvõrgu kaudu ja muud võrgus olevad süsteemid In-Band-halduse kaudu.

Out-of-Band-haldus on kõige turvalisem, aga ka kõige kallim haldusvõrgu variant.

Selle eeliseks on nt aktiivsed võrgukomponendid, mille käideldavust on võimalik rünnata, nagu nt perimeertri marsruuterit. Ainult nii on võimalik Denial-of-Service-ründe korral suhelda võrgukomponentidega.

Suurte võrkude puhul soovitatakse kaaluda haldusvõrgu sobivat segmenteerimist, et anda näiteks võrguadministraatoritele juurdepääs üksnes sellele võrguosale, mille eest nad vastutavad.

Laialt on levinud In-Band-haldus, sest selle korral ei vajata võrgu- ega süsteemikomponentidel täiendavat võrku ega täiendavaid liideseid. Selle jaoks tuleks kaitsta haldussuhtlust, mis tagatakse vastava haldusprotokolliga.

Võrgu- või süsteemikomponentide lokaalset haldust üksinda on võimalik kasutada ainult väga väikestes võrkudes, ja ka siis üksnes põhjendatud erandjuhtudel.

Täpsemalt tuleb kaaluda IT-süsteemide haldust turvalüüsi DMZ-s (demilitariseeritud tsoonis) SNMP kui võrguhaldusprotokolli kasutamise korral. Turvalüüsi jaoks määratletud eeskirju ei tohi võrguhalduse korral leevendada.

Seda on kõige hõlpsam teostada, kui suhtluseks kasutatakse jälgitavate komponentidega Out-Of-Band-võrku.

Kui suhtlus toimub In-Band'is turvalüüsi kaudu, tuleb arvestada järgmisega:

- kuna asutusesiseses võrgus ei lubata sageli DMZ UDB-ühendusi, ei tule In-Bandsuhtlus UDP kaudu asutusesisese halduri ja DMZ komponentide vahel kõne alla.

Selliseks juhuks pakuvad erinevad tootjad võimalusi vahetada haldusteavet muude ühendusele orienteeritud protokollide kaudu. Ühtse standardi puudumise tõttu viidatakse siinkohal tootja jagatavale teabele.

M 2.583 Sobiva võrguhaldussüsteemi valik

Algatamise eest vastutavad: IT juht

Rakendamise eest vastutavad: administraator

Keerulise võrgu ja selle komponentide haldamiseks tuleks valida sobiv võrguhaldussüsteem.

Selleks tuleb kindlaks määrata võrgu hetkeolukord (vt M 2.139 Olemasoleva võrgukeskkonna läbivaatus), võrguhalduse kontseptsioon (vt M 2.143 Võrguhalduse kontseptsiooni väljatöötamine) ja selgitada välja nõuded võrguhaldussüsteemile (vt M 2.143 Võrguhalduse kontseptsiooni väljatöötamine).

Olenevalt hallatava võrgu suurusest võib selline ettevõtmine nõuda erinevaid lahendusi.

- Väikeste ja keskmiste võrkude korral võib võrguhaldust teostada üksikute tööriistade kogumikega või ka võrguhaldussüsteemiga.
- Suurte võrkude haldamiseks tuleks kasutada võrguhaldussüsteemi.

Seetõttu on õige võrguhaldussüsteemi valimine väga oluline. Soetatava süsteemi valimisel tuleks arvestada järgmiste valikukriteeriumitega:

Millised on toote poolt pakutavad funktsioonid?

1) Kulud

- tarkvara soetamiseks,
- täiendava riistvara soetamise kulud (mõningate süsteemide puhul on tarvis soetada üks või mitu tsentraalset haldusserverit),
- installeerimise ja kasutamisega seotud kulu (olenevalt olukorrast tuleb palgata eksperte väljastpoolt),
- töötajate koolituskulud,
- muud kulud (nt olemasoleva platvormi migratsiooni kulud, lokaalse tarkvara kohandamine/uusarendused, ehituslikud meetmed nagu nt turvalise serveriruumi ehitamine).

2) Investeeringukindlus

- Millisel määral on võrguhalduse toode skaleeritav (nt hallatavate komponentide arv)?
- Millised on vaadeldava lahenduseni viivad migratsiooniteed?
- Kuidas on olemasoleva lahenduse migratsiooniteed häälestatud mõne teise toote suhtes?

3) Teiste toodete integreerimisvõimalused

- Kas olemasolevat võrguhaldussüsteemi on võimalik integreerida?
- Kas olemasolevat andmevarundussüsteemi on võimalik integreerida?
- Millised kolmandate tootjate poolt loodud rakendused on selle toote puhul saadaval?

4) Usaldusväärsus ja töökindlus

- Kas on olemas teavet või koguni garantiisid maksimaalse seisakuaja kohta?
- Kas tsentraalsete komponentide puhul on võimalik kasutada hotswapfunktsiooni?
- Kas süsteemil on olemas oma backup- ja recovery- mehhanismid? Haldussüsteemi sees peavad olema mehhanismid korrapäraseks taaskäivitamiseks, mis hakkavad tööle võrguhaldussüsteemi äralangemise korral. See hõlmab muu hulgas võimalust varundatud andmete laadimiseks ja automaatseks järjepidevuse kontrolliks, mis ideaaljuhul peaks omakorda suutma lahendada ka tuvastatud ebakõlad.
- Kas tootele väljastatakse regulaarselt täiendusi? Kas nende lisamine on lihtne?

5) Turvalisus: haldusfunktsioonide juurdepääsude piiramine

- Kas haldusülesandeid on võimalik jaotada? Kas näiteks komponentide haldamist on võimalik piirata teatud valdkondade kaupa?

6) Turvalisus: võrguhaldus võrgu kaudu

- Kuidas kaitstakse kaugpöördusi?
- Kas kaugpöörduste puhul on võimalik kasutada krüpteeringut?
- Kas on tagatud, et enne kaugpöörduse teel läbiviidavat haldust toimub (tugev) autentimine?
- Kas õigust kaugpöörduse teel haldust teostada on võimalik siduda teatud kindlate isikute või rollidega?
- Kas kasutajat informeeritakse kaugpöörduste kohta automaatselt?

7) Turvalisus: andmete turvalisus, andmekaitse

- Kas kogutud andmed pannakse turvaliselt hoiule (juurdepääsupiirangud, krüpteerimine)?
- Kas halduskomponentide vahel aset leidev andmeside toimib turvaliselt (autentimine, krüpteerimine, tervikluse tagamine)?
- Kas viirusetõrjeprogrammide integreerimine on võimalik?
- Kas kogutud andmete liiki on võimalik reguleerida (anonüümseks muutmine, tagasiulatuv jälgimine, tõestatavus)?
- Millised on pakutavad logimisvõimalused?

8) Kasutajasõbralikkus

- Kas on olemas graafiline kasutajaliides?
- Kui lihtne on navigeerimine?
- Kas tootel on kohaliku keele või erinevate keelte tugi (globaalse kasutuse jaoks)?

- Kas toode informeerib kasutajat erandite ja hoiatuste kohta?
- Kas seirefunktsiooni on võimalik ka detailselt seadistada?
- Kas võrgukomponentide keerukus on piisavalt „peidetud” (selleks, et kasutaja ei peaks olema ilmtingimata iga hallatava komponendi ekspert)?
- Kas tootel on olemas veebiabi ja kasutusjuhendid?

9) Ergonoomilisus keerukate süsteemide haldamisel

- Kas erinevaid võrguprotokolle, võrgukomponente ja operatsioonisüsteeme toetatakse (nt marsruuteritega)?
- Kuidas käitub platvorm geograafiliselt jagatud süsteemidega ja kuidas toimub nende kuvamine?
- Kui lihtne on uute komponentide süsteemi integreerimine või nende süsteemist eemaldamine (autodiscovery, käsitsi)?

10) Vastavus standarditele (olenevalt keskkonnast võib olla vajalik, et toode vastaks vähemalt ühele standardile)

- Application Program Interface (API), nendeks juhtudeks, kui võrguhaldussüsteemi on tarvis ise laiendada.

Siin loetletud aspekte tuleks võtta kui haldussüsteemide hindamise pidepunkte.

Olenevalt kohalikest tingimustest tuleks kindlaks määrata nõuded võrguhaldussüsteemile, mis kaasatakse otsustamisele kui „K.O.-kriteeriumid”. Eespool nimetatud kriteeriumid tuleks seada tähtsuse järjekorda, mis peegeldaks kohalikest oludest tulenevaid eelistusi.

Võrguhaldussüsteemile esitatavaid nõudmisi ja välja valitud võrguhaldussüsteemi kasutusvõimalusi ei ole reeglina võimalik üksteisega täielikult kooskõlla viia.

Seetõttu tuleb eelnevalt koostatud võrguhalduse kontseptsioon pärast konkreetse toote väljavalimist vastavalt toote funktsioonidele ümber töötada.

Kontrollküsimused:

- Kas sobiva võrguhaldussüsteemi valik toimub varem kindlaks määratud nõuete alusel?

M 2.584 Võrgu- ja süsteemihaldustööriista eeskirjadekohane kasutusest kõrvaldamine

Algatamise eest vastutavad: andmekaitseametnik, infoturbeametnik
Rakendamise eest vastutavad: administraator

Võrgu- ja süsteemihaldustööriistas kogutakse, töödeldakse ja salvestatakse andmeid võrgu ja ühendatud süsteemide kaudu. Need andmed võivad mh hõlmata IP-aadresse, kasutajanimesid ja IT-süsteemide nimesid. Seetõttu tuleb tagada, et kui tööriist kasutusest kõrvaldatakse, ei oleks kõvakettal ja muudel andmekandjatel enam kaitsmist vajavaid andmeid. Enne andmekandjate edastamist, parandamist või kasutusest kõrvaldamist tuleb kõikidelt andmekandjatelt andmed turvaliselt kustutada.

Parandamise korral ei piisa ka üksnes kõvaketta vormindamisest või operatsioonisüsteemi kustutamisfunktsiooni kasutamisest. Need tuleb sobivate kustutamisprogrammidega nii üle kirjutada, et andmeid ei oleks võimalik enam taastada. Täiendavaid andmeid andmekandjate turvalise kustutamise ja hävitamise kohta võib leida meetmest M 2.167 Andmete kustutamiseks või hävitamiseks sobivate lahenduste valik . Kui andmekandjad tuleb ära anda ilma andmete turvalise kustutamiseta (nt parandamine, garantiiajal tootjale tagastamine), tuleb olenevalt andmete konfidentsiaalsusest hoida lepingutingimuste ja võimaluse korral kahjunõuetega ära soovimatud teabevood ja ründed. Vajaduse korral tuleb garantiinõuetest loobuda.

Kui võrgu- ja süsteemihaldustööriist kõrvaldatakse kasutusest, on soovitatav andmekandjad lisaks kustutamisele ka mehhaaniliselt hävitada („purustamine”).

Kui andmekandjaid ei ole võimalik kohe hävitada, tuleb neid kuni hävitamiseni kaitsta volitamata juurdepääsu eest. Magnetilisi andmekandjaid saab kustutada ka elektromagnetiliselt demagneetimisseadmega.

Kui andmekandjatel olevaid andmeid kustutavad kolmandad isikud, peab tellimus hõlmama muu hulgas ka andmekaitsega seotud nõudeid ja sõlmida tuleb tellimuse andmete töötlemise leping.

Kontrollküsimused:

- Kas on tagatud, et pärast võrgu- ja süsteemihaldustööriista kasutusest kõrvaldamist ei ole andmekandjatel kaitsmist vajavaid andmeid?

M 2.585 Identiteedi ja volituste halduse kontseptsioon

Algatamise eest vastutavad: infoturbametnik, IT-juht

Rakendamise eest vastutavad: infoturbeametnik, IT-juht

Selles meetmes kirjeldatakse, millised põhimõttelised etapid tuleb läbi viia identiteedi- ja volituste halduse raames. Asutuse äriprotsesside, teabe ja IT-süsteemide asjakohaseks kaitsmiseks on nõutav eesmärgipärane ja sobiv identiteedi- ja volituste haldus. Selle alusena peavad vastavas asutuses olema kindlaks tehtud seadusest tulenevad, töökorralduslikud ja tehnilised raamtingimused. Selle põhjal tuleb kindlaks määrata üldine protseduur üldiseks identiteetide ja volituste käsitlemiseks asutuse erinevates valdkondades.

Ikka ja jälle on tegemist tõsiste probleemidega, sest mõned kasutajad on kogunud endale mittevajalikke õigusi või on kustutamata kasutamata kasutajatunnused, nt pärast töötajate töölt lahkumist. Selle vältimiseks peab olema identiteedi- ja volituste halduse peamine eesmärk anda kõikidele seaduslikele kasutajatele alati täpselt need õigused, mis on nende vastavate ülesannete täitmiseks vajalikud (teadmistarbe ja minimaalõiguste põhimõtted). Selle jaoks on vaja selgelt määratletud protseduure ja turvanõudeid. Asutuses või ettevõttes on tavaliselt palju hallatavaid objekte ja kasutajaid. Seetõttu on mõistlik reguleerida identiteedi- ja volituste haldust tsentraalselt.

Volituste haldus peaks hõlmama volituste kõiki liike ja variante, mis on asutuses asjakohased, samuti pääsuõigusi. Volituste struktuur peaks kõikide äriprotsesside jaoks ja kõikidel süsteemidel olema võimalikult ühtne, samad rollid tuleks tähistada ka samade nimedega. Samuti tuleb kindlaks määrata, millisel kujul ja millise struktuuriga andmeid teatud identiteetidele edastatakse.

Ühe tähtsama punktina tuleb kindlaks määrata, millised ülesanded ja kohustused kellelgi identiteedi- ja volituste halduse raames on. Sageli hoolitseb ülesannete eest identiteedihalduse raames personaliosakond ja volituste halduse eest IT-osakond.

Kogu asutuse jaoks peab identiteedi- ja volituste halduse jaoks olemas olema üldine kontseptsioon, millest saab (vajaduse korral) tuletada sobivad eeskirjad üksikute valdkondade või süsteemide jaoks. Kontseptsioon peaks kirjeldama identiteedi- ja volituste halduse erinevaid ülesandeid ja etappe, mida tuleb kohandada üksikutele valdkondadele.

Siia alla kuuluvad järgmised komponendid:

- ülevaate koostamine identiteetide ja volituste rühmadest ja liikidest, mida

tavaliselt asutuse erinevates valdkondades hallatakse,

- nõuded identiteetide, kasutajatunnuste ja volituste haldamiseks,
- kasutajatunnuste, volituste ja autentimisvahendite käsitlemine kasutajate poolt,
- nõuded administraatorite, hädaolukorra likvideerijate ja teiste privileegidega kasutajate kasutajatunnuste käsitlemiseks ning nõuded ajaliselt piiratud juurdepääsu andmiseks laiendatud volitustele,
- volituste struktuuride, dokumentatsiooni ja kinnitamisprotseduuride kindlaks määramine volituste andmiseks,
- haldusprotsesside kindlaks määramine ja järgimine,
- nõuded sihtsüsteemide jaoks antavate volituste loomiseks ja nende piiratud eraldamiseks:

1. volituste regulaarne kontrollimine selle suhtes, kas kõikidel isikutel ja protsessidel on vajalikud volitused, et neid ei oleks liiga palju ega liiga vähe (teadmistarve ja minimaalõigused),
2. kõik volitused peavad olema ajakohased, nt ei tohi olla kasutajatunnuseid, mis ei ole enam aktiivsed, kuid mida ei ole kustutatud,
3. kasutajate volitused antakse otse sihtsüsteemidele, vältides identiteedi- ja volituste haldust.

Iga valdkonna kohta tuleb kõigepealt selgeks teha, milline on kaitstavate andmete ja äriprotsesside kaitsevajadus, millised on võimalikud ohud ja millised turvameetmed on juba olemas. Peale selle tuleb reguleerida, kes tohib andmeid ja äriprotsesse kasutada.

Suuniste koostamine

Identiteedi- ja volituste halduse kohta peavad olemas olema suunised, milles kirjeldatakse konkreetselt kõnealuse valdkonna või sihtrühmade (nt administraatorid, kasutajad, vastutavad spetsialistid) üksikuid ülesandeid ja protsessietappe.

See hõlmab järgmisi punkte:

- Kes vastutab identiteetide, kasutajatunnuste ja volituste haldamise eest?
- Kes võib volitusi anda?
- Mida peavad kasutajad teadma kasutajatunnuste, volituste ja autentimisvahendite õige käsitlemise kohta?

Peale selle peavad olemas olema nõuded konkreetse autentimise liigi ja teostuse kohta, nt paroolide valduse, teadmise või biomeetriliste omaduste autentimise liigi kohta ning minimaalsed nõuded paroolidele (vt M 2.11 Paroolide kasutamise reeglid ja M 2.220 Pääsu reguleerimise suunised).

Reguleerida tuleb ka seda, millised isikud, millisel moel ja millistele andmetele ligi pääsevad, nt ainult sisevõrgu kaudu või mobiilseadme ja töökoha vahel, ning millised IT-süsteemid on seejuures juurdepääsuks lubatud. Seejuures tuleb järgida konkreetseid raamtingimusi, nt olemasolevat turvapoliitikat ja seadusest tulenevaid nõudeid. Juba olemasolevad volituste kontseptsioonid tuleb konsolideerida

ja ühendada ühte üldisesse kontseptsiooni. Seejuures ei tohi unustada ka eraldiasuvaid rakendusi. Seetõttu on enamasti kasulik kasutada kasutajate ja õiguste haldamiseks mõeldud tööriistu.

Funktsioonide eraldamine

Identiteedi- ja volituste haldus peab ülesanded ja funktsioonid ning seega ka volitused asjakohaselt üksteisest eraldama, ja jaotama need erinevatele töötajatele seadusest tulenevate või töökorralduslike nõuete alusel (vt M 2.5 Vastutuse ja ülesannete jaotamine).

Rollide eraldamine

Isikutel võivad olla erinevad rollid. Seejuures peavad need rollid olema siiski töökorralduslikult ja tehniliselt selgelt üksteisest eraldatud, eriti erinevate turbenõuete korral. Vältida tuleks paljude turvalisuse seisukohast oluliste rollide koondumist ühe isiku kätte (nt haldamine ja kontrollimine, vt ka M 2.38 Administraatorirollide jagamine).

Volituste määramine, muutmine ja kustutamine

Identiteedi- ja volituste halduse tähelepanu keskpunktis on volituse määramine, muutmine ja kustutamine (vt M 2.586 Volituste andmine, muutmine ja äravõtmine).

Paroolide käsitlemine

Asutuses peab autentimismehhanismide rakendamine olema reguleeritud. Peale selle tuleb ka kasutajaid sellega tutvustada (vt nt M 3.63 Kasutajate koolitus autentimiseks kataloogiteenuste abil , M 4.1 IT-süsteemide paroolkaitse ja M 4.7 Algparoolide muutmine).

Igas asutuses peab olemas olema asjakohane protseduur identiteetide ja volituste käsitlemiseks. Seetõttu soovitatakse kasutada asjakohaselt meetme M 2.587 Identiteedi ja volituste halduse protsesside protseduur ja kontseptsioon üldisi protsesse.

Kontrollküsimused:

- Kas on kindlaks määratud, millised ülesanded ja kohustused on kellelgi identiteedi ja volituste halduse raames?
- Kas identiteedi- ja volituste halduse kohta on olemas vastav kontseptsioon?

M 2.586 Volituste andmine, muutmine ja äravõtmine

Algatamise eest vastutavad: infoturbametnik, IT-juht

Rakendamise eest vastutavad: administraator, infoturbeametnik

Asutuses tuleb ühele kasutajale anda mitmeid erinevaid volitusi ja neid ka hallata (vt M 2.6 Sissepääsuõiguste andmine , M 2.7 Süsteemi ja võrgu pääsuõiguste andmine ja M 2.8 IT-rakendustele ja andmetele pääsuõiguste andmine). Ülesannetel põhinevate volituste andmiseks ja haldamiseks on soovitatav välja töötada rollimudel iga vastava rakenduse või vastava süsteemi jaoks. See muudab haldamise ülevaatlikumaks ja lihtsamaks.

Kasutajatunnustel ja volitustel on oma elutsükkel, neid määratakse, muudetakse ja kustutatakse. Volitusi tuleks hallata tsentraalselt, seejuures on abiks asjakohased kasutaja ja õiguste haldusele mõeldud tööriistad, et vähendada kulutusi administreerimisele ja hooldamisele.

Volituste andmine ja muutmine

Kasutajatunnuste ja volituste andmise korral on sageli nõutav terve rida kinnitamisprotseduure, mis tuleb omavahel kokku viia ja mida tuleb järgida. Seetõttu on soovitatav kasutada selle jaoks standardiseeritud ja võimalikult automatiseeritud läbivaatamise ja määramise protseduuri.

Identiteedi- ja volituste halduse puhul võib vaadelda järgmisi üldisi rolle:

- Kasutaja: üksikisik, kes pääseb andmetele, rakendustele või IT-süsteemidele ligi kasutajatunnuse abil. Välja arvatud rühma kasutajatunnused, on kasutaja tavaliselt identne omanikuga.
- Kinnitaja: isik, kes kinnitab pääsuõiguste andmise, tavaliselt vastutavad spetsialistid. Kinnitaja ei tohi kinnitada õigusi iseenda jaoks.
- Vastutav spetsialist: andmete, rakenduste, tööprotsesside, äriprotsesside või süsteemide „omanikud". Neil on viimane sõna kõikides küsimustes, mis puudutavad sisusid ja kasutamist ning vastavate andmete, rakenduste või süsteemide nõudeid.
- IT-osakond: sealsete töötajate ülesanne on kinnitatud volitused tehniliselt ellu viia.

Üldiselt tuleks kasutajatunnuseid ja volitusi anda alati seadusest tuleneva vajaduse alusel määratud tegevuste täitmiseks, st nii, nagu see on vajalik tööülesannete täitmiseks (teadmistarbe põhimõte). Peale selle tuleks volitused anda alati piirangutega. Väljastada tohib alati üksnes nii palju õigusi, kui tegelikus kontekstis erialaste ülesannete täitmiseks vaja (minimaalõiguste printsiip).

Enne uute kasutajatunnuste loomist või volituste andmist tuleb silmas pidada järgmist:

- Tuleb esitada taotlus, millest selgub taotluse esitaja roll, funktsioonide ulatus ja ka taotluse esitaja ülesannete ajalised piirangud. Soovitatav on esitada taotluste vormid, et kajastatud oleks kogu vajalik teave (vt M 2.30 Kasutajate ja kasutajarühmade määramise protseduurid). Selleks võib kasutada

ankeete, veebiblankette või e-kirju. Taotlusi peab olema lihtne esitada ja töödelda, aga need peavad sisaldama ka kogu nõutavat teavet.
- Taotlus tuleb kinnitada volitusele vastava rolli liigi kohaselt. Privileegidega kasutajatunnused peavad täiendavalt kinnitama vastava ressursi vastutavad spetsialistid.
- Kõik volituste määramised, muutmised ja kustutamised tuleb säilitada dokumenteeritult.
- Iga kasutajatunnuse peab saama siduda üheselt ühe registreeritud kasutajaga. Samuti peab iga rühma kasutajatunnuse puhul olema üheselt tõestatav, millised isikud sinna rühma kuuluvad. Iga rühma kasutajatunnuse jaoks peab olema nimetatud isik või rolliomanik, kes vastutab kasutajatunnuse kasutamise eest.
- Enne kui isikule antakse kasutajatunnus või autentimisvahend, nagu parool, tuleb seda isikut kohustada kinni pidama kõikidest turvanõuetest ja -eeskirjadest.
- Esmaseks sisselogimiseks antud parooli peab kasutaja esimesel sisselogimisel ära muutma (vt M 2.11 Paroolide kasutamise reeglid).
- Tagatud peab olema, et parooli lähtestamist või autentimisvahendi kohandamist saavad taotleda ainult volitatud kasutajad.

Kui see raskendab rühmas tegutsevate isikute jaotust, tuleks võimaluse korral vältida rühma kasutajatunnuste loomist. See kehtib eelkõige administratiivsete kasutajatunnuste ja turvalisusega seotud valdkondade kohta.

Kui vajatakse juurdepääsu andmetele ilma kasutajatunnuse omaniku nõusolekuta, peab selle juurdepääsu kinnitama nii volitatud kinnitaja kui ka infoturbeametnik. Selline juurdepääs tuleb dokumenteerida ja omanikku sellest teavitada.

Volituste äravõtmine

Kui töötajad lahkuvad asutusest või vahetavad ametikohta, tuleb mittevajalikud kasutajatunnused ja volitused kindlaksmääratud aja jooksul sulgeda ning määratletud ooteaja järel täielikult kustutada. Seejuures võib olla kasulik volitused küll kustutada, kuid dokumentidesse kirja panna, mis ajast mis ajani olid kõnealusel kasutajatunnusel millised volitused, et tegevusi oleks võimalik kontrollida ka pärast töötajate lahkumist. Oluline on, et volitusi muudetaks või eemaldataks järjekindlalt.

Kasutajatunnuste ja autentimisvahendite äravõtmise või lukustamise võimalused on näiteks kasutajatunnuste inaktiveerimine, paroolide muutmine ja töötõendite äravõtmine. Peale selle tuleb kasutajatunnus eemaldada rollide jaotusest ja rühmadest. Selle eeldus on, et volituste halduse eest vastutavat osakonda teavitatakse kohe, kui töötajad lahkuvad. Vajaduse korral tuleb lisada vastav punkt personaliosakonna asjakohasesse kontrollnimekirja.

Soovitatav on kasutajatunnused kõigepealt üksnes inaktiveerida (nt 30 päevaks), et neid oleks vea korral võimalik hõlpsasti uuesti rakendada. Kõik kasutajatunnused ja nendega seotud andmed tuleb siiski keskmiselt nt 90 päeva jooksul pärast töötaja lahkumist tootmissüsteemidest eemaldada. Selleks et tagada seal salvestatud andmete ja tegevuste kontrollitavus pikemaks ajaks, tuleks andmed kopeerida mõnda teise piirkonda, nt arhiivisüsteemi, sidudes need sobiva omanikuga (nt audit).

Kontrollküsimused:

- Kas kõik kasutajatunnused ja volitused on väljastatud üksnes tegeliku vajaduse alusel?
- Kas personalimuutuste korral muudetakse mittevajalikud kasutajatunnused ja volitused kasutamiskõlbmatuks?
- Kas elluviidavad volituste muudatused dokumenteeritakse?

M 2.587 Identiteedi ja volituste halduse protsesside protseduur ja kontseptsioon

Algatamise eest vastutavad: infoturbametnik, IT-juht

Rakendamise eest vastutavad: IT-juht, infoturbeametnik

Identiteetide ja volituste haldus muutub suureneva kasutajate arvu tõttu üha kulukamaks. Mida suurem on vajadus käsitsi tegevuste järele, seda rohkem võib tekkida vigu ja turvalisusega seotud probleeme. Seetõttu on soovitatav, et ka väiksemad asutused seaksid sisse identiteedi ja volituste halduse ning kasutaksid seda. Alljärgnevalt kirjeldatakse identiteedi ja volituste halduse üldisi protsesse, mis näitavad, kuidas täita vajalikke ülesandeid ja nõudeid.

Identiteedi- ja volituste haldus koosneb järgmistest üldistest protsessidest:

Asutuse turvakontseptsioonist tulenevalt peaksid identiteedi- ja volituste haldusega seotud nõuded olema kirja pandud vastavas suunises. Suunis peaks hõlmama vähemalt nõudeid selle kohta, kuidas määrata, muuta, kustutada ja kontrollida identiteete, kasutajatunnuseid ja volitusi.

Igas asutuses peab olemas olema asjakohane protseduur identiteetide ja volituste käsitlemiseks. Seetõttu soovitatakse asutuses asjakohaselt tõhusa identiteedi ja volituste halduse jaoks luua alljärgnevalt kirjeldatud meetmete üldistes protsessides sisalduvad ülesanded.

Suuniste haldamise protsess

Suuniste haldamise protsessi raames luuakse suunised rollide ja (ühekordsete) volituste taotlemiseks, muutmiseks ja äravõtmiseks ning identiteetide ja kasutajakontode halduseks IT-süsteemides ning kontrollitakse ja täiendatakse neid.

Identiteedi- ja volituste halduse suunises kirjeldatakse järgmiste protsessiosade protseduure ja seda, kuidas need omavahel kokku sobima peaksid:

- identiteediprofiilide haldamine,
- volituste profiilide haldamine,
- kasutajatunnuste haldamine,
- rollide haldamine,
- identiteetide ja volituste analüüs ning
- kontode haldamine.

Volituste andmised, muutmised ja kustutamised tuleb protokollida ja andmeid kindlaks määratud aja jooksul (nt 10 aastat) säilitada. Suunised tuleks oluliste muudatuste korral või teatud aja järel üle vaadata.

Identiteediprofiilide haldamise protsess

Identiteediprofiilide haldamise protsess hõlmab identiteediprofiilide loomist, muutmist ja kustutamist. Identiteediprofiilid on näiteks asutuse töötajate algandmed.

Tavalised töödeldavad andmed on muu hulgas järgmised:

- nimi,

- organisatsiooni allüksus,
- ülesande kirjeldus.

Identiteedi haldamise protsessis algatatakse teabe töötlemine taotluste vormis (vt M 2.30 Kasutajate ja kasutajarühmade määramise protseduurid). Taotlused sisaldavad olulisi andmeid töötaja kohta (kehtib ka IT-süsteemide puhul) ja vastavat tööülesande kirjeldust. Taotlusi võib algatada ka nt töötaja töölevõtmise protsessis või tööülesande kirjelduse muutmise korral (nt töötajale antakse uus tööülesanne). Muudatused dokumenteeritakse identiteediprofiilis.

Identiteediprofiilide haldamise protsessi tulemus on identiteediprofiili loomine algandmete ja konkreetse tööülesande kirjeldusega. Asutuses peab olema reguleeritud, kes algatab volituste andmise ning kogu protsessi käik tuleb dokumenteerida.

Alljärgnevalt nimetatakse asutuse osakonnad, kus võib toimuda uue identiteediprofiili loomine või identiteediprofiilide muutmine:

- töötajate või kolmandate isikute töölevõtmine, töölt lahkumine, tööülesannete muutmised (personaliosakond, haldus, erialaosakond),
- asutusevälised töötajad / töölevõtmine, töölt lahkumine, muutmine (ostu-, hankeosakond),
- volitatud kolmandad isikud, nt kliendid / tulemine ja lahkumine, muutmine (müügiosakond, kasutajatugi jne).

Identiteetide ja volituste analüüsi protsessis kontrollitakse identiteete taotluse alusel kaitsevajaduse suhtes. Suunise haldamise protsessis reguleeritakse raamtingimused identiteetide loomiseks ja muutmiseks. Identiteetide ja volituste analüüsi ning suunise haldamise protsessidest saadud tulemustega saab taotluse alusel luua, muuta või kustutada andmeid. Loodud või täiendatud identiteediprofiili andmed edastatakse taotlusega edasiseks töötlemiseks kasutajaprofiili haldamise protsessi.

Volituste profiili haldamise protsess

Volituste profiili haldamise protsessis kirjeldatakse meetodit, et võrrelda töötaja tööülesande kirjeldust, mis loodi identiteediprofiili haldamise protsessis, ning sinna juurde kuuluvaid rolle ja ühekordseid volitusi. Võrdlemise protseduuri jaoks vajatakse volituste profiili haldamise protsessis mitmesugustest allikatest erinevaid andmeid identiteediprofiilide kohta, nt töötaja algandmeid personalihaldusest või erialaste ülesannete andmeid osakondadest. Siia kuuluvad ka võrreldavad andmed asutuseväliste töötajate kohta ja IT-süsteemide tehnilised õigused.

Töötaja volituste profiilis hallatakse kõiki rolle ja ühekordseid volitusi, mis sinna alla kuuluvad. Rollidel põhinevate volituste ja ühekordsete volituste vaheline

suhe on kvalitatiivne ja kehtib seega ka IT-turbe kohta. Kogemused on näidanud, et puhas rollidel põhinev volituste määramine on liiga jäik ja seetõttu ei toimi. Seevastu nõuab liiga suur hulk ühekordseid volitusi liiga suuri kulutusi hooldusele. Praktikast saadud kogemuste põhjal soovitatakse, et rollidel põhinevate volituste ja ühekordsete volituste suhte sihtväärtus oleks 80 : 20.

Tuleb uurida, kas ülesandeid ja sinna juurde kuuluvaid volitusi on võimalik üksteisega ühendada (identiteetide ja volituste analüüsi protsess) või vajaduse korral uuesti ümber jaotada (vt M 2.5 Vastutuse ja ülesannete jaotamine).

Rollide haldamise protsess

Rollide haldamise protsessis määratakse üksikute rollide jaoks volituste profiilid. Rollid koondavad enda alla ülesanded, vastutused ja nendega kokku kuuluvad volitused, et kergendada kasutajate haldust. Üht rolli-volituste profiili võib kasutada paljude töötajate sama tegevuse jaoks. Selleks antakse rollile pääsuõigused, mis on vajalikud tööülesande täitmiseks. Rollid peaksid olema määratletud modulaarselt ja piiritletult, et neid oleks võimalik mis tahes viisil kombineerida. Rollide kärpimine tuleb kooskõlastada vastutava spetsialisti tasandil.

Põhimõtteliselt koosneb rollide haldamise protsess kahest tasandist. Vastutava spetsialisti tasandil määratletakse rollid ja administratiivsel tasandil määratakse nendele rollidele volituste profiilid, muudetakse ja kustutatakse neid.

Suuniste haldamise protsessis antakse juhised rollide loomiseks. Identiteedi-profiilide haldamise protsessi ja rollide haldamise protsessi vahel toimub töötajate tööülesannete profiilide ja tegelikult määratud rollide võrdlemine (kavandatud ja saavutatud eesmärgi võrdlus). Kasutajate haldamise protsessis määratakse töötajate rollide jaotus, kustutatakse või muudetakse neid. Rollide haldamise protsessis koondatakse ühekordsed volitused kontohalduses ühe kasutajakonto jaoks üheks volituste profiiliks. Profiilide turvalisuse analüüsimise protsessis uuritakse rolle ja liigitatakse need vastava kaitsevajaduse alusel.

Kasutajatunnuste haldamise protsess

Kasutajatunnuste haldamise protsessis kirjeldatakse protsesside operatiivset osa identiteedi ja volituste halduses ning see hõlmab kasutajatunnuste, esialgsete paroolide ja volituste määramist, kustutamist ja muutmist.

Üldised toimingud on nt

- uued töötajad,
- uute kasutajatunnuste määramine,
- töötajate töölt lahkumine,
- tööülesannete muutmine,
- kasutajatunnuste lukustamine pikema äraoleku korral,
- kasutajatunnuse kustutamine.

Toimingu „Uued töötajad" raames tuleb luua kasutajatunnus, anda välja algne parool, koostada töötaja algandmed, peab toimuma määramine organisatsiooni üksusesse ja rollide ning volituste määramine. Uus seadistamine toimub ka täiendavate kasutajatunnuste loomiseks.

Toiming „Töötajate töölt lahkumine" hõlmab vastava töötaja kõikide määratud rollide ja volituste kustutamist ning vajaduse korral autentimisloa tagastamist.

Toiming „Tööülesannete muutmine" hõlmab organisatsiooniüksuse vahetamist, projektide juures töö alustamist ja lõpetamist ning muid vastava tähtajaga tööülesannete muutmisi. Mõnede volituste määramine võib olla vajalik enne või pärast toimunud ülesannete muutmist.

Toiming „Kasutajatunnuste lukustamine pikema äraoleku ajal" toimub töötajate pikema äraoleku korral, nt lapsehoolduspuhkus või taastusravi. Volitused jäävad selle ajavahemiku jooksul alles.

Toiming „Kasutajatunnuse kustutamine" hõlmab kasutajatunnuse, sh kõikide algandmete ja volituste täielikku kustutamist.

Kõik kasutajatunnused peavad olema üheselt määratud töötajale kui kasutajatunnuse omanikule. Rühma ja süsteemi kasutajatunnuste korral peab olema nimetatud vähemalt üks vastutav isik.

Töötajatel võib olla mitu kasutajatunnust. Tuleb selgeks teha, kas

- kasutajatunnused on eraldatud,
- kasutajatunnused on eraldatud, aga neid on võimalik ühendada või
- kasutajatunnused on ühendatud.

Igal juhul tuleks automaatselt kontrollida, kas on olemas topeltkirjed (dubletid). Sellised kirjed toovad kaasa läbipaistvuse puudumise identiteedi ja volituste halduses.

Alljärgnev kirjeldus näitab kasutajatunnuste haldamise protsessi koos vastavate liidestega. Kasutajaprofiilide haldamise protsessis toimub töötajate ülesannete ning vastavate rollide ja volituste vastendamine. Kasutajatunnuste haldamise protsessis toimub volituste loogiline määramine ülesande jaoks IT-süsteemide sees. Suuniste haldamise protsess hõlmab raamtingimuste seadmist, kuidas toimub volituste määramine IT-süsteemides. Kasutajatunnuste haldamise protsessi lõpuks on olemas loodud või muudetud kasutajatunnus koos vastavate volitustega.

Abiprotsessid

Kasutajatunnuste haldamise protsessis kirjeldatakse abiprotsesse kasutajatunnuste haldamise protsessi läbiviimiseks. See hõlmab peamiselt IT-ga seotud tegevusi.

Kasutajatunnuste haldamise protsess hõlmab järgmisi alamprotsesse:

- kasutajatunnuste andmise, muutmise, lukustamise ja kustutamise dokumenteerimine,

- paroolide taastamine, kasutajatunnuste lukustusest vabastamine,
- kasutajatunnuste/logiandmete auditeerimine.

Kasutajatunnuste andmise, muutmise, lukustamise ja kustutamise dokumenteerimine

Ühekordseid volitusi ja kasutajatunnuseid tohib anda, kustutada ja muuta ainult siis, kui selleks on olemas seaduslik taotlus. See tuleb dokumenteerida. Käsitsi toimuva administreerimise korral peaksid ülesandeid protsessi sees teostama vähemalt kaks vastutavat isikut ja seeläbi üksteist vastastikku toetama ning kontrollima.

Paroolide taastamine, kasutajatunnuste lukustusest vabastamine

See alamprotsess hõlmab parooli taastamise ja kasutajatunnuse lukustusest vabastamise tegevusi ning kasutajatunnuse ja parooli konfidentsiaalset edastamist kasutajale. Siin peab olema tagatud, et oma paroolide taastamist või autentimisvahendi kohandamist saaksid taotleda ainult volitatud kasutajad.

Kasutajatunnuste/logiandmete auditeerimine

Üksikute kasutajatunnuste volituste lubatavust tuleks regulaarselt kontrollida. Kasutajatunnuste andmise, muutmise, lukustamise ja kustutamise alamprotsess annab selleks vajalikke andmeid. Turvalise identiteedi- ja volituste halduse juurde kuulub pääsulogide regulaarne hindamine. Tuleb uurida, kas süsteemis on aktiivsed üksnes lubatud kasutajatunnused. Siinjuures on abiks aktiivsete kasutajatunnuste ja kinnitatud kasutajatunnuste automaatne võrdlemine. Vajaduse korral võib analüüsida täiendavaid aspekte. Turvaintsidendi kahtluse korral on nõutav süstemaatiline hindamine. Kui töötajad on saanud õiguse töödelda iseseisvalt algandmeid ja paroole, tuleb tagada, et nad pääseksid ligi ainult oma andmetele.

Identiteetide ja volituste analüüsi protsess

Identiteetide, kasutajaprofiilide ja rollide esmakordseks loomiseks või muutmiseks tuleb järgida taotletavat turbeastet. Identiteetide, volituste profiilide ja rollide esmakordseks loomiseks, muutmiseks ja tagasivõtmiseks peaks olemas olema kindel protseduur, mis arvestab andmete kaitsevajadusega. Mida suurem asutus, seda rohkem on hallatavaid identiteete, kasutajaprofiile ja rolle ning seda olulisem on kontrollitav, formaalne protseduur.

Protsessi käigus vaadatakse läbi järgmised teabeallikad:

- rollide haldamise protsessi rollid,
- volituste profiilide haldamise protsessi volituste profiilid,
- identiteediprofiilide haldamise protsessi identiteediprofiilid.

Tulemused edastatakse täiendavaks töötlemiseks algprotsessidele

Identiteetide ja volituste analüüsi protsessi tulemusena reguleeritakse, kes ja millises ulatuses ning milliseid andmeid ja IT-rakendusi võib kasutada, nt võivad volitused olla jaotatud mitme kasutajatunnuse vahel (vt ka M 2.5 Vastutuse ja

ülesannete jaotamine). Selleks, et otsustada, kas hangitud või antavad volitused on taotletava turbeastme jaoks asjakohased, peavad vastavad vastutavad spetsialistid analüüsima kõiki andmeid, IT-süsteeme ja teenuseid (vt M 2.217 Teabe, rakenduste ja süsteemide hoolikas liigitamine ja käitlus).

M 2.E12 E-ID rakendusjuhiste järgimine

Algatamise eest vastutavad: turvajuht või IT juht

Rakendamise eest vastutavad: IT juht

Igas asutuses, kus kasutatakse ID-kaardi/PKI lahendusi, tuleb järgida üldisi avalikke E_ID rakendusjuhiseid. Need on toodud aadressil https://eid.eesti.ee/index.php/EID_rakendusjuhend, kuhu ilmuvad vajadusel ka vastavad täiustused. Asutuse IT juht peab tagama, et kõik lahendusi seadistavad inimesed oleksid nimetatud juhistega kursis ning täidaksid neid. Probleemsetel kohtal, kus millegipärast on teatud (nt arhitektuurilistel) põhjustel vaja mõningates juhistest taganeda, tuleb tekkivad riskid asutuse infoturbejuhiga läbi arutada ning saada erandile turvajuhi kirjalik nõusolek.

Kontrollküsimused:

- Kas kõik asjassepuutuvad inimesed on nimetatud juhenditega kursis?
- Kas juhendeid tehtavad üksikud erandid on kartud põhjaliku riskianalüüsiga ning saanud turvajuhi kirjaliku kinnituse?

M 2.E13 Asutusesisesed reeglid ID-kaardi/PKI kasutamiseks

Algatamise eest vastutavad: turvajuht või IT juht

Rakendamise eest vastutavad: IT juht

Igas asutuses, kus kasutatakse ID-kaardi/PKI lahendusi, peavad olema kirjalikult fikseeritud reeglid nende kasutamiseks, **mis vastavad alljärgnevatele tingimustele:**

- Iga infosüsteemi ja selle komponendi täpsusega tuleb fikseerida, milliseid ID-kaardi/PKI lahendusi ning millises rollis ja konfiguratsioonis seal kasutatakse.
- Iga kasutaja (kasutajarolli) ja iga vahendi (ID-kaart, mobiil-ID, digi-ID) täpsusega tuleb fikseerida milliste teenuste juures (turvaline autentimine, signeerimine, transpordikrüpto vormingus krüpteerimine, uksekaardina kasutamine jms) on nad kasutatavad.
- Reeglid tuleb kindlasti välja töötada asutuse IT juhi ja turvajuhiga koostöös ning nimetatud isikud peavad need ka kirjalikult kinnitama. Lisaks peavad asutuse IT juht ja asutuse turvajuht kinnitama kõik nimetatud reeglite olulised muutused, mille käigus muudetakse kasutatavaid lahendusi, pääsude olemust või kasutajarolle ja/või nende õigusi.

Reeglid peavad vastama e-ID rakendusjuhistele, mis on toodud aadressil http://eid.eesti.ee/index.php/EID_rakendusjuhend (vt M 2.E12 E-ID rakendusjuhiste järgimine):

- Nimetatud reeglid peavad olema kooskõlas vastavate tehniliste lahenduste dokumentatsiooniga. Suure osa ID-kaardi/PKI lahenduste tehnilisest dokumentatsioonist leiab Sertifitseerimiskeskuse ASi poolt hallatavalt ID-kaardi lahenduste veebilehelt http://www.id.ee/.
- Reeglites tuleb kindlasti sätestada ka nende reeglite ning ID-kaardi/PKI lahenduste alane koolitus ja teavitus. Koolitus ja teavitus on turvajuhi või tema poolt määratud isiku kohustus ning peab hõlmama kõiki rolle, kes nimetatud lahendustega kokku puutuvad (vt M 3.E2 Töötajate koolitus ID-kaardi/PKI lahenduste kasutamise osas).

Toodud reeglid võib koostada eraldiseisva dokumendina või konsolideerida teiste normdokumentidega, nt asutusesisese IT vahendite kasutamise korraga. Võimaliku konsolideerimise otsustab IT juht või tema poolt määratud isik koostöös turvajuhiga.

Kontrollküsimused:

- Kuidas on tagatud ID-kaardi/PKI kasutusreeglite vastavus asutuse üleüldise IT poliitkaga ja IT turvapoliitikaga? Kes seesuguse kooskõla ja vastavuse eest vastutab?
- Kas nende reeglite koostamisel on vajalik kasutada ka välist oskusteavet/eksperte?
- Kas oleks mõistlik kaaluda ka reeglidokumendi (sh selle muudatuste) kinnitamist asutuse juhi poolt?

M 2.E14 Digitempli turvaline evitamine asutuses

Algatamise eest vastutavad: IT juht

Rakendamise eest vastutavad: IT juht või tema määratud isik

Digitempel on digiallkirja analoog juriidiliste isikute (asutuste) jaoks – kui digiallkiri seob dokumendi püsivalt füüsilise isikuga, siis digitempel seob dokumendi püsivalt juriidilise isikuga. Tihti kasutatakse digitemplit juhtumitel, kus dokumendi seos isikuga pole niivõrd oluline, kuivõrd on oluline just seos asutusega. Samuti võib üks dokument olla korraga varustatud nii digiallkirja kui ka -templiga. Sageli kasutatakse digitemplit mingi registri või andmebaasi väljundite tõestusväärtuse tagamiseks – sel juhul digitembeldamise juures otsene inimtegevus puudub ja tembeldatakse infosüsteemi automaatset väljundit.

Digitempli kasutuselevõtule peab asutuses eelnema põhjalik analüüs, mis leiab mh vastused järgmistele küsimustele:

- Milliste eesmärkide realiseerimiseks on tarvilik digiallkirja asemel või digiallkirjale lisaks digitempli kasutamine? Kas neid eesmärke ei saa realiseerida digiallkirjaga?
- Milliseid dokumente hakatakse digitembeldama ja kuidas see toimub? Millistele infosüsteemi komponentidele või osadele digitembeldussüsteem lisatakse? Millisel määral hakatakse digitembeldamist kasutama automaatselt (nt mingi andmebaasi päringute vastuste juures) ja millisel määral kasutatakse digitembeldamisel inimest (töötajat, kellele antakse vastavad õigused, kuid nõutakse ka kohustusi ja vastutust). Miks otsustakse digitemplit hakata andma automaatselt ilma inimese juuresolekuta? Kas asutuses on läbi mõeldud ning uute turvameetmetega maandatud täiendavad riskid, mis sellisel juhtumil tekivad?
- Kes hakkab digitembeldussüsteemi haldama ja selle üle järelevalvet pidama?
- Kellele ja millisel viisil digitembeldatud dokumendid edastatakse või salvestatakse?

Vastavate põhimõtete väljatöötamisel peavad mh osalema ka asutuse IT juht ja turvajuht, tulemus peab olema igal juhul kinnitatud asutuse tippjuhi poolt (kuna digitempel antakse asutuse nimel). Vajadusel – nt keerukate turvaprobleemide ilmnemisel, millel ei ole ühest lahendust – tuleb kaasata piisavate kogemustega väliseid eksperte. Tulemus tuleb fikseerida kirjalikult. Digitembeldamissüsteemi evitamisel tuleb mh arvestada ka vastavate lahenduste (krüptopulk, digitembeldustarkvara jm) tootjate juhendite, nõuete ja soovitusega. Täpsemat teavet saab veebilehelt http://www.sk.ee/teenused/digitempli-teenus/.

Eriline rõhk tuleb digitembeldussüsteemide plaanimisel panna digitembeldamiseks kasutatava krüptopulga füüsilisele pääsule ning kasutusõigustele. Kui digiallkiri seob dokumendi füüsilise isikuga (ja vastutus allkirjade õigsuse ning allkirja andmise vahendi korrektse kasutamise ja valdamise eest lasub kindlal isikul), siis digitempel seob dokumendi juriidilise isikuga. Seega on seadme kasutamise eest vastutamise skeem keerulisem ja vajab kindlat asutusesisest regulatsiooni.

Eraldi tuleb vaadata kahte juhtumit.

- Digitembeldamisseade ja/või selle kasutusõigus on asutuse mõne töötaja ja/või töötajate käes, kes annavad digitempleid käsitsi nii nagu tavalisi digiallkirjasidki.

Kõik seesugused õiguste andmised tuleb kooskõlastada asutuse juhi ning turvajuhiga. Turvajuht peab need ka dokumenteerima. Kasutatavaid PIN- ja PUK-koode peavad digitempli kasutajad sel juhul käitlema käesolevas meetmes kirjeldatud juhiste järgi.

- Kui digitempli andmise seadme pääsureegleid on vaja muuta nii, et kelleltki töötajatest võetakse digitembeldamise õigus ära, tuleb lisaks seadme halda- ja muutmisele igal juhul kasutatavad PIN- ja PUK-koodid muuta. Seesuguste PIN- ja PUK-koodide muutmist korraldab ja selle eest vastutab asutuse turvajuht või tema määratud isik.
- Digitembeldamisseade toimib automaatselt koostöös mingi infosüsteemi komponendiga ilma inimese otsese juuresolekuta (nt tembeldatakse kõiki andmebaasi päringute vastuseid). Sel juhul tuleb tähelepanu kindlasti pöörata kolmele aspektile.
- Digitembeldamisseade peab füüsiliselt asuma turvalises paigas, kus see oleks ligipääsetav vaid teatud isikutele. Tüüpiliselt tuleb see paigutada kas serveriruumi (vt B 2.4 Serveriruum), kaitsekappi (vt B 2.7 Kaitsekapid) või lukustatavasse tuppa, kuhu on ligipääs vaid teatud isikutel, kes seadme toimimise eest vastutavad. Vastav asukoht ja pääs peavad saama turvajuhi heakskiidu ja seis tuleb kirjalikult dokumenteerida.
- Hoolikalt tuleb üle vaadata, milline infosüsteemi komponent ning milliseid dokumente digitembeldamiseks ette annab. Tuleb välistada, et mingil juhul ei tembeldataks dokumente, mis ei ole digitembeldamiseks ette nähtud; vastavat omadust tuleb turvatestimisel ka spetsiaalselt kontrollida (vt M 5.150 Penetratsioonitestide läbiviimine)
- Automaatselt toimival digitembeldamisseadmel peab olema määratud kindel administraator (ülem), kas vastutab selle seadistamise ja töösoleku eest.

Nimetatud administraatori määramine või vastavate õiguste muutmine tuleb teha asutuse IT juhi ja turvajuhi juuresolekul ja teadmisel.

Lisaks eeltoodule tuleb arvestada, et automaatse digitembeldussüsteemi evitamine tekitab võrrelduna inimese poolt antud digiallkirjadega alati täiendavaid turvariske, mis tuleb kindlasti maandada täiendavate (peamiselt halduslike ja füüsiliste) turvameetmetega, mis puudutavad digitembeldussüsteemi haldamist, käitlemist ja ligipääsu.

Kontrollküsimused:

- Kas ja kuidas on välistatud digitempli andmine dokumentidele, mida asutus ei soovi?
- Kas ja kuidas on välistatud digitempli andmise seadme kasutamine volitamata isikute poolt (nt asutuse nende töötajate poolt, kellele vastavat õigust pole antud)?
- Kas ja kuidas on välistatud infosüsteemide kuritahtlik manipuleerimine, mille tulemuseks on digitempli andmise õiguste volitamata laienemine?

M 2.E15 ID-kaardi või sarnase seadme PIN-ja PUK-koodide turvaline käitlemine

Algatamise eest vastutavad: turvajuht

Rakendamise eest vastutavad: kasutajad

ID-kaardi, mobiil-ID, digi-ID ja sellega sarnaste seadmete PIN- ja PUK-koodidel on tavaliselt järgmine roll:

- PIN1 koodi sisestamine võimaldab autentimise võtmepaari privaatvõtme kasutamist pöördkonstrueerimatu seadme sees. PIN1 koodi läheb vaja turvalisel autentimisel, ID-kaardi korral lisaks ka CDOC-vormingus krüpteeritud failide dešifreerimisel. Minimaalne PIN1 pikkus on neli numbrit.
- PIN2 koodi sisestamine võimaldab signeerimise võtmepaari privaatvõtme kasutamist pöördkonstrueerimatu seadme sees. PIN2 koodi läheb vaja digiallkirja andmisel. Minimaalne PIN2 pikkus on viis numbrit.
- PUK kood võimaldab PIN1 ja PIN2 koodi muuta ilma PIN-koode endid teadmata. PUK-koodi minimaalne pikkus on kaheksa numbrit. PIN- ja PUK-koode tuleb käidelda viisil, mis välistab nende sattumise volitamata isikute kätte. Mõistlik oleks järgida PIN- ja PUK-koodide käitlemisel alljärgnevaid näidisreegleid:
- Algsed, seadme soetamisel (turvaümbrikus vm kujul) saadud PIN- ja PUKkoodid tuleb esimesel kasutamisel vahetada oma personaalsete, algsest erinevate koodide vastu. Selleks tuleb kasutada ID-kaardi ja/või mobiil-ID haldusvahendit.
- PIN- ega PUK-koode ei tohi mitte kunagi mitte mingitel juhtumitel mitte kellelegi üle anda – nad on personaalsed autentimisvahendid.
- Vahetatud PUK-kood tuleb peidetud kujul deponeerida. Näiteks PUK-koodi 56741638 võib kanda telefoniraamatusse kujul “Peeter N. 56741638 “, märkmikusse kujul” Mihkel, 5,6 m pikkused lauad, 74 tk, 1638 EUR “, sahvriseinale kujul” Tartu sõidukulu 57.74 EUR, algus kell 16:38 "vms. Kui väljamõeldud peidetud kujul deponeerimissüsteemi turvalisuses jäädakse kahtlema, tuleb kasutatava meetodi põhimõtete osas konsulteerida asutuse turvajuhiga.
- PIN-koode ei tohi kunagi kusagile mingil kujul üles kirjutada. Kui PIN-koodid lähevad meelest, tuleb nende muutmiseks kasutada eelmainitud kujul deponeeritud PUK-koodi.
- PIN-koode ei tohi sisestada arvutis, mille turvasätete efektiivsuses ei ole kasutaja veendunud (nt sõbranna koduarvuti, avaliku interneti punkti arvuti).
- PIN-koode ei tohi sisestada paikades, kus keegi võib seda pealt vaadata (avalikud kohad, külastajad kabinetis, kes näevad klaviatuuri vms).
- PIN-koode ei tohi sisestada arvutites, millede turvaseaded on uuendamata (Windows-keskkondades nt hüüumärgiga kollane kilp käsureal) või viirusetõrjeprogrammi viiruste definitsioonid on aegunud (vt M 2.159 Viiruseskanneri värskendamine).
- PIN-koode ei tohi sisestada arvutites, millel on olnud tõsine turvarike (Windows-keskkondades nt diagonaalristiga punane kilp käsureal) ning selle järgselt ei ole arvutit IT spetsialisti poolt seadistatud/kontrollitud tasemel, kus selgitati välja ka turvarikke põhjus.
- Kui tekib vähimgi kahtlus, et kasutatud PIN-koodid on lekkinud (keegi on nende sisestamist pealt vaadanud vms) tuleb PIN-koodid koheselt vahetada.

- Kui arvutis, kus PIN-koode kasutati, leitakse troojalane ehk trooja hobune (vt M 2.224 Trooja hobuste tõrje , M 3.69w Sissejuhatus viirustest tulenevatesse ohtudesse ja M 6.23 Käitumisreeglid arvutiviiruste esinemisel), tuleb PIN-koodide võimaliku vahetamise osas kindlasti konsulteerida asutuse turvajuhiga. Turvajuht otsustab, kas konkreetne troojalane võis PIN-koode varastada või mitte, otsustades ühtlasi ka PIN-koodide vahetamise vajaduse.

Kui uue seadme – ID-kaart, mobiil-ID vms – hankimise järel on PIN- ja/või PUK-koodide kohene muutmine teatud põhjusel raskendatud (nt puudub vastav haldusvahend või kohene juurdepääs sellele vms), siis tuleb lähtuda alljärgnevatest reeglitest:

- PUK-kood tuleb peidetud kujul deponeerida (vt reeglid eespool) ning algne koodide kandja (turvaümbrik vms) tuleb hävitada (vt M 2.13 Tundlike ressursside jäljetu hävitamine).
- Mitte hetkekski ei tohi seadet koos PIN- ja PUK-koodide kandjaga jätta järelevalveta (ka lukustatud ruumidesse). Kui tekib vajadus algsete koodide kandjat ja seadet teatud ajaks hoiustada, tuleb neid hoida eri kohtades. Üliränk, kuid kahjuks sagedane turvaeksimus on keelatud PIN-koodide üleskirjutatud kujul hoidmine koos seadmega – nt muutmata koodidega ID-kaardi hoidmine koos turvaümbrikuga!
- Esimesel võimalusel tuleb digikeskkonnas (vastavas haldusvahendis) PIN- ja PUK-koodid vahetada.
- Vajadusel võib eeltoodud võtetega ka PIN-koodid deponeerida. Sealjuures tuleb konkreetse deponeerimisotsuse korral alati arvestada asjaoluga, et valesti läbiviidud deponeerimine võib tekitada konfidentsiaalsuskao. Kahtluse korral tuleks kavandatav deponeerimisviis läbi arutada asutuse turvajuhiga. Kõiki nimetatud reegleid ja põhimõtteid (sh näidisreegleid) tuleb käsitleda töötajate koolitamisel (vt M 3.E2 Töötajate koolitus ID-kaardi/PKI lahenduste kasutamise osas).

Kontrollküsimused:

- Kas kõikide nende töötajate korral, kes kasutavad töö juures ID-kaarti, mobiil-ID-d või sarnast seadet, on nende seadmete PUK-koodid peidetult deponeeritud?
- Kas asutuse töökohtade ülesehitus tagab PIN-koodide pealtvaatamiskindla sisestamisvõimaluse?

M 2.E16 Transpordikrüpto vormingute kasutuskeeld andmete säilitamiseks

Algatamise eest vastutavad: turvajuht
Rakendamise eest vastutavad: kasutajad

Transpordikrüptoks ettenähtud vormingute (nt CDOC) kohaselt krüpteeritud dokumente ei tohi kasutada andmete säilitamiseks. Transposrikrüpto (nt CDOCi) ainus eesmärk on kaitsta dokumendi konfidentsiaalsust side (transpordi) faasis.

Transposrikrüpto vormingud ei ole mõeldud dokumentide turvaliseks säilitamiseks, kuna dešifreerimisvõti eksisteerib ainult ühes eksemplaris adressaadi IDkaardis.

Kui transpordikrüpto põhimõtetel krüpteeritud failikrüpteeringu adressaadi ID-kaart kaob, hävib või rikneb, kaob dešifreerimiseks kasutatav privaatvõti jäädavalt ja lõplikult. Sama leiab aset juhtumeil, kus ID-kaardi autoriseerimise võtmepaari uuendatakse – ka sel juhul kirjutatakse vana võtmepaar (sh privaatvõti) uuega üle ning vana privaatvõtit enam alles ei jää.

Mainitud juhtumitel ei ole faili enam võimalik dešifreerida (avada). Igasugune võtmetaaste transpordikrüpto korral puudub (vt M 2.163 Krüptoprotseduure ja -tooteid mõjutavate tegurite määramine ja M 6.56 Andmevarundus krüptoprotseduuride kasutamisel). Edukalt adressaadini jõudnud transpordikrüpto (nt CDOC-i) vormingus fail tuleb esimesel võimalusel dešifreerida. Edasi tuleb dokumenti säilitada kas avateksti (st krüpteerimata) või mingil muul kujul krüpteeritult, kus on arvestatud ka võtmetaaste vajadusi. Nimetatud reegleid tuleb käsitleda ka töötajate koolitamisel.

Kontrollküsimus:

- Kes, kas ja kuidas võib olla veendunud, et asustuses ei säilitata ühtki olulist dokumenti transpordikrüpto vormingus?

M 2.E17 ID-kaardi või sarnase seadme kasutuskeeld tundmatute turvasätetega keskkonnas

Algatamise eest vastutavad: turvajuht
Rakendamise eest vastutavad: kasutajad

Kui asutuse töötajad kasutavad oma ametiülesannete täitmiseks oma isiklikke ID-kaarte, mobiil-ID-d, digi-ID-d ja/või sarnaseid seadmeid, ei tohi nad samu seadmeid kasutada tundmatute turvasätetega keskkonnas. Tundmatute turvasätetega keskkonnaks tuleb siin üldjuhul lugeda keskkondi, mille turvaseadete – viirusetõrje, kahjurvara tõrje, turvauuendused jms – olemasolu ja toimimise kohta puudub kasutajal selge ja usaldusväärne ülevaade (nt sõbra või sõbranna arvuti, naabri arvuti, avaliku internetipunkti arvuti vms).

Täpsemad reeglid nimetatud valdkonna osas kehtestab vajaduse korral asutuse turvajuht. Eelkõige vajavad seesuguseid turvajuhi kehtestatud reegleid olukorrad, kus ID-kaarti või sarnaseid lahendusi kasutavad töötajad oma koduarvutites või isiklikes sülearvutites, milledel on kodus teisigi kasutajaid (pms pereliikmeid) ning kus kasutajaprofiilide ja nende tegevuste osas puudub töötajal tihtipeale usaldusväärne kontroll ning ülevaade.

Kontrollküsimused:

- Kas töötajad on teadlikud, et ID-kaardi või sarnase seadme kasutamine tundmatute turvasätetega arvutis võib olla ohtlik?
- Kas turvajuht või tema määratud isik on kõikide tööasjus ID-kaarte või sarnaseid seadmeid kasutavate töötajatega vestelnud nende seadmete kasutamisest töövälises keskkonnas ning vajadusel töötajaid turbe osas harinud?

M 2.E18 ID-kaardi või digi-ID edasiandmiskeeld teisele isikule (tavakasutaja)

Algatamise eest vastutavad: turvajuht

Rakendamise eest vastutavad: kasutajad

ID-kaart, mobiil-ID ja digi-ID on isiku personaalsed autentimis- ja signeerimisvahendid, mida teisele inimesele üle ei anta. Teise inimese isikut tõendava dokumendi kasutamine on seadusega karistatav. Ainsaks erandiks on siin ID-kaart (õigusliku nimetusega Eesti Vabariigi isikutunnistus), millel on lisaks digipoolele ka visuaalne pool, mis toimib isikut tõendava dokumendina nii Eesti-siseselt kui ka Euroopa Liidu sees. Seetõttu on paratamatus anda aeg-ajalt ID-kaart isiku tuvastamiseks üle piiri- ja/või tolliametnikule, politseinikule, pangatöötajale, lennujaama turvatöötajale, hotelli administraatorile vms. Seesugusel üleandmisel peab ID-kaardi omanik alati veenduma, et kaardist ei tehta ebaseaduslikku koopiat (v.a. juhtumid, kus kserokoopia tegemine on vajalik), ei kasutataks kaardi digipoolt jms. Üldjuhul on lubamatu, et eraõiguslik klienditeenindaja (nt hotelli administraator) läheb ID-kaardiga selle omaniku silme alt ära kusagile taharuumi vms.

Nimetatud reegleid ja ohtusid peab asutuse turvajuht (või tema määratud isik/tellitud koolitaja) käsitlema ka töötajate koolitamisel (vt M 3.E2 Töötajate koolitus ID-kaardi/PKI lahenduste kasutamise osas).

Kontrollküsimus:

- Kas töötajad on teadlikud, et ID-kaardi kergekäeline käest andmine võib lõppeda halvemal juhul identiteedivargusega?

M 2.E19w ID-kaardi või digi-ID kaasavõtmiskohustus arvuti juurest lahkumisel

Algatamise eest vastutavad: turvajuht

Rakendamise eest vastutavad: kasutajad

Asutuses oleks mõistlik evitada hea tava, et arvuti juurest lahkumisel võetakse alati arvutist välja ka ID-kaart, võttes selle endaga kaasa. Kui arvuti juurest lahkumisel jäetakse ID-kaart arvutiga liidestatuks, tekib risk, et ID-kaardiga autentides alustatud turvaline sessioon võis jääda lõpetamata – kaardi väljavõtmisel arvutist niisugune sessioon reeglina alati lõpetatakse. Samuti kaasnevad sellega kasutajate isiklikud riskid – lühikesena planeeritud eemaleminek arvutist võib osutuda pikemaks ning viia situatsioonideni, kus kasutajal läheb ID-kaarti turvalisel autentimisel, signeerimisel või isikut tõendava dokumendina vaja. Sellest juhisest ei ole vaja lähtuda juhtumeil, kus töötajal on omaette kabinet, mille ukse ta lukustab ruumist lahkumisel – sh ka lahkumisel lühikeseks ajaks, nt kohvi järele või WCsse – ning teistel isikutel ruumi pääsemiseks pääsuvahendeid pole. Sel korral on PKI teenuste volitamata kasutamine välistatud füüsiliste turvameetmetega (vt M 1.23 Lukustatud uksed).

Teisest küljest peab SSO kasutamisel olemas ID-kaardi eemaldamisel arvutist ettevaatlik – kaardi eemaldamisel katkestatakse mitmed teenused. SSO kasutamise korral tuleb koostöös IT juhi ja turvajuhiga leida konkreetse olukorra jaoks sobiv kompromisslahendus käideldavuse ja tervikluse/konfidentsiaalsuse vahel (koos vastava riskianalüüsi läbitegemisega). Selle lahenduse tulemiks peavad olema konkreetsed reeglid lõppkasutajatele, millal ja millistel asjaoludel ID-kaart arvutist eemaldatakse ning millal seda teha ei tohi (vt G 4.E1 Teenusekatkestuste oht SSOga ühislogimisel).

M 2.E20 ID-kaardi või digi-ID edasiandmiskeeld teisele isikule (administraator)

Algatamise eest vastutavad: turvajuht

Rakendamise eest vastutavad: rakenduste loojad, dokumendihalduse korraldajad

Digisignatuur kui krüptograafiline mehhanism seob faili ta signeerijaga (allkirjastajaga) bittide-baitide tasemel. Samal ajal tuleb digiallkirja korral siduda selle andjaga dokumendi sisu ehk tähendus. See on võimalik siis, kui digiallkirjaga varustataval failil kui bitijadal on ühene tähendus , st seda ei tohi erinevate süsteemide ja/või erineva tarkvaraga saada interpreteerida mitut erinevat moodi.

Probleemid võivad tekkida kahel juhul:

1. Faili sisust ja/või nimest ei selgu kasutatav failivorming ning erinevad tarkvaratooted ja/või keskkonnad võivad sama dokumenti näidata erinevalt (erinevate adekvaatkuvadega). Nt faililaiend DOC viitab Microsoft Wordi poolt kasutatavale dokumendivormingule, kuid ei selgu, millist versiooni sellest kasutatakse (vt M 4.134z Sobivate andmevormingute valimine).
2. Digiallkirjastatav fail sisaldab aktiivsisu (makrosid), mis muuhulgas võivad dokumendi sisu (adekvaatkuva, WYSIWYG) teha lisaks failis sisalduvale sõltuvaks kuupäevast, kellaajast, kasutatavast arvutist vm faktoritest.

Mida ja millisel moel siin asutuse sees reguleerida, jääks turvajuhi otsustada (koostöös IT juhi, dokumendihalduse eest vastutaja jt ametnikega). Turvajuhi poolt tehtav vastav otsus peab põhinema signeeritavate dokumentide iseloomu, tekkiva riski suurust ning infosüsteemile ning asutusele toimivat mõju kaaludes. Samuti peab tehtud otsus olema kirjalikult fikseeritud, soovitavalt asutuse turvapoliitika tasemel (vt M 2.192 Infoturbepoliitika koostamine). Kõige rangemal juhul oleks asutuse sees lubatud vaid kindlas vormingus dokumentide signeerimine (PDF, võibolla ka RTF vms) ning rangelt oleks keelatud makrosid sisaldada võivates vormingutes (nt MS Office'i vormingud DOC, DOCX, XLS, XLSX jms) dokumentide signeerimine. Kõige leebemal juhul oleks lubatud digiallkirja andmine ka DOC- ja DOCX-vormingus dokumentidele, kuid sellele peab eelnema nende kontroll (tuleb veenduda kasutatud vormingureeglite õigsuses, makrode mittekasutamises jms).

Lisaks tuleb kõikidele asutuses digiallkirjastamisega tegelevate töötajatele teadvustada kindlasti järgmisi asju:

- fail (kui bitijada) ning faili adekvaatkuva (WYSIWYG) ei pruugi alati olla üheselt seotud, st bitijadal võib olla mitu adekvaatkuva (tähendust);
- fakti, et masslevinud DOC- ja DOCX-vormingupere võimaldab aktiivsisu (makrode) kasutamist, mis võib teatud juhtudel faili adekvaatkuva – seega ka tähendust – muuta.

Vastavate teemadega peavad kursis olema nii rakenduste arendajad kui ka asutuse dokumendihalduse korraldajad. Rakenduste arendajad peavad rakenduste

koostamisel välistama mitmetimõistmist kasutatavaid failivorminguid. Kui digiallkirju antakse aga ID-kaardi utiliidi või mingi muu massiliseks kasutamiseks mõeldud standardlahenduse (nt DigiDOCi portaali) abil, jääks sobiva vormingu valimine asutuse dokumendihalduse reeglite korraldada. Nimetatud teemasid peab asutuse turvajuht (või tema määratud isik/tellitud koolitaja) käsitlema ka töötajate koolitamisel (vt M 3.E2 Töötajate koolitus ID-kaardi/PKI lahenduste kasutamise osas).

Kontrollküsimused:

- Kas digiallkirjastamisega tegelevad töötajad on teadlikud, et fail ja selle adekvaatkuva ei pruugi alati olla üheselt seotud?
- Kas digiallkirjastamisega tegelevad töötajad suudavad MS Wordi dokumentides ära tunda makrode olemasolu ja teadvustada nende mõju dokumendi adekvaatkuvale?

M 2.E21 Digitembeldussüsteemi tegevuse lõpetamine

Algatamise eest vastutavad: IT-juht, turvajuht

Rakendamise eest vastutavad: administraator, IT-juhi poolt määratud isik

Digitembeldussüsteemi tegevuse lõpetamisel või sellisel ümberkonfigureerimisel, kus tembeldamiseks kasutatavad tehnilised seadmed (krüptopulgad vms) oma varasema funktsiooni kaotavad, tuleb tagada, et neid seadmeid enam digitembeldamiseks kasutada ei saaks. Tegevuse lõpetamise protsessi peab kindlasti olema kaasatud asutuse turvajuht. Turvajuhi osalusel määratakse ka konkreetsed tegevused, millega digitembeldamise edasine tegevus võimatuks tehakse.

Need võivad olla näiteks:

- krüptopulga PIN-koodide muutmine ja uute PIN-koodide deponeerimine seifi (nt turvajuhi või asutuse juhi vastutusele);
- krüptopulgaga seotud sertifikaadi peatamine või tühistamine;
- krüptopulga või sarnase seadme füüsiline hävitamine;
- krüptopulga deponeerimine seifi (nt turvajuhi või asutuse juhi vastutusele).

Samuti võib olla see mitu eelnimetatud tegevust korraga. Vastav protseduur tuleb turvajuhi osalusel välja töötada (kaaludes reaalseid riske ning mõju infosüsteemile ja asutusele), samuti turvajuhi osalusel dokumenteerida. Kuna erinevalt digiallkirja andmise seadmetest (ID-kaart, digi-ID, mobiil-ID) on digitempel ja seda anda võimaldav krüptopulk seotud mitte konkreetse füüsilise isikuga (kes automaatselt selle toimimise eest ka vastutab), vaid asutusega, siis seepärast ongi digitembeldussüsteemi turvaliseks lõpetamiseks teatavad protsessuaalsed tegevused vajalikud (vt M 2.46 Krüpteerimise õige korraldus).

Kontrollküsimus:

- Kas võib olla kindel, et aktiivselt käibelt kõrvaldatud digitembeldusseadmete poolt asutuse nimel keegi digiallkirja anda ei saa?

M 2.E22 Krüptograafiliste algoritmide vahetatavuse nõue

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: IT-turbe osakond

Krüptograafilised algoritmid vananevad varem või hiljem ja muutuvad lõpuks ebaturvaliseks. Vananenud krüptograafiliste algoritmide vahetamist IT-komponentides on oluliselt lihtsam korraldada, kui IT-komponente on võimalik kiiresti ümber seadistada teistele krüptograafilistele algoritmidele, mis on (veel) turvalised. Selleks tuleb kehtestada nõuded loodavatele IT-lahendustele, tarkvarale ja riistvarale, samuti IT-lahenduste hangetele, et saadavas tootes või teenuses oleksid krüptograafilised algoritmid ümberseadistatavad/vahetatavad ja dokumentatsioon sisaldaks juhiseid, kuidas krüptograafilisi algoritme teistega asendada.

Ehkki see meede ei lahenda krüptograafiliste algoritmide vahetamise probleemi täielikult, sest ka IT-komponendis kasutatud kõik alternatiivsed krüptoalgoritmid võivad vananeda, pikendab see siiski oluliselt krüptograafilisi algoritme kasutatavate IT-komponentide eluiga ja parandab oluliselt organisatsiooni reageerimisvõimet vananevatest krüptograafilistest algoritmidest tulenevatele ohtudele.

Kontrollküsimused:

- Kas organisatsiooni IT-komponentides kasutatud krüptograafilised algoritmid on kiiresti asendatavad teiste algoritmidega?
- Mida selle tagamiseks tehakse?

M3: Personal

Meetmete nimekiri

M 3.1 Uute töötajate esmane juhendamine ja väljaõpe

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, personalijuht
Rakendamise eest vastutavad: personaliosakond, juhid

Uutele töötajatele tuleb tutvustada IT kasutamisega seotud sisekorrareegleid, tavasid ja protseduure. Uued töötajad, keda ei ole veel piisavalt juhendatud, ei tea, kes on nende kontaktisik, kui neil peaks tekkima küsimusi seoses IT turbega, nad ei tea, milliseid turvameetmeid tuleb neil võtta ja neil pole aimu ettevõttes või ametiasutuses kehtestatud IT turvastrateegiast. Sellega seoses võib IT kasutuse raames tekkida rikkeid ja kahjusid. Seetõttu on ülimalt oluline viia uued töötajad süstemaatiliselt kurssi tööülesannetega.

Esmane juhendamine ja väljaõpe peaks hõlmama vähemalt järgmisi punkte:

- Kõiki uusi töötajaid tuleks juhendada ja koolitada seoses nende töökohal asuvate oluliste IT-süsteemide ja IT-rakendustega. Lisaks tuleks tõsta uute töötajate teadlikkust ka seoses kõikide oluliste IT turbemeetmetega ning neid selles valdkonnas ka koolitada (vt B 1.13 Infoturbe teadlikkus ja -koolitus).
- Töötajatele tuleks tutvustada kõiki kontaktisikuid, eriti neid, kes tegelevad IT ja selle turbega seotud küsimuste lahendamisega.
- Uutele töötajatele tuleks tutvustada ametiasutuse või ettevõtte IT-turvaeesmärke. Neile tuleb tutvustada kõiki ettevõttesiseseid IT turvet käsitlevaid korraldusi ja ettekirjutusi. Töötajaid tuleks informeerida käitumisreeglitest ja teavitamiskanalitest, mida tuleb rakendada kõikvõimalike potentsiaalsete turvaintsidentide korral.

Esmase juhendamise korraldamisel on abiks infolehed või kontrollnimekirjad, mis aitavad säilitada ülevaadet selle kohta, millised juhendamisprotseduuri etapid on juba läbitud ja millised veel läbimata.

Kontrollküsimused:

- Kuidas leiab aset uute töötajate IT-alane juhendamine?
- Kui palju antakse igale uuele töötajale aega oma tööülesannetesse sisse elamiseks?
- Kas uutele kolleegidele antakse abiks mõni kogenum kaastöötaja?

M 3.2 Uute töötajate kohustamine eeskirju järgima

Algatamise eest vastutavad: personalijuht, andmekaitsespetsialist, IT-turvaosakond

Rakendamise eest vastutavad: personaliosakond, juhid

Inimesi tööle võttes tuleks neid kohustada järgima asjakohaseid eeskirju ja sisekorrareegleid. Sellega täidetakse korraga kahte eesmärki: teavitatakse töötajaid IT-turbele kehtestatud ettekirjutustest ja eeskirjadest ning luuakse ühtlasi töötajatele piisav motivatsioon neid ka järgida. Siinkohal ei piisa kõikvõimalike kohustuste suulisest mainimisest, vaid töötajatele tuleb jagada ka vastavate eeskirjade ja ettekirjutuste väljatrükid ning lasta nende kättesaamist allkirjaga kinnitada, või luua töötajatele kuskil tsentraalses kohas pidev võimalus vastava dokumentatsiooniga tutvuda. Eriti oluline on informeerida kõiki töötajaid sellest, et kõik töötulemused ja kogu töö käigus saadud informatsioon on mõeldud eranditult vaid ettevõttesiseseks ja tööülesannete täitmisel kasutamiseks.

Kontrollküsimused:

- Kuidas kehtestatakse kohustused?
- Kas kohustused fikseeritakse kirjalikult?
- Kas uus töötaja saab vajaminevate dokumentidega tutvuda ning saab endale nende koopiad?
- Kas töötajad on teadlikud nende tööülesannetele kehtivast seaduslikust raamistikust?

M 3.3 Asendamise korraldamine

Algatamise eest vastutavad: organisatsiooni juht, IT turvaosakond

Rakendamise eest vastutavad: juhid

Asendamise korra kehtestamise eesmärk on tagada tööülesannete jätkuv täitmine nii planeeritavate juhtumite (puhkus, töölähetus) kui ka ettenägematute olukordade (haigus, õnnetus, töölt lahkumine) puhul. Seetõttu peab olema juba enne nimetatud sündmuste esinemist reguleeritud, kes tohib keda ja millistes ülesannetes ning millise kompetentsi piires asendada. Eriti oluline on see infotöötluse valdkonnas, kus läheb reeglina tarvis eriteadmisi, mida ei ole võimalik nii kiiresti edasi anda, et valdkonnas ebapädev töötaja suudaks kedagi kiiresti asendada.

Asenduskorra kehtestamisel tuleks kinni pidada järgnevatest raamtingimustest:

- tööülesannete ülevõtmine asenduse raames eeldab, et protseduur või projekt peab olema piisavalt dokumenteeritud;
- reeglina ei piisa selleks vaid asendustöötaja määramisest. Kontrollida tuleb ka seda, millist koolitust oleks asendustöötajal tarvis, et ta suudaks vastavad tööülesanded ka reaalselt üle võtta. Kui peaks selguma, et leidub töötajaid, keda ei ole võimalik nende eriteadmiste tõttu kiiresti asendada, tähendab see seda, et nende väljalangemisel satub igapäevaste tööprotsesside tavapärane jätkumine tõsisesse ohtu. Siinkohal on ülimalt oluline koolitada välja ka sobiv asendustöötaja;
- tuleb määratleda, kes ja millises mahus täidab asenduse raames erinevaid tööülesandeid;
- asendustöötajale tohib vajalikud juurde- ja sissepääsuõigused anda vaid asendamise ajaks;
- kui eriolukordades ei ole võimalik leida erinevatele isikutele kompetentseid asendustöötajaid või neid koolitada, tuleks juba varakult mõelda sellele, milliseid väliseid jõude tuleks asenduste tagamiseks sellistel juhtudel kaasata.

Kontrollküsimused:

- Kuidas on reguleeritud asendamise kord organisatsiooni erinevates allüksustes?
- Kas kompetentseid asendustöötajaid on piisavalt võtta?
- Kas lähiminevikus on tekkinud olukordi, kus tuli rakendada välist asenduspersonali?
- Kas organisatsiooni allüksustes on olemas nn teadmiskeskused (ingl single point of knowledge) või mõni töötaja, kes valdab ainuisikuliselt eriteadmisi, mis on IT-kasutuseks hädavajalikud.

M 3.4 Väljaõpe enne programmi tegelikku kasutamist

Algatamise eest vastutavad: personalijuht, ülemused

Rakendamise eest vastutavad: juhid, üksikute IT-rakenduste eest vastutavad töötajad

IT-rakenduste ebapädevast kasutamisest tingitud kahjud on välditavad, kui võimaldada kasutajatele enne tööle asumist põhjalik väljaõpe. Seetõttu on ülimalt oluline, et kasutajad läbiksid enne IT kasutusel põhinevate tööülesannete ülevõtmist ilmtingimata ka piisava koolituse. See puudutab nii standardsete programmipakettide kui ka spetsiaalselt arendatud tarkvara kasutama õppimist. Lisaks on tarvis koolitusi läbi viia ka siis, kui IT-rakenduses on toimunud suured muudatused. Juhul kui vastava IT-rakenduse kohta on olemas kergesti mõistetavad käsiraamatud, võib koolituse asemel kehtestada ka nõude, et töötajatel tuleb end uue materjaliga iseseisvalt kurssi viia. Siinkohal on aga kõige olulisem eeldus asjaolu, et töötajatele tuleb uue materjaliga tutvumiseks jätta piisavalt aega.

Kontrollküsimused:

- Kas töötajad, kes peavad hakkama esimest korda täitma IT-toega tööülesandeid, läbivad eelnevalt piisava koolituse?
- Kas uute IT-rakenduste juurutamiseks koostatakse vastav koolituskava?
- Millised uued IT-rakendused on töösse lisandunud pärast viimast kontrollimist?
- Kuidas toimus töötajate juhendamine? Millistest koolitusüritustest on töötajad sellest ajast saadik osa võtnud?

M 3.5 Turvameetmete koolitus

Algatamise eest vastutavad: infoturbeametnik, ülemused

Rakendamise eest vastutavad: infoturbeametnik, ülemused

Elektroonikakindlustusfirmade kahjustatistika alusel on võimalik leida arvukaid konkreetseid tõestusi selle kohta, et paljudel juhtudel peitub kahjude tekkepõhjus oskamatuses kasutada elementaarseid turvameetmeid. Kahjude vältimiseks tuleb iga töötajat koolitada, kuidas kogu tegevuse jaoks olulise teabe ja IT-ga hoolikalt ümber käia ning teda selleks ka motiveerida. Arusaam infoturbemeetmete vajalikkusest saab töötajates tekkida vaid siis, kui neile edastatakse hädavajalikud asjakohased teadmised.

Alljärgnevalt on välja toodud olulisemad teemad, mida turvameetmeid käsitlevad koolitused peaksid kindlasti kajastama.

Põhjalikumad ning sihtgruppidest lähtuvad koolituste kirjeldused leiate meetmest M 3.45 IT-turbealaste koolituste sisu kavandamine .

- **Infoturbealane teavitustöö** – kõikide töötajate tähelepanu tuleb juhtida turvaküsimuste tähtsusele. Sobiv lähtepunkt, kuidas inimeste teadlikkust tõsta, on seletada neile, millisel määral sõltub nt ametiasutuse või ettevõtte töövõime ning sellest omakorda ka inimeste töökohad asjaolust, kas tööprotsessid toimivad tõrgeteta või mitte. Lisaks tuleb teabe väärtuse väljatöötamisel lähtuda usaldusväärsusest, terviklusest ja kättesaadavusest. Nimetatud teadlikkuse tõstmise meetmeid tuleb regulaarsete ajavahemike tagant korrata.
- **Töötajatele suunatud infoturbemeetmed** – selle teema raames tuleks töötajaid informeerida turvameetmetest, mis on välja töötatud infoturbe kontseptsiooni raames ja mis on igale töötajale kohustuslikud. Olenevalt tööprotsessist või tööülesandest võib olla ka teisi väärtusi, mida tuleb kaitsta, või millel on muu kaitsevajadus. Töötajatele tuleb teada anda, milline tähtsus on teabel või muudel objektidel asutuse jaoks ja mida tuleb selle käsitlemisel järgida. Kõnealune koolitusmeetmete valdkond on väga oluline, sest paljusid turvameetmeid suudetakse efektiivselt rakendada alles pärast piisavat asjakohast koolitust ja motiveerimist.
- **Tootepõhised turvameetmed** – selle teema raames tuleks töötajatele esitleda turvameetmeid, mis on seotud konkreetse tootega, nt IT-süsteemiga, ning mis kuuluvad tihti juba ka algsesse tarnepaketti. Siia alla võivad kuuluda nt lisaks sisselogimise paroolidele veel ka dokumentide ja andmeväljade krüpteerimisvõimalused. Asjakohased soovitused ja viited, kuidas faile kõige paremini struktureerida ja organiseerida, võivad nt vähendada oluliselt andmevarundusele kuluvat aega ja vaeva.
- **Käitumine kahjurvara esinemisel** – siin tuleb töötajatele teatada, kuidas käituda arvutiviiruste või muu kahjurvaraga. Vastava koolituse võimalikud teemad on järgmised (vt M 6.23 Käitumisreeglid arvutiviiruste esinemisel):

1. kahjurvaraga nakatumise tuvastamine,
2. kahjurvara tööpõhimõtted ja liigid,
3. kohesed meetmed, mida võtta kahtluse korral,

4. kahjurvara elimineerimise meetmed,
5. ennetavad meetmed.

- **Autentimine** – töötajad peavad oskama olemasolevate autentimismehhanismide ja selleks kasutatavate autentimisvahendite, nt paroolide või andmekandjatega õigesti ümber käia. Näiteks tuleks selgitada paroolide tähtsust infoturbele ning tutvustada raamtingimusi, mida tuleb järgida, et üleüldse oleks võimalik tagada paroolide efektiivne rakendamine (vt lisaks M 2.11 Paroolide kasutamise reeglid).
- **Andmevarunduse tähtsus ja selle läbiviimine** – korrapärane andmevarundus on kõige tähtsam turvameede igas teabekoosluses. Töötajatele tuleks tutvustada ametiasutuse või ettevõtte andmevarunduse kontseptsiooni (vt moodul B 1.4 Andmevarunduspoliitika) ja konkreetseid ülesandeid, mida igal töötajal andmevarunduse heaks teha tuleb. Eriti oluline on see neis valdkondades, kus töötajad peavad andmeid varundama iseseisvalt.
- **Isikuandmete kasutamine** – isikuandmeid sisaldavate andmetega töötamisele tuleb kehtestada erinõuded. Töötajaid, kes puutuvad oma tööülesannete raames kokku isikuandmeid sisaldavate andmetega, tuleb koolitada seoses seadusest tulenevate ettekirjutustega. Siia alla kuuluvad nt vastamine infopäringutele, reageerimine inimeste endi isikuandmete muudatus- ja parandusettepanekutele, seadusest tulenevad andmete kustutustähtajad, konfidentsiaalsuse kaitse ja andmete edastamine.
- **Hädaolukorras rakendatavate meetmete koolitus** – kõiki töötajaid peab koolitama seoses kehtivate hädaolukorra meetmetega. Siia alla kuuluvad teabe edastamine evakuatsiooniplaanide kohta, käitumisreeglid tulekahju või muude hädaolukordade korral, tulekustutite kasutamine, hädaolukorra teavitamissüsteem (keda tuleb kõige esimesena olukorrast teavitada).
- **Ennetavad meetmed manipuleerimisrünnete vastu** – töötajaid tuleks teavitada ohtudest, mis kaasnevad manipuleerimisrünnetega. Selgitada tuleks tüüpilisi katseid, kuidas süstemaatilise läbiproovimisega püütakse jõuda konfidentsiaalse teabeni ja meetodeid, kuidas end selle vastu kaitsta. Kuna manipuleerimisründed on tihti seotud vale identiteedi kasutamisega, tuleks töötajate tähelepanu juhtida regulaarselt sellele, et nad kontrolliksid oma vestluspartneri identiteeti ning väldiksid ennekõike telefoni teel konfidentsiaalse teabe edastamist.

Koolitusi planeerides tuleks alati arvestada ka sellega, et töötajate ühekordne koolitamine kogu nende töösuhte vältel ei ole kindlasti mitte piisav. Peaaegu kõikide koolitusliikide puhul, eriti aga loenguvormis tehtud koolituste puhul kehtib tõsiasi, et koolitusel osalejad puutuvad lühikese aja jooksul kokku väga suure hulga uue informatsiooniga. Kuuldud teabest jõuab inimese püsimällu ainult väga väike osa, mis tähendab, et koolituse lõppedes on uutest teadmistest tihti lausa 80% juba ära unustatud. Seetõttu tuleb infoturbealaseid koolitusi ikka ja jälle korrata ning juhtida töötajate tähelepanu kõnealuse valdkonnaga seonduvatele probleemidele.

Sel otstarbel on võimalik:

- korraldada lühikesi koolitusi, mis kajastavad värskeid turbeteemasid,

- kasutada regulaarselt toimuvaid kokkusaamisi, nagu nt osakonna koosolekuid,
- rakendada interaktiivseid koolitusprogramme, millele on töötajatel vaba juurdepääs.

Kontrollküsimused:

- Kas töötajaid koolitatakse seoses infoturbemeetmeid puudutavate teemadega?
- Kas töötajatele antakse teada, milline tähtsus on teabel või muudel objektidel asutuse jaoks ja mida tuleb selle käitlemisel järgida?
- Kas töötajaid, kes puutuvad kokku isikuandmeid sisaldavate andmetega, koolitatakse seoses seadusest tulenevate turvameetmetega?
- Kas töötajaid koolitatakse või teavitatakse korrapäraselt seoses infoturbealaste teemadega?

M 3.6 Reguleeritud protseduur töösuhete lõpetamiseks

Algatamise eest vastutavad: personalijuht, juhid, IT turvaosakond

Rakendamise eest vastutavad: personaliosakond, juhid

Olukorras, kus mõni töötaja lahkub töölt või kui tema tööülesanded muutuvad, tuleb pöörata tähelepanu alljärgnevale:

- Enne töötaja lahkumist tuleb hoolitseda selle eest, et tema asendaja viidaks õigeaegselt kurssi uute ülesannetega. Sel otstarbel on soovitatav, et lahkuv ja uus töötaja täidaksid kasvõi lühikest aega oma tööülesandeid koos.
- Enne lahkumist peab töötaja tagastama kõik dokumendid (muu hulgas näiteks ka institutsioonist laenatud raamatud), võtmed ja laenatud IT-seadmed (nt sülearvutid, andmekandjad ja dokumendid). Eriti oluline on tagasi nõuda kõik ametiasutuse või ettevõtte isikukaardid ja kõikvõimalikud muud sissepääsu võimaldavad kaardid. Biomeetriliste juurdepääsukontrollisüsteemide (iirise skänneri, sõrmejäljelugeja ja käejäljelugeja) puhul tuleb lisaks kustutada ka vastavad juurdepääsuõigused või neid vastava asendustöötaja jaoks muuta.
- Kõik lahkuva töötaja sisenemis- ja pääsuõigused tuleb talt kas tagasi küsida või ära kustutada. Siia alla kuuluvad ka välised pääsuõigused, mis toimivad läbi andmeedastusseadmete. Juhul kui mõne IT-süsteemi pääsuõigused on jagatud erandkorras mitme isiku vahel (nt ühise parooli kasutamise puhul), tuleb ka ainult ühe töötaja lahkudes vastav pääsuõigus siiski ära muuta.
- Enne töötaja lahkumist tuleks talle veel kord sõnaselgelt meelde tuletada, et seni kehtinud vaikimiskohustused jäävad kehtima ka edaspidi ning töö käigus saadud infot ei tohi kellegagi jagada.
- Kui lahkuval töötajal oli avariiplaanis oma kindel roll, tuleb avariiplaan ümber teha.
- Töötajate lahkumisest ja nende tööülesannete muutumisest tuleb informeerida kõiki turvalisuse eest vastutavaid töötajaid, eriti uksehoidjaid.
- Töölt lahkunud isikute puhul tuleb tagada, et neil ei oleks võimalik pääseda kontrollimatult ametiasutuse või ettevõtte territooriumile, eriti aga ruumidesse, kus asuvad IT-süsteemid. Ka tööülesannete muutumine võib kujutada endast olukorda, mille puhul tuleb muuta töötaja sisenemisõigust teatud ruumidesse, nt keelata juurdepääs serveriruumile.
- Olenevalt vajadusest võib ajavahemikuks alates vallandamisotsuse teatavaks tegemisest kuni töötaja töölt lahkumiseni töötajalt ära võtta kõik IT-süsteemidega seotud sisenemis- ja pääsuõigused ning kehtestada talle sisenemiskeelu strateegilise tähtsusega ruumidesse.

Praktikas on ennast hästi tõestanud vastavad kontrolllehed, millel on lahkuva töötaja jaoks üles loetletud kõik kohustuslikud tegevused, mida ta peab läbi viima enne ametiasutusest või ettevõttest lahkumist, saades tegevuse teostades kontrolllehele vastava valdkonna vastutava isiku / juhi allkirja.

Kontrollküsimused:

- Kas töötaja töölt lahkumine toimub kindlate protseduurireeglite alusel?
- Kas töötaja lahkumisest informeeritakse kõiki vastutavaid osapooli?

- Kuidas tagatakse töölt lahkuva isiku kõigi sisenemis- ja pääsuõiguste tagasinõudmine või kustutamine?

M 3.7z Kontaktisik isiklikes küsimustes

Algatamise eest vastutavad: personalijuht, töötajate esindus
Rakendamise eest vastutavad: personaliosakond, töötajate esindus

Usaldusisikute määramine

Tööülesannete puuduliku täitmise põhjused võivad tihti peituda töötajate isiklikes probleemides. Probleemidena võivad kõne alla tulla nt suur võlakoormus, sõltuvused, aga ka probleemid töökohal (üle- ja alakoormus või kolleegide tagakiusamine). Probleemide käes vaevlevate töötajate abistamiseks võib paljudel juhtudel olla kasu töökohas olevast usaldusisikust, kelle poole saavad töötajad oma probleemidega pöörduda. Vastav kontaktisik peaks ühelt poolt toetama probleemide käes vaevlevat inimest ja kaitsma tema huve, teisalt aga pidama silmas ka ettevõtte või ametiasutuse huve ning püüdma koostöös vastava isikuga leida probleemidele võimalikke lahendusi. Nimetatud kontaktisikute poole peavad saama pöörduda ka töötajate ülemused ja kolleegid, nt juhul, kui kellegi puhul on korduvalt täheldatud asjaolusid, mis lubavad arvata, et vastava töötaja usaldusväärsus on langenud. Sellisel juhul peab usaldusisikul olema võimalus pöörduda ise vastavate töötajate poole ja pakkuda neile abi. Usaldusisiku funktsioone võivad täita nt töötajate esindus ehk ametiühingud. Vastava usaldusisiku funktsiooni loomisest tuleb teavitada kõiki töötajaid. Eestis esindab töötajate tööalaseid ja sotsiaalmajanduslikke huve ja õiguste kaitset Eesti Ametiühingute Keskliit (www.eakl.ee). Tööalast abi pakub ka Tööinspektsioon (www.ti.ee).

Kontrollküsimus:

- Kelle poole on töötajatel võimalik pöörduda oma isiklike probleemidega?

M 3.8z Tööõhkkonda kahjustavate tegurite vältimine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, personalijuht, töötajate esindus

Rakendamise eest vastutavad: juhid, personaliosakond, töötajate esindus

Positiivne õhkkond töökohal motiveerib ühelt poolt töötajaid IT-turvameetmetest kinni pidama ja teiselt poolt vähendab see IT-kahjusid, mis võivad tekkida hooletuse või ettekavatsetud tegevuse tagajärjel. Tööõhkkonnas valitsevad pinged võivad tuleneda paljudest nii tööga seotud kui ka töövälistest asjaoludest, kuid kõige sagedamini esineb neid siis, kui töökohas leiavad aset suured muudatused. Sellised muudatused on näiteks restruktureerimine, saneerimine, allüksuste müük või ühinemine ning väljasttellimine.

Nimetatud muudatused võivad mõjuda tööõhkkonnale negatiivselt, kuna need tekitavad inimestes enamasti väga erinevaid hirme (nt hirm kompetentsi kaotamise ees, hirm tööülesannetega jätkuva toimetuleku ees ja hirm kaotada töökoht). Loetletud pingetega on võimalik paremini toime tulla, kui enne muudatuste tegemist valitseb töökohas võimalikult hea sisekliima. Ka IT turbe seisukohast tuleks püüda töökohas luua võimalikult positiivne õhkkond.

Kõiki erinevaid võimalusi pole siinkohal küll võimalik loetleda, kuid alljärgnevalt on toodud siiski väike valik võimalikest meetmetest, mille rakendamist tuleks siiski iga juhtumi puhul eraldi analüüsida:

- puhketoa loomine,
- ületundide vältimine,
- suurte väljavõtmata puhkuste vältimine,
- tööpausidest kinnipidamine,
- hästi korraldatud tööülesannete jaotus,
- ühtlane töökoormus,
- töötulemustele vastav õiglane töötasu,
- toimiv asenduskord.

Kommunikatsioon

Organisatsioonis esinevad kommunikatsiooniprobleemid viivad pikas perspektiivis vältimatult turvaprobleemide tekkimiseni. Äärmuslikel juhtudel võib selle tagajärjel aset leida ka turvaintsident. Selleks, et töötajad hakkaksid turvameetmetest mööda hiilima, piisab, kui neid pole meetmete otstarbest informeeritud, mille tulemusena hakkavad nad turbemeetmetesse suhtuma kui „tüütutesse" lisakohustustesse. Ka negatiivsete teadete edastamise korral tuleb toimida selliselt, et sõnumitooja ei peaks kartma, et tema suhtes hakatakse seetõttu rakendama sanktsioone. Tööl tuleb tagada selline sisekliima, et igal töötajal oleks võimalik edastada infot ametiasutuses või ettevõttes esinenud turvaintsidentide kohta ja loota, et sellega tegeletakse avatult.

Töötajate motiveerimine

Töötajate motiveerimiseks ei piisa sugugi ainult rahast, eelkõige on tähtis, et inimesed saaksid oma töö eest piisavalt tunnustust. Töötajaid tuleks võimalikult

palju kaasata ka otsuste langetamisse. Kui see pole võimalik, tuleks töötajaid teavitada vähemalt põhjustest, mille alusel neid puudutavaid otsused langetati, et nad saaksid vastavate otsuste rakendamises aktiivselt osaleda.

Väljasttellimine

Tihti väljendub töötajate protest teatud konkreetse riistvara või tarkvara valiku suhtes seeläbi, et kasutajad püüavad jätta muljet, nagu oleks neile pealesurutud riist- ja tarkvara palju ebaturvalisem kui nende eelistatud lahendus. Tööõhkkonnal ja töötajate omavahelistel suhetel võib olla määrav tähtsus suuremate muudatuste puhul, nagu nt juhtudel, kus kavatsetakse hakata midagi väljast tellima. Rahulolematud või ärritatud töötajad võivad sellise plaani koguni nurjata (nt võivad olulise oskusteabe valdajad esitada muudatuse kriitilises faasis lahkumisavalduse või hakata turbealaseid ettekirjutusi teadlikult ignoreerima), mis võib nii mõnegi ettevõtte väga kriitilisse olukorda viia. Suuremate restruktureerimiste ja väljasttellimise planeerimise puhul on soovitatav arvestada alljärgnevate aspektidega.

Töötajate kaasamine

- Välise teenusepakkuja valimisprotsessi tuleb juba võimalikult vara kaasata ka töötajad. Edasise otsustusprotsessi käigus tuleks töötajad kaasata võimalike ülevõtmislepingute koostamisse.
- Töötajaid tuleb põhjalikult ja piisavalt varakult informeerida eesseisvatest muudatustest ning nende käsutusse tuleb anda kontaktisik, kes suudab lahendada nende probleeme ja vastata nende küsimustele. Olukord, kus vajalikku infot saadakse mitte ettevõtte või ametiasutuse juhtidelt, vaid hoopis ajakirjanduse vahendusel, tekitab töötajates suurt umbusaldust, rikub usaldussuhted ning loob suurepärase pinnase kõikvõimalike spekulatsioonide ja kuulujuttude tekkeks.
- Organisatoorset laadi ümberkorralduste puhul tuleks puudutatud töötajatele selgitada nende tulevikuperspektiive. Tihti sõltuvad välised teenusepakkujad suurel määral sellest, kas võimalikult suur osa eelnevalt organisatsiooni sees vastavaid tööülesandeid täitnud töötajaid tuleb neile üle või mitte. Tihti on ainult seeläbi võimalik tagada teenuse piisav kvaliteet. Töötajad, kes tunnevad hirmu oma tuleviku ees, või kes leiavad, et neid koheldakse ebavõrdselt, muutuvad oma tööülesannete täimisel kas lohakamaks või esitavad koguni lahkumisavalduse.
- Keerukaid ja koormavaid tegevusi, mis on restruktureerimiste raames vältimatud, tuleks ka piisavalt hinnata ja tunnustada. Vajalik lisatöö tuleks tasustada.

Töötervishoiu ja tööohutuse seaduse leiate Riigi Teatajast.

Kontrollküsimused:

- Millise hinnangu annavad tööõhkkonnale töötajad?
- Millise hinnangu annavad tööõhkkonnale juhid?
- Milliseid tööõhkkonda negatiivselt mõjutavaid tegureid nimetatakse kõige sagedamini?

- Kas suuremate restruktureerimiste korral on töötajate käsutusse antud vastutav kontaktisik?
- Kas muudatusi kajastavatesse protsessidesse kaasatakse ka töötajad ning kas töötajatel on võimalik esitada ka omapoolseid ettepanekuid?

M 3.9z Ergonoomiline töökoht

Algatamise eest vastutavad: tehnikaosakonna juhataja, töötajate esindus

Rakendamise eest vastutavad: juhid, töötajate esindus, kasutajad

Pidevat koormust, mis langeb inimestele halvasti sisseseatud töökohal töötades, ei tohi alahinnata, kuna sellise kestva olukorra tagajärjel võivad töötajatel ilmneda tervisehäired. Ergonoomiliselt sisseseatud töökohaga on võimalik niisugust koormust vähendada. Ergonoomilisuse tõstmise korral paraneb ka töö efektiivsus. Sellest ei võida mitte ainult töövõtja tervis, vaid see tagab ka ökonoomsema tööviisi ning turvameetmete parema ellurakendamise. Seetõttu peaksid töökohad olema võimalikult ergonoomilised. Arvutitöö puhul peab töötaja tooli, laua, monitori ja klaviatuuri asend olema võimalikult riskivaba IT-kasutuse tagamiseks individuaalselt reguleeritav. Muuhulgas tähendab see ka seda, et töötaja tooli seljatuge, tooli kõrgust ja asendit peab saama reguleerida, kuid ka seda, et kõiki töövahendeid olema võimalik paigutada selliselt, et nende kasutamine koormaks töötajat minimaalselt.

Sobivalt sisseseatud töökoht soodustab muuhulgas ka turvameetmete järgimist. Kui töökohas on olemas lukustatavad kirjutuslauad või kapid, võib andmekandjad, dokumendid ja lisatarbed panna sinna luku taha. Ka töökohas kasutatavad IT-süsteemid, eriti monitorid, peavad olema ergonoomiliselt paigutatud. Näiteks monitor peaks alati asuma akna suhtes sellise nurga all, mille korral ei lange valgus otse monitorile. Lisaks peaks olema võimalik IT-süsteemidega segamatult töötada.

Kasutajad ei tohiks olla olukorras, kus ülejäänud kolleegid saavad üle ta õla vaadata. Seda oleks mõistlik vältida ka selleks, et volitamata isikud ei saaks tutvuda tundliku informatsiooniga. Täiendavaid juhiseid annavad määratud töökeskkonnaspetsialist või töökeskkonnavolinik, erialaliidud ja töökaitseeksperdid.

Kontrollküsimused:

- Kas kõikide töötajate töökohad on sisustatud ergonoomiliselt?
- Kas kõik töötajad on üldjuhul oma töökohtade ergonoomilisusega rahul?

M 3.10 Usaldusväärse administraatori ja tema asetäitja valimine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, personalijuht, IT-juht, kodukeskjaama eest vastutav töötaja, IT turvaosakond

IT-süsteemide ja kodukeskjaama administraatorite ning nende asendajate suhtes peab käitajal olema väga suur usaldus. Nimetatud isikutel on olenevalt rakendatavatest süsteemidest kas väga laialdased või tihti ka lausa täieulatuslikud volitused. Administraatoritel ja nende asendajatel on võimalik ligi pääseda kõikidele salvestatud andmetele ja neid vahel isegi muuta ning nende võimuses on jagada pääsuõigusi ka selliselt, et see võib endaga kaasa tuua nende märkimisväärse väärkasutuse. IT-süsteemide administraatoreid ja nende asendajaid tuleb valida väga hoolikalt. Nimetatud isikutele tuleb regulaarselt meelde tuletada, et neil on lubatud oma volitusi rakendada ainult vajalike administreerimisülesannete täitmiseks.

Kuna administraatorid mängivad rakendatava riist- ja tarkvara seisukohast võtmerolli, peab olema tagatud, et töötaja rivist väljalangemise korral saaks jätkuvalt täita talle usaldatud tööülesandeid. Selleks peavad asendajateks määratud isikud ennast süsteemikonfiguratsiooni hetkeseisuga kursis hoidma ning omama juurdepääsu administreerimistöödeks vajalikele paroolidele, võtmetele ja turvalubadele.

Juhul kui ettevõttes või asutuses on korraga tööl mitu võrdsete süsteemiteadmistega administraatorit, võivad nad üksteist ka vastastikku asendada, kui nende töökoormus seda võimaldab. Kõikide valdkondade puhul, kus põhivastutus IT-süsteemide haldamise eest lasub administraatoril, tuleks välja koolitada ka kaks asendajat, kuna kogemused on näidanud, et peaadministraatori eemalviibimise ajal ei pruugi ka tema ainukesel asendajal jätkuda alati piisavalt aega kõikide vajalike administreerimisülesannete täitmiseks. IT probleemivaba käitamise tagamiseks tuleb eriti just suuremate personalimuudatuste või organisatsiooni struktuuris toimuvate ümberkorralduste puhul kindlasti välja selgitada, kas ametisse määratud administraatorid ja nende asendajad suudavad eesseisva töökoormusega toime tulla. Eriti suure töökoormuse kasvuga tuleb arvestada nt kolimiste korral, mille raames peavad administraatorid lisaks oma tavatööle leidma aega veel ka täiendava asukoha sisseseadmiseks. Sellistes olukordades tuleb lisaks tagada, et vanas asukohas saaks töö kuni lõpliku ümberkolimiseni jätkuda tõrgeteta.

Kontrollküsimus:

- Mille alusel hinnati administraatori ja tema asendajate usaldusväärsust?

M 3.11 Hooldus- ja halduspersonali väljaõpe

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, personalijuht, IT-juht, kodukeskjaama eest vastutav töötaja, IT turvaosakond

Rakendamise eest vastutavad: juhid

Hooldus- ja halduspersonalil on tarvis üksikasjalikke teadmisi kasutatavate IT-komponentide kohta. Seetõttu tuleks vastavat personali koolitada vähemalt sellises mahus, **et nad suudaksid alljärgnevat:**

- viia iseseisvalt läbi igapäevaseid administreerimisega seotud tegevusi,
- tuvastada ja kõrvaldada iseseisvalt lihtsamaid vigu,
- viia iseseisvalt läbi regulaarseid andmevarundusi,
- mõista välise hoolduspersonali tehtud töid,
- tuvastada ja kiiresti kõrvaldada süsteemide suhtes toime pandavaid manipuleerimiskatseid ja volitamata juurdepääse.

Asjakohaseid koolitusi pakuvad reeglina kas IT-süsteemide või kodukeskjaamade tootjad. Kodukeskjaamade administraatorid peaksid **muu hulgas suutma ka alljärgnevat**:

- hinnata kodukeskjaama tööfunktsiooni, võttes aluseks vastavate seadmete küljes asuvad kontrollnäidud,
- kodukeskjaama iseseisvalt kasutusele võtta ja kasutusest kõrvaldada.

Kontrollküsimus:

- Kas administraatorid on läbinud vajaliku erialase koolituse?

M 3.12 Töötajate teavitamine kodukeskjaama (PBX) signaalidest ja teadetest

Algatamise eest vastutavad: kodukeskjaama eest vastutav töötaja, IT-turvaosakond, töötajate esindus

Rakendamise eest vastutavad: IT-turvaosakond, administraator

Kõik töötajad peaksid tundma kodukeskjaama hoiatavaid teateid, signaale ja sümboleid.

Siia alla kuuluvad ennekõike:

- Otsekõnest märku andev signaal
- Hoiatussignaal täiendava sidepartneri juurdelülitumise kohta
- Valjuhääldi sümbol
- Otsekõnest märku andev ekraaninäit
- Automaatse tagasihelistamise ekraaninäit
- Ekraaninäit/näidu muutumine kolme helistaja vahel toimuva konverentskõne kohta

Kuna teatud liiki funktsioonid, mille rakendamine võib olla keelatud (nt märkamatu juurdelülitumine) võivad endaga kaasa tuua IT-turvalisuse languse, peaksid töötajad eriti hästi tundma vastavate funktsioonide hoiatavaid ekraaninäite ja hoiatussignaale.

Kontrollküsimused:

- Kas töötajad suudavad tuvastada olukordi, kus keegi kolmas lülitub telefonivestlusesse?
- Kas töötajad teavad, milliste näitude või signaalidega annab telefon märku otsekõne funktsioonist?
- Kas telefonilt on võimalik välja lugeda, kas valjuhääldi on sisse lülitaud või mitte?

M 3.13 Töötajate teavitamine kodukeskjaama (PBX) kasutusega seotud ohtudest

Algatamise eest vastutavad: kodukeskjaama eest vastutav töötaja, IT-turvaosakond, töötajate esindus

Rakendamise eest vastutavad: IT-turvaosakond, administraator

Töötajaid tuleb informeerida digitaalse kodukeskjaama kasutamisega seotud ohtudest. See võib aset leida nt kas lühida juhendamise või infolehtede laialijagamise näol. Töötajatele tuleb selgitada, et kodukeskjaama tavapäratu käitumine on olukord, millest tuleb kindlasti informeerida asjakohaseid osapooli. Kodukeskjaama manipulatsioonide korral tuleks sellest informeerida mõnda sõltumatut kontrollorganit nagu IT-turvaosakond või andmekaitsespetsialist.

Kontrollküsimused:

- Kas teadlikkuse tõstmise meetmeid korratakse regulaarselt?
- Kas uutele töötajatele selgitatakse kodukeskjaama kasutamisega seotud võimalikke ohte?

M 3.14 Töötajate juhendamine informatsiooni ja andmekandjate edasiandmise korrektsetest protseduuridest

Algatamise eest vastutavad: organisatsiooni juht, IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: vastutav spetsialist, IT-turvaosakond

Töötajad peavad olema piisaval määral informeeritud raamtingimustest ja piirangutest, mida tuleb järgida informatsiooni edasiandmisel (vt M 2.45 Andmekandjate üleandmine). Pealiskaudse juhendamise tõttu võib tekkida palju erinevaid turvaprobleeme. Töötajaid tuleks muuhulgas informeerida näiteks järgnevast:

- Milliste suhtluspartneritega on lubatud vahetada erinevat liiki informatsiooni (vt M 2.42 Võimalike suhtluspartnerite määramine)?
- Millist liiki andmekandjaid tohib kasutada info edastamiseks andmekandjatega ning kuidas neid turvaliseks muuta?
- Enne suhtluspartnerile konfidentsiaalse info edastamist tuleb kontrollida tema identiteeti.

Lisaks tuleb kehtestada üldised reeglid, mida peab järgima andmekandjate vahetamisel ning need ka näiteks intranetis avalikustada. Töötajatele tuleb vastavate ettekirjutuste järgimine muuta kohustuslikuks. Kõiki andmekandjate vahetamises osalevaid töötajaid tuleb informeerida ka võimalikest konkreetsetest ohtudest, mis võivad tekkida nii enne transporti, selle kestel kui ka selle järgselt. Seetõttu tuleb töötajaid tingimata koolitada põhjalikult vastavate turvameetmete osas, mida nad on kohustatud järgima. Enne ootamatult postkasti saabunud digitaalsete andmekandjate lugemist tuleb saatjateks märgitud kontaktisikute käest järele küsida, kas nad on vastavad andmekandjad ka tegelikult saatnud või mitte (vt M 2.224 Trooja hobuste tõrje). Tundmatutelt saatjatelt laekunud saadetiste puhul tuleks saadetistest informeerida IT-turvaosakonda, välja arvatud juhul, kui juhtkond on kehtestanud teistsugused reeglid. Juhtudel, kus andmete edastamisel kasutatakse spetsiaalseid kaitsemehhanisme (nt krüpteerimist või kontrollsumma protseduuri), tuleb asjassepuutuvaid töötajaid piisavalt koolitada, et nad suudaks vastavaid mehhanisme ka turvaliselt kasutada.

Täiendavad kontrollküsimused:

- Kas kõikidele töötajatele on teada informatsiooni ja andmekandjate edastamisele kehtestatud reeglid?
- Kas töötajad on kursis sellega, kuidas tuleks vajadusel kasutada krüpteerimis- või kontrollsumma protseduure?
- Kas kõikidele töötajatele on piisavalt selgitatud erinevaid ohte, mis võivad tekkida andmevahetuse käigus?

M 3.15 Kõigi töötajate juhendamine faksi kasutamise alal

Algatamise eest vastutavad: IT-turvaosakond

Rakendamise eest vastutavad: IT-turvaosakond

Kõiki töötajaid tuleb informeerida eripäradest, mis on seotud info edastamisega faksi teel, ning sellest, et faksi teel saadetud dokumentide juriidiline kehtivus on oluliselt piiratud. Tavaliste faksiaparaatide kasutamise korral peaks faksiaparaadi juures olema ka lihtsasti mõistetav kasutusjuhend. Faksiserveri kasutamise puhul peaksid kasutajad saama vähemalt lühiülevaate faksi klienttarkvarast. Oluline on kindlaks määrata, vajadusel tööalase ettekirjutusena, järgnevad punktid:

- Faksi eest vastutav töötaja, kes hoolitseb muuhulgas ka selle eest, et sissetulnud faksid edastataks adressaadile ning faksiga seotud probleemide puhul teistele töötajatele kontaktisik.
- Faksiaparaadi või faksiserveri volitatud kasutajad.
- Ühtse faksiblanketi kasutamine.
- Konfidentsiaalse info edastamise keeld faksi saatmisel. Kui seda pole võimalik kehtestada, peaksid faksi saatja ja vastuvõtja enne kaitsmist vajava info faksi teel edastamist oma plaanides telefonitsi kokku leppima.
- Kohustus kasutada konfidentsiaalset infot sisaldavate faksisaadetiste puhul võimalusel krüpteerimistoega faksiaparaate.
- Kontrollida faksi korrektset kohaletoimetamist, st saadetise kohaletoimetamise kinnitust või edastuslogisid, lisada vastavad kinnitused saadetise dokumentide juurde ning korraldada vajadusel nende arhiveerimine.
- Kohustus teha automaatse faksiedastussüsteemiga varustatud faksiserveri kasutamisel sisenevatest faksidest kas väljatrükid või korraldada nende elektrooniline arhiveerimine.
- Kohustus luua faksiserveri kaudu väljuvatest faksidest dokumendikaustade jaoks väljatrükid, või need elektrooniliselt arhiveerida.
- Kohustus kontrollida aadressiraamatuid ja kättetoimetamise kontaktiloendeid, et vältida fakside saatmist valedele isikutele.

Täiendavad kontrollküsimused:

- Kas kõiki töötajaid on informeeritud faksi korrektsest kasutamisest ning kas uued töötajad läbivad asjakohase koolituse?
- Kas kõik töötajad teavad, kelle poole on võimalik faksiga seotud probleemide korral pöörduda?

M 3.17 Töötajate juhendamine modemi kasutamise alal

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: IT-turvaosakond

Töötajaid tuleb teavitada modemi kasutamisega seotud võimalikest ohtudest ning kohustuslikest turvameetmetest ja reeglitest. Eriti oluline on siinkohal informeerida töötajaid sellest, millist mõju võib avaldada modemi töökindlusele erinevate konfiguratsioonide valimine. Iga modemikasutaja peaks ennast kurssi viima modemi kasutamisega ning tegema endale selgeks, millised on vastava seadme võimalused ja piirid.

Täiendav kontrollküsimus:

- Kas kasutusjuhendeid ja ohutusjuhised hoitakse seadmete juures?

M 3.18 PC kasutajate väljalogimiskohustus

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: IT juht, IT-turvaosakond, kasutajad

Kui ühte IT-süsteemi või IT-rakendust kasutavad erinevad töötajad, kellele on antud erinevad õigused salvestatud andmetele või süsteemides asuvatele programmidele ligipääsemiseks, saab vajalikku turvet tagada vaid piisava juurdepääsukontrolli abil, milleks tuleb igal kasutajal ennast pärast oma tööülesannete sooritamist kas vastavast IT-süsteemist või IT-rakendusest välja logida. Kui töötajatel on võimalik mõne teise identiteedi all kas IT-süsteemis või IT-rakenduse all edasi töötada, on täiesti võimatu tagada mõistlikku juurdepääsukontrolli. Seetõttu tuleb kõiki töötajaid kohustada ennast pärast tööülesannete täitmist vastavast IT-süsteemist või IT-rakendusest välja logima. Tehnilistel põhjustel (nt selleks, et kõik avatud failid suletaks), tuleks IT-süsteemidest ja IT-rakendustest väljalogimisele kehtestada teatud reeglid ka siis, kui juurdepääsukontrolli ei rakendata.

Ekraanilukk

Kui töökohalt viibitakse eeldustekohaselt eemal vaid lühikest aega, võib väljalogimise asemel hoopis käsitsi sisse lülitada ka ekraaniluku (vt M 4.2 Ekraanilukk). Pikemaajalise eemalviibimise puhul tuleks kasutada seadistust, mis aktiveerib ekraaniluku automaatselt.

Automaatne väljalogimine

Mõningad IT-süsteemid ja IT-rakendused võimaldavad määrata kindlaks ajavahemiku, mille möödudes logitakse kasutaja, kes ei osale selle aja vältel aktiivselt üheski tegevuses, neist automaatselt välja. Antud võimluste kasutamist tuleks hoolikalt planeerida, kuna nende rakendamisega võib kaasneda andmekadude tekke oht. Automaatset väljalogimist võib rakendada nt arvutikogude (PC pools) puhul, mis on mõeldud suurele hulgale erinevatele kasutajatele, kuna sisseloginud kasutaja võib muidu mõne töökoha ekraaniluku volitamata sisselülitamise teel blokeerida. Lühiajalisele eemalviibimisele kehtestatavad reeglid, mida kasutajad peavad tingimata järgima, tuleb välja töötada vastavalt konkreetsete töökohtade iseärasustele. Ekraaniluku automaatne käivitumine peaks näiteks mitme kasutajaga süsteemide puhul toimima kiiremini kui üksikkasutaja süsteemis, st juba näiteks 5 minuti möödumisel.

Kontrollküsimused:

- Kas ka uusi töötajaid ning asendustöötajaid kohustatakse kehtestatud reegleid järgima?
- Kas väljalogimise kohustust tuletatakse töötajatele regulaarselt meelde?

M 3.20 Kaitsekappide kasutamise juhised

Algatamise eest vastutavad: IT-turvaosakond

Rakendamise eest vastutavad: IT-turvaosakond

Kaitsekappide muretsemise järel tuleb töötajatele selgitada nende korrektset käsitsemist. Töötajat tuleb juhendada ka siis, kui ta hakkab täitama uusi tööülesandeid, mis sisaldavad muuhulgas ka kaitsekappide kasutamist. Töötajatele tuleb edastada vähemalt järgmised juhised:

- Näidata kaitsekapi luku õiget kasutamist. Mainida tuleb tüüpilisi vigu, näiteks koodide segipaiskamata jätmist koodlukkude kasutamisel. Töötajatele tuleb selgitada võtmete haldamisele ja deponeerimisele kehtivaid reegleid ning töötajate asenduskorda. Ilmtingimata tuleb töötajatelt nõuda kaitsekappide sulgemist ka siis, kaitsekappe ei kasutata vaid lühikese aja jooksul.
- Serveri klaviatuuri tuleb kindlasti hoida serverikapis, et vältida volitamata sisestusi konsooli vahendusel.
- Serverikapi kasutamise puhul tuleb selgitada, et sinna ei tohi panna hoiule mittevajalikke süttimisohtlikke materjale (väljatrükke, üleliigseid käsiraamatuid, printeripaberit).
- Serveri varukoopiad sisaldavaid andmekandjaid tuleks hoida alati mõnes muus tuletõkketsoonis. Nende võib hoida serverikapis ainult juhul, kui mõnes muus tuletõkketsoonis hoitakse lisaks ka varukoopiaid.
- Konditsioneeriga varustatud serverikappide kasutamisel tuleks minimeerida aegu, millal serverikapp on avatud. Vajadusel tuleks aeg-ajalt ka kontrollida, et serverikappi poleks tekkinud kondensaati.

Täiendav kontrollküsimus:

- Kas inimesed, kes peavad käsitsema kaitsekappe, läbivad ka asjakohase koolituse?

M 3.21 Kaugtöötajate turbealane koolitus

Algatamise eest vastutavad: ülemused, IT-turvaspetsialist

Rakendamise eest vastutavad: ülemused, IT-turvaspetsialist

Kaugtöötajad täidavad oma tööülesandeid kas ajutiselt või ka alaliselt väljaspool tööandja või tööde tellija tööruume. Seetõttu kehtivad kaugtöö tegijatele ootuspäraselt veidi teistsugused turbemeetmed kui töötajatele, kes viibivad pidevalt oma tööandja tööruumides. Sellest tulenevalt on ka hädavajalik koostada institutsiooni üldkehtiva turvakontseptsiooni põhjal eraldi turvakontseptsioon ka kaugtöötajatele (vt M 2.117 Kaugtöötajate pääsu reguleerimine). Lisaks tuleks kaugtöötajatele koostada ka asjakohased turvasuunised ja need neile laiali jagada. Lähtuvalt kaugtöötajate jaoks loodud turvasuunistest tuleb töötajatele tutvustada asjakohaseid turvameetmeid ning vajadusel neid ka meetmete korrektse rakendamise alal koolitada.

Kaugtöötajaid koolitades tuleks ennekõike pöörata tähelepanu järgnevatele punktidele:

- Tööalaseid dokumente tuleb kaugtöökohas hoida turvaliselt, st pärast kasutamist tuleb need panna lukustada kappidesse.
- Kaugtöökohast lahkudes tuleb lukustada kõikvõimalikud välisuksed (ka rõdule ja terrassile viivad uksed).
- Kaugtöökohas kasutatavas ITs võivad teha struktuurilisi ja turbealaseid muudatusi ainult institutsiooni enda administraatorid.
- Kaugtöökohas kasutatavat arvutit tohib avalikesse sidevõrkudesse ühendada vaid selleks ettenähtud ühenduste kaudu. Isiklikul otstarbel kasutatavad kodujaama- ja internetiühendused peavad olema tööotstarbelistest eraldatud.
- Andmekandjatel põhinevaks andmevahetuseks institutsiooni IT-süsteemide ja kaugtöötaja töökoha PC vahel tohib kasutada vaid institutsiooni enda hangitud andmekandjaid. Andmekandjaid transportides tuleb arvestada, et need peavad ilmtingimata olema krüpteeritud, et nende võimaliku kaotsiminekuga ei kaasneks konfidentsiaalse info avalikustamine. Tööotstarbel ja eraviisiliselt kasutatavad IT-süsteemid ja andmekandjad tuleks hoida hoolikalt teineteisest lahus, et vältida muuhulgas nt kahjurvara levikut.
- Juurdepääsukaitsetega tuleb tagada, et kaugtöökohale ei eksisteeriks volitamata juurdepääse, rakendades selleks nt Boot - ja ekraanilukke. Paroole, ka neid, mis tagavad juurdepääsu töökohaarvutile ja andmesidearvutile, tuleb hoida salajas.

Lisaks tuleb kaugtöötajaid piisavalt koolitada kaugtöökohaarvutitega korrektselt ümberkäimise vallas et kaugtöötajad suudaksid iseseisvalt kõrvaldada lihtsamaid tõrkeid ja vigu (nt oskaksid vahetada printeri värvikassetti).

Kontrollküsimused:

- Kas kaugtöötajatele on tutvustatud nende töö eripärast tulenevaid turvakontseptsioone ja -suuniseid?
- Kas kaugtöötajaid on piisavalt koolitatud, et nad oskaksid turbemeetmeid ka ellu rakendada?

M 3.23w Sissejuhatus krüptograafia põhimõistetesse

Algatamise eest vastutavad: IT turvaosakond, IT-juht

Rakendamise eest vastutavad: IT turvaosakond, IT-juht

Krüpteerimist võimaldavate toodete rakendamisega võib kasutajate jaoks kaasneda täiendav töökoormus ja see võib olenevalt kasutatava toote keerukusest eeldada kasutajatelt koguni sügavamaid teadmisi. Seetõttu peaksid kõik töötajad, kes peavad hakkama oma töös kasutama krüptograafilisi tooteid või protseduure, läbima vastava koolituse, mis aitab neil mõista selliste lahenduste vajalikkust ja kasulikkust. Lisaks tuleks töötajaid koolitada ka krüptograafiliste põhimõistete vallas. Eriti kehtib see nende töötajate puhul, kes peavad hakkama tegelema krüptokontseptsiooni koostamise, krüptograafiliste toodete väljavalimise, installeerimise ja haldamisega. Järgneva teksti eesmärk on anda edasi elementaarseid teadmisi peamistest krüptograafias kasutatavatest mehhanismidest. Järgnevalt on püütud erinevate näidete põhjal selgitada, millistes situatsioonides tuleks kasutada erinevaid krüptograafilisi tehnikaid.

Krüptograafia koostisosad

Krüptograafilisteks meetoditeks nimetatakse erinevaid matemaatilisi meetodeid ja tehnikaid, mille abil püütakse kaitsta infot volitamata kättesaamise ja/või ettekavatsetud manipulatsioonide eest. Informatsiooni kaitsmise näol krüptograafiliste meetodite abil on vastupidiselt infrastruktuurilistele ja tehnilistele turvameetmetele tegemist matemaatilis-loogiliste kaitsemeetmetega. Krüpteerimisprotseduuride käigus rakendatakse matemaatilist arvutuskäiku – algoritmi –, muutes selle konkreetseks tehnikaks. Lahendus toimib selliselt, et potentsiaalsel ründajal tuleb lahendada teatud liiki matemaatiline probleem, millega ta ei pruugi toime tulla ning seda mitte piisavate oskuste puudumise, vaid väga konkreetse „võtmeinfo“ puudumise tõttu.

Krüptograafiliste meetodite rakendamise eelduseks on alati järgnev situatsioon:

andmete saatja A (tähistatakse krüptograafias tavaliselt nimega „Alice”) saadab läbi ebaturvalise andmeedastuskanali teate andmete vastuvõtjale B (tähistatakse nimega „Bob”). Saatja ja vastuvõtja võivad siinjuures olla ka identsed, andmeedastuskanalina võib käsitleda ükskõik millist andmete transportimisvõimalust. Kohapeal hoitavate andmete krüpteerimise puhul on saatja ja vastuvõtja muidugi samad, „kanali” all tuleb siinkohal käsitleda andmekandjat.

Krüptograafilised üldeesmärgid

Teoreetilistel ja praktilistel kaalutlustel eristatakse nelja krüptograafilist põhieesmärki:

1. Konfidentsiaalsus/salastatus: mitte ühelgi volitamata kolmandal osapoolel (nimetagem teda „Eve”) ei tohiks olla võimalik jõuda teate ehk faili sisuni.

2. Terviklus: tuvastada teate ehk failiga toimunud volitamata manipuleerimist (nt selle osade lisamist, ärajätmist, osade asendamist).

3. Autentsus:

- Identiteedi tõestamine (sidepartnerite omavaheline autentimine): anda sidepartnerile (nt isikule, organisatsioonile, IT-süsteemile) võimalus tõestada teisele sidepartnerile selgelt oma identiteeti.

- Päritolu tõestamine (teadete autentimine): A peab suutma B-le tõestada, et teade pärineb tõepoolest temalt, ning et teadet ei ole vahepeal muudetud.

4. Salgamatus (õiguslik siduvus, tagasilükkamatus): võrreldes teadete autentimisega on siinkohal põhitähelepanu tõestatavusel kolmandate osapoolte suhtes.

- Päritolu salgamatus: A-l ei tohi olla alust tagantjärele väita, et tema ei saatnud teadet vastuvõtjale B.
- Kättetoimetamise salgamatus: B-l ei tohi olla alust tagantjärele väita, et ta pole saatjalt A laekunud teadet kätte saanud.

Muidugi on loetletud valdkondade vahel veel ka omad seosed, kuid sellele vaatamata on tänapäevase krüptograafia peamised arusaamad siiski järgmised:

konfidentsiaalsuse ja autentsuse tagamist vaadeldakse kui krüptograafilise süsteemi kahte sõltumatut põhieesmärki: autentimine vähendab teate võimalike saatjate ringi, salastamine aga võimalikke vastuvõtjaid.

Krüpteerimine on peamine konfidentsiaalsust tagav krüptograafiline meede. Sõnumi terviklust, autentsust ja salgamatust (non-repudiation) tagavad peamised meetmed on räsifunktsioonid, sõnumiautentimiskoodid (message authentication code, MAC), ajatemplid, autentimisprotokollid, digiallkirjad.

Alljärgnevalt kirjeldatakse lühidalt peamisi krüptograafilisi kontseptsioone.

I. Krüpteerimine

Krüpteerimise (šifreerimise) käigus muudetakse loetav tekst olenevalt lisainfost, mis kannab nimetust „võti", vastavaks salatekstiks, mis jääb nendele, kellel puudub vastav juurdekuuluv võti, loetamatuks. Transformeerimist ehk salateksti muutmist loetavaks tekstiks nimetatakse dekrüpteerimiseks. Kõikides moodsates krüpteerimisalgoritmides on nii loetavad tekstid, salatekstid kui ka võtmed bitijadadena.

Selleks, et krüpteerimisalgoritmid oleksid ka reaalselt kasutatavad, peavad nad täitma vähemalt järgmisi tingimusi:

- Dekrüpteerimise kindlus, st ainuke viis, kuidas krüpteeritud teksti tohib olla võimalik dekrüpteerida, on kasutada selleks juurdekuuluvat võtit ning ennekõike peab kasutatavaid võtmeid olema piisavalt palju, et välistada kasutatavate võtmete tavapärast ükshaaval läbiproovimist.
- Algoritme peab olema võimalikult lihtne kasutada.
- Krüpteerimine ja dekrüpteerimine peavad toimima „piisavalt kiiresti".

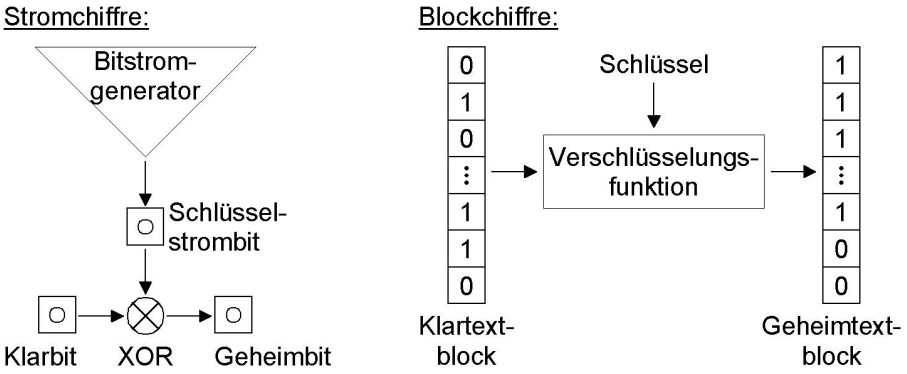
Dekrüpteerimise kindlust tuleb alati vaadelda koos kõige värskemate tehniliste ja matemaatiliste võimalustega. Krüpteerimisalgoritmide tõhususe hindamisel on tähtis, et nende rakendamise hetkel oleks praktiliselt võimatu krüpteeritud teksti võtit teadmata dekrüpteerida, st tehnikal, mida saab sel hetkel kasutada, peaks kuluma selleks üleliia palju aega.

Kui sidepartnerid A ja B soovivad luua teineteise vahel konfidentsiaalse ühenduse, toimivad nad järgmiselt:

1. Lepitakse kokku krüpteerimisprotseduuris.
2. Lepitakse kokku võti ehk võtmepaar.
3. A krüpteerib oma teate ja saadab selle adressaadile B.
4. B dekrüpteerib A käest vastu võetud salateksti.

Šifreerimisprotseduuride puhul on olemas kaks suurt klassi.

Sümmeetrilised krüpteerimisprotseduurid, mis kasutavad ühte ja sama võtit nii krüpteerimiseks kui ka dekrüpteerimiseks. Seetõttu nimetatakse sümmeetrilisi protseduure aeg-ajalt ka ühe-võtme-protseduurideks, kuna teksti šifreerimiseks ja dešifreerimiseks piisab ühe võtme tundmisest. Tuntud sümmeetrilised krüpteerimisprotseduurid on nt DES, Tripel-DES, IDEA või RC5. Sümmeetriliste protseduuride puhul tehakse veel täiendavalt vahet jadašifrite ning plokkšifrite vahel. Jadašifrite puhul genereeritakse võtme abil võimalikult juhusliku välimusega bitijada, mis liidetakse loetaval kujul bitijadale (modulo 2). Loetaval kujul bitijada krüpteeritakse bitt biti haaval (võtmejadabittide juurdeliitmise teel). Jadašifrite turbe tagamiseks on oluline, et ühe ja sama võtmejadaga ei krüpteeritaks mitte kunagi kahte (erinevat) teadet, mille vältimiseks tuleb rakendada spetsiaalseid meetmeid (sünkroonimisinfo vastava täiendava võtme näol). Jadašifrite näited: on RC4 ja SEAL.



Joonis: šifreerimine

Stromchiffre – jadašiffer; Blockchiffre – plokkšiffer, Bitstromgenerator – bitijada generaator; Schlüssel – võti; Schlüsselstrombit – võtmejadabitt; Verschlüsselungsfunktion – krüpteerimisfunktsioon; Klartextblock – loetaval kujul tekstiplokk; Geheimtextblock – salatekstiplokk; Klarbit – loetav bitt; XOR – XOR; Geheimbit – salabitt

Plokkšifrite puhul seevastu rakendatakse krüpteerimise käigus tervet šifrite plokki, mille suurus on tänapäeval reeglina 64 bitti. Enamiku sümmeetriliste krüpteerimisprotseduuride näol on tegemist plokkšifritega, kuhu kuuluvad muu hulgas ka DES, IDEA ning RC5. Plokkšifrite jaoks on defineeritud terve rida erinevat liiki tööviise (ning need on muudetud ka standarditeks).

Siia alla kuuluvad järgmised:

- ECB-tööviis (electronic code book mode, „koodiraamatulik tööviis”), mille puhul krüpteeritakse iga plokk teistest plokkidest sõltumatult eraldi;

- CBC-tööviis (cipher-block chaining mode, „krüptogrammiplokkide aheldusega tööviis”) ja CFB-tööviis (cipher feedback mode, „krüptoploki tagasisidega tööviis”), mille puhul rakendatakse olenevalt täiendavast käivitusvektorist šiffertekstiplokkide sõltuvust kõigi eelnevate šiffertekstiplokkide suhtes;
- OFB-tööviis (output feedback mode, „väljundi tagasisidega tööviis”), mille võib kokku võtta selliselt, et rakendatavat plokkšifrit kasutatakse vastava „plokijada“ genereerimiseks, mis liidetakse loetaval kujul plokkidele bitthaaval juurde (modulo 2).

Sümmeetriliste protseduuride kasutamisel tuleb arvestada, et mõlema sidepartneri vahel peab olema eelnevalt toimunud võtmevahetus. Võtme kättetoimetamine peab aset leidma turvaliste kanalite kaudu (nt kuller, isiklik üleandmine) ning lisaks peavad mõlemad sidepartnerid tagama, et vastavat võtit hoitakse salajas. Turvaliseks võtmevahetuseks on võimalik kasutada erinevaid protseduure. Suletud süsteemides pole võtmevahetusega tavaliselt erilisi probleeme, kuna sellistel juhtudel on turvalised kanalid juba loodud. Avatud süsteemides, kus eksisteerib suur hulk sidepartnereid, on selle korraldamine märksa keerukam. Peamine probleem on siinkohal asjaolu, et suure hulga sidepartnerite puhul on tegemist ka suure hulga võtmetega, mida on vaja enne side alustamist omavahel vahetada ning lisaks peavad potentsiaalsed sidepartnerid juba ette teada olema.

Asümmeetriline šifreerimisprotseduur kasutab seevastu hoopis kahte erinevat (matemaatiliselt omavahel suhestatud) võtit: avalikku võtit (public key) krüpteerimise otstarbeks ja privaatvõtit (private key) dekrüpteerimiseks. Vastaval võtmepaaril peavad olema järgnevad omadused: kõikidele neile, kes teavad ainult avalikku võtit, peab olema praktiliselt võimatu tuletada selle põhjal sinna juurde kuuluvat privaatvõtit või dekrüpteerida teateid, mille krüpteerimiseks on kasutatud avalikku võtit. Asümmeetriline krüpteerimine kätkeb endas nn ühesuunalist omadust: kui avalik võti ära unustatakse või ära kustutatakse, pole teate algse kuju taastamine enam võimalik. Nimetus avaliku võtmega krüpteerimine tuleneb sellest, et vastava avaliku võtme võib avalikustada, kartmata protseduuri turvalisuse kompromiteerimist. Privaatvõtit tuleb aga ilmtingimata salajas hoida.

Kui Alice tahab saata Bobile mõnda krüpteeritud teadet, peab ta muretsema endale vastavast vabalt juurdepääsetavast failist Bobi avaliku võtme ning krüpteerima selle abil Bobile saadetava teate. Pärast teate kättesaamist peab Bob Alice’i saadetud teate oma võtme abil dekrüpteerima. Juhtudel, kus Alice ja Bob soovivad kasutada konfidentsiaalsuse tagamiseks asümmeetrilist protseduuri, ei lähe neil võtmete vahetamiseks enam tarvis eraldi turvalist kanalit, kuid Alice peab siiski olema veendunud, et ta kasutab tõepoolest ikka Bobi avalikku võtit, mitte mõnda muud võtit, mille kohta on talle püütud jätta muljet, nagu oleks tegemist Bobi võtmega. Juhul kui Alice peaks krüpteerimiseks kasutama õige võtme asemel hoopis mõnda talle ettesöödetud võtit, võib vastav kurikael, kellel on teada sinna juurde kuuluv sobiv salajane võti, krüpteeritud teate lahti krüpteerida. Reeglina on teate saatjal tarvis mõne usaldusväärse kolmanda osapoole kinnitust, et tema kasutatav avalik võti kuulub tõepoolest vastavale

adressaadile. Nimetatud kinnituse ehk sertifikaadi loob enamasti samuti mõni krüpteerimisprotseduur ning see lisatakse avalikule võtmele.

Kaks tuntumat asümmeetrilist krüpteerimisprotseduuri on RSA-protseduur (nimi põhineb selle kolmel looja nimel: Rivest, Shamir, Adleman) ning ElGamali protseduur. Viimaste hulka kuuluvad ka elliptilistel kõveratel põhinevad krüpteerimisprotseduurid.

Sümmeetrilistel ja asümmeetrilistel šifreerimisprotseduuridel on osaliselt üksteist täiendavaid eelised ja puudused:

(Heade) sümmeetriliste protseduuride eelised:

- kiire toimimine, st võimaldavad suurt andmete läbilaskevõimet;
- turvalisuse määrab suures osa võtme pikkus, st heade sümmeetriliste protseduuride puhul ei tohiks probleeme tekitada ründed, mis põhinevad ainuüksi kõikide võtmete läbiproovimisel (jõuründed);
- kõrge turvalisus suhteliselt lühikeste võtmepikkuste juures;
- võtmete lihtne genereerimine, kuna võtmena on lubatud reeglina kasutada suvalist, kindla pikkusega bitijada ning samuti võib võtmeks valida ka juhuslikke arve.

Sümmeetriliste protseduuride puudused:

- iga osaleja on kohustatud kõikide oma sidepartnerite võtmeid salajas hoidma;
- võtmete omavaheliseks jagamiseks sobivad need vähem kui asümmeetrilised protseduurid, eriti paljude sidepartnerite korral;
- salgamatuse eesmärkidel on need kehvemini kasutatavad kui asümmeetrilised protseduurid, kuna sümmeetriliste krüpteerimisprotseduuride puhul ei ole üheselt äratuntav, kes kahest võimalikust sidepartnerist kõnealuse teate krüpteeris. Seda on võimalik välja selgitada ainult kolmanda osapoole sekkumisel, kes tuleb teadete liikumistesse kaasata vastavate krüptograafiliste protokollide abil.

(Heade) asümmeetriliste protseduuride eelised:

- konfidentsiaalses sides tuleb igal sidepartneril hoolitseda ainult enda privaatvõtme salajas hoidmise eest;
- kergem kasutada koos digitaalsete allkirjadega;
- elegantsed lahendused võtmete vahetamiseks võrgukeskkondades, kuna avalikke võtmeid ehk võtmesertifikaate võib salvestada vabalt ligipääsetavatesse tsentraalsetesse serveritesse, ilma et see ohustaks protseduuri turvalisust;

- sobivad hästi kasutamiseks salgamatuse tagamise eesmärgil.

Asümmeetriliste protseduuride puudused:

- aeglane toimimine, st võimaldavad enamasti vaid väga väikest andmete läbilaskevõimet;
- turvalisus: kõikide teadaolevate avaliku võtmega protseduuride puhul saab nende vastu kasutada palju paremaid ründemeetodeid kui lihtsalt kõikide võtmete läbiproovimist, mistõttu vajatakse nende puhul (vastupidiselt sümmeetrilistele protseduuridele) sama kõrge turvalisuse tagamiseks suhteliselt pikki võtmeid. Nende turvalisus baseerub „ainult" oletataval, kuid erialaringkondade tunnustatud matemaatilise probleemi algoritmilisel keerukusel (nt suure arvu tükeldamisel algfaktoriteks);
- võtmete genereerimine on reeglina keerukas ning ajamahukas, kuna eesmärk on vältida „nõrkade" võtmepaaride loomist.

Hübriidprotseduurid püüavad omavahel kombineerida mõlemat liiki krüpteerimise eeliseid: asümmeetrilist krüpteerimist kasutatakse selleks, et edastada sümmeetriliseks protseduuriks vajalik seansivõti (sessioon key) ja andmete põhimass krüpteeritakse sümmeetrilise protseduuriga. Seansivõtit rakendatakse reeglina ainult ühe seansi (andmeedastuse) tarbeks ning seejärel see hävitatakse. Asümmeetrilist võtmepaari kasutatakse olenevalt olukorrast ka pikema aja jooksul.

II. Tervikluse kaitse

Tervikluse kaitsmise eesmärk on tagada teate vastuvõtjale võimalus kindlaks teha, kas teade on jõudnud temani algsel, st võltsimata kujul. Tervikluse kaitsmise üldpõhimõte seisneb selles, et teate saatmisel teadet ei muudeta ega krüpteerita, kuid sellele pannakse kaasa teatud liiki täiendavat infot, mis lubab kontrollida, kas teade on jõudnud vastuvõtjani võltsitult või mitte. Eelduseks on siinkohal asjaolu, et kontrollimist võimaldav info peab jõudma vastuvõtjani muutmata kujul.

Seetõttu on kontrollandmetele kehtestatud järgmised nõuded:

- Kontrollimist võimaldavat infot peab olema võimalikult vähe, et andmeedastusele seeläbi lisanduv andmemaht jääks võimalikult väikseks.
- Kontrollinfo põhjal peab olema võimalik tuvastada praktiliselt kõiki teatega toimunud manipulatsioone, ka seda, kui muudetud on kas või ühte bitti.
- Kontrollinfot peab olema võimalik edastada manipuleerimata kujul ehk peab olema võimalik tuvastada, kas kontrollinfot on manipuleeritud või mitte.

Kontrollinfo arvutamiseks rakendatakse reeglina kahte järgnevat protseduuri: räsifunktsioone (hash) ja sõnumiautentimiskoode (message authentication codes).

(Ühesuunaline) räsifunktsioon kujutab endast andmete transformeerimist järgmiste omadustega:

- Tihendamisomadused (compression): suvalise pikkusega bitijadad teisendatakse kindlaksmääratud bitijadadeks, mille pikkus on reeglina algsest bitijadast lühem (enamasti 128–160 bitti).
- Ühesuunalisuse omadus: etteantud räsiväärtuse põhjal peab olema praktiliselt võimatu leida mõnda teadet, mille räsiväärtus vastaks etteantud räsiväärtusele.
- Vasturääkivuskindlus: ühe ja sama räsiväärtuse kohta peab olema praktiliselt võimatu leida kahte teadet, mis seostuksid mõlemad ühe ja sama räsiväärtusega.

Mõlemale sidepartnerile teadaoleva räsifunktsiooni abil on võimalik nii sidepartneril A kui ka B kontrollida teate terviklust. Alice rakendab oma teate suhtes räsifunktsiooni ning saadab teate Bobile koos sinna juurde kuuluva räsiväärtusega sellisel kujul, mis tagab räsiväärtuse võltsimiskindluse. Bob rakendab laekunud teatel omakorda räsifunktsiooni ning võrdleb oma tulemust Alice'i käest saadud räsiväärtusega. Kui mõlema väärtused kattuvad, võib oletada, et mitte ühtki bitti vastavast teatest ei ole vahepeal muudetud.

Sõnumiautentimiskood on krüptograafiline kontrollsumma teadete turvamiseks, st andmete transformeerimine, mille käigus lisandub arvutuskäiku salajane võti, mida iseloomustavad järgmised omadused:

- Tihendamisomadused (compression): suvalise pikkusega bitijadad teisendatakse kindlaksmääratud bitijadadeks, mis on reeglina algsest bitijadast lühemad.
- Võltsimiskindlus: kõigil, kellel ei ole võtit, peab olema praktiliselt võimatu välja arvutada mõne uue teate MAC-väärtust ja seda isegi siis, kui nende valduses peaksid olema mõned vanad teated koos nende MAC-väärtustega.

Kui Alice'il ja Bobil on MAC ja ühine salajane MAC-võti, autendib Alice oma teateid lihtsalt seeläbi, et laseb välja arvutada teate MAC-väärtuse ja saadab selle koos teatega edasi Bobile. Bob arvutab omakorda saadud teate MAC-väärtuse, kasutades selleks talle teadaolevat võtit. Kui saadud tulemus kattub Alice'i väärtusega, võib ta oletada, et teade on autentne (st teadet ei ole vahepeal muudetud ning see pärineb tõepoolest Alice'ilt). Seega autentis Alice oma teate Bobi jaoks seeläbi, et kasutas ainult talle ja Bobile teadaolevat võtit.

MACe konstrueeritakse tihti sümmeetriliste šifreerimisprotseduuride baasil. Kõige tuntum variant on siinkohal teadete krüpteerimine DESi abil või mõne muu plokk-šifreerimisprotseduuriga kas CBC- või CFB-režiimis. MAC-koodi moodustab sealjuures teatele viimasena lisatav krüpteeritud plokk. Nimetatud variantide kõrval esineb aga ka selliseid MACe, mis ei põhine šifreerimisprotseduuridel.

Teate MAC-väärtust võib vaadelda ka kui selle teate võltsimiskindlat, võtmest sõltuvat krüptograafilist kontrollsummat. MACide kasutamine autentimise eesmärgil eeldab mõlemalt sidepartnerilt, et nad peavad suutma tagada salajaste autentimisvõtmete turvalisuse. Tervikluse kaitsmise lisavõimalusena saab teate vastuvõtja äsja lühidalt kirjeldatud protseduuri abil veel ka täiendavalt kontrollida, kas teade, mille manipuleerimiskindlust on juba tõestatud, saab tõepoolest pärineda vastavalt kindlalt teadaolevalt saatjalt. Nimetatud järeldus võib põhineda eeldusel, et ainult sellel konkreetsel teate saatjal saavad olla krüpteerimiseks ning kontrollinformatsiooni kontrollimiseks vajalikud võtmed.

Ajatemplid

Ajatemplid võimaldavad kontrollida ja tõestada andmete terviklust. Ajatempli loomiseks arvutatakse esmalt andmetest räsifunktsiooni abil räsi, mis seejärel saadetakse päringuna ajatempliteenuse osutajale. Ajatempliteenuse osutaja kas signeerib saadetud päringu koos ajanäiduga (nn signeeritud ajatempel) või räsib päringu räsifunktsiooni abil kokku teiste (teistelt kasutajatelt) saadud päringutega ja valikustab (publitseerib) tekkiva räsi (nn räsitud ajatempel). Ajatempel tõendab, et andmeid (esitatud kujul) ei ole ajatempli väljastamise hetkest alates muudetud. Signeeritud ajatempel eeldab tõendina kasutatud digitaalsignatuuri algoritmi turvalisust, turvalist privaatvõtme haldust ja samuti teenuse osutaja usaldusväärsust. Räsitud ajatempel eeldab tõendina kasutatud räsifunktsiooni turvalisust ja publitseerimisel kasutatud andmekandja terviklust, kuid ei eelda turvalist võtmehaldust ega teenuse osutaja usaldusväärsust.

III. Autentsuse tõestamine

Kasutajate autentimisel sidepartnerite või IT-süsteemide ja klientide autentimisel serverite suhtes peaks olema võimalik

- tuvastada ja ära hoida volitamata juurdepääse,
- lubada volitatud juurdepääsude toimimist ning
- tagada tundlike andmete edastamisel läbi võrkude nende piisav kaitse.

Selleks on tarvis rakendada protseduure, mis lubaksid kõigil sides osalejatel veenduda kindlalt oma sidepartnerite identiteedis. Selle nõudega kaasneb ajaline aspekt: Alice'il on soov veenda Bobi reaalajas, et see on tõepoolest tema, kes Bobiga sidet peab. Põhilised tehnikad, mida selleks kasutatakse, on krüptograafilised pretensiooni ja vastusega protokollid (challenge-response-protokollid). Selleks saadab Bob Alice'ile andmeid ja esitab talle väljakutse (challenge) tõestada talle teatud saladuse tundmist (st võtmeinfo valdamist) ning Alice tõestab talle seda vastavat saladust konkreetselt avalikustamata, saates Bobile vastuse (response), mis sõltub saladusest ja saadud väljakutsest. Bob aga kontrollib saadud vastuse põhjal, kas talle laekunud vastuse arvutamiseks on kasutatud õiget saladust. „Tugeva" autentimise tagamiseks ei tohi vastavad väljakutsed korduda. Pretensiooni ja vastusega protokollide puhul võib rakendada nii sümmeetrilisi kui ka asümmeetrilisi tehnikaid.

Näide:

- Alice ja Bob lepivad eelnevalt kokku, et kasutavad sümmeetrilist krüpteerimisprotseduuri ning lepivad kokku ka ühise krüptograafilise võtme. Autentimise eesmärgil saadab Bob Alice'ile väljakutseks ühe juhusliku numbri. Alice krüpteerib saadud juhusliku numbri ühise salajase võtmega ning saadab tulemuse tagasi Bobile. Järgmise sammuna dekrüpteerib Bob vastuvõetud teate ja kontrollib, kas tulemus vastab tema alguses valitud juhuslikule arvule. Kui tulemused kattuvad, on tõepoolest tegemist Alice'iga, kuna ainult tema teab salajast võtit.

IV. Digitaalne allkiri

Digitaalse allkirja kui krüptograafilise konstruktsiooni eesmärk on luua digitaalsete failide ja teadete jaoks käsitsi antava allkirja vaste. Selleks rakendatakse mõningaid juba eelpool kirjeldatud krüpteerimisprotseduure, nagu räsifunktsioonid ja asümmeetriline protseduur. Digitaalsete allkirjade kasutamise peamine eeldus on asjaolu, et iga sidepartner peab valdama ühte ainult talle teadaolevat saladust, mille abil on tal võimalik ükskõik milliste failide juurde koostada oma digitaalne allkiri. Digitaalseid allkirju peab olema võimalik avalikult kättesaadava info põhjal kontrollida. Selliselt vaadelduna kujutab digitaalne allkiri endast spetsiaalset tervikluse kaitset, millel on veel täiendavad eripärad.

Digitaalne allkiri on teatele või failile lisatav kontrolliinfo, millega on seotud järgmised omadused:

- Digitaalse allkirja abil on võimalik üheselt kindlaks määrata, kes on selle allkirja koostanud.
- Lisaks on võimalik autentselt kontrollida, kas fail, millele vastav digitaalne allkiri on lisatud, on ka tõepoolest just seesama fail, mis selle digitaalse allkirjaga tegelikult allkirjastati.

Seega, kui avalikult ligipääsetava informatsiooni põhjal on võimalik kinnitada digitaalse allkirja õigsust, kinnitab see ühelt poolt allkirjastatud faili terviklust ning teiselt poolt ka selle salgamatust, kuna on selge, et vastavat digitaalset allkirja oli võimalik salajase info abil luua vaid inimesel, kes on eksimatult seostatav vastava digitaalse allkirjaga. Siinkohal tuleb arvestada, et erinevate failidega kaasnevad ka erinevad digitaalsed allkirjad ning seda, et ka kõige väiksemad failides toimuvad muudatused teevad digitaalsete allkirjade kontrollimise võimatuks.

Näide:

- Levinud näide digitaalsete allkirjade kasutamise kohta on RSA-protseduuri rakendamine ümberpööratud kujul. Selleks peab igal osalejal olema ainult talle teadaolev salajane allkirjastamisvõti. Avalikult ligipääsetavad on kontrollivõtmete sertifikaadid, kus on võltsimatul kujul ära toodud sobiva avaliku võtme ja sobiva salajase allkirjastamisvõtme omanikku kajastavate andmete vahelised seoses. Vastavaid sertifikaate väljastavad usaldusväärsed üksused, kes on eelnevalt kontrollinud osalejate isikuandmeid.

Digitaalse allkirja loomiseks ja arvutamiseks ükskõik millise faili jaoks toimitakse alljärgnevalt:

1. samm: Alice laseb vajaliku faili jaoks arvutada räsiväärtuse.

2. samm: Alice krüpteerib räsiväärtuse ainult talle teadaoleva salajase allkirjastamisvõtmega. Tulemusena valmibki selle faili jaoks Alice'i digitaalne allkiri.

3. samm: Alice saadab digitaalse allkirja koos kontrollivõtme sertifikaadi ja failiga Bobile.

4. samm: Bob kontrollib sertifikaati (nt mõne sertifitseerimiskeskuse avaliku võtme abil).

5. samm: Bob laseb saadud faili jaoks arvutada räsiväärtuse.

6. samm: Bob dekrüpteerib digitaalse allkirja, kasutades selleks kontrollivõtme sertifikaadis sisalduvat avalikku kontrollivõtit.

7. samm: Bob võrdleb omavahel sammus nr 4 arvutatud räsiväärtust ja dekrüpteeritud allkirja. Kui need on identsed, on sellega digitaalse allkirja õigsus tõestatud. Kui need ei ole identsed, puudub Bobil alus edasiste järelduste tegemiseks.

8. samm: pärast digitaalse allkirja õigsuse kontrollimist võib Bob teha järgmised lõppjäreldused:

- Kui on tõestatud, et salajane võti on tõepoolest ainult Alice'i valduses, võib Bob olla kindel, et kontrollivõtme sertifikaadis sisaldunud digitaalse allkirja on loonud tõepoolsest Alice.
- Temani jõudnud fail on identne failiga, mille jaoks Alice lasi arvutada oma digitaalse allkirja.

Siinkohal tuleb rõhutada, et digitaalsed allkirjad suudavad tagada eranditult vaid terviklust ja salgamatust, kuid need ei taga mitte mingil moel konfidentsiaalsust. Digitaalselt allkirjastatud teade edastatakse loetava teksti kujul ning juhul, kui see on konfidentsiaalne, tuleb seda veel täiendavalt krüpteerida. Kui digitaalselt allkirjastatud fail sisaldab allkirjastaja tahteavaldust, on võimalik vastavat tahtevaldust ümberlükkamatult ja vajaduse korral ka kohtus seostada vastava allkirjastajaga. Kasutatud kontrollivõtmete sertifikaadid on omakorda usaldusväärses üksuses digitaalselt allkirjastatud failid, mida on võimalik analoogselt kontrollida ning mis annavad infot kontrollivõtme ja isiku kohta, kes valdab selle juurde kuuluvat salajast võtit.

Siinkohal juhime tähelepanu digitaalsete allkirjade ja MACide vahelisele erinevusele:

- Digitaalse allkirja õigsust on võimalik kontrollida igaühel, kellel on kontrollivõtme sertifikaat, MACe seevastu saavad kontrollida vaid need osapooled, kelle valduses on salajane autentimisvõti.
- Alice'i failidele lisatavaid digitaalseid allkirju saab koostada ainult Alice, teate MAC-väärtust on seevastu võimalik genereerida mõlemal osapoolel, st nii Alice'il kui ka Bobil (ja ka kõikidel teistel, kellel on olemas salajane autentimisvõti).

Sel põhjusel on MACe võimatu kasutada salgamatuse tagamise eesmärgil.

Võtmehaldus

Krüpteerimise korral tekib alati ka kohustus hoida krüpteeringuid piisavalt turvaliselt. Tekib küsimus, kuidas oleks võtmeid kõige otstarbekam

- koostada/lähtestada,
- kokku leppida / rakendada,
- laiali jagada / transportida,
- vahetada/värskendada,
- salvestada,
- kinnitada/sertifitseerida,
- tagasi võtta,
- hävimise/kaotamise puhul taastada,
- hävitada/kustutada,
- arhiveerida ja
- deponeerida (usaldusväärselt hoiule jätta).

Nimetatud aspekte tuleb vaadelda võtme kogu kasutusea kontekstis. Võtmehalduseks on võimalik kasutada krüptograafilisi tehnikaid ning enamasti just seda ka tehakse. Kõikide krüptomoodulite tarbeks tuleb juurutada krüptograafial põhinev turvasüsteem. Salajasi võtmeid tuleb kaitsta volitamata leidmise, muutmise ja asendamise eest. Avalikke võtmeid tuleb kaitsta volitamata muutmise ja asendamise eest. Informatsiooni kaitsmine krüptograafiliste meetodite abil eeldab enekõike sobiliku võtmehalduse olemasolu. Võtmehalduse tagamiseks läheb tarvis ressursse, mida rakendatakse vaid sellel ühel otstarbel!

Sertifitseerimisüksused

Sertifitseerimisüksusi (trust center) läheb tarvis alati siis, kui kasutajate arv on juba paisunud liiga suureks ning tekib soov võtta kas digitaalsete allkirjade või krüpteerimise jaoks kasutusele asümmeetrilised krüpteerimisprotseduurid. Sellised protseduurid vajavad allkirja koostamisel ehk krüpteerimisel teistsugust võtit kui allkirja kontrollimisel ehk dekrüpteerimisel. Selleks koostatakse kasutajaga seotud omavahel korrespondeeriv võtmepaar. Üks võti, nn avalik võti tehakse avalikult ligipääsetavaks. Teine võti, nn privaatvõti tuleb hoida absoluutselt saladuses. Privaatvõtmega, st tõepoolest vaid selle võtmega, on võimalik koostada digitaalset allkirja või siis teksti dekrüpteerida ning ainult sinna juurde kuuluva avaliku võtmega, st eranditult selle võtmega, on võimalik kontrollida teksti õigsust või seda krüpteerida. Kui tekib vajadus kindlustada avalike võtmete ehtsus ja tagada ka võtmete turvaline seostamine nende omanikega, läheb tarvis juba mainitud sertifitseerimisüksust, mis kinnitab isiku seotust avaliku võtmega oma väljastatava sertifikaadi abil.

Nimetatud sertifitseerimisüsketes tegeletakse reeglina järgmiste ülesannetega:

- Võtmete genereerimine: võtmeid genereeritakse sertifitseerimisüksusele ja vajaduse korral ka sides osalejatele.
- Võtmete sertifitseerimine: osalejate andmed, korrespondeerivad avalikud võtmed ja täiendavad andmed kogutakse kokku sertifikaadiks ning sellel lisatakse sertifitseerimisüksuse digitaalne allkiri.
- Isikupärastamine: sertifikaat ning olenevalt olukorrast ka avalik ja privaatvõti kantakse üle mõnele digitaalallkirja komponendile (reeglina mõnele kiipkaardile).

- Identifitseerimine ja registreerimine: osalejad identifitseeritakse isikut tõendava dokumendi alusel ning seejärel registreeritakse.
- Kataloogiteenus: sertifikaadid tehakse mõne avalikult ligipääsetava kataloogi kaudu kättesaadavaks. Lisaks peab kataloogiteenuse kaudu olema võimalik hankida infot selle kohta, kas sertifikaat on suletud või mitte.
- Ajatempliteenus: teatud liiki andmete puhul võib olla vajalik seostada need mõne usaldusväärse ajahetkega. Selleks lisatakse andmetele vastava ajahetke kinnitus ning lõpptulemusele lisatakse omakorda ajatempliteenuse digitaalne allkiri.

Lisateenusena võivad sertifitseerimisüksused pakkuda ka veel võtmete hoiustamist, kui krüpteerimiseks on tarvis kasutada krüptograafilisi võtmeid. Et võimaldada krüpteeritud andmete kasutamist ka pärast võtme kaotsiminekut, pakutakse võtme omanikule (ja ainult talle) võimalust luua võtmest duplikaat, mis pannakse hoiule sertifitseerimisüksuse turvalistesse tingimustesse.

Võtmeväljastuskeskused

Sümmeetriliste krüpteerimisprotseduuride turvalisus sõltub sellest, kas ühiselt kasutatav salajane võti on teada ainult nendele kasutajatele, kes on volitatud konfidentsiaalse infoga ümber käima. Kui salvestatud andmetele peab olema juurdepääs vaid andmete omanikul, on turbe tagamine küllaltki lihtne, kuna vastaval omanikul tuleb kaitsta ainult oma võtit, et keegi võõras ei saaks seda enda valdusesse. Hoopis teine on aga olukord siis, kui üks sidepartner tahab edastada teisele ebaturvalise sidekanali kaudu teateid, mida on tarvis kaitsta sümmeetrilise krüpteerimisprotseduuriga. Sellistel juhtudel peab salajane võti olema nii saatjal kui ka vastuvõtjal, st sidepartnerite vahel peab eksisteerima võimalus rakendada turvatud andmevahetust. Praktikas realiseeritakse see sageli sidevõtmete krüpteeritud laialijagamisega, milleks kasutatakse nn võtmeväljastuskeskusi (key distribution centre, KDC), mille käigus ehitatakse võtmetest üles terved turvatehniliselt üksteisest sõltuvad hierarhiad. Siin rakendatavad protseduurid on kohati väga keerulised ning sõltuvad oma turbeotstarbest tulenevalt väga paljudest erinevatest komponentidest, eriti KDCde füüsilisest, organisatoorsest, personalialasest ja tehnilisest turvalisusest ning ka KDCdega sidepidamiseks kokkulepitud võtmetest. Salajase võtme kompromiteerimine, st selle avalikuks tulek kellelegi volitamata kolmandale osapoolele toob endaga kaasa kõikide selle võtmega krüpteeritud andmete ehk kõikide sellest võtmest sõltuvate andmete konfidentsiaalsuse kadumise. Nimetatud olukord võib olla eriti kriitiline juhtudel, kus kompromiteeritakse mõnda võtmeväljastushierarhia tsentraalse tähtsusega võtit.

Krüptoprotseduuride rakendamine

Pädeva rakendamise korral pakuvad krüptograafilised protseduurid suurepärast kaitset järgmiste ohtude vastu:

- informatsiooni jõudmine volitamata isikuteni,
- andmete teadlik manipuleerimine volitamata isikute poolt,
- andmete omanikuinfoga manipuleerimine.

Kõikide ohtude vältimiseks ei piisa siiski ainult krüptograafia kasutamisest.

- Krüptograafiliste meetodite kasutamine ei aita mitte vähimalgi määral kaasa andmete käideldavuse tagamisele (krüpteerimisvõimaluste ebapädeva kasutamise korral ähvardab koguni andmekao oht!).
- Krüptograafilised meetodid ei suuda mitte midagi ette võtta teenusetõkestusrünnete vastu (vt G 5.28 Teenuse halvamine). Need võivad aga kaasa aidata vastavate rünnete varajasele tuvastamisele.
- Need ei aita ka info juhuslike võltsingute (nt „müra“ tagajärgede) vastu. Kuid need võimaldavad võltsimisi tagantjärele kindlaks teha.

M 3.26 Personali juhendamine IT-vahendite turvalise kasutamise kohta

Algatamise eest vastutavad: infoturbeametnik, IT-juht, personalijuht

Rakendamise eest vastutavad: personaliosakond, ülemused

Paljud turvaprobleemid saavad alguse kas IT väärast kasutamisest või selle valest konfigureerimisest. Selliste probleemide ennetamiseks tuleb kõikidele töötajatele ja kõikidele asutusevälistele IT kasutajatele tutvustada asutuse IT-vahendite turvalist kasutamist. Selleks tuleb kõiki töötajaid teavitada ja koolitada (vt lisaks M 2.198 Personali teavitamine infoturbe küsimustest ja M 3.5 Turvameetmete koolitus).

Kõikidele IT-kasutajatele tuleb selgeks teha, millised õigused ja kohustused neil IT-vahendite kasutamisel on. Neile tuleks kätte jagada spetsiaalsed suunised, mida nad peavad IT kasutuse raames järgima. Vastavas suunises peaks olema kirjeldatud, millised on raamtingimused IT-süsteemide kasutamisel ja milliseid turvameetmeid peab järgima. Siinkohal on tähtis, et kasutajatele oleks selgelt ja üheselt arusaadavalt välja toodud, millised tegevused on neile täiesti keelatud. Vastavad suunised peavad olema kohustuslikud, arusaadavad, ajakohased ja alati käepärast.

Suuniste kohustusliku iseloomu dokumenteerimiseks peaksid need olema varustatud kas ametiasutuse/ettevõtte juhtkonna või vähemalt IT-spetsialisti allkirjaga. Neid soovitatakse koostada lühidalt ja arusaadavalt, nii et neid jagatakse näiteks postrite, märkmelehtede, flaierite, kaartide ja muu seesugusena. Lisaks peaksid need olema kättesaadavad ka intraneti keskkonnas. Kasutajasuunised peaksid põhimõtteliselt sisaldama üksnes reegleid, mida saab ka kasutada ning mis on sõnastatud nii positiivselt kui võimaik.

Kasutajasuunises võiks lause

„Kasutajatele on keelatud tegeleda omaalgatuslikult tarkvara installeerimisega.”

kõlada hoopis nii:

„Kõik IT-süsteemid on varustatud standardse konfiguratsiooniga, mille loomisel on arvestatud teie töötingimuste eripäradega, et pakkuda teile maksimaalset turvalisust. Probleemide korral suudame teile standardse konfiguratsiooni uuesti installeerimisega garanteerida kiire lahenduse. Seetõttu, kui vähegi võimalik, ärge palun muutke seadistusi. Kui tekib vajadus kasutada täiendavat riist- või tarkvara, pöörduge palun kasutajatoe poole.”

Täiendavaid kasutajasuuniste näiteid leiate IT etalonturbe abivahendite alt.

Kasutajasuunised peavad sisaldama vähemalt järgmisi üldist IT kasutust puudutavaid punkte:

- juhis, et ükskõik milliseid IT-süsteeme või IT-komponente tohib kasutada ainult konkreetse loaga,
- juhis, et IT-süsteemide teavet võivad muuta vaid need isikud, kes on selleks volitatud;
- paroolide kasutamine (vt M 2.11 Paroolide kasutamise reeglid);
- lubamata tarkvara kasutamise keeld (vt M 2.9 Aktsepteerimata riist- ja tarkvara kasutuse keeld);

- juhis, et ametialaseid IT-süsteeme tohib kasutada üksnes ametialasteks eesmärkideks või olemasolu korral selle reegli võimalike erandite täpne kirjeldus;
- juhised, kuidas IT-süsteeme ja andmekandjaid turvaliselt hoida ning üles seada;
- kaitse arvutiviiruste ja muu kahjurvara eest;
- andmevarunduste tegemine;
- internetiteenuste kasutamine.

Lisaks nimetatud suunistele peavad kasutajate jaoks olemas olema ka selged eeskirjad, kus sätestatakse, kes tohib erinevale teabele ligi pääseda, kellele tohib teavet edasi anda ja milliseid meetmeid rakendatakse vastavate eeskirjade rikkumiste puhul.

Kui töötaja lahkub töökohalt, peab ta eelnevalt veenduma, et kõiki töövahendeid (dokumente, andmekandjaid jne) hoitakse turvaliselt (vt lisaks M 2.37 Korrastatud töölaud). Kõik IT-süsteemid peaksid olema varustatud paroolidega, et kaitsta neid volitamata juurdepääsu eest. Järelevalveta IT-süsteemide korral tuleb arvuti vähemalt lukustada. Kõikide IT-süsteemide aluskonfiguratsioon peaks olema koostatud võimalikult suurte piirangutega. Töökohaarvutite standardne konfiguratsioon peaks võimaldama kasutada vaid selliseid teenuseid, mida ühe kasutajagrupi liikmed ka tõepoolest vajavad (vt lisaks M 4.109z Tööjaamade tarkvara reinstalleerimine). Täiendavaid programme ja funktsioone tuleks paigaldada või sisse lülitada vaid juhul, kui töötajaid on eelnevalt õpetatud, kuidas nendega ümber käia ning kui töötajaid on teavitatud ka võimalikest turvaprobleemidest.

Iga kasutajatele mõeldud suunis tuleks välja töötada koostöös puudutatud rühmade esindajatega, eriti oluline on kaasata sellesse õigel ajal ka töötajate esindus ning andmekaitse- ja infoturbeametnikud. Iga kasutajasuunise muudatuse korral tuleb jälgida, et kõik puudutatud isikud oleksid alati varakult kaasatud. Muudetud kasutajasuunised tuleb kõikidele kasutajatele ka teatavaks teha.

Tööülesannete kirjelduses peaksid olema kirjas ka infoturbe seisukohast olulised ülesanded ja kohustused. Siia alla kuulub muu hulgas nt ka kohustus järgida majasiseseid infoturbesuuniseid (vt lisaks M 2.198 Personali teavitamine infoturbe küsimustest). Kõik, kes on tunnistajaks olukorrale, kus IT-süsteeme või teenuseid rakendatakse vastupidiselt ametiasutuses või ettevõttes kehtestatud eesmärkidele, peaks sellest viivitamata oma ülemusele teatama.

Kontrollküsimused:

- Kas kõikidele IT-kasutajatele on tutvustatud asutuse IT-vahendite turvalist kasutamist?
- Kas IT-vahendite kasutuse jaoks on olemas kohustuslik, lihtsasti mõistetav, ajakohane ja kättesaadav suunis?

M 3.27 Koolitus Active Directory haldamiseks

Algatamise eest vastutavad: IT-juht, IT-turbespetsialist

Rakendamise eest vastutavad: IT-juht, administraator

Active Directory on Windows Server tsentraalne andmebaas, kuhu saab koondada kasutajaandmeid, grupikuuluvuse infot ja muud halduseks vajalikku infot. Samuti saabActive Directory's hallata kliente.

Windows-võrgu haldamiseks läheb tarvis detailseid teadmisi nii Active Directory'st kui ka selle aluskontseptsioonidest. Vastasel korral on oht väärkonfiguratsioonide tekkeks, mille tagajärjeks võivad olla märgatavad turvatehnilised puudujäägid. Administraatorite teemakohane koolitamine, eriti aga Active Directory turvamehhanismide osas, on seetõttu lausa vältimatu.

Koolituse sisu

Algteadmised

Sõltuvalt võrgu suurusest ja keerukusest, ei pruugi Active Directory kasutamine olla mitte sugugi ainult ühe administraatori õlul, vaid sellega võib tegeleda ka terve rida spetsiaalsete ülesannete ja valdkondadega seotud erinevaid administraatoreid. Sellest tulenevalt ei vaja kõik Active Directory't haldavad administraatorid ilmtingimata ühesugust koolitust. Süsteemi turvalise käitamise tagamiseks peaks aga siiski iga administraator omama piisavalt algteadmisi, et ta oleks võimeline oma kitsaid tööülesandeid nägema ka üldkontekstis. Igal juhul peaksid koolitused sisaldama järgnevaid punkte ja neid ka selgitama. Kui sügavalt konkreetne administraator üksikuid punkte tundma peab, sõltub tema tulevasest tegevusvaldkonnast.

Põhitõed

- Ülevaade Windows-serverite turvamehhanismidest.
- Muudatused värskete Windows-Client-operatsioonisüsteemide turvamehhanismides (arvestades operatsioonisüsteemide uute versioonidega või värskete Service Pack'idega kaasnevate muudatustega).
- Turvahaldus (MMC, Security Editor, GPMC).
- Active Directory ja DNS
- Domeenidevahelised usaldussuhted
- Kõikide domeenikontrollerite kui Kerberos-andmekandjate hädavajalik füüsiline kaitse.

Active Directory

- Üldinfo: Planeerimine, juurutamine, administreerimine
- Skeemihaldus
- Replikeerimine
- Andmevarundus
- Volituste jagamine
- Autentimine
- Grupipoliitikad

PKI (Public Key Infrastruktuur)

- PKI toimimisviis

- Sertifikaadid ja sertifikaatide erinevad tüübid
- PKI kasutuselevõtu planeerimine
- PKI juurutamine
- PKI haldamine
- Kasutajate suhtlemine PKIga

EFS (Encrypting File System)

- EFSi toimimisviis
- EFSi konfigureerimine (Recovery-Agent, sertifikaadid)
- Võtmete varukoopiate loomine
- Krüpteeritud kujul salvestatud failide kaitsmine võrgusides

IPSec

- IPSec'i toimimisviis
- IPSec'i konfigureerimine
- Kolmanda tootja ipsecmon.exe või IPSec-Monitor'iga ümberkäimine

WFP (Windows File Protection)

- WFP toimimisviis
- WFP konfigureerimisvõimalused

DFS (Distributed File Service)

- DFSi toimimisviis
- DFSi administreerimine
- DFS-struktuuri planeerimine
- DFSi kaudu ligipääsetavate andmete turve

Active Directory üksikuid alateemasid tuleks käsitelda järgneva detailsusega:
Skeemihaldus
Tavajuhtudel pole Active Directory skeemi muutmine selle kasutuselevõtust tulenevate põhjuste tõttu sugugi hädavajalik. Selles osas võib koolitus piirduda ka skeemi muutmisest tulenevate probleemide ja tagajärgede selgitamisega. Kui aga süsteemis on planeeritud teha individuaalseid muudatusi, tuleb vastavalt ka Active Directory koolituse raames tegeleda asjakohaste täiendavate teemadega.

Active Directory replikeerimine

- Active Directory replikeerimiseks rakendatavad mehhanismid (RPC ja SMTP)
- Active Directory sisu replikeerimiseks kasutatavad eelseadistatavad parameetrid

- Active Directory detsentraliseeritud haldamisega kaasnev probleemistik seoses replikeerimiskonfliktidega

Andmevarundus

- Probleemid seoses Active Directory varukoopiate loomisega
- Domeenikontrollerist loodud varukoopia sisselugemine
- Domeenikontrollerite avarii korral rakendatavad kohustuslikud meetmed, mis sisaldavad endas FSMO-rolle

Volituste jagamine Active Directory's

- Pääsuõiguste jagamine AD-objektidele atribuudi tasandil
- Pääsuõiguste pärimine ja pärimisfunktsiooni blokeerimine
- Võimalikud pääsuõigused
- Administratiivsete ülesannete delegeerimine üksikute OUde tasandil

Autentimine

- Kerberos
- PKI
- Smart Cards

Grupipoliitikad

- Lokaalsed grupipoliitikad ja Active Directory'sse salvestatud grupipoliitikad
- Grupipoliitikate abil teostatavad konfigureerimisvõimalused
- Millistes olukordades kasutatakse grupipoliitikaid? Kuidas on neid võimalik konfigureerida?
- Grupipoliitika objektid (GPOd) on Active Directory's olevad objektid
- Grupipoliitika objekte on võimalik siduda asukohtade / domeenide / OUdega
- Grupipoliitikate läbitöötamise järjekord
- Võimalused grupipoliitika kasutamise kontrollimiseks
- Grupipoliitikate pääsuõiguste jagamine
- Grupipoliitika objekti sidumisel AD-objektiga kaasnev võimalus No Override
- AD-objektide omadus Block Policy Inheritance

Kontrollküsimused:

- Kas kõiki administraatoreid on koolitatud Active Directory'ga töötamise vallas?
- Kas kõikide turvamehhanismide käsitsemist on selgitatud, kas kasutuskeskkonna jaoks vajalikke funktsioone suudetakse tuvastada?

M 3.28 Windowsi klientoperatsioonisüsteemide turvamehhanismide koolitus kasutajatele

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: ülemused, IT-juht

Windows operatsioonisüsteemidega arvutitesse salvestatud andmete turvalisus sõltub suures osas ka sellest, kui hästi oskavad kasutajad Windows turvamehhanismidega ümber käia. Nende efektiivseks rakendamiseks tuleks Windows arvutite kasutajaid vastavalt koolitada.

Turvamehhanismidele lähenemine kasutaja vaatevinklist

Windows arvutite kasutamisel on võimalik suur osa turvaseadistusi kasutajate jaoks vastava eeltöö ja eelseadistustega juba administraatorite poolt ette paika panna. Ühesuguste ja kontrollitavate arvutikonfiguratsioonide saavutamiseks on selline eeltöö lausa vältimatu (M 2.326 Windows 7 grupeerimissuuniste planeerimine).

Isiklike failide ja kaustade pääsuõigused

Mõningaid turvalisust puudutavaid seadistusi saavad teha ka kasutajad ise. Siia kuuluvad nt kasutaja isiklikele failidele ja kaustadele antavad juurdepääsuõigused. Vastavaid pääsuõigusi on võimalik nii piirata kui ka laiendada üksikute kasutajate ning ka kasutajagruppide lõikes. Kui teatud kasutaja jaoks konfigureeritud pääsuõigustes peaks tekkima konflikt (nt põhjusel, et vastav kasutaja ei kuulu ei kasutajagruppi A ega -gruppi B, kuid juurdepääs on lubatud vaid grupile A ning grupile B on see keelatud), siis sellisel juhul juurdepääs tõkestatakse. Enamasti kehtib ka siin reegel, et juurdepääs kasutaja isiklikele failidele on administraatori poolt juba eelseadistatud ning uutele failidele ja kaustadele kantakse vastavad pääsuõigused üle automaatselt. Kuna aga kasutajatel on reeglina võimalik vastavaid pääsuõiguseid ka ise muuta, peab iga kasutaja tingimata eelnevalt läbima ka asjakohase koolituse (vt M 4.149 Windows'i faili- ja ühiskasutusõigused).

Krüpteerimissüsteem

Üheks täiendavaks valdkonnaks, mida koolitused peaksid ilmtingimata käsitlema, on EFSi (Encrypting File System 'i) kasutamine. Lisaks tüüpilistele eksimustele, mida EFSi kasutamise käigus ette tuleb, peaksid koolitused ennekõike keskenduma selgitustööle, millises ulatuses on võimalik EFSiga kaitsta failide konfidentsiaalsust ning kus on selle kaitse piirid (vt M M 4.147z EFS-i turvaline kasutamine Windows 'i keskkonnas). Windows 7 korral tuleks analüüsida ka seda, kas paralleelselt oleks mõistlik kasutada veel ka BitLockeril põhinevat kõvaketta krüpteerimist ja krüptofailisüsteemi EFS. Kasutajatele tuleks kindlasti õpetada, kuidas võtmeinfot õigesti hallata, et tagada andmete käideldavus. BitLockeril põhineva kõvakettakrüpteerimise kasuks otsustamisel (vt M 4.337z BitLockeri Drive Encryption kasutamine) tuleb funktsiooni kasutamise koolitusel töötajatele kindlasti selgitada ka selle lahendusega saavutatavat konfidentsiaalsuse turbeastet.

Samuti tuleb töötajatele koolituse raames tutvustada BitLockeriga seotud autentimisprotseduuri, mida rakendatakse Windows 7 käivitamisel, taastamisparooli kasutamise põhimõtteid ja kõnealuse turbelahenduse kaitsetoime piire. Windows 7

pakub andmete varundamiseks erinevaid lahendusi (vt M 6.76 Avariiplaani koostamine Windowsi süsteemi tõrke puhuks).

Töötajatele tuleb selgitada, milliseid andmevarunduslahendusi nad peaksid kasutama. Samuti peavad töötajad teadma, kus varundatud andmed asuvad, kuidas varukoopiatele vajaduse korral juurde pääseda ja mida nad peavad andmete taastamiseks tegema.

Koolituse sisu

Windows klientoperatsioonisüsteemide turvalist kasutamist käsitleva koolituse hädavajalikud teemad võtavad kokku järgmised märksõnad:

NTFS failisüsteemi pääsuõiguste rakendamine

- Failide kaitsmine pääsuõigustega
- Pääsuõiguste pärimine
- Failide kopeerimine ja ümberpaigutamine
- Faili üleandmine uuele kasutajale
- Töötajate teadlikkuse tõstmine pääsuõigustest tulenevast failide turbe vähenemisest
- Administraatoriõigustega kasutajatega kaasnevad ohud seoses neile avaneva võimalusega pääsuõigustest mööda hiilida
- Otsene juurdepääs riistvarale (nt vargus) loob võimlause pääsuõigustest mööda minna
- Failid ei ole võrgu kaudu transportimisel kaitstud
- Kasutajakontode haldamise (UAC) funktsioon, tööpõhimõtted ja käsitsemine (vt M 4.430 Logiandmete analüüs), juhul kui kasutajad sellega kokku puutuvad Integreeritud Windows Firewalli kasutamine
- Tööpõhimõte ja kaitsetoime

EFSi kasutamine (vt M 4.147z EFS-i turvaline kasutamine Windows ’i keskkonnas)

- EFSi kasulikkus (EFS pakub failidele täiendavat konfidentsiaalsuskaitset)
- EFSi käsitsemine
- Probleemid seoses nn tagantjärele krüpteerimisega
- Sobiva parooli valimine (EFSi efektiivsuse tagamisel on määravaks parooli kvaliteet)
- Täiendava start-parooli kasutamine läbi SYSKEY (oluline lokaalsete kasutajakontode rakendamisel
- Teadlikkuse tõstmine kaitse vähenemisest, mis on tingitud EFSi kasutamisest
- Administraatoriõigustega kasutajatega kaasnevad ohud seoses neile avaneva võimalusega krüpteeringust mööda hiilida.
- Krüpteeritult salvestatud failid ei ole võrgu kaudu transportimisel kaitstud, välja arvatud juhul, kui EFSi kasutatakse koos WebDAViga.
- EFS-i kasutamine Windows 7 keskkonnas BitLockeri täiendusena, juhul kui krüpteerimist on tarvis kasutada samal ajal, kui süsteem töötab.

BitLockeri kasutamine Windows 7-s

- Krüpteeritud ja krüpteerimata partitsioonid
- BitLockeri kaitsetoime avaldub vaid siis, kui süsteem on välja lülitatud (offline-krüpteering)
- Sobiv ümberkäimine autentimisvahenditega (USB-pulgad ja/või PIN-koodid)
- Taastamisparooli kasutusotstarve ja nende sobiv käsitsemine, juhul kui kasutajad nendega kokku puutuvad
- Reageerimine BitLockeri veateadetele, eelkõige juhtudel, kus on tuvastatud tervikluse rikkumine

Täiendavad turvasuunised

- Failide turvaline kustutamine (vt M 4.56 Turvaline kustutus Windows operatsioonisüsteemides)
- CD-ROMide automaattuvastust ehk Autostart -funktsiooni käsitlevad turvasuunised (vt M 4.57 CD-ROMi automaattuvastuse blokeerimine)
- Turvasuunised USB-salvestusvahendite turvaliseks kasutamiseks (vt M 4.200z USB-salvestuskandjatega ümberkäimine ja M 4.339 Vahetavate andmekandjate volitamata kasutamise tõkestamine Windows 7-s)
- Turvasuunised Windows 7 turvatehnoloogiate, nagu Security Center, Windows Firewall ning WPA (WiFi Protected Access), turvaliseks kasutamiseks
- Kasutajakontode haldamise (UAC) funktsioon, tööpõhimõtted ja käsitsemine (vt M 4.340 Windows kasutajakonto haldamise (UAC) kasutamine alates Windows 7-st), juhul kui kasutajad sellega kokku puutuvad

Kontrollküsimused:

- Kas Windowsi operatsioonisüsteemide turvalise kasutamise kohta on töötajatele läbi viidud asjakohane koolitus?
- Kas töötajaid on juhendatud isiklike failide pääsuõiguste väljajagamise osas?
- Kas kasutajaid on teavitatud tarkvaratööriistade turvamehhanismide olemasolust ning kas neile on õpetatud nende õiget rakendamist?

M 3.29 Novell eDirectory haldamise koolitus

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: IT-juht, administraator

eDirectory-kataloogiteenuse haldamiseks läheb tarvis detailseid teadmisi nii sellest tootest kui ka selle aluskontseptsioonidest. Vastavate teadmiste puudumise korral on oht väärkonfiguratsioonide tekkeks, mille tagajärgedeks võivad olla märgatavad turvatehnilised puudujäägid. Seetõttu on administraatorite koolitamine selles valdkonnas möödapääsmatu. Järgnevalt on toodud lühike kokkuvõte teemadest, mida tuleks käsitleda administraatorite koolitusel.

Hierarhiline struktuur

eDirectory-kataloogiteenuse struktuuri iseloomustab puukujuline hierarhiline ülesehitus. Kataloogipuu üksikud sõlmpunktid koosnevad *Container* -objektidest, mis võivad omakorda sisaldada veel teisi objekte, ning nn *Leaf* -objektidest, mis moodustavad kataloogipuu lõpp-punktid (lehed). Iga objekt kuulub kindla objektiklassi alla. Objektiklass määrab kindlaks väärtused ehk atribuudid või ka omadused, mida on võimalik omistada vastavasse objektiklassi kuuluvale objektile. Lisaks defineeritakse neis veel ka hierarhilisi suhteid, nt määrates, millised võivad olla potentsiaalsed isa- ja laps-objektid. Selleks eksisteerib eDirectory's juba terve hulk eelnevalt defineeritud objektiklasse. Objektiklasside definitsioonid määratletakse nn skeemis. Kui üksikute objektiklasside definitsiooni on tarvis muuta, näiteks vastava atribuudikogumi täiendamisega, siis saab seda teha skeemi muutmise ehk täiendamise abil. Skeemi muutmine on vaieldamatult üks kõige tundlikumaid tegevusi, mida ühes eDirectory-kataloogipuus üleüldse teha annab. Selline muudatus mõjutab kogu puud, mistõttu tuleb puu senine kontseptsioon uuesti põhjalikult läbi mõelda. Seetõttu nõuab eDirectory skeemi administreerimine põhjalikku kataloogiteenuse tundmist ning suuri teadmisi turvalisusest.

Pääsuõigused ja õiguste pärimine

Kataloogiteenuse igale üksikule objektile ja igale objektiklassile saab objekti üksikutele atribuutide lõikes kehtestada eraldi pääsuõigusi. Pääsuõiguste sidumine leiab sealjuures aset *Trustee* -suhete baasil, st ACL'i (*Access Control List* 'i) tehakse vastavad *Trustee* -sissekanded. Võimalikud õigused ulatuvad seejuures *Supervisor* -tasemest, st täielikust administreerimisõigusest, kuni sirvimisõiguseni (*browse*), mis võimaldab vastava kataloogipuu lõiguga ainult tutvuda. Objektidele kehtestatud pääsuõigused päranduvad seejuures standardselt puu hierarhias ülevalt alla. Pärimisprotsessi on aga siiski võimalik ka mõjutada, milleks tuleb rakendada nn pärimisõiguste filtrit ehk IRFi (*Inherited Rights Filter* 'it). Selle abil on võimalik automaatset pärimist välja lülitada. Lisaks on võimalik üksikute objektide, st objektiklasside X ja Y vahel defineerida veel ka nn turvaekvivalendid. Selle käigus saavad kõikidest objekti X *Trustee* 'dest automaatselt ka objekti Y *Trustee* 'd, st objektiga Y seotakse vähemalt samasugused pääsuõigused nagu objektiga X.

Efektiivsed volitused

eDirectory-juurdepääsu puhul rakenduvad tööle *efektiivsed volitused* , mis kujutavad endast eespool kirjeldatud õiguste väljajagamise tagajärgi ning need arvutatakse iga üksiku juurdepääsu korral dünaamiliselt eraldi.

Autentimine

Intraneti keskkonnas rakendavad kasutajad eDirectory'sse pääsemiseks vastavat klienttarkvara. Kliendi juurdepääs eDirectory kataloogiteenusele toimub läbi tootjafirma protokolli, mille käigus edastab eDirectory sisselogiva kasutaja privaatvõtme kliendile krüpteeritult. Vastavasse krüpteeringusse on kaasatud kasutaja

parool. Kui klient sisestab nüüd oma parooli, on tal võimalik privaatvõti dekrüpteerida ning kliendi ja eDirectory-serveri vahel leiab aset autentimine, milleks kasutatakse *Challenge-/Response* -protseduuri. Pärast edukat autentimist on kasutajal olemas talle eDirectory kataloogiteenuse kasutamiseks määratud pääsuõigused.

LDAP-juurdepääs

Võrgurakendused ja internetikasutaja pöörduvad eDirectory kataloogiteenuse poole tavaliselt LDAP-protokolli (*Lightweight Directory Access Protocol* 'i) vahendusel. Standardsete lahendustena eksisteerivad siinkohal kolm ühenduse liiki: *anonymous bind* , *proxy user anonymous bind* ning *NDS-user bind* . Siinjuures kehtib eelseadistus, et anonüümsele *Login* 'ile antakse pääsuõigused objektile [Public], millega on standardina seotud terve kataloogipuu piiramata sirvimisõigus (*browse*). Anonüümne *Login* ei eelda autentimise toimumist. Parooliga autentimist saab konfigureerida selliselt, et parooli lubatakse edastada kas loetava teksti kujul või mitte. Turvatud ühenduse puhul läbi LDAP saab kasutada SSL-protokolli, ning lisaks saab koguni valida, kas rakendada ühe- või kahepoolset autentimist.

Sertifikaatide server

eDirectory-sertifitseerimisserver on olulise tähtsusega õiguste määramisel ja seega süsteemi turvalisuse jaoks. Sertifikaadi haldamisest sõltuvad ka võrgus asetleidvad autentimised, samuti krüpteeritud kanali loomine SSLi (*Secure Sockets Layer* 'i) kaudu. Seetõttu on eDirectory-sertifitseerimisserveri administreerimine väga oluline.

Partitsioonide loomine

eDirectory-kataloogiteenus võimaldab skaleeritavuse ja jõudluse parandamiseks kataloogiteenuse andmebaasi ka mitme serveri peale laiali partitsioneerida. Kataloogipuu partitsioneerimisel tuleb järgida tervet rida erinevaid reegleid.

Replikeerimine

Sarnaselt sellele eelnenud toodetega toetab ka eDirectory-kataloogiteenus replikatsioonide loomist, et tõsta veatolerantsi ja võimaldada süsteemi suuremat läbilaskevõimet. Replikatsioonidest eksisteerib erinevaid liike, nt *Master Replica* , *Read/Write Replica* , *Read-Only Replica* , *Filtered Read/Write Replica* , *Filtered Read-Only Replica* ning *Subordinate Reference Replica*.

Rollidel põhinev administreerimine ja delegeerimine

eDirectory toetab rollidel põhinevat administreerimist ning administreerimisülesannete delegeerimist. Sõltuvalt planeerimise käigus vastu võetud otsustest tuleb asuda koolitama erinevaid administraatoreid, lähtuvalt nende konkreetsetest tööülesannetest. Eriti kehtib see skeemiadministraatorite kohta, kes peavad olema võimelised tegema muudatusi kogu andmebaasi ülesehituses terve kataloogipuu raames (vt eelpool).

Klienttarkvara

Ka eDirectory-klienttarkvara ja LDAP-pääsuõiguste administreerimine eeldab administraatoritelt põhjalikke teadmisi süsteemi konfigureerimisvõimaluste kohta. Seejuures on turvakeskkonna defineerimisel oluline roll kasutataval operatsioonisüsteemil, eriti oluline on see failisüsteemi turvalisuse jaoks. Lisaks tuleb võimalikult täpselt oma ülesannetesse pühendada veel ka nii sisselogimise kui ka seire eest vastutavad administraatorid.

Koolituse sisu

Algteadmised

Sõltuvalt eDirectory-kataloogipuu suurusest pole kataloogipuu administreerimine tavaliselt mitte ainult ühe, vaid on mitme administraatori ülesanne, kellest igal on oma eriülesanded ja tegevusvaldkonnad. Sellest tulenevalt ei vaja kõik

eDirectory-kataloogi haldavad administraatorid sugugi mitte ühesugust koolitust. Süsteemi turvalise käitamise tagamiseks peaks aga siiski iga administraator omama piisavalt algteadmisi, et ta oleks võimeline nägema oma kitsaid tööülesandeid ka üldkontekstis. Igal juhul peaksid koolitused sisaldama järgnevaid punkte ja neid ka selgitama. Kui sügavalt konkreetne administraator üksikuid valdkondi tundma peab, sõltub tema tulevasest tegevusvaldkonnast.

Põhitõed

- Ülevaade eDirectory turvamehhanismidest
- Turvahaldus (ConsoleOne, iMonitor)
- Puustruktuur ja nimeteisendus
- Pärimine kataloogipuu piires
- Kõikide eDirectory-serverite, kaasa arvatud replikatsioonide hädavajalik füüsiline kaitse

Kataloogiteenus

- Üldinfo: Planeerimine, juurutamine, administreerimine
- Skeemihaldus
- Partitsioonide loomine
- Replikeerimine
- Andmevarundus
- Volituste jagamine
- Õiguste pärimine ja efektiivsete õiguste arvutamine
- Autentimine

Public Key infrastruktuur (PKI)

- PKI toimimisviis
- Sertifikaadid ja sertifikaatide erinevad tüübid
- PKI kasutuselevõtu planeerimine
- Kasutajate suhtlemine PKI'ga
- eDirectory-peamised haldusobjektid
- eDirectory-sertifikaadiserveri administreerimine

Secure Sockets Layer (SSL)

- SSL-protokolli tööpõhimõte
- SSLi konfigureerimine

Lightweight Directory Access Protocol (LDAP)

- LDAP-juurdepääs eDirectory'le
- Kasutajate võimalikud ühendamisviisid

Novell Client

- Novell Client'i tööpõhimõte

- Novell Client'i autentimine

Üksikuid alateemasid tuleks käsitleda järgneva detailsusega:
Skeemihaldus
Tihti pole eDirectory skeemi muutmine administraatori poolt selle kasutuselevõtust tulenevatest põhjustest sugugi hädavajalik. Selles osas võib koolitus piirduda ka skeemi muutmisest tulenevate probleemide ja tagajärgede selgitamisega. Kui aga skeemis on planeeritud teha individuaalseid muudatusi, tuleb vastavalt ka eDirectory koolituse raames tegeleda täiendavate asjakohaste teemadega.
Replikeerimine

- Replikeerimiseks rakendatavad mehhanismid
- eDirectory sisu replikeerimiseks kasutatavad eelseadistatavad parameetrid
- eDirectory detsentraliseeritud haldamisega kaasnev probleemistik seoses replikeerimiskonfliktidega

Andmevarundus

- Probleemid seoses eDirectory varukoopiate loomisega
- eDirectory-serverist loodud varukoopia sisselugemine
- eDirectory puustruktuuri defineerivate serverite avarii korral rakendatavad kohustuslikud meetmed (st esimene eDirectory installatsioon kataloogipuu sees)

Volituste jagamine eDirectory's

- Pääsuõiguste jagamine eDirectory-objektidele atribuudi tasandil
- Pääsuõiguste pärimine ja pärimisfunktsiooni blokeerimine
- Turvaekvivalentide defineerimine
- Efektiivsed pääsuõigused
- Rollidel põhinev administreerimine
- Administratiivsete ülesannete delegeerimine

Ka neil juhtudel, kus eDirectory-kataloogi ja selle baasiks oleva operatsioonisüsteemi administreerimisega seotud töörollid on teineteisest lahutatud, tuleks siiski ka eDirectory-administraatoritele tagada vajalikud algteadmised vastava operatsioonisüsteemi kohta. Vastasel korral võib see raskendada koostööd võimalike probleemide lahendamisel.
Täiendavad kontrollküsimused:

- Kas kõiki administraatoreid on koolitatud eDirectory'ga töötamise vallas?
- Kas töötajatele on õpetatud kõikide oluliste turvamehhanismide käsitsenud?

M 3.30 Novell eDirectory klienttarkvara kasutamise koolitus

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: IT-juht, juhid

Intraneti keskkonnas kasutamiseks installeeritakse eDirectory-kataloogiteenus kas ühele või reeglina pigem mitmele serverile. eDirectory's loodud kasutajad ja kasutajagrupid saavad kataloogiteenuse poole pöörduda neile eDirectory kasutamiseks jagatud volituste alusel, kasutades selleks sobivat eDirectory klienttarkvara. Sõltuvalt rakendatava klienttarkvara liigist leiab juurdepääs eDirectory'le kasutaja jaoks aset piisavalt arusaadavalt, mistõttu pole kasutajatele ilmtingimata hädavajalik teha täiendavaid koolitusi eDirectory-tarkvara eripärade kohta. Kui aga rakendatav klient eeldab kasutaja autentimist eDirectory suhtes nagu näiteks Novell Client for Windows'i puhul, tuleb kasutajaid siiski koolitada, käsitledes vähemalt järgmisi punkte:

- Login-mehhanismi tööpõhimõte ja selle kasutamine.
- Paroolide kasutamine.
- SSL-autentimise rakendamine kasutaja sertifikaadi või parooli abil.

LDAP-klienttarkvara rakendamisel, mis lubab kasutajal läbi lapata hierarhiliselt koostatud kataloogipuud või lubab sõnastada LDAP-atribuutide tasandil oma päringuid, tuleb kasutajaid täiendavalt koolitada järgmistel teemadel:

- eDirectory infomudeli ülesehitus
- päringute efektiivne sõnastamine

Lisaks tavapärastele kataloogiteenuse klientidele (Novell Client for Windows ning Unix-operatsioonisüseemide Libraries) saab eDirectory's kasutada veel ka üht täiendavat klient-rakenduste klassi, mis on loodud spetsiaalselt kasutajate haldamiseks (ka heterogeensetes) IT-kooslustes: Novell Account Management mooduleid. Vastavad rakendused on seotud juba konkreetsete operatsioonisüsteemide sisselogimisfunktsiooniga ning võtavad sellega enda kanda ka kasutajate autentimise. Lisaks on tervele reale erinevatele platvormidele (Linuxile, FreeBSDle, HP-UXile, MVSile, OS/390le, Solarisele) saadaval ka

- Kasutaja autentimine
- Kataloogipuu läbilappamine
- Erinevad Clientrakendused NDS-AS'id (NDS Authentication Service).

NDS-AS eeldab Netware'i kasutamist (alates versioon Netware 5.0, SP 4A). Autentimine on eDirectory-kataloogiteenuste turvalise käitamise tagamisel väga olulisel kohal. Kataloogiteenuse poolt vaadelduna peab siinkohal olema tagatud, et autentimine leiaks ühelt poolt aset nii kliendi poolt süsteemi suhtes ning teiselt poolt kindlasti ka kasutaja poolt kliendi suhtes. Autentimise edukal läbimisel võimaldab eDirectory kasutajale automaatselt ligi pääseda kõikidele tema jaoks lubatud objektidele ja teenustele (nn Background Authentication). Sel moel toimib Single Sign-On.

Autentimise käigus läbitakse järgnevad sammud:

- Kasutaja sisestab Novell Client'i oma kasutajanime, mis suunatakse otse edasi eDirectory'le.
- eDirectory otsib oma kataloogist välja selle juurde kuuluva privaatvõtme ja dekrüpteerib selle.
- Antud krüpteerimisse on kaasatud nii kasutaja parool kui ka kliendi saladus.
- Nimetatud krüpteeritud private key edastatakse päringu esitanud kliendile.
- Seejärel küsitakse kasutajalt tema parooli, mille ta edastab kliendile.
- Seejärel dekrüpteerib klient saadud parooli ja Client-Credential'i abil privaatvõtme ja hoiab seda oma töömälus.

Tuginedes nimetatud private key'le ning sertifikaadis olevale vastaspoolele, leiab aset tegelik autentimine eDirectory suhtes vastava Challenge-/Responseprotseduuri abil. Kui see osutub edukaks, logitakse kasutaja sisse ning kasutaja privaatvõti kustutatakse kliendi töömälust. Väljapoole jääb süsteemist seeläbi mulje nagu oleks tegemist paroolkaitsega turvatud autentimisskeemiga, seestpoolt vaadelduna on aga tegemist asümmeetriliste krüptograafiliste mehhanismide kasutamisega. eDirectory-serveritesse salvestatud andmete turvalisus sõltub suures osas ka sellest, kui hästi oskavad kasutajad turvamehhanismidega ümber käia. Nende efektiivseks rakendamiseks tuleks kasutajatele korraldada vastavaid eDirectoryklienttarkvara kasutamise koolitusi. Turvamehhanismidele lähenemine kasutaja vaatevinklist eDirectory-klienttarkvara kasutamisel on võimalik suur osa turvaseadistusi kasutajate jaoks vastava eeltöö ja eelseadistustega juba administraatorite poolt ette paika panna. Ühesuguste ja kontrollitavate klientkonfiguratsioonide saavutamiseks on selline eeltöö lausa vältimatu. Mõningaid turvalisust puudutavaid seadistusi peavad aga kasutajad tegema ka ise. Näiteks operatsioonisüsteemi tasandil kuuluvad selle alla reeglina kasutaja isiklikele failidele ja kaustadele antavad juurdepääsuõigused. Failidele antavate pääsuõiguste haldamine otse läbi eDirectory vahendite on rakendatav vaid Single SignOn Challenge-Responseprotseduur Isiklike failide ja kaustade pääsuõigused failiserverite puhul, mille operatsioonisüsteemiks on Netware. Kaudselt on võimalik juurdepääse failidele hallata ka teiste platvormide puhul, milleks on tarvis kasutada Organizational Roles funktsioone.

Koolituse sisu
Järgnevas loetelus püütakse kokku võtta olulisemad koolituste teemad. Loetelust tuleks vastavalt konkreetsele kasutusvaldkonnale teha sobilik valik:

- Login-mehhanismi tööpõhimõte ja selle kasutamine.
- Paroolide kasutamine
- SSL-autentimise rakendamine kasutaja sertifikaadi või parooli abil
- eDirectory infomudeli ülesehitus
- Päringute efektiivne sõnastamine
- Baasteadmised kasutatavate operatsioonisüsteemide ja nende turvakonfiguratsiooni kohta
- Failide turvaline kustutamine (vt M 4.56 Turvaline kustutus Windows operatsioonisüsteemides).

Täiendavad kontrollküsimused:

- Kas kasutajaid on koolitatud eDirectory turvalisuse vallas?
- Kui kasutajatele on kataloogiteenuse all antud volitused pääsuõiguste jagamiseks enda objektidele, kas neid on ka koolitatud vajalike kontseptsioonide ja mehhanismide osas?
- Kas kasutajaid on teavitatud tarkvaratööriistade turvamehhanismide olemasolust ning kas neid on koolitatud nende õige rakendamise vallas?

M 3.31 Exchange 2000 süsteemiarhitektuuri ja turbealane koolitus administraatoritele

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: IT-turvaosakond, IT-juht

Exchange 2000 süsteemi korrektseks ja turvaliseks haldamiseks on vastutavate administraatorite koolitamine möödapääsmatu. Juba väikesed vead konfiguratsioonis võivad vähendada süsteemi turvalisust. Sel põhjusel tuleb administraatoreid informeerida Exchange 2000 süsteemiarhitektuurist ning eeskätt tuleb neile edastada teadmised kõikvõimalike turvamehhanismide kohta.

Teadmised Active Directory kohta

Exchange 2000 integreerub suures osas Windows 2000 Active Directory'ga. Active Directory on Windows 2000'de tsentraalne andmebaas, kuhu salvestatakse kasutajaandmed, grupikuuluvuse info ja muud halduseks vajalikud andmed. Sel põhjusel läheb Exchange 2000'de administreerimiseks tarvis teadmisi Active Directory'st ja selle aluseks olevatest kontseptsioonidest. Vastasel korral võivad kergesti tekkida väärkonfiguratsioonid, mille tagajärjel võivad turvalisuses tekkida märgatavad puudujäägid. Seetõttu on administraatorite koolitamine selles valdkonnas möödapääsmatu. (vt M 3.27 Koolitus Active Directory haldamiseks).

Routing Group

Exchange 2000'de installeerimisel mõnele Windows 2000 serverile leiab aset skeemi täiendamine, et luua spetsiaalsed Exchange-objektid ning genereerida olemasolevate objektide jaoks ka täiendavad atribuudid. Edasises installeerimistöös on tarvis määratleda nn *Routing Group* 'id ning *Administrative Group* 'id. *Routing Group* kätkeb endas kokkuliidetud Exchange 2000 servereid, mis suhtlevad omavahel suurel ribalaiusel. Administratiivne grupp määrab kindlaks meilisüsteemi, st osasüsteemide administratiivsed piirid. Antud piirid võivad olla ka domeeniülesed, kuid need peavad jääma siiski *Forest* 'i piiridesse.

Global Catalog Server

Exchange 2000 süsteem eeldab pidevalt käideldava *Global Catalog Server* 'i olemasolu, mida pakuvad spetsiaalsed Windows 2000 domeenikontrollerid. Lisaks peavad olema sisse seatud ja korralikult toimima ka Windows 2000 võrguteenused (eriti DNS). Seejärel tuleb sisse seada välised ühendused ning vajadusel ka ühendused võõraste meilisüsteemidega nagu nt X.400 või ccMail'iga. Selle käigus tuleb aktiveerida vajalikud protokollid ning vastavatele tulemüüridele tuleb defineerida asjakohased reeglid. Seejärel tuleb konfigureerida veel meilikontod ja uudistegrupid. See tehakse Windows 2000 grupipoliitikatega. Täiendavaid üldisi juhised leiate M 2.231 Windowsi grupipoliitika planeerimine . Kirjeldatavad valdkonnad puudutavad aga ainult Exchange/Outlook 2000-süsteemi serverikomponente. Terviksüsteemi jaoks on veel täiendavalt oluline ka klient-komponentide administreerimine. Vastavalt eespool lühidalt kirjeldatud protseduurile tekib selle tagajärjel terve rida erinevaid administratiivseid ülesandeid, mille lahendamisega peavad hakkama tegelema kas üks või mitu antud valdkonnale spetsialiseerunud meeskonda. Süsteemi sujuvaks käitamiseks on seetõttu on ülimalt oluline, et administraatorid ja nende asendajad on läbinud intensiivse koolituse. Administraatorite koolitus peaks käsitlema vähemalt järgnevaid teemasid:

Põhitõed

- Ülevaade Windows 2000'de turvamehhanismidest
- Turvahaldus (MMC-Snap-In)

- Active Directory ja DNS
- Domeenidevahelised usaldussuhted
- Juurdepääsukontrolli tagamise võimalused serverites

Active Directory

- Replikeerimine
- Active Directory replikeerimiseks rakendatavad mehhanismid (RPC ja SMTP)
- Active Directory sisu replikeerimiseks kasutatavad eelseadistatavad parameetrid
- Active Directory detsentraliseeritud haldamisega kaasnev probleemistik seoses replikeerimiskonfliktidega
- Andmevarundus
- Probleemid seoses Active Directory varukoopiate loomisega
- Domeenikontrollerist loodud varukoopia sisselugemine
- Volituste jagamine
- AD-objektide pääsuõigusi saab laiali jagada ainult atribuutide tasandil
- Pääsuõiguste pärimine ja pärimisfunktsiooni blokeerimine
- Võimalikud pääsuõigused
- Administratiivsete ülesannete delegeerimine üksikute OU'de tasandil
- Grupipoliitikad
- Lokaalsed grupipoliitikad ja Active Directory'sse salvestatud grupipoliitikad
- Grupipoliitikate poolt võimaldatavad konfigureerimisvõimalused
- Millistes olukordades kasutatakse grupipoliitikaid? Kuidas on neid võimalik konfigureerida?
- Grupipoliitika objektide (GPOde) käsitlus Active Directory objektidena
- Grupipoliitika objekte on võimalik siduda asukohtade / domeenide / OUdega
- Grupipoliitikate läbitöötamise järjekord
- Võimalused grupipoliitika kasutamise kontrollimiseks (pääsuõigused, *No Override* , *Block Policy Inheritance*)

Exchange 2000

- Exchange 2000 süsteemi arhitektuur
- Rutiinsete ülesannete aluskontseptsioonid
- Marsruutimisrühmad (*Routing Groups*)
- Administratiivsed grupid
- Ühendused (*connectors*) võõraste meilisüsteemidega
- *Outlook Web Access* (OWA)
- E-Mail-Filter
- *E-Mail-Folder* ja *Public Folder* ning nende objektidega seotud volituste väljajagamine
- *Client-Server* -kommunikatsiooni turve (*Outlook 2000 Client*, *Browser*, rakendatavad protseduurid)

Outlook 2000

- Kasutajaprofiilid

- Aktiivsisu ja potentsiaalselt ohtlikud failiformaadid
- *Auto-Reply* -funktsioon

Täiendavad kontrollküsimused:

- Kas kõiki administraatoreid on koolitatud Windows 2000'de ja Active Directory'ga töötamise vallas?
- Kas töötajatele on õpetatud, kuidas käsitseda kõiki Exchange 2000'de olulisi turvamehhanisme?
- Kas koolituste raames käsitleti võimalikke meilikliente, eriti Outlook 2000'det.

M 3.32 Outlook 2000 turvamehhanismide koolitus kasutajatele

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: IT-turvaosakond

Exchange/Outlook 2000 on keeruline süsteem, mille väär kasutamine ning konfigureerimine võib endaga tahtmatult kaasa tuua turvaaukude tekkimise. Eriti kehtib see neil juhtudel, kus kasutajad ei ole läbinud piisavat koolitust ja ei tea, kuidas Exchange/Outlook 2000-süsteemidega õigesti ümber käia. Süsteem konfigureeritakse reeglina küll selliseks, et kasutajatel on võimalik seda iseseisvalt muuta ainult teatud kindlates piirides. Sellele vaatamata võib siiski ka puhtalt teadmatusest selle kohta, milliseid turvamehhanisme ja turvaseadistusi on kasutajal võimalik rakendada, välja kujuneda olukord, kus süsteemi käitatakse ebaturvaliselt.

Exchange 2000'de põhitõed

Seetõttu peaksid kõik kasutajad läbima koolituse, kuidas Outlook 2000'ga kõige paremini ümber käia. Lisaks tavapärasele klienttarkvara kasutamiskoolitusele on siiski tarvis meiliteenuse kasutajatele selgitada ka Exchange 2000-süsteemi üldisi tööpõhimõtteid. Eriti hoolikalt tuleb kasutajatele selgitada olemasolevaid turvamehhanisme, et nad oleksid võimelised neid ka korrektselt ja mõistlikult rakendama. Koolitus peaks käsitlema muuhulgas järgmisi teemasid:

- Ülevaade: Exchange-serveri juurdepääsukontroll
- Ülevaade: meilikontode juurdepääsukontroll
- Sertifikaatide aktsepteerimine (mida kujutavad endast *Cross* -sertifikaadid?)
- Autentimine läbi Web-liidese ning selle head ja halvad küljed
- Internet-sertifikaatide turvaline kasutamine
- Turbe kehtestamine sidele: pordi krüpteerimine ja SSL'i kasutamine
- Aktiivsisu käivitamise piiramine Outlook 2000'des
- Meilide krüpteerimine ja meilide digitaalsed allkirjad
- Outlook 2000'de täiendava turbe sisselülitamine
- Kasutajaprofiilide salvestamine
- *Offline* -kaustade kasutamine
- Isiklike kaustade turvaseadistused (krüpteerimine)
- *Out of Office* -funktsiooni kasutamisega seotud ohud
- Jaotusloendite kasutamine
- Asendustöötaja volituste kasutamine (*send as*)
- Käitumisreeglid seoses Outlook Web Access'i kasutamisega (juhul, kui seda funktsiooni üleüldse võimaldatakse kasutada)
- Ümberkäimine Outlook-blanklettidega

Antud loetelu kujutab endast vaid üht väljavõtet kõikidest hädavajalikest turbealastest teemadest, mistõttu tuleb seda kindlasti vastavalt konkreetsetele vajadusele veel ka kohandada ja täiendada. Lisaks tavapärasele Outlook 2000-turvamehhanismide alasele koolitusele peavad kasutajad olema kursis ka kehtestatud turbealaste ettekirjutustega, et nad oskaksid vastavaid ettekirjutusi turvamehhanismide rakendamisel ka korrektselt ellu viia.

M 3.33z Personali taustakontroll

Algatamise eest vastutavad: personalijuht, IT turvaosakond

Rakendamise eest vastutavad: personaliosakond, ülemused

Uue või võõra personali usaldusväärsuse kontrollimine on Eestis reguleeritud vaid valitud töökohtade puhul (lennundus, lastega töötajad jt). Eestis puudub töötaja taustakontrolli range regulatsioon ühe kindla seadusega.

Reeglina tuleks aga enne uute või väljastpoolt tulevate töötajate projekti ülevõtmist kontrollida järgmist:

- kas neil on ette näidata piisavaid soovitusi, näiteks teistes sarnastes projektides osalemise kohta ja
- kas kandideerija elulookirjeldus on piisavalt muljetavaldav ning kas see on täielik või esineb seal lünki.

Lisaks võib tööandjal olla mõttekas veenduda kandidaadi akadeemilise ja tööalase kvalifikatsiooni olemasolus, tehes nt vastava järelepärimise loetletud ülikoolile ja küsides infot kas eelneva tööandja või eelnevate klientide käest. Ka kandideerija identiteeti tuleks kontrollida, nt paludes tal esitada isikut tõendava dokumendi.

Juhul kui siseülesannetes hakatakse kasutama välist personali või kui neid kaasatakse mõnda projekti, koostöösse või väljasttellimise projekti, kus neil avaneb juurdepääs sisemistele rakendustele ja siseinfole, tuleks vastava personali suhtes läbi viia samasugused kontrolliprotseduurid, nagu seda tehakse oma püsitöötajatega. Väliste teenusepakkujatega sõlmitavate lepingute puhul tuleks lepinguga kindlaks määrata kohustus, kumb pool peab vastutama niisuguste kontrollide läbiviimise eest ning kui põhjalik peaks selline kontrollimine olema.

Kontrollküsimused:

- Kuidas kontrollitakse oma töötajate ja võõra tööjõu usaldusväärsust?
- Kas uute töötajate soovituskirju kontrollitakse?

M 3.34 Arhiivisüsteemi haldamise koolitus

Algatamise eest vastutavad: IT-juht, IT turvaosakond

Rakendamise eest vastutavad: IT-juht, arhiivi haldaja, administraator

Arhiivisüsteemi korrektse ja turvalise administreerimise tagamiseks peavad selle eest vastutavad töötajad, eriti aga administraatorid ja arhiivi haldajad tundma hästi arhiivis rakendatavaid süsteeme. Selleks on hädavajalik viia arhiivi haldamise ja administreerimise eest vastutavatele töötajatele läbi asjakohased koolitused. See peab aitama kaasa konfiguratsioonivigade ja väära käitumise vältimisele.

Koolitusel tuleks käsitleda vähemalt järgmisi teemasid:

- Arhiivisüsteemi ja selle aluseks oleva operatsioonisüsteemi arhitektuur ja turvamehhanismid
- Arhiivisüsteemi installeerimine ja käsitsemine, erinevate arhiiviandmekandjate käsitsemine ning arhiveerimiseks kasutatavate andmekandjate märgistamine (vt M 2.3 Andmekandjate haldus)
- Arhiivisüsteemi ja selle andmekandjate jaoks vajalike kasutustingimuste (kliima jms) tagamine
- Administreerimisega seotud tegevuste dokumenteerimine
- Arhiivisüsteemi süsteemi kajastavate sündmuste logimine
- Tegutsemisjuhised andmehulkade värskendamiseks (vt M 2.263 Arhiveeritud andmeressursside regulaarne regenereerimine ja M 2.264 Krüpteeritud andmete regulaarne regenereerimine arhiveerimisel)
- Algteadmised krüpteerimisest ja digitaalsetest allkirjadest juhul, kui rakendatakse krüptograafilisi protseduure
- Kasutusest kõrvaldatud arhiiviandmekandjate korrektne hävitamine
- Arhiivisüsteemi seire ja hooldus (operating)
- Eskalatsiooniprotseduurid reageerimisaegadest mittekinnipidamisel
- Eskalatsiooniprotseduurid arhiiviandmekandjate minimaalse jääksalvestusmahu vähenemisel
- Eskalatsiooniprotseduurid arhiivisüsteemi manipuleerimise või saboteerimise korral või vääramatust jõust põhjustatud sündmuste puhul
- Eskalatsiooniprotseduurid arhiveeritud andmete volitamata juurdepääsude puhuks

Administraatorite ja arhiivi haldajate koolitused tuleb dokumenteerida Süsteemis tehtavate muudatuste korral tuleb administraatoritele ja arhiivi haldajatele korraldada vastavad täiendkoolitused.

Kontrollküsimused:

- Kas arhiivisüsteemi administraatorid on läbinud ettekirjutustele vastava asjakohase koolituse?
- Kas administraatoritele korraldatakse pidevalt täiendkoolitusi, nt süsteemis tehtavate muudatuste kohta?

M 3.35 Arhiivisüsteemi kasutamise koolitus kasutajatele

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: IT-juht, arhiivi haldaja

Arhiveerimine on ülimalt vastutusrikas ülesanne, mille täitmisega kaasnevad väga kõrged nõuded. Töötajaid, kes hakkavad vastavate ülesannetega rinda pistma, tuleb eriti hoolikalt informeerida ja neid selle tööga kaasnevaks vastutuse kandmiseks ette valmistada. Selleks on tarvis süsteemi kasutajaid koolitada.

Sellealane koolitus peaks muu hulgas kajastama järgmisi teemasid:

- Protseduurireeglid analoogsel kujul oleva info ümbertöötlemiseks – töötajatele tuleb selgitada, milline on korrektne tööde järjekord dokumentide sisselugemisel, ümbertöötlemisel elektroonilisele kujule ning elektroonilisel arhiveerimisel ning seda kõike tuleb praktiliste näidete põhjal ka harjutada.
- Arhiveerimisele kehtivad seadustest tulenevad raamtingimused – arhiveerimise puhul on tarvis järgida ka seadustest tulenevaid eeskirju (M 2.245 Elektroonilise arhiveerimise õiguslike tegurite väljaselgitamine). Töötajatele tuleb selgitada kehtivaid nõudeid ja tagajärgi, millega tuleb arvestada, kui vastavaid nõudeid ei järgita.
- Dokumentide konfidentsiaalsuse ja tervikluse kaitse – töötajatele tuleb ette näidata, kuidas tuleb korrektselt ümber käia konfidentsiaalsete dokumentidega, samuti näidata, kuidas leiab aset arhiveeritud dokumentide tervikluse tagamine ja tervikluse kontrollimine. Töötajaid tuleb informeerida võimalikest tagajärgedest, mis järgnevad sellele, kui töötajad oma tööülesandeid valesti täidavad.
- Eripärad seoses WORM-andmekandjate kasutamisega – kindlasti tuleb töötajaid informeerida ühekordselt kirjutatavate andmekandjate kasutamise eripäradest, st tuleb arvestada, et salvestatud andmeid ei ole võimalik enam kustutada (parimal juhul on andmetest võimalik arhiveerida uus versioon). Sellega ei pruugi kaasneda mitte ainult vajaliku salvestusmahu järsk vähenemine, vaid ka andmekaitse- ja konfidentsiaalsusprobleemid, kuna andmed märgistatakse küll tähistusega „kustutamisele määratud", kuid tegelikult neid ei kustutata.
- Organisatsiooni eripärasid kajastavad turvapoliitikad ja nende rakendamine elektroonilisel arhiveerimisel – arhiivisüsteemi kontseptsiooni loomise käigus nähakse üldjuhul ette erinevaid turvameetmeid, mille rakendamise eest peavad hakkama hoolt kandma arhiivisüsteemi erinevad kasutajad. Ülesanne võib seisneda nt andmekandjate märgistamises, aga ka konfidentsiaalse või mõnda muud liiki infoga ümberkäimine. Organisatsioonis kehtestatud turvapoliitikatest tuleb informeerida kõiki kasutajaid. Töötajatele korraldatud koolitused tuleb dokumenteerida.

Kontrollküsimused:

- Kas arhiivisüsteemi kasutajatele on ette nähtud koolitused, mis õpetavad arhiivisüsteemiga ümberkäimist?
- Kas kasutajate osavõtt koolitustest dokumenteeritakse?

M 3.38 Marsruuterite ja kommutaatorite koolitus administraatoritele

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT-turvaosakond

Rakendamise eest vastutavad: IT-juht, IT-turvaosakond

Marsruuterite ja kommutaatorite käitamisel on oluline, et kõiki asjassepuutuvaid töid teeks personal, kes oleks võimeline kõiki olemasolevaid funktsioone ja turvaseadeid optimaalselt ära kasutama. Seetõttu tuleb ilmtingimata vastavaid administraatoreid ka koolitada. Koolitustel tuleks edastada piisavalt teadmisi marsruuterite ja kommutaatorite töölerakendamiseks ning käitamiseks vajalike protseduuride, tööriistade ja tehnikate kohta. Sama kehtib ka väljavalitud toote valmistajapoolsete eripärade kohta. Käesolev meede kirjeldab nõudeid koolitustele, mis peaksid administraatoritele õpetama, kuidas installeerida ja käitada marsruutereid ja kommutaatoreid tavapärases keskkonnas. Koolituste käigus tuleks omandada teadmised installeerimise, käitamise, hoolduse ja veaotsingutega seotud käskude põhitõdedest ja kontseptsioonidest ning omandada ka oskused neid õigesti kasutada.

Koolitus peaks kujutama endast õppeprotsessi, kus teooria ja praktika on omavahel tasakaalus. Ka neil juhtudel, kus tööülesanded on ära jagatud administraatorite grupi vahel selliselt, et igaüks tegeleb vaid oma kindla vastutusalaga, peavad vajalikud baasteadmised olema vaieldamatult siiski kõikidel administraatoritel.

Ka individuaalselt vajaminevate teadmiste sihipärane kogumine ja hoidmine saab toimuda ainult baasteadmistele toetudes. Paljudele toodetele pakuvad kas tootjad või spetsiaalsed edasimüüjad küllaltki põhjalikke seminare, mis võimaldavad samm-sammult tutvuda vastavate toodetega ja süvendada oma individuaalseid teadmisi. Kvaliteetsete koolituspakkumiste olemasolu on samuti üheks kriteeriumiks, millega tuleks ühe või teise tootja kasuks otsustamisel kindlasti arvestada.

Koolituste eelarve

Koolitusmeetmete eelarvet tuleks hakata planeerima juba konkreetsete IT-komponentide soetamisprotsessi käigus ning administraatoritele tuleks koostada ka koolituskava.

Koolitus peaks käsitlema järgmisi punkte:

Põhitõed

- ISO/OSI kihtide mudel.
- Võrgutopograafiad / -topoloogiad ning ülekandmistehnikad
- Juhtmestik
- Aktiivsed võrgukomponendid
- Algteadmised IPst ja selle juurde kuuluvatest protokollidest (IPadresseerimine, Subnetting, IP, ICMP, TCP, UDP)
- Ülevaade tootjafirmadest ja toodetest

Kommuteerimine (Switching)

- Kommutaatori tööpõhimõtte kirjeldus
- “Cut Through ”ning “Store and Forward ”

- Transparent Bridging funktsioon (IEEE 802.1d)
- Spanning Tree Algorithm (IEEE 802.1d)
- VLAN (VLAN'i tüübid, Tagging , IEEE 802.1q)

Marsruutimine

- Marsruuteri tööpõhimõtte kirjeldus
- Staatiline ja dünaamiline marsruutimine
- Dünaamilised marsruutimisprotokollid (RIPv1, RIPv2, OSPFv2, BGPv4, IGRP, EIGRP)

WAN-ühendus

- Algteadmised WAN-tehnoloogiatest ja protokollidest
- Edastusliigid (püsiühendus, sissevalimisega ühendus)
- Virtuaalsed privaatvõrgud (VPNid)
- Kaugsideühendused (xDSL, ISDN)
- WAN-protokollid (PPP, Frame Relay)

Kasutuselevõtt

- Monteerimine ja juhtmestik
- Marsruuterite ja kommutaatorite kasutuselevõtt ja konfigureerimine (põhitähelepanu operatsioonisüsteemil)

Kasutamine

- Seadmete ja tööriistade haldamine
- Integreerimine võrguhaldussüsteemide (NMS'ide) alla
- Logimine (syslog)
- Konfiguratsioonifailide varundamine ja haldamine

Vigade kõrvaldamine

- Veaallikad ja vigade põhjused
- Mõõte- ja analüüsitööriistad
- Veaotsingu testimisstrateegiad
- Nõuded turvalistele võrguinstallatsioonidele

IT-turvalisus

- IT-turvalisuse põhitõed ning marsruuterite ja kommutaatorite olulised turbeaspektid
- Autentimine, autoriseerimine
- Krüptoprotseduurid ja rakendused

- Ründestsenaariumid (Denial of Service ründed, ARP-Spoofing , IPSpoofing)
- Veaallikas „ Default settings “
- Ennetusmeetmed, reageerimine ja analüüs
- Intsidentide käsitlemine

Kontrollküsimused:

- Kas koolitusmeetmete läbiviimiseks on olemas vastav eelarve?
- Kas eelnevalt loetletud punktidele toetudes on administraatoritele koostatud oma koolituskava?

M 3.43 Turvalüüsi administraatorite koolitus

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT-turvaosakond

Rakendamise eest vastutavad: IT-juht, IT-turvaosakond

Turvalüüsi puhul on tegemist võrgu jaoks tsentraalse turvaelemendiga, mis kaitseb võrku väljast tulevate ohtude suhtes. Seetõttu peavad turvalüüsi administraatorid olema piisavalt koolitatud, et nad suudaksid optimaalselt ära kasutada kõiki olemasolevaid funktsioone ja turvaseadeid. Koolitustel tuleks edastada piisavalt teadmisi turvalüüsi komponentide töölerakendamiseks ning käitamiseks vajalike protseduuride, tööriistade ja tehnikate kohta. Sama kehtib ka valmistajapoolsete eripärade kohta väljavalitud toodetel, mida rakendatakse turvalüüsi erinevate komponentidena.

Koolitusnõuete koostamisel arvutite operatsioonisüsteemide kohta, kui arvuteid rakendatakse turvalüüsi komponentidena, samuti aktiivsete võrgukomponentide kohta (eriti marsruuterite puhul, mis moodustavad paketifiltri otstarbel kasutades kindla osa tulemüürist) tuleks täiendavalt arvestada asjassepuutuvate operatsioonisüsteemide moodulitega ning mooduliga B 3.302 Marsruuterid ja kommutaatorid .

Enamatel juhtudel peaks koolitused kajastama järgmisi teemasid:

- Administreerimise põhitõed ja kontseptsioonid, turvalüüsi iga üksiku komponendi käskude tundmine turvalüüsi kasutuselevõtmise, käitamise, hooldamise ja vigade otsimise osas. Koolitus peaks kujutama endast õppeprotsessi, kus teooria ja praktika on omavahel tasakaalus.
- IT-turbe põhitõed, eelkõige ennetavad meetmed, reageerimine, analüüs ja turvaintsidentide käsitlemine (vt B 1.8 Turvaintsidentide käsitlus)
- Ründestsenaariumid (nt Denial of Service ründed, ARP-Spoofing , IPSpoofing, DNS-Spoofing , viirused ja muu kahjurvara)
- Võrkude struktureerimise põhitõed
- ISO/OSI kihtide mudel
- Algteadmised IPst ja selle juurde kuuluvatest protokollidest (IPadresseerimine, Subnetting , IP, ICMP, TCP, UDP) ning erinevad filtreerimisvõimalused seoses Header-Data 'ga
- Marsruutimise põhitõed, staatiline ja dünaamiline marsruutimine, rakendatavate marsruutimisprotokollide põhitõed ja turbeaspektid.
- Olulisemate rakenduskihis kasutatavate protokollide põhitõed (nt SMTP, HTTP ja HTTPS, Secure Shell, SMB/CIFS) ning erinevad filtreerimisvõimalused, kasutades protokollikäskusid või käsuparameetreid.
- Põhitõed teema kohta virtuaalsed privaatvõrgud (VPNid)
- Põhitõed teemade kohta Intrusion Detection/Intrusion Prevention (IDS/IPS).
- Põhitõed krüpteeritud andmetega ümberkäimise kohta (nt krüpteerimine HTTPS'i või IPSec'i abil) ning võimalused krüpteeritud andmete töötlemiseks.
- Kasutamine

- Seadmete ja tööriistade haldamine
- Logimine
- Konfiguratsiooniandmete varundamine ja haldamine
- Vigade kõrvaldamine
- Veaallikad ja vigade põhjused
- Mõõte- ja analüüsitööriistad, tööriistad mis võimaldavad automaatselt kontrollida turvalüüsi erinevate komponentide korrektset funktsioneerimist.
- Veaotsingu testimisstrateegiad
- Nõuded turvalistele võrguinstallatsioonidele
- Olulised õiguslikud aspektid, nt seoses andmekaitsega, seadusest tulenevad kohustused seoses võrguühendustega ning muud olulised ettekirjutused.

Ka neil juhtudel, kus tööülesanded on ära jagatud administraatorite grupi vahel selliselt, et igaüks tegeleb vaid oma kindla vastutusalaga, peavad siiski kõikidel administraatoritel olema vajalikud baasteadmised. Ka individuaalselt vajaminevate teadmiste sihipärane kogumine ja hoidmine saab toimuda ainult baasteadmistele toetudes. Paljudele toodetele pakuvad kas tootjad või spetsiaalsed edasimüüjad küllaltki põhjalikke seminare, mis võimaldavad samm-sammult tutvuda vastavate toodetega ja süvendada oma individuaalseid teadmisi. Kvaliteetsete koolituspakkumiste olemasolu on samuti üks kriteerium, millega tuleb ühe või teise tootja kasuks otsustamisel kindlasti arvestada. Koolitusmeetmete eelarvet tuleks hakata planeerima juba konkreetsete IT-komponentide soetamisprotsessi käigus ning administraatoritele tuleks koostada ka koolituskava.

Kontrollküsimused:

- Kas koolitusmeetmete läbiviimiseks on olemas vastav eelarve?
- Kas eelnevalt loetletud punktidele toetudes on administraatoritele koostatud oma koolituskava?

M 3.44 Juhtkonna teadlikkuse tõstmine infoturbe alal

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT turvaosakond

Rakendamise eest vastutavad: IT turvaosakond

Juhatus peab tagama turvalisuse!

Pidev ja aktiivne ametiasutuse või ettevõtte juhtkonna toetus on üks asjaolu, mis määrab, kas töötajatele korraldatavad turbealased teavitamiskampaaniad kujunevad edukaks või mitte. Seetõttu on ilmtingimata vajalik, et enne töötajatele suunatud IT turbealaste teavitamiskampaaniate korraldamist informeeritaks turbetemaatika vajalikkusest ka juhtkonda.

Olulisem info, mida tuleks juhatusele kindlasti edasi anda, on järgmine:

- ülevaade turbega seotud riskidest ja nendega seotud kuludest – otsustuspädevusega isikute tähelepanu võib saavutada nt sellega, et esitleda neile turvaintsidente puudutavaid aruandeid juhtumitest, mis võivad potentsiaalselt esineda ka oma institutsioonis (tuua näiteid sama valdkonna institutsioonide või sarnase IT-lahendusega institutsioonide kohta). Näited konkreetsete, lähiümbruses või sarnastes institutsioonides asetleidnud turvaintsidentide kohta võivad juhatuse otsustamisjulgust märgatavalt suurendada. Selliseid näiteid pole tänapäeval enam sugugi tarvis erialaajakirjadest taga otsida, kuna näiteks nii häkkerirünnakutest kui ka viiruste esinemistest kirjutatakse juba piisavalt ka ajakirjanduses ning loomulikult leidub palju sellealast infot internetis. Selleks otstarbeks võib kasutada ka reaalselt oma institutsioonis minevikus aset leidnud kahjujuhtumeid. Kogemustele toetudes võib väita, et konkreetsete kahjunumbrite väljatoomine on alati küllaltki keeruline. Mõningatel juhtudel võivad abiks olla statistikad ja aruanded, mida avaldavad aeg-ajalt kas politseiinstitutsioonid või mõned erialaajakirjad;
- mõju igapäevastele tööprotsessidele – lisaks on oluline kirjeldada võimalike turvaintsidentide mõju igapäevastele kriitilise tähtsusega tööprotsessidele. Juhtkond ei pruugi alati teada, millised on konkreetsed seosed IT-rakenduste ja IT-süsteemide vahel. Juhtkonna toetuse võitmiseks ei piisa reeglina ainult võimalike turvariskide loetlemisest.

Tasakaalukas argumenteerimisprotsess peaks muu hulgas käsitlema ka järgmisi punkte:

- seadustest tulenevad turbenõuded – olenevalt institutsiooni eripäradest võivad täiendavaid IT turvet käsitlevaid nõudeid endaga kaasa tuua ka seadused ja muud juriidilised eeskirjad, nagu nt andmekaitseseadused, sotsiaalseadustikud, äriseadustikud, tsiviilseadustikud, kriminaalseadustikud jne. Paljude IT turvet puudutavate seaduste sõnastused võivad tunduda esmapilgul väga üldsõnalised, mis võib aeg-ajalt jätta eksliku mulje, nagu ei oleks nende puhul üldsegi tegemist kohustusega. Tegelikult on nende sõnastuste taga siiski konkreetne kohustus tagada vajalik IT turbeaste. Iga institutsioon peab uurima, milliseid ettekirjutusi ja seadusi neil tuleb järgida;
- sertifitseerimisega kaasnevad eelised – IT turbeprotsesside sertifitseerimine on üks viis, kuidas pakkuda ametlikku kinnitust, et kõnealune institutsioon väärtustab IT turbe tagamist. Institutsiooni IT usaldusväärsus äripartnerite

ja avalikkuse silmis saab seeläbi vaid kasvada. Ettevõtetele võib sertifikaadi olemasolu tuua lisaks veel ka konkurentsieeliseid riigihangetel;
- institutsiooni tegevusvaldkonnale ette nähtud standardsed IT turbelahendused – IT turvastandardite rakendamise täiendav motivatsiooniallikas võib olla ka teadmine sellest, kuidas toimivad selles valdkonnas teised sarnased organisatsioonid. Infot oma tegevusvaldkonnale või -harule väljatöötatud standardite kohta leiab erialaajakirjadest, üritustelt või ka läbi otseste kontaktide vastavate tööstuskodade ja erialaliitudega.

Juhatuse teadlikkuse tõstmist on kõige sobivam alustada lühikese ettekandega, millele järgneb esitlus, kus selgitatakse värskete (enda ja võõraste) juhtumite põhjal IT turbetemaatika olulisust. Esitluse raames tuleks nt ära seletada tõsiasi, et tehniliste meetmete rakendamine ilma personalialaste ja töökorraldust puudutavate turvameetmete võtmiseta on täiesti mõttetu. Juhatuse toetuse võitmiseks on palju abi sellest, kui suudetakse ära tõestada vastavate meetmete rakendamise kasulikkus. Turvariskide ja nende võimalike lahenduste esitlemisega on juhatust kindlasti võimalik veenda IT turbemeetmete rakendamise vajalikkuses. Kogemuste põhjal võib väita, et IT turvet hakatakse edukalt ellu rakendama vaid siis, kui terve institutsiooni juhtkond näitab selles head eeskuju. Seega on mõttekas panna kõikidele juhtivtöötajatele kohustus, et nad tuletaksid oma alluvatele pidevalt meelde IT-alaseid turvaettekirjutusi, ja hoolitseda selle eest, et töötajad oleksid teemaga seoses piisavalt informeeritud.

Kontrollküsimused:

- Kas juhatus toetab piisaval määral IT turbega seotud teavitamiskampaaniaid?
- Kas IT turbealane initsiatiiv saab alguse ametiasutuse või ettevõtte juhtkonnast?

M 3.45 IT-turbealaste koolituste sisu kavandamine

Algatamise eest vastutavad: personalijuht, IT turvaosakonna meeskond

Rakendamise eest vastutavad: ülemused, personaliosakond, IT turvaosakonna meeskond

Kõikidel töötajatel peavad olema oma töö kohta põhjalikud baasteadmised, mille hulka kuuluvad ka piisavad teadmised IT-turbest. Selle tagamiseks tuleb erinevatele sihtgruppidele, nt eri valdkondade IT-kasutajatele, ülemustele, IT turvaosakonna meeskonnale, IT-spetsialistidele, administraatoritele jne korraldada asjakohaseid IT-turbealaseid koolitusi. Enne koolitusmeetmetega alustamist tuleks analüüsida, milline on töötajate kvalifikatsioon ja milliseid koolitusi oleks tarvis.

Selle käigus tuleks koguda järgmisi andmeid:

- koolitustunnistused,
- töökogemus, täiendkoolitused, lisateadmised,
- töötajate ülesanded ja töörollid oma organisatsiooni allüksuse lõikes.

Koolituste sisu tuleks jagada erinevateks mooduliteks, et igal sihtgrupil oleks võimalik läbida piisav koolitus, mille põhjalikkus sõltub konkreetsetest vajadustest. Alljärgnevalt kirjeldatakse erinevate koolitusmoodulite olulisemaid teemasid, mille hulgast tuleks erinevatele sihtgruppidele välja valida kõige sobilikumad ning neid töörollide alusel ka kohandada. Siinse ülevaate eesmärk on hõlbustada koolitusteemade väljavalimist nii organisatsioonisiseste koolituste korraldamisel kui ka väliste koolituste puhul. Lisaks järgnevale loetelule tuleks läbi uurida ka kõik konkreetset IT-kooslust puudutavad IT etalonturbekataloogi moodulid, et välja selgitada, kas seal kirjeldatud vajalikud meetmed on ainult välja kuulutatud või on vastavad koolitused ka tõesti toimunud. Siin kirjeldatud moodulid tuleks liigitada erinevate sihtgruppide alusel, nagu kirjeldatakse järgnevas näites. Tähega „X” on tähistatud need moodulid, mis sobivad vaadeldavale töörollile. Tähistus „O” ehk valikuline näitab valikut, mille puhul tuleb igal konkreetsel juhul eraldi otsustada, kas seda koolitusmoodulit on vaadeldavale töörollile tarvis või mitte.

Koolitusmoodulid

Moodul 1: IT-turbe põhialused
Moodul 2: IT-turve töökohal
Moodul 3: seadused ja ettekirjutused
Moodul 4: organisatsiooni IT turvakontseptsioon
Moodul 5: riskihaldus
Moodul 6: IT turvaosakond
Moodul 7: IT-süsteemid
Moodul 8: operatiivvaldkond
Moodul 9: turbemeetmete tehniline realiseerimine
Moodul 10: avariiennetus/avariiplaanid
Moodul 11: uuemad arengud IT valdkonnas
Moodul 12: IT-turbe ettevõttemajanduslik pool
Moodul 13: infrastruktuuri turvalisus

Moodul /funktsioon	1	2	3	4	5	6	7	8	9	10	11	12	13
Ülemused	X	X	X	X							O	X	
IT-turvaosakond	X	X	X	X	X	X	X	X	X	X	X	X	X
Andmekaitsespetsialist	X	X	X	X							X	O	
Infrastruktuuri eest vastutav töötaja	X	X	X	X	X	O				X			X
Kasutajad	X	X											
Administraatorid	X	X		X	X		X	X	X	X	X		O

Tabel. Võimalikud koolitusmoodulid tööfunktsioonide lõikes

Selles näites on mõlemad moodulid 1 ja 2 aluskoolitus kõikidele töötajatele ning need tuleb viia vastavusse teavitusmeetmetega (vt M 2.198 Personali teavitamine infoturbe küsimustest). Kõik muud moodulid kajastavad tööülesannete lõikes erinevaid täiendavaid koolitusvaldkondi. Olenevalt asutuse tüübist on mõistlik määratleda järgmised sihtrühmad ja nende koolituseesmärgid (vt M 3.93 Teavitus- ja koolitusprogrammide sihtrühmade analüüs). Oluline on, et ei unustataks ka töötajaid, kellel pole otseselt infotehnoloogia kasutamise vajadust, nagu nt turva- ja puhastusteenistus.

Moodul 1: infoturbe alused

Asutused sõltuvad suurel määral piisavalt kättesaadavast ja rünnete vastu kaitstud IT-st ja taristust. Seetõttu on teavitamise ja koolituse tähtsaim ülesanne vahendada töötajatele infoturbe väärtust asutuse jaoks ja vastavat põhiteavet.

Muu hulgas peaks selles moodulis käsitlema järgmisi teemasid:

- motiveerimine

1. juhtumite näited ohtudest ja riskidest
2. rünnete, sh manipuleerimisel põhineva ründe tagajärjed

- teave kui asutuse väärtus ja teabe kaitsevajadus
- mõisted:

1. infoturve
2. usaldusväärsus, terviklus, kättesaadavus
3. turvalisus, ohutus, andmekaitse ja nende piirangud infoturbe tagamiseks

- infoturve oma asutuses

1. asutuse ülesanded ja eesmärgid
2. asutuse turvanõuded ja riskid
3. asutuse teabeturbe strateegia ja kontseptsiooni ülevaade
4. töötajate ülesanded ja kohustused

- töötajatele kehtivad olulised turvareeglid

1. siseste turvareeglite ülevaade
2. strateegilise teabe kasutamine (sh paroolid)
3. e-posti ja interneti kasutamine
4. kaitse kahjurvara eest ja andmevarundus
5. kaasaskantavate seadmete kasutamine
6. töötamine võõrastes või avalikes keskkondades

Moodul 2: infoturve töökohal

Töötajatel on tihti võimalik ainuüksi lihtsate turvameetmete järgimisega aidata palju kaasa kõikvõimalike kahjude vältimisele.

Töökohal rakendatav infoturvet käsitlev moodul peaks muu hulgas sisaldama järgmisi põhiteemasid:

- töötajate teavitamine
- kasutajate tüüpiliste vigade vältimise motiveerimine

1. kergekäeline paroolide kasutamine
2. krüpteerimisest loobumine
3. teabe ebapiisav kaitsmine
4. liigne usaldus
5. sülearvutite vargused

- ennetavad meetmed manipuleerimisel põhinevate rünnete vastu
- organiseerimine ja turvalisus

1. asutuse turvanõuded ning nende tähendus igapäevatööle
2. asutuses kehtestatud vastutusalad ja teavitamiskanalid (koos infoturbeametniku isikliku tutvustamisega)

- sissepääsu ja juurdepääsu kaitse

- andmevarunduse ja selle läbiviimise olulisus
- e-posti ja interneti turvalisus
- kaitse kahjurvaraprogrammide eest
- oluliste IT-süsteemide ja rakenduste turbeaspektid
- seadustest tulenevad aspektid
- käitumine turvaintsidentide korral

1. turvaintsidentide avastamine
2. teavitamiskanalid ja kontaktisikud
3. käitumisreeglid kahtluse korral

Loetletud teemade puhul on tegemist vaid ühe võimaliku valikuga. Koolitusmoodul nimega **„Infoturve töökohal"** peaks olema alati kohandatud asutuse individuaalsetele vajadustele.

Moodul 3: seadused ja ettekirjutused
See koolitusmoodul peab hõlmama töötajatele kehtivaid õiguslikke nõudeid, mille piires tuleb vaadelda teabeturvet asutuse sees.

Siia juurde kuuluvad turbenõuded, mis võivad tuleneda järgmistest allikatest:

- lepingud (nt klientide, tarnijate, väljasttellimise-partnerite, laenuandjatega)
- seadusandlikud nõuded, asjakohased õigusaktid, eeskirjad, infoturbe standardid, suunised jne
- asutuse muud nõuded (nt teadlik turueraldus, tootestrateegia, turbega seotud maine jne)

Oluline on, et töötajaid ei kohustata üksnes vastavatest nõuetest kinni pidama, vaid need tuleb töötajatele ka südamele panna ning selgitada taustu ja tagajärgi. Vastavad nõuded võivad olenevalt asutuse tegevusvaldkonnast ja asukohariigist väga suurel määral erineda. Tähtis roll on infoturvet puudutavatel standarditel ja suunistel ning nende konkreetsel kasutamisel asutuses, sest siin on teadlikult töödeldud juba tervet hulka ülejäänud nõudeid.

Teemade näited on järgmised:

- andmekaitse asutuses
- andmekaitseametniku roll ja tööülesanded
- andmekaitseseadused
- organisatsiooni kohustused
- isikukaitseandmete kasutamine töötajate poolt, nt protokolliandmete puhul
- töökaitse
- töökaitseametniku roll
- eeskirjad arvutimonitoridega töötamisel
- õiguslikud või seadusandlikud nõuded, mis puudutavad infoturvet, kui need on asutuse jaoks siduvad, nt PCI DSS, Basel III jne
- tehnilise taristu seadused ja normid
- tuleohutus, kliimaseadmed, juhtmeühendused, piksekaitse jne

- juriidilised vastutusriskid ja IT kasutus
- TK- või internetiteenuste kasutamine või pakkumine
- ettevõtte vastutus väljaspool ettevõtet (nt KonTraG, kahjurvara kahjud)
- vastutus seoses IT-komponentide kasutamisega isiklikul otstarbel
- õiguslikud raamid töötajate järelevalvel
- muud õiguslikud raamtingimused
- IT-toodetele kehtivad väljaveotingimused, nt krüpteerimisel
- digitaalsed allkirjad ja nende juriidilised aspektid
- tarkvara litsentsi- ja omandiõigused
- sise-IT rünnete käsitlemine
- karistus häkkimise korral
- seadusest tulenevad tõrjemeetmed
- häkkimiskuritegudega kaasnev kriminaaljälitus

Moodul 4: asutuse turbekontseptsioon

See koolitusmoodul süvendab moodulis 2 käsitletud teemasid. Lisaks sellele peaks moodul suutma hoida süsteemi ja tööülesannete eest vastutavaid isikuid piisavalt kursis, et kohandada turbekontseptsiooni tehnoloogiliste, töökorralduslike või õiguslike muudatuste alusel.

Selle teema alla kuuluvad muu hulgas järgmised valdkonnad:

- nõuete ja riskide üksikasjalikud teadmised, mis on turbekontseptsiooni aluseks;
- turbekontseptsiooni spetsiifilised riskid ja turvameetmed halduse, töökorralduse, taristu, IT-süsteemide ja töötajate valdkondadest;
- nende turvameetmete kohandamine uute tehniliste, organisatoorsete ja juriidiliste tingimustega;
- turbekontseptsiooni audit ja järjepidevus.

Moodul 5: riskihaldus

See koolitusmoodul näitab vastutavatele isikutele, kuidas infoturvet süstemaatiliselt analüüsida, hinnata ja käsitleda.

- Definitsioonid ja näited järgmiste mõistete kohta: risk, oht, kitsaskoht, turvaeesmärk

Tüüpilised ohud:

- vääramatu jõud: tuli, vesi, plahvatus, torm, maavärin, äike, streik, demonstratsioon jne,
- organisatsioonilised puudused: puuduvad või mitteküllaldased regulatsioonid, mittenõuetekohane õiguste andmine, kontrollimatu IT-süsteemide kasutamine, konfidentsiaalse teabe / andmekandjate kasutamine jne,
- inimvead: eksimus, hoolimatus, uudishimu, teadmatus jne,
- tehnilised rikked: elektrikatkestus, kliimaseadme avarii, ülepinge, lülituselementide või lülitusskeemide avarii, mehaanilised ja elektroonilised rikked jne,

- ründed: kahjurvaraprogrammid, vargus, sabotaaž, spionaaž, manipuleerimine, vandalism, häkkimine ja kräkkimine, sealhulgas ründe toimepanijate tüüpide ja motivatsioonide vastandamine, nt siseringi kuuluvad isikud või ründe toimepanijad väljastpoolt.

Riskihaldus

riskihalduse mõisted: riskianalüüs, riskide hindamine, riskide käsitlemine, aktsepteerimine, jääkrisk, ohtude ülevaate koostamine, täiendavate ohtude määratlemine, ohuhinnang, riskide tuvastamine ja hindamine, riskide käitlemine (vähendamine, vältimine, ülevõtmine, ülekanne), jääkriskide käsitlemine.

Moodul 6: turbehaldus

See koolitusmoodul esitab olulised alused, kuidas vastutavad isikud võivad infoturvet asutuses rakendada.

Selle teema alla kuuluvad muu hulgas järgmised valdkonnad:

- turbehaldus
- eesmärk ja ülesanded
- protsess (infoturbe haldussüsteem, ISMS) ja strateegia (poliitika)
- ressursside eraldamine
- töökorraldus ja vastutusalad
- standardid, nagu ISO/IEC 2700x, IT etalonkaitse, ITIL, CobiT jne
- ülevaadete, auditite, juhtkonnapoolsete hindamiste läbiviimine
- parandusmeetmete planeerimine ja rakendamine
- töötajate kaasamine
- turbekontseptsioon
- turbekontseptsiooni eesmärgid ja sisu
- turbekontseptsiooni ülesehitus
- töötajate, süsteemi ja tööülesannete eest vastutavate töötajate kohustus järgida turbekontseptsiooni
- süsteemi- ja rakendusekesksed turbesuunised
- volituste haldus
- volituste andmise kontseptsioonid, volituste andmise korraldamine
- süsteemiressursside pääsuõigused, nende andmine ja kehtivuse ajaline piiramine
- autentimine (nt erinevate mehhanismide tugevused ja nende valimine)
- kaugpöördus (nt kaugtöö puhul)
- infoturbealane teavitamine ja koolitus
- sobivate programmide väljatöötamine asutuse raamtingimuste alusel
- infoturbevaldkonna hindamine ja sertifitseerimine
- toote/süsteemi sertifitseerimine (nt ITSEC-i, Common Criteria jms kohaselt)
- turbehalduse sertifitseerimine (nt IT etalonkaitse järgi)
- ekspertide sertifikaadid (nt TISP, CISA, CISSP, infoturbe koordinaator, Security+ jne)
- infoturbe spetsiifilised probleemid
- suhtlemine juhtkonna ja erialaosakonnaga

- kulude ja aktsepteerimisega seotud probleemid

Moodul 7: IT-süsteemid

Selles koolitusmoodulis kirjeldatakse juhtimisinstrumente, mis peavad tagama vajalike turvanormide täitmise IT-süsteemide kogu kasutusaja erinevates faasides.

Selle teema alla kuuluvad muu hulgas järgmised valdkonnad:

- turbemeetmed erinevates IT-kasutusaja faasides
- planeerimine
- soetamine/arendamine
- testimine ja hindamine
- rakendamine või installeerimine
- aktiivne kasutamine
- ressursside väljavahetamine
- valmisolek hädaolukorraks
- süsteemi turvalise käitamise planeerimine
- IT-süsteemi kasutusvaldkonna ja otstarbekuse kindlakstegemine
- süsteemi kaitsemeetmete määratlemine
- süsteemi käitamise eest vastutava isiku määramine
- iga kasutusaja faasi jaoks vajalike turvamehhanismide installeerimis- ja konfigureerimistööd
- konfiguratsioonide, paikamise ja muudatuste haldamise kehtestamine seatud turvaeesmärkide alusel
- operatiivse kasutamise kasutusloa väljastamise kriteeriumid
- turvamehhanismide testimine ja kasutusloa väljastamine

Moodul 8: operatiivvaldkond

Selles koolitusmoodulis kirjeldatakse protseduure ja meetmeid, mis on vajalikud operatiivsete süsteemide ja rakenduste kaitseks.

Selle teema alla kuuluvad muu hulgas järgmised valdkonnad:

- taristut käsitlevad meetmed
- juurdepääsukontrollid, tehasevalve, signalisatsioonisüsteemid jne
- maja tehnika, elektri- ja veevarustus jne
- tuleohutusseadeldised
- kliimaseadmed
- organisatsioonilised meetmed
- süsteemide ja konfiguratsioonide, rakenduste, tarkvara, riistavara seisu jms dokumenteerimine
- regulaarne logifailide kontrollimine
- andmevarundusega seotud ettekirjutused
- andmekandjate vahetusega seotud ettekirjutused
- tüüptarkvara litsentsi- ja versioonihaldus
- personali puudutavad meetmed
- töötajate väljavalimine, tööga kurssi viimine ja koolitamine

- töösuhte lõpetamise reeglid
- funktsioonid ja vastutusalad
- funktsioonide lahutamine ja funktsioonipõhine volituste andmine
- asendamise korraldamine
- uute töötajate kohustamine eeskirju järgima
- riistvara ja tarkvara käsitlevad meetmed
- operatsioonisüsteemi turvalisuse põhitõed
- riistvara ja tarkvara turvaline konfigureerimine
- kaitse kahjurvaraprogrammide eest
- riistvara või rakendusprogrammide turbefunktsioonide kasutamine
- täiendavate turbefunktsioonide juurutamine
- volituste haldamine
- logimine
- sidealased meetmed
- TK-seadmete ja võrguteenuste turvaline konfigureerimine
- e-posti ja interneti turvalisus
- väliste kaugpöörduste turve
- virtuaalsed privaatvõrgud (virtual private networks, VPN)
- kaasaskantavate IT-süsteemide ja traadita side turvaline kasutamine
- teave turvaaukudest (nt CERT-ide kaudu) ja turvaintsidentide käsitlus

Moodul 9: turvameetmete tehniline teostus

Selles koolitusmoodulis edastatakse teadmisi, kuidas on võimalik ellu viia moodulites 6 kuni 8 kirjeldatud juhtimis- ja kontrolliinstrumente.

Selle teema alla kuuluvad muu hulgas järgmised valdkonnad:

- krüptograafiaalased baasteadmised
- probleemide piiritlemine: konfidentsiaalsus, terviklus, autentsus
- põhimõisted, nagu loetaval kujul tekst, šifreeritud ehk salatekst, võtmed
- sümmeetriline, asümmeetriline ja hübriidne krüpteerimine
- avaliku võtme taristud
- digitaalsed allkirjad
- loetelu teadaolevatest „headest” ja „halbadest” algoritmidest
- identifitseerimine ja autentimine, nt
- mõistete definitsioonid (teadmine, omand, omadus)
- autentimine läbi teadmiste: paroolid, ühekordsed paroolid, pretensiooni ja vastusega protseduurid (challenge-response procedures), digitaalsed allkirjad
- autentimine läbi omandi: volitustõendid, kiipkaardid, nt
- biomeetrilised protseduurid: sõrmejäljetuvastus, käeveenituvastus, iirisetuvastus, näotuvastus, nt
- ainulogimisega pöördus
- volituste haldus
- logimine ja jälgimine, nt
- tehingulogimise tehnilised võimalused

- sissetungi tuvastamise, reaktsiooni ja tõrje süsteem (IDS, IRS, IPS): erinevused aktiivsete ja passiivsete süsteemide vahel
- kõikide haldustegevuste sunniviisiline protokollimine
- andmekaitseaspektid
- ülevaade haldamiseks kasutatavatest tarkvaratööriistadest
- tööriistad, mille abil on võimalik rakendada ja kontrollida turbealaseid ettekirjutusi
- lisatooted täiendamiseks või operatsioonisüsteemide (nn karastatud operatsioonisüsteemid) turbefunktsioonide parandamine
- võrguhaldustarkvara
- kaughalduse (remote management) tarkvara
- tulemüürid (turvalüüsid)
- internetil baseeruvad tehnikad (OSI-mudel, TCP/IP)
- võimalikud lahendused (staatilised paketifiltrid, olekufiltriga tulemüürid, rakenduslüüsid)
- content security
- kõrgkäideldavad tulemüürid
- konfidentsiaalsuse kaitse: krüptograafilised meetodid ja tooted, juurdepääsukaitse, nt kõvaketta krüpteerimise, OSI-mudeli erinevate kihtide krüpteerimise kaudu
- protokollid kihtidele 1 ja 2 (ISDN-krüpteering, ECP ja CHAP, WLAN, Bluetooth)
- protokollid kihile 3 (IPSec, IKE, SINA)
- protokollid kihile 4 ja kõrgematele kihtidele (SSL, TLS, S/MIME)
- kättesaadavuse kaitse
- organisatsioonilised meetmed kättesaadavuse tõstmiseks (SLA-d, muudatuste haldus, SPOF-i vältimine)
- andmevarundus, andmete taastamine
- salvestustehnoloogiad
- kättesaadavust suurendavad võrgukonfiguratsioonid
- taristulised meetmed kättesaadavuse suurendamiseks
- kliendi, serveri ja rakendustasandi kättesaadavus (server-standby, tõrkesiire)
- andmete replikeerimismeetodid
- taaskäivitamise ja tööprotsesside jätkamise meetmed
- tehnilised võimalused kodukeskjaamade kaitseks
- kaitse pealtkuulamise vastu
- andmekaablite kaitse, nt alarmi alla lülitatud ja plommitud kaablišahtid, turvatud jagajad (sõlmed), teadete krüpteerimine jne
- hooldus-, kaughooldus- ja administraatorijuurdepääsude turvamine
- iga süsteemijuurdepääsu protokollimine, logifailide kustutuskaitse
- oma süsteemi nõrkade kohtade tuvastamine penetratsioonitestidega
- häkkerite töömeetodid, veebilehtede häkkimine, kaitse nuuskimise, skannerite, paroolimurdjate jms vastu

Moodul 10: hädaolukorra haldus

See koolitusmoodul peab andma põhialused asutuse hädaolukorra halduse loomise ja järjepidevuse jaoks. Teema poolest on kõnealuse mooduli puhul tegemist

mooduli 5 „Riskihaldus” jätkumooduliga. Koolituse sisud võib üles ehitada järgmise struktuuri alusel:

Sissejuhatus: eesmärk, ülesanded, mõisted, jätkusuutlikkuse turbe (business continuity) ja IT-teenuse jätkusuutlikkuse (IT service continuity) piirang, standardid

- protsessi ülevaade
- protsessi algatamine
- kontseptsioon
- hädaolukordade ennetamise kontseptsiooni rakendamine
- hädaolukordade likvideerimine ja kriisihaldus
- testid ja harjutused

Moodul 11: uuemad arengud IT-valdkonnas

Kõnealune koolitusmoodul peab hoidma IT-süsteemide käitajaid kursis valdkonnas toimunud uuendustega. Tagamaks pidevat ajaga kaasaskäimist, tuleks seda koolitusseminari külastada regulaarselt, umbes iga kahe aasta tagant. Alternatiivina võib nimetatud sihtrühma käsutusse anda ka ressursid, et end kättesaadavate teabeallikate abil iseseisvalt teemaga kursis hoida.

Selle teema alla kuuluvad muu hulgas järgmised valdkonnad:

- riistvara arhitektuurid, liidesed, siinisüsteemid, perifeeria
- salvestus-/arhiveerimistehnoloogiad ja -süsteemid
- kõrgkäideldavuslahendused
- kliendi ja serveri operatsioonisüsteemid
- tarkvara arhitektuurid
- terminaliserver, N-Tier, Host versus Client/Server
- andmebaasid
- mobiilitehnoloogia
- andmeait, SharePoint jne
- võrgutehnoloogia
- infoturve, kõiki nimetatud teemasid puudutavad uued ohud ja nõrgad kohad
- teavitus krüptograafiliste algoritmide ja protokollide turvalisuse hetkeseisust

Moodul 12: IT-turbe ettevõttemajanduslik pool

See moodul on mõeldud spetsiaalselt juhtkondadele ja teistele otsusetegijatele, et aidata infoturvet integreerida võimalikult katvalt ettevõtte plaanidesse.

Selle teema alla kuuluvad muu hulgas järgmised valdkonnad:

- infoturbe ettevõttemajanduslikud eelised
- riskide minimeerimine
- töötlemise kiirendamine
- kulude kokkuhoid
- käibe suurendamine
- uute ärivaldkondade avastamine

- muu kasu
- infoturbega seotud investeeringute kalkulatsioon
- kuluülevaate koostamine
- käitamiskulude ja protsesside jätkamisega kaasnevate kulude piirang
- varjatud kulud
- infoturbesse tehtavate investeeringute tasuvuse arvutamine
- investeeringu tulususe arvutamine
- juhatusele esitatavad põhjendused
- turvameetmete haakumine kõigi muude ettevõtteprotsessidega
- äriprotsesside ja äriintsidentidega arvestamine turvameetmete puhul
- mõju- ja vastutusvaldkonnad, tüüpilised komistuskivid
- infoturbega arvestamine IT soetamisel ja IT-projektides
- infoturbe edufaktorid
- millest sõltub infoturbega seotud projekti edukus?
- ootuste väljaselgitamine
- turbelahenduste kontseptsioon
- kontseptsiooni koostamine
- jaotamine osaprojektidesse
- osaprojektide teostamine
- moodulite ja funktsioonide testimine
- aktsepteerimis- ja integreerimistestid
- kasutuselevõtt
- sagedasemad vead infoturbe ellurakendamisel
- projektijuhtimise vead
- muud tüüpilised vead

Moodul 13: taristu turvalisus

Selles moodulis käsitletakse infotehnoloogia kaitsmist läbi ehituslike ja tehniliste meetmete.

Muu hulgas on siinkohal olulised järgmised punktid:

- objekti kaitse
- asukoha kaitse: ümbrus, piirded, vaba ligipääsuga ala kaitse, naabrusest tulenevad ohud, tsoonide loomine
- ehitustehnika: kaitse sissetungi eest, tuleohutus, kaitse vee eest jne
- tehniline seire
- seadmete kaitse
- sissepääsu kontroll
- pääsla
- ruumide lukustamine
- tehniline sissepääsukontroll
- elektritoide
- ülepingekaitse
- katkematu elektritoide
- trassid/kaabliühendused

- tuleohutus
- kliimaseadmed

Kontrollküsimused:

- Kas on tagatud, et kõiki töötajaid koolitatakse nende ülesannete ja vastutusalade järgi infoturbega seotud teemadel?
- Kas infoturbega seotud koolituste sisusid kontrollitakse regulaarselt nende ajakohasuse poolest ja kas neid sobitatakse koolitusvajadusega?
- Kas infoturvet puudutavate koolituste sisud on struktureeritud ja kavandatud olemasolevate töötajate sihtrühmade, ülesannete ja vastutusalade järgi?

M 3.46 Kontaktisik turvalisuse alal

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT turvaosakond

Rakendamise eest vastutavad: IT turvaosakond

Igas organisatsioonis peaksid olemas olema kontaktisikud, kelle poole saab pöörduda turbega seotud küsimustega, nii näiliselt lihtsate kui ka tehniliste küsimustega. Sellised isikud võivad olla IT administraatorid, IT-rakenduste eest vastutavad töötajad või IT turvaspetsialistid (vt M 2.12 IT-kasutajate nõustamine ja M 6.60 Turvaintsidentide käsitlusprotseduurid ja teavitamiskanalid). Kahjuks on inimeste valmisolek konkreetsetest turvaprobleemidest kellelegi teatada ikka veel väga madal. Kui IT turvaspetsialist on töötajatele muu hulgas selline kontaktisik, kelle poole võib pöörduda ka kõikide üldiste IT turbeküsimustega, vähendab see töötajate seas kartust konkreetsetest turvaintsidentidest teada anda.

Kuna paljud turbeprobleemid on seotud IT-süsteemide kasutamisega isiklikul otstarbel, peaksid IT turvaspetsialistid töötajaid informeerima võimalikest ohtudest ka sellest vaatevinklist, mis ei ole konkreetselt seotud tööga, nagu nt arvutiviirustest ja Trooja hobustest internetis surfamisel või siis oma andmete kaitsmisest internetipõhistel ostutehingutel. See suurendab töötajate avatust turbeküsimuste suhtes ning kasvatab mõistmist IT turvaspetsialisti töö vajalikkuse suhtes, pealegi võivad paljud eksikombel vaid isiklikeks probleemideks peetud juhtumid esineda ka bürookeskkonnas.

Kõik töötajad peavad teadma, kes on turbeküsimuste kontaktisik ja milliseid teavitamiskanaleid tuleb kasutada võimalike turvaintsidentide kohta käiva info edastamiseks. Selleks võib näiteks majasiseses telefoniraamatus või intranetis olla ära toodud vastavate kontaktisikute loetelu, mis sisaldab nimesid, telefoninumbreid ja meiliaadresse.

Kontrollküsimused:

- Kas ametiasutuses või ettevõttes on olemas kontaktisik turbeküsimustes?
- Kas kõik töötajad teavad, kes on kontaktisik turbeküsimustes?

M 3.47z IT-turbealased tegevus- ja rollimängud

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT turvaosakond

Rakendamise eest vastutavad: IT turvaosakond

Turbealaseid koolitusi peetakse tihti liiga igavaks. Seetõttu ei saavuta vastavad koolitused ka soovitud õpiefekti. Rollimängudes osalemine jääb töötajatele palju täpsemini ja pikemaks ajaks meelde kui materjal, mida on vaid slaididena tahvli peale näidatud. Plaani- ja rollimängud aitavad potentsiaalseid ohte ja tüüpilisi nõrki kohti arusaadavamaks teha ning annavad ühtlasi ka võimaluse leida probleemidele lahendused ja seda kõike enda töökeskkonnas. Plaanimänge võib korraldada praktiliste näidete baasil, nt meedias kajastatud värskete turvaintsidentide põhjal, samuti on võimalik tellida vastav harjutus selle valdkonna koolitajatelt. Plaanimängude sisu peaks olema kohandatud võimalikult täpselt oma institutsiooni oludele. Niimoodi on osalejatel palju kergem ennast pakutavates lahendustes ära tunda. Simuleerides erinevaid turvaintsidente, mis võivad mõjuda negatiivselt igapäevatöös kriitilise tähtsusega protsessidele, suudavad töötajad tõelise ohu korral palju paremini reageerida.

Samamoodi nagu koolituste puhul on ka siin ülimalt oluline, et tegevused planeeritaks kooskõlas erinevate sihtgruppide vajadustega. Osalejad peavad suutma mõista rollimängude olulisust ja nende läbimängimine peab tooma neile oma töökeskkonnas ka reaalselt kasu. Kõikide püüdluste käigus, mil töötajaid soovitakse informeerida IT-turbe vajalikkusest, tuleks ilmtingimata säilitada positiivne ja konstruktiivne meeleolu. Hirm võimalike turvaintsidentide ees võib ühelt poolt viia nende mahavaikimiseni ja teiselt poolt pole välistatud ka paanika tekkimine.

Järgmised näited tõestavad, et tegevusmängud võivad olla kas väga lihtsalt teostatavad harjutused, mida saab koolituse raames läbi viia, või ka keerulised simulatsiooniharjutused. Vastutavate läbiviijate ülesanne on arendada erinevate sihtrühmade vajaduste järgi nõuetekohaseid olukordi.

Töötõendite kandmine

Lühikeste rollimängude abil saavad töötajad hästi harjutada, kuidas nad peavad käituma, kui kohtavad asutuse sees asutusevälisеid isikuid. Võib harjutada, kuidas võiksid töötajad selles olukorras optimaalselt reageerida, näiteks pakkudes asutusevälistele isikutele „paremaks orienteerumiseks” saatmist vestluskaaslase juurde. Ka nende külastajate puhul, kes küll tunnevad majareegleid, kuid seda eitavad, võib harjutada olukorda, milles külastaja keeldub näiteks tõendi kandmisest, sest ta tunneb isiklikult ettevõtte juhti.

Manipuleerimise tüüpi ründed

Simulatsioonide käigus võivad töötajad harjutada, kuidas nad peaksid käituma manipuleerimise tüüpi rünnete korral. Selleks vastandatakse kaks väljavalitud sihtrühma, nagu nt IT-haldajad ja erinevad administraatorite rühmad, ühises simulatsioonis arvatavalt kahjutu küsimusega. Alles pärast nende küsimuste valdkon-

naülest vaatlemist saab selgeks, et tegemist on ründega. Simulatsiooni eesmärk on teha need seosed vastavate harjutuste kaudu selgeks, et selle tulemusel oleks võimalik kohaselt reageerida. Seda tüüpi simulatsiooni saab praktikas väga hästi läbi viia töötubades koos esitlusmaterjalide, nagu märkuste tahvli ja esitluskaartidega.

Simulatsiooniharjutused

Eriti olulised on simulatsioonid, milles harjutatakse toimetulekut turvaintsidentidega kuni hädaolukordadeni välja. Kuidas peavad töötajad end olukorda sobitama, omandama mingi olukorra käigus võimalikult hästi neile määratud rolle ja kohustusi ka raskendatud tingimustes (pinge, juhiste kuhjumine, ebaselged või sageli vahelduvad olukorrad, ressursside puudus, sideprobleemid jne). Simulatsioonide eesmärk seisneb esmajoones isiklike omaduste treenimises näitlikes olukordades, mida saab hiljem kasutada võimalikult paljudes intsidentides. Seetõttu peab simulatsiooni juhendama kogenud koolitaja, kes räägib pärast selle läbiviimist antava ülevaate käigus osavõtjatega nende kogemustest ja neid süvendab (vt M 6.117 Testid ja valmisoleku harjutused).

Kontrollküsimused:

- Kas tegevusmängudes harjutatakse keerulisi olukordi?
- Kas teavituste ja koolituste sisusid on nende kasuliku toe poolest kontrollitud tegevusmängudega?

M 3.48z Koolitajate või koolitusfirmade valimine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, infoturbeametnik, personalijuht

Rakendamise eest vastutavad: infoturbeametnik, personaliosakond

Teavitus- ja koolitusprogrammide eest vastutavad isikud peavad selgitama, kas ja millises ulatuses tahavad nad koolitajatena kasutada oma töötajaid või asutuseväliseid teenuseosutajaid. Lisaks sellele tuleb kindlaks määrata koolituse vorm.

Kui koolitajatena kasutatakse oma töötajaid, peavad neil olema vajalikud erialased teadmised ning nad peavad olema võimelised neid teadmisi ka sihtrühmadele edastama. Lisaks nõutavatele infoturbealastele teadmistele peavad koolitajatel olema väljakujunenud pedagoogilised ja suhtlemisalased oskused. Teavitusmeetmete puhul on tähtsad veel ka piisavad teadmised asutusest, selle turvakultuurist ja töökeskkonna tööprotsessidest. Lisaks on veel oluline, et koolitaja peab suutma sisu edasi anda oma auditooriumi jaoks arusaadavas keeles, st ta peab suutma asetada koolituse käigus käsitletavaid infoturbeaspekte vastavate tööde ja projektide konteksti. Asutusesisestele koolitajatele tuleb anda vajalik aeg, et teavitus- ja koolitusmeetmeid mitte üksnes ellu viia, vaid neid ka ette valmistada ja hinnata.

Kuludest ja kvalifikatsioonist tulenevalt võiks vähemalt esialgu olla eelistatud lasta koolitust läbi viia asutusevälistel spetsialistidel. Sellistel juhtudel tuleb selgitada, milliseid rahalisi ressursse on selleks võimalik kasutada. Asutusevälised koolitajad tuleb hoolikalt eespool nimetatud kriteeriumide alusel välja valida ja oma ülesandeks ette valmistada. Eriti tuleb neid teavitada vajalikust asutusesisesest taustateabest. Ka teavitus- või koolitusmeetmete asutusevälise läbiviimise korral on vajalikud asutusesisesed ressursid.

Nimetada tuleb koolituse vastutav koordinaator, kes:

- valib välja pädevad koolituse pakkujad,
- esitab õppesisud ja -meetodid ning annab koolitajate käsutusse nõutava teabe,
- koordineerib asutusesisest koolituse planeerimist, ettevalmistamist ja läbiviimist,
- loob suhtlusliidesed koolitajate ja oma töötajate vahel,
- analüüsib osalejate hinnanguid ja määrab kindlaks nõuetekohased parandusmeetmed, vajaduse korral koos koolitajatega.

Koolituse koordineerimise võib enda peale võtta infoturbeametnik või ka personaliosakonna töötaja. Infoturbeametnik ja personaliosakond peavad siinjuures igal juhul koostööd tegema.

Teadaolevalt on mitmeid väliseid teenuseosutajaid, kes pakuvad nõuetekohaseid teavitus- või koolitusmeetmeid, mis vastavad asutuse vajadustele või mida on võimalik vastuvõetavate kulutustega nendele kohandada. Teavitus- või koolitusmeetmete korral, mis hõlmavad mitmete tsüklite vältel suurt osa töötajatest, on otstarbekas kaaluda train-the-trainer-kontseptsiooni. Selle käigus viivad kas sobivad asutusesisesed töötajad või välised koolitajad ellu algsed meetmed, kusjuures eesmärk on, et sellel koolitusel osalejad võtaksid koolitaja rolli hiljem ise üle. Sellel võib nende töötajate jaoks olla väga positiivne mõju nende enda teavitamisele infoturbest ja ka motiveerimisele. Tänu sellele saavad nad koolitusse põimida ka oma isiklikke kogemusi. Just koolitusteemade puhul, mis käsitlevad kultuuri- ja teatud käitumisviiside aspekte asutuses, saab asutusesisene koolitaja oma asutusesiseseid protsesse puudutavate sügavamate teadmiste ja tuntuse alusel tõsta osalejate heakskiitu ning koolituse õpitulemuste edukust. Kui rakendatakse train-the-trainer-kontseptsiooni, peavad algsed meetmed ettenähtud erialaste teemade kõrval sisaldama ka juhiseid õppematerjali metoodilis-pedagoogiliseks edasiandmiseks.

Kontrollküsimused:

- Kas infoturbealaste teavitus- ja koolitusmeetmete jaoks valiti nõuetekohased koolitajad?
- Kas nimetati koolituse koordinaator?
- Kas erinevate koolitusfirmade pakkumisi on omavahel võrreldud, et välja selgitada, milline neist on oma sisu, kvaliteedi ja hinna poolest kõige sobivam?
- Kas osalejad hindavad läbiviidud teavitus- ja koolitusmeetmeid ning kas neid kogemusi hinnatakse asutusesiseselt regulaarselt?

M 3.49 Koolitus etalonturbe protseduuride alal

Algatamise eest vastutab: infoturbeametnik

Rakendamise eest vastutavad: infoturbeametnik, ülemused

Infoturbe eest vastutavad isikud peavad IT etalonturbe edukaks kasutamiseks tundma hästi selle metoodikat.

IT etalonturbe protseduuridesse süvenemiseks on mitmeid võimalusi:

- iseseisev õpe,
- etalonturbealaseid koolitusi pakkuvad välised koolitajad,
- osalemine oma asutuse korraldatavatel etalonturbekoolitustel.

Kui kavandatakse uut IT etalonturbe koolitust või tuleb teha väljastpoolt pakutavat koolitust puudutav otsus, tuleks vaadelda järgmisi teemasid:

- Infoturbeteadlikkuse suurendamine
- Mis on infoturbe haldussüsteem (ISMS)?
- Kuidas juurutada toimivat turbeprotsessi?
- Ülevaade etalonturbe kontseptsioonist (filosoofiast, rakendusvaldkondadest, struktuurist)
- Infoturbepoliitika koostamine

1. infoturbe eesmärkide defineerimine
2. infokoosluse defineerimine

- Infoturbe haldus

1. organisatsiooni struktuurid (infoturbehalduse jaoks sobilike organisatsioonistruktuuride esitlemine)
2. töörollid (infoturbeametnik, infoturbehalduse meeskond jne)
3. vastutusalad

- Turbekontseptsioon: tüüpiline ülesehitus ja teemad
- Struktuurianalüüs

1. rühmade moodustamine
2. rakenduste ja sinna juurde kuuluvate andmete koostamine
3. võrguplaani koostamine
4. IT-süsteemide tuvastamine
5. ruumide haldamine

- Kaitsevajaduse määratlemine

1. protseduur
2. kaitsevajadusi kirjeldavate kategooriate defineerimine koos individuaalsete hindamistabelite kohandamisega
3. kahjude stsenaariumid
4. rakenduste, IT-süsteemide, sideühenduste ja ruumide kaitsevajaduste määratlemine

- Etalonturbest lähtuv modelleerimine

1. ülevaade etalonturbe moodulitest
2. kihimudel
3. infoturbe üldkehtivad põhimõtted
4. taristu turvalisus
5. IT-süsteemide turvalisus
6. turvalisus võrgukeskkonnas
7. rakenduste turvalisus
8. tervikluse kontrollimine
9. meetmete kasutustsükli mudel

- Baas-turvakontroll

1. rakendatava metoodika kirjeldus
2. ellurakendamise seisund
3. täiendav turvaanalüüs: etalonturbest lähtuv riskianalüüs
4. turvameetmete realiseerimine
5. kõikide puuduvate meetmete väljaselgitamine
6. meetmete konsolideerimine
7. kulud ja kulude hindamine (eelarvestamine)
8. meetmete realiseerimine (ellurakendamise järjekord, vastutavad töötajad, teavitusplaan)

- Abivahendid tööks etalonturbekataloogidega
- Kasutajatele tuleks esitleda järgmisi võimalusi:

1. juhendid, mis peavad inimesi infoturbeks motiveerima
2. veebipõhine kursus sissejuhatuseks etalonturbe metoodikasse
3. tabelid ja ankeedid, mis on abiks ellurakendamisel
4. näidispoliitikad ja profiilid kui näidisrakendused
5. IT etalonturbel põhineva tööriista tugi infoturbe kontseptsioonide koostamisel, haldamisel ja edasiarendamisel. Erinevad tootjad pakuvad selle jaoks kohaseid IT etalonturbe tööriistu.

- ISO 27001 lühitutvustus

Standardite sari ISO 2700x

Standardi ISO 27001 ülesehitus

ISO 27001 normide rakendamine ISKE standarditele ja lisa A teemade rakendamine kihi 1 moodulitele

Sertifitseerimine ISO 27001 alusel lähtudes etalonturbest: sertifitseerimisskeemi ülevaade

Põhjaliku etalonturbekoolituse raames peaks osalejatel olema võimalus harjutada neile esitletud metoodikat näidete varal. Uute IT etalonturbe alaste koolituste väljatöötamiseks on BSI veebilehtedel abivahendite all saadaval ka teemakohased slaidid. Neid on võimalik kasutada lähtematerjalina oma koolituste väljatöötamisel. Kõikide koolituste sisu antakse lühidalt edasi ka ülevaadetes ja struktuuri

diagrammides. IT etalonturbe metoodikasse ja etalonturbekataloogide kasutamisse sissejuhatavate koolituste puhul on välja toodud ka võimalikud koolituste teemad.

Kontrollküsimused:

- Kas infoturbe eest vastutavad isikud on kursis IT etalonturbe metoodikaga?
- Kas IT etalonturbe koolituse kavandamisel määratakse koolituse teemad eelnevalt kindlaks?
- Kas IT etalonturbe koolitusel harjutatakse metoodikat ka näidete varal?

M 3.50z Personali valimine

Algatamise eest vastutavad: personalijuht, IT turvaosakond

Rakendamise eest vastutavad: personaliosakond, juhid

Töötajatelt eeldatavad kvalifikatsioonid ja oskused tuleks võimalikult täpselt kirja panna juba uutele töötajatele esitatavates nõuetes. Seda, kas need on kandidaatidel ka tõepoolest olemas, tuleks esmalt kontrollida esitatud dokumentide alusel ja hiljem vestluse käigus täpsustada. Isikute puhul, kes peavad hakkama täitma turbega seotud ülesandeid (nt turvaspetsialistide, andmekaitsespetsialistide, administraatorite, finantsidega seotud või konfidentsiaalsele infole ligipääsu omavate töötajate puhul) peab olema tagatud vastavate isikute usaldusväärsus (vt M 3.33z Personali taustakontroll). Eriti oluline on jälgida, et ei tekiks huvide konflikte ega liigset üksteisest sõltuvust, mis võiks kahjustada tööülesannete täitmist. Huvide konfliktid võivad tekkida eriti neil juhtudel, kus töötajad peavad täitma korraga erinevaid tööülesandeid, millega kaasnevad kas liiga laialdased volitused või volitused, mis on omavahel vastuolus. Lisaks tuleks veel ka jälgida, et töötajate tööülesannete täitmisega seoses ei tekiks huvide konflikte väljaspool ametiasutust või ettevõtet, nt eelnevate töökohtadega seoses või muude kohustuste tõttu. Huvide konflikti vältimiseks pärast töökohavahetust võib töötajatega kokku leppida, millistel tingimustel ja millise aja möödudes võib töötaja tööle asuda konkureeriva tööandja juurde.

Neil juhtudel, kus töötajate erialane kvalifikatsioon pole kõigis nõutud valdkondades piisaval tasemel, peab töötajatel olema võimalik oma kvalifikatsiooni tõsta. Vajaliku kvalifikatsiooni ja tööoskuste saavutamiseks ning nende värskendamiseks tuleks töötajaid regulaarselt koolitada, samuti tuleks neile regulaarselt meelde tuletada infoturbe olulisust (vt B 1.13 Infoturbe teadlikkus ja -koolitus).

Loetletud punktidega tuleks arvestada ka hooajaliste töötajate ning ajutiste teenuseosutajate valimisel.

Kontrollküsimused:

- Kas uute töötajate puhul on uuritud nende usaldusväärsust?
- Kas andmed esitatud dokumentides on korrektsed ja kontrollitavad?
- Kas töökohal nõutava kvalifikatsiooni omandamiseks on tarvis korraldada täiendavaid koolitusi?

M 3.51z Personali rakendamise ja kvalifitseerimise kontseptsioon

Algatamise eest vastutavad: IT turvaosakond, personalijuht

Rakendamise eest vastutavad: personaliosakond, ülemused

Iga töötaja jaoks tuleb koostada tööülesannete kirjeldus. Igaüks peab teadma, mida ta peab tegema. Tööülesanded peaksid olema jaotatud selliselt, et need ei kattuks omavahel, kuna vastasel korral hakkavad tekkima probleemid vastutusega. Töötajad peaksid tundma kõiki kontaktisikuid, kes on seotud nende töövaldkonnaga. Siia alla kuuluvad ennekõike need isikud, kes täidavad kas sarnaseid ülesandeid või on selle valdkonna tugiisikud. Töötajad peaksid näiteks teadma, kes vastutab IT tugiteenuse eest, ühelt poolt seetõttu, et probleemid lahendataks kohe pärast nende tekkimist võimalikult kiiresti, ja teiselt poolt seetõttu, et inimesed ei tüütaks kogemata valesid tugitöötajaid (vt G 5.42 Inimestega manipuleerimine (Social Engineering)).Võimalikult varakult tuleb paika panna töötajate asenduskord.

Töörollid, mida töötajad peavad hakkama täitma asuma, peavad olema selgelt defineeritud. Sellele toetudes tuleb töötajatele välja jagada vajalikud volitused (vt M 3.1 Uute töötajate esmane juhendamine ja väljaõpe ja M 3.2 Uute töötajate kohustamine eeskirju järgima). Kõik töötajad peavad olema läbinud koolituse nii oma tööülesannete kohta kui ka tööülesannete täitmiseks vajalike IT-süsteemide kasutamise kohta. Lisaks tuleb kõiki töötajaid loomulikult juhendada ka seoses kõigi kehtestatud turvaettekirjutustega. Selleks on soovitatav koostada vastav koolituse kontseptsioon (vt B 1.13 Infoturbe teadlikkus ja -koolitus).

Kontrollküsimused:

- Kas töötajate tööülesanded on kirjalikult fikseeritud?
- Kas töötajate asenduskord on kindlaks määratud?
- Kas töötajad teavad, millist vastutust kannavad institutsiooni piires nende kolleegid?
- Kas töötajate jaoks on loodud teadlikkuse ja koolituste kontseptsioon?

M 3.52 SAP süsteemide koolitus

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: juhid, administraator, kasutajad

SAP süsteemi on küllaltki keeruline nii administreerida, käitada kui ka kasutada. Seetõttu tuleb kõiki töötajaid, kes peavad SAP süsteemiga töötama, ilmtingimata selles valdkonnas ka koolitada. Eriti teravalt puudutab see administraatoreid.

Koolitused

Koolitusi erinevate SAP teemade kohta pakub nii SAP ise kui ka teised ettevõtted. Koolituste spekter ulatub siinkohal lihtsatest koolitustest inimestele, kes peavad kasutama SAP süsteemi kasutama igapäevaselt oma lihtsas bürootöös, st alates rakendusepõhisest koolitustest kuni selliste koolitusteni, mis on mõeldud administraatoritele ja käsitlevad seetõttu ka spetsiifilisi tehnikavaldkondi. Suurte ettevõtete ja ametiasutuse puhul on mõttekas koostada oma koolitusvariant ja see organisatsiooni sees kättesaadavaks teha. Koolituse sisu tuleb viia kooskõlla koolitatava personali tööalaste vajadustega. Koolituse üks osa peaks alati käsitlema ka turbega seotud teemasid, et tõsta töötajate turbealast teadlikkust ning soodustada SAP süsteemi turvalist kasutamist. Turbealast teadlikkust on soovitav regulaarsete ajavahemike tagant värskendada (*Security-Awareness-Programm*), mida saab kasutada ka muudatuste või uute olukordade, mehhanismide ja protseduuride tutvustamiseks. Peamiseks eesmärgiks on luua inimestes turbealane teadlikkus, st olukord, kus inimesed ei suhtu vastavasse infosse mitte ainult kui uudistesse, vaid hakkaksid seda kasutama ennetavatel eesmärkidel.

SAP infoallikad

SAP pakub oma toodete ja lahenduste kohta laialdast infot, mis on kättesaadav veebikeskkonnas. Kohu info on kättesaadav läbi interneti (vt M 2.346 SAP dokumentatsiooni kasutamine *).* Administraatorid peaksid neid infoallikaid kasutama regulaarselt, eriti selleks, et informeerida ennast Java-põhiste tehnoloogiate kohta. Info hankimise raames tuleks erilist tähelepanu pöörata turvet käsitlevatele teemadele.

Täiendavad kontrollküsimused:

- Kas kasutajaid on koolitatud SAP süsteemi kasutamise vallas?
- Kas administraatoreid on koolitatud?
- Kas administraatorid kasutavad regulaarselt online -infoallikaid, et viia ennast kurssi uute tehnoloogiate ja ka uuenenud turbeinfoga?

M 3.53w Sissejuhatus SAP süsteemidesse

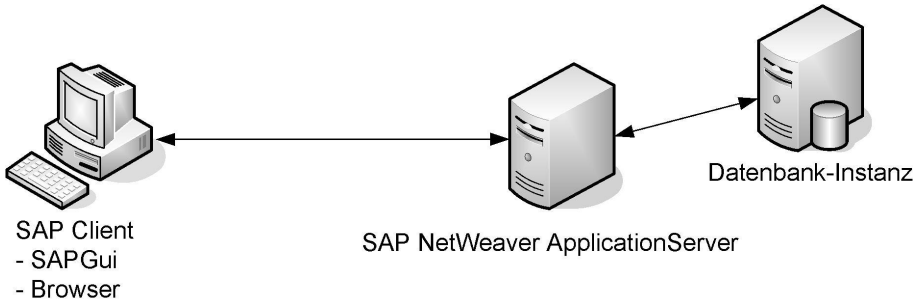
Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: IT-juht, administraator, kasutaja

SAP süsteemiinstallatsiooni tuumkomponendid

SAP süsteemiinstallatsioon koosneb lihtsustatud kujul järgmistest tuumkomponentidest:

- SAP NetWeaver ApplicationServer – käitab SAP rakendusi või mooduleid.
- Andmebaasi instants – peab andmebaasi, kuhu salvestatakse kõik SAP süsteemi andmed.
- SAP kliendid – koosnevad kas SAP graafilisest kasutajaliidesest või mõnest tavalisest brauserist.



Joonis. SAP süsteemi ülevaade

SAP Client – SAP klient; SAPGui – SAP graafiline kasutajaliides; Browser – brauser; Datenbank-Instanz – andmebaasiinstants

SAP NetWeaver ApplicationServer koosneb üldjuhul kahest komponendist: ABAP-pinust ja Java-pinust. Siin toimub olenevalt kasutatud programmeerimiskeelest rakenduste ja moodulite tegelike funktsioonide käitamine.

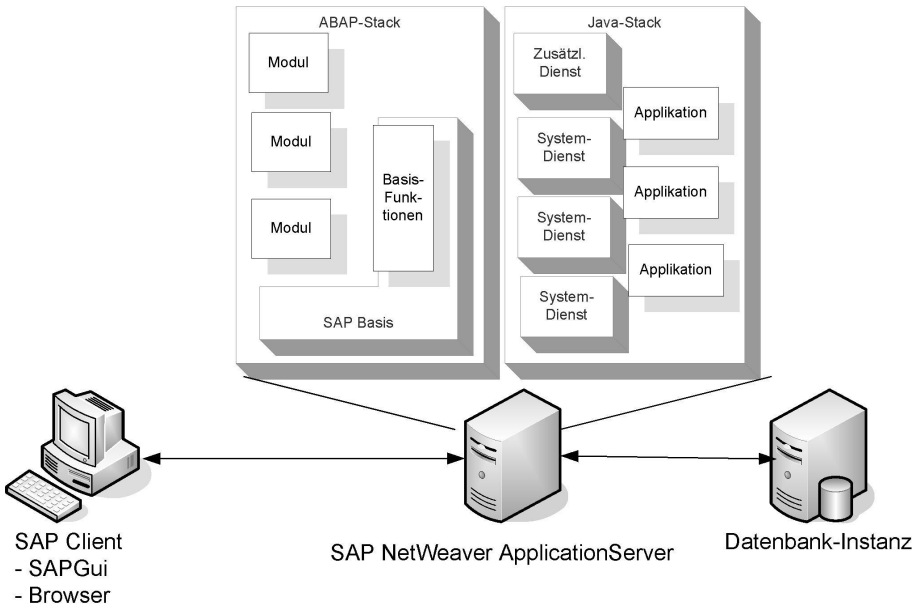
ABAP-pinu

ABAP-pinu kujutab endast SAP süsteemi traditsioonilist käitamiskeskkonda. Eelkõige kehtib see nende süsteemiversioonide puhul, mis kannavad tähistust SAP R/3, kuna R/3 komponentide ja moodulite käitamine leiab aste ABAP-pinus. ABAP-pinu koosneb nn SAP baasist, mis kujutab endast (ABAP-) programmide ja funktsioonide kogumit, mis juurutavad põhifunktsioone (nt kasutajate haldamist). Lisaks on võimalik juurde installeerida veel ka täiendavaid ABAP-programme. Need on kokku võetud rakenduspõhistesse moodulitesse (nt HCM, FI). ABAP-pinu programmid käivitatakse nn transaktsioonide abil. Selleks on igale ABAP-programmile omistatud oma transaktsioon. Enamasti rakendatakse aga hoopis selliseid transaktsioone, mis käivitavad programme, mis võivad omakorda lubada veel täiendavate programmide käivitamist (nt Transaction SE38, programmide käivitamine).

Java-pinu

Java-pinu koosneb üksikutest nn süsteemiteenustest, mis juurutavad Java-pinu süsteemifunktsioone. Funktsioonide laiendamiseks on võimalik installeerida ka

veel täiendavaid teenuseid ja rakendusi. Rakendustel on võimalik juurde pääseda erinevate teenuste funktsioonidele. Java-pinu teenuseid, funktsioone ja rakendusi kasutatakse üldjuhul läbi internetipõhiste protokollide (nt läbi HTTP).

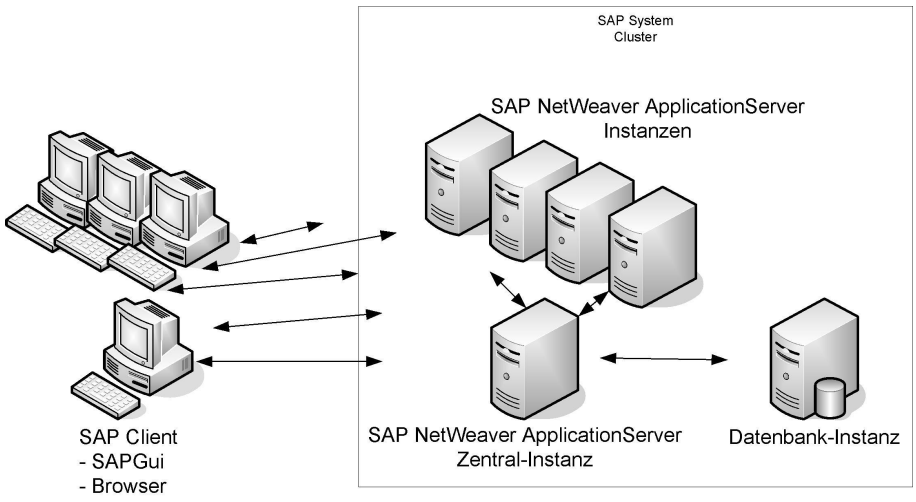


Joonis. SAP süsteemi ABAP-pinu ja Java-pinu

ABAP-Stack – ABAP-pinu; Modul – moodul; Basisfunktionen – baasfunktsioonid; SAP Basis – SAP baas; JavaStack – Java-pinu; Zusätzl. Dienst – lisateenus; Systemdienst – süsteemiteenus; Applikation – rakendus; SAP Client – SAP klient; SAP Gui – SAP graafiline kasutajaliides; Browser – brauser; Datenbank-Instanz – andmebaasiinstants

Instantsid

Selleks, et SAP süsteemid suudaksid toime tulla suure arvu kasutajatega, on SAP süsteemis loodud võimalus siduda mitmeid üksikuid NetWeaver ApplicationServeri instantse kokku üheks instantsiks (ühisnimetusega klaster). Need kannavad ühiselt kasutajate tekitatavat koormust ja moodustavad kliendi poolt vaadatuna omaette SAP süsteemi. Töö jaotamine erinevate serverite vahel leiab aset süsteemisiseste mehhanismide abil. Üks nimetatud instantsidest on peainstants, mida nimetatakse ka tsentraalseks instantsiks. Tsentraalset instantsi on võimalik täiendavate instantsidega laiendada, milleks tuleb sellele juurde installeerida täiendavaid SAP NetWeaver ApplicationServereid. Üksikud instantsid suhtlevad omavahel, et kliendid käsitleks klastrit SAP süsteemina.

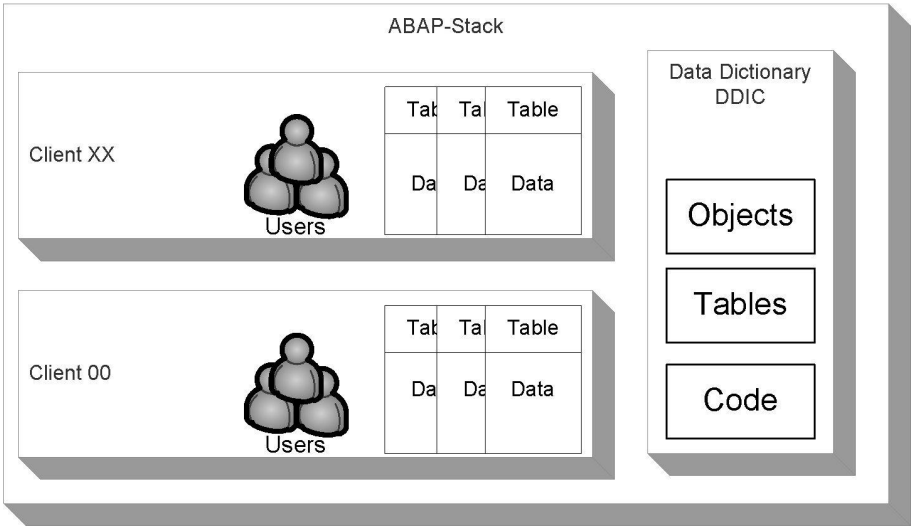


Joonis. SAP instantsid

SAP System Cluster – SAP süsteemiklaster; SAP NetWeaver ApplikationServer Instanzen – SAP NetWeaver ApplikationServeri instantsid; SAP Client – SAP klient, SAP Gui – SAP graafiline kasutajaliides; Browser – brauser; SAP NetWeaver ApplikationServer Zentral-Instanz – SAP NetWeaver ApplikationServeri tsentraalne instants; Datenbank-Instanz – andmebaasiinstants

Mandandid ja DDIC

ABAP-pinu on haldustehniliselt vaadelduna jaotatud nn mandantideks. Lisaks on olemas veel ka andmesõnastik (data dictionary, DDIC), kus hoitakse kõiki ABAP-pinu objekte. Olulisemad neist on tabelid, ABAP-programmid ja muud ABAP-programmides kasutatavad objektid. Mandandid kujutavad endast suletud hulka kasutajaid, funktsioone ja tabeleid. Juurdepääsud mandantide vahel ei ole üldjuhul võimalikud. Erandi moodustavad siinkohal mandantidest nii-öelda sõltumatud objektid (nt tabelid), mis on ligipääsetavad kõikidele mandantidele. Neis objektides tehtud muudatused mõjuvad ka kõikidele teistele mandantidele.



Joonis. SAP süsteemi mandandid

ABAP-Stack – ABAP-pinu; Client – klient; Table –tabel; Data – andmed; Data Dictionary/DDIC – andmesõnastik; Objects – objektid; Tables – tabelid; Code – kood

Kasutajad

Kasutajate puhul eristab ABAP-pinu kahte erinevat kasutajaliiki: kasutajad, kellel on olemas oma kasutaja põhikirje, ja kasutajad, kellel oma kasutaja põhikirje puudub. Põhjusel, et kasutaja põhikirjet omavaid kasutajaid hallatakse transaktsiooniga SU01, nimetatakse neid kasutajaid tihti ka SU01-kasutajateks. Nn internetkasutajatel seevastu aga oma kasutaja põhikirjet ei ole. Internetkasutajaid hallati senimaani transaktsiooniga SU05. SAP sellist teguviisi aga enam ei soovita. Pigem soovitatakse internetkasutajate loomiseks kasutada transaktsiooni SU01 ja teha sissekanne viitega nn referentskasutajale, mida oleks võimalik kasutada referentsina ka erinevatel internetkasutajatel. SU01-kasutajatest saab nende rakendusvaldkonna alusel luua erinevaid tüüpe, millega võivad olla seotud erinevad piirangud:

- Dialoog-kasutajad: kasutajal on lubatud ennast interaktiivselt SAP süsteemi sisse logida (dialoog-sisselogimine).
- Süsteem-kasutajad: dialoog-sisselogimine SAP süsteemi ei ole võimalik. Seda kasutajatüüpi on võimalik rakendada taustatöötluseks (pakktöötlus).
- Kommunikatsioon-kasutajad: kasutajal on lubatud kasutada tehnilisi kommunikatsiooniliike (remote function call, RFC). Dialoog-sisselogimine SAP süsteemi ei ole võimalik.
- Teenindus-kasutajad: kasutajat rakendatakse tehnilise kasutajana. Dialoog-sisselogimine on võimalik.
- Referents-kasutajad: kasutaja on referentsiks internet-kasutajale. Sisselogimine süsteemi ei ole võimalik.

SAP infoallikad

SAP süsteemid on keerulised ja koosnevad paljudest komponentidest. SAP süsteemide käitajate abistamiseks pakub SAP omalt poolt igasuguseid viiteid ja soovitusi nn SAP märkmete näol (SAP notes). Vastavatel märkmetel on oma konkreetsed identifitseerimisnumbrid ning need on kättesaadavad SAP Service Marketplace'i kaudu.

M 3.54 Salvestisüsteemide administraatorite koolitus

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT-turvaosakond

Rakendamise eest vastutavad: IT-turvaosakond, IT-juht

Salvestisüsteem on instants, kus hoitakse kas paljusid või koguni kõiki organisatsiooni immateriaalseid väärtuseid. Lisaks muutub salvestisüsteemide haldamine tänu üha laienevatele funktsioonidele aina keerulisemaks ja nõuab pidevalt uute teadmiste omandamist. Seetõttu on salvestisüsteemide administraatoreid tarvis ilmtingimata piisavalt koolitada, et nad ei tekitaks ainuüksi oma tegevusega mõttetuid lisaprobleeme, et nad suudaksid õigeaegselt tuvastada tehnilisi probleeme ning oskaksid optimaalselt ära kasutada kõiki pakutavaid funktsioone ja turvaomadusi. Koolitustel tuleks edastada piisavalt teadmisi salvestisüsteemi komponentide töölerakendamiseks ning käitamiseks vajalike protseduuride, tööriistade ja tehnikate kohta. Lisaks baasteadmistele vastavast tehnoloogiast on tarvis omandada teadmisi ka salvestisüsteemi erinevate komponentide tootjapoolsete eripärade kohta. See tähendab, et uute toodete kasutuselevõtmisel peavad administraatorid saama vastavate toodete kohta spetsiaalse täiendkoolituse. Koolitusmeetmete eelarvet tuleks hakata planeerima juba konkreetsete IT-komponentide soetamisprotsessi käigus ning administraatoritele tuleks koostada ka koolituskava.

Koolituse sisu peaks käsitlema järgmisi punkte:

- Salvestisüsteemide ja salvestivõrkude põhitõed
- Ülevaade võrkudest ja protokollidest
- Massmälusüsteemide ülesehitus
- Storage Area Network 'i tööpõhimõte (SANi kasutamise korral)
- SAN-Switching (SANi kasutamise korral)
- Massmälude andmevarundus
- Salvestisüsteemide ja salvestivõrkude sisseseadmine
- Monteerimine ja juhtmestik
- Salvestusüksuste, SAN-Switch 'ide ja Backup -seadmete sisseseadmine ja konfigureerimine
- Salvestisüsteemide ja salvestivõrkude käitamine
- Seadmete haldamine, tarkvaratööriistad
- Integreerimine võrguhaldussüsteemide (NMSide) alla
- Logimine
- Konfiguratsiooni seadistamine, haldamine ja varundamine
- Salvestisüsteemide ja salvestivõrkude vigade kõrvaldamine
- Veaallikad ja vigade põhjused
- Mõõte- ja analüüsitööriistad
- Veaotsingu testimisstrateegiad
- Salvestisüsteemide ja salvestivõrkude IT-turve
- IT-turbe põhitõed ning valdkonna jaoks olulised IT-turbeaspektid
- Viirusetõrje
- Autentimine, autoriseerimine
- Krüptoprotseduurid ja rakendused
- Veaallikas „ Default settings “

- Ennetavad meetmed, reageerimine ja analüüs
- Turvaintsidentide käsitlemine
- Disaster Recovery meetmed

Ka neil juhtudel, kus tööülesanded on ära jagatud administraatorite grupi vahel selliselt, et igaüks tegeleb vaid oma kindla vastutusalaga, peavad kõikidel administraatoritel olema vajalikud baasteadmised. Ka individuaalselt vajaminevate teadmiste sihipärane kogumine ja hoidmine saab toimuda ainult baasteadmistele toetudes. Paljudele toodetele pakuvad kas tootjad või spetsiaalsed edasimüüjad küllaltki laialdasi seminare, mis võimaldavad samm-sammult tutvuda vastavate toodetega ja sügavdada oma individuaalseid teadmisi. Kvaliteetsete koolituspakkumiste olemasolu on samuti üks kriteerium, millega tuleks ühe või teise tootja kasuks otsustamisel kindlasti arvestada.

Kontrollküsimused:

- Kas salvestisüsteeme käsitlevate koolitusmeetmete läbiviimiseks on olemas piisav eelarve?
- Kas eelnevalt loetletud punktidele toetudes on administraatoritele koostatud oma koolituskava?

M 3.55 Konfidentsiaalsuslepingud

Algatamise eest vastutavad: personalijuht, andmekaitsespetsialist, IT-turvaosakond

Rakendamise eest vastutavad: personaliosakond, ülemused

Organisatsioonivälised töötajad saavad tihti oma tööülesannete täitmiseks juurdepääsu konfidentsiaalsetele andmetele või jõuavad oma tööga tulemusteni, mida on tarvis käsitleda konfidentsiaalsetena. Sellistel juhtudel tuleb töötajatele panna kohustus käia nendega ümber moel, mis oleks kooskõlas kehtestatud nõuetega. Selleks tuleks koostada konfidentsiaalsuslepped (non-disclosure agreements) ja lasta välistel töötajatel need allkirjastada.

Konfidentsiaalsuslepetes peaks olema reguleeritud:

- milliseid andmeid tuleb käsitleda konfidentsiaalsetena,
- kui pikk on sõlmitavate konfidentsiaalsuslepete kehtivusaeg,
- mida tuleb teha sõlmitud konfidentsiaalsuslepete lõppemisel, nt kas vastavad andmekandjad tuleb hävitada või tagastada ,
- kuidas on reguleeritud informatsiooni omandiõigused,
- millised ettekirjutused kehtivad vajaduse korral konfidentsiaalse info kasutamise ja edasiandmise kohta täiendavatele partneritele,
- millised on konfidentsiaalsusleppe rikkumise tagajärjed.

Konfidentsiaalsuslepetesse võib lisada ka viiteid organisatsiooni olulisematele turvapoliitikatele ja muudele poliitikatele. Neil juhtudel, kus väljastpoolt tulevatele töötajatele antakse juurdepääs organisatsiooni IT infrastruktuurile, peaksid vastavad töötajad allkirjastama lisaks konfidentsiaalsuslepetele ka IT turvapoliitikad, kus käsitletakse IT-süsteemide kasutamist. Konfidentsiaalsuslepped loovad õigusliku aluse, millega saab kohustada väljastpoolt tulevaid töötajaid infoga konfidentsiaalselt ümber käima. Seetõttu tuleb konfidentsiaalsuslepete teksti pidevalt värskendada, et selles oleks alati sõnaselgelt kajastatud kõik organisatsioonile kõnealuses valdkonnas kehtivad seadused ja kohustused. Erinevate valdkondade jaoks võib olla mõttekas koostada erinevad konfidentsiaalsuslepped. Sellistel juhtudel peab olema selgelt määratletud, milliseid nõudeid tuleb erinevates valdkondades kajastada.

Kontrollküsimused:

- Kas välistele töötajatele pandi enne juurdepääsu võimaldamist konfidentsiaalsele infole kohustus, vastava infoga konfidentsiaalselt ümber käia?
- Kas konfidentsiaalsuslepetes arvestatakse piisavalt kõikide oluliste aspektidega, mis tagaksid organisatsiooni siseinfo piisava kaitse?

M 3.56 IP-kõne administraatorite koolitus

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: IT-juht, IT-turvaosakond

Telefoniga helistamine on sõltumata sellest, millist konkreetset tehnoloogiat organisatsiooni kodukeskjaamana kasutatakse, alati üheks peamiseks sideliigiks. Seetõttu peavad administraatorid olema piisavalt koolitatud, et nad suudaksid optimaalselt ära kasutada kõiki vajalikke funktsioone ja turvaseadeid. Koolitustel tuleks edastada piisavalt teadmisi VoIP-komponentide töölerakendamiseks ning käitamiseks vajalike protseduuride, tööriistade ja tehnikate kohta. Sama kehtib ka valmistajapoolsete eripärade kohta väljavalitud toodetel, mida rakendatakse VoIP-komponentidena. IP-kõne efektiivseks kasutamiseks läheb tarvis laialdasi teadmisi võrkudest. Ka neid teadmisi tuleb koolitustel edasi anda.

VoIP-komponente rakendatakse sageli standardsetes IT-süsteemides, mis on varustatud oma operatsioonisüsteemiga. Antud koolitusvaldkonna kohta leiate asjakohast infot vastavatest erinevaid operatsioonisüsteeme käsitlevatest IT etalonturbe moodulitest.

Enamikul juhtudel peaks koolitused kajastama vähemalt järgmisi teemasid:

- Põhitõed VoIP - kompressioonist ning kõneteadete edastamisest koos võimalike kaasnevate mõjudega nagu Jitter , Delay ja Echo.
- Põhitõed rakenduskihis kasutatavatest protokollidest (nt RTP'st, SIP'ist ja H 3.23'st)
- Haldamine:
- Turbega seotud administreerimise põhitõed ja kontseptsioonid, iga üksiku VoIP-komponendi käskude tundmine, mis puudutab selle kasutuselevõtmist, käitamist, hooldamist ja vigade otsimist. Koolitus peaks kujutama endast õpiprotsessi, kus teooria ja praktika on omavahel tasakaalus.
- Administreerimisalased teadmised IT-süsteemidest, mille peal tahetakse hakata käitama VoIP-komponete.
- Ülevaade olulisematest seaduslikest aspektidest seoses IP-kõne kasutuselevõtmisega, nt andmekaitseaspektidest.
- Seadmete ja tööriistade haldamine
- Logimine:
- Konfiguratsiooniandmete varundamine ja haldamine
- Ründestsenaariumid (nt Denial of Service ründed, ARP-Spoofing , IPSpoofing, DNS-Spoofing , viirused ja muu kahjurvara).
- Põhitõed teema kohta virtuaalsed privaatvõrgud (VPNid)
- Põhitõed krüpteeritud andmetega ümberkäimise kohta (nt krüpteerimine SRTP või IPSeci abil) ning võimalused krüpteeritud andmete töötlemiseks.
- Võrgutehnika:
- Võrkude struktureerimise põhitõed ning teenuse kvaliteet
- Algteadmised IPst ja sellele toetuvatest protokollidest (IP-adresseerimine, ICMP, TCP, UDP)
- Võrgu virtuaalne segmenteerimine (VLAN)
- Vigade kõrvaldamine:

- Veaallikad ja vigade põhjused
- Mõõte- ja analüüsitööriistad, tööriistad, mis võimaldavad automaatselt kontrollida turvalüüsi erinevate komponentide korrektset funktsioneerimist.
- Veaotsingu testimisstrateegiad

Ka neil juhtudel, kus tööülesanded on administraatorite grupi vahel ära jagatud, peavad kõikidel administraatoritel siiski olema vajalikud baasteadmised. Ka individuaalselt vajalike teadmiste sihipärane kogumine ja hoidmine saab toimuda ainult baasteadmistele toetudes. Paljudele toodetele pakuvad kas tootjad või spetsiaalsed edasimüüjad küllaltki laialdasi seminare, mis võimaldavad samm-sammult tutvuda vastavate toodetega ja süvendada oma individuaalseid teadmisi. Kvaliteetsete koolituspakkumiste olemasolu on samuti üks kriteerium, millega tuleb ühe või teise tootja kasuks otsustamisel kindlasti arvestada. Koolitusmeetmete eelarvet tuleks hakata planeerima juba konkreetsete IT-komponentide soetamisprotsessi käigus ning administraatoritele tuleks koostada ka koolituskava.

Kontrollküsimused:

- Kas koolitusmeetmete läbiviimiseks on olemas piisav eelarve?
- Kas eelnevalt loetletud punktidele toetudes on administraatoritele koostatud oma koolituskava?

M 3.57w IP-kõne kasutamise stsenaariumid

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: IT-juht, administraator

IP-kõnele ehk kõne edastamisele läbi IP-võrkude on olemas erinevaid kasutusvaldkondi. Erinevate kasutusvaldkondadega kaasnevad erinevad ohud ning ka erinevad turvanõuded. Järgnevalt on toodud ülevaade erinevatest võimalikest kasutusvaldkondadest.

VoIP rakendamine ühendatud lõppseadmes

Esimene kasutusvaldkond on IP-kõne rakendamine organisatsiooni telefonisides, kasutades selleks firma või ametiasutuse isiklikke võrke. See hõlmab kas täielikult või ka ainult komponentide haaval IP-telefonide kasutamist, LANil põhineva telekommunikatsioonisüsteemi kasutamist, mis peab üle võtma edastusfunktsiooni ja looma ühenduse välismaailmaga ning vastava IP-võrgu kasutamist, mis ühendab kodukeskjaama lõppseadmetega. Ühendus digitaalse kaugkõnevõrguga võib toimuda kas läbi lokaalsete *Gateway* 'de või läbi mõne *VoIP-Provider* 'i. Nn hübriidseadmete puhul on tavalistesse kodukeskjaamadesse integreeritud ka VoIP-moodulid, mis lubavad selle külge ühendada IP-telefone, tihti tootjapoolseid süsteemitelefone. Siinkohal on eesmärk andme- ja sidevõrgud omavahel integreerida. Võimaliku kokkuhoiu kõrval, mis saavutatakse liinide, võrgukomponentide, juhtimise, administreerimise ja hoolduse arvelt, eksisteerivad aga ka täiendavad ohud, kuna näiteks juba väheste teadmistega on võimalik sideühendusi pealt kuulata. Teatud osa kokkuhoiupotentsiaalist kahaneb tänu vajaminevatele turvameetmele oluliselt, eriti nt neil juhtudel, kus olemasolevat andmevõrku on tarvis hakata IP-kõne kasutamiseks ümber kohandama, kuid antud tehnoloogia turvaliseks ja usaldusväärseks kasutamiseks on asjakohaste turvameetmete rakendamine möödapääsmatu.

VoIP kasutamine kodukeskjaamade ühendamiseks

Kodukeskjaamade traditsiooniline ühendamine leiab enamasti aset läbi eraldiseisvate valimis- või püsiliinide. IP-kõne üks kasvav rakendusvaldkond on ka lokaalsete telekommunikatsiooniseadmete ühendamine (*trunking*) läbi IP-ühenduste. Selle lahenduse puhul kasutatakse traditsiooniliste kodukeskjaamade ühendamiseks WAN-andmevõrku. Terve asukoha telefoni- ja andmevõrgu ühendamine loob siinkohal suurema paindlikkuse ning võimaldab efektiivsemalt kasutada olemasolevat ribalaiust, mis tähendab lõppkokkuvõttes ka potentsiaalset kokkuhoidu.

VoIP kasutamine helistamiseks läbi interneti

Üks täiendav rakendusvõimalus on kõne edastamine läbi avalike IP-võrkude. Üha suurenevad ribalaiused *Backbone* - ja lõppühenduste valdkondades, mis on tänapäeval jõudnud juba küllaltki arvestatava kõnekvaliteedini, kiirendavad aina enam internetikõnede kasutuselevõttu ka isiklikuks otstarbeks. Selleks on võimalik kasutada tarkvaratelefone, mis on enamasti sarnaselt *Messaging* -teenustele registreeritud läbi tsentraalsete kataloogide. Üha enam leiavad kasutust kompaktsed ja soodsa hinnaga *VoIP-Gateway* 'd, mis võimaldavad tavaliste telefonidega (analoog- või ISDN-telefonidega) kasutada ka läbi interneti helistamise teenust. Samuti on võimalik isiklikuks otstarbeks soetada ka soodsa hinnaga käeshoitavaid telefoniseadmeid. Ettevõtted ja ametiasutused pole hetkel kõne edastamises läbi avalike IP-võrkude sugugi esirinnas. Peamine põhjus on siin asjaolu, et puuduvad mehhanismid, mis suudavad tagada teatud kindla kõne- ja edastuskvaliteedi.

M 3.58w Sissejuhatus traadita kohtvõrgu põhimõistetesse

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: IT-juht, IT-turvaosakond, administraator

WLANe on võimalik käitada kahes erinevas arhitektuuris. Ad-hoc -režiimis on omavahel otseses sideühenduses kas kaks või rohkem mobiilset lõppseadet, mis on varustatud WLAN-kaardiga (Clients). Enamikel juhtudel käitatakse WALNi infrastruktuuri-režiimis, st klientidevaheline side toimib läbi tsentraalse sidesilla, läbi nn Access Point 'i. Läbi Access Point 'i leiab aset ka ühendus traadiga LANsegmentidega. Infrastruktuuri-käitamisrežiimile on erinevaid kasutusvaldkondi:

- Kasutades korraga mitut Access Point 'i, on võimalik installeerida omavahel kattuvaid siderakukesi, mille abil saab tagada sideühenduse säilimise ka siis, kui klient liigub ühest siderakust teise (uitühedus, ingl roaming). Sellise lahendusega on võimalik teenusega laialdaselt katta suuri alasid. Ühe sideraku edastuskaugus sõltub väga suurel määral ümbritsevatest oludest ning jääb umbes 10 kuni 150 m vahele.
- Kahte Access Point 'i on võimalik kasutada ka sillana (Bridge) kahe, traadiga ühendatud LANi vahel. Samuti on võimalik Access Point 'i kasutada releena (Repeater 'ina) tööulatuse suurendamiseks.
- Kasutades Access Point 'ide juures asjakohaseid komponente (suunaantenne), võib WLANe kasutada ka erinevate tööasukohtade omavahelisse võrku ühendamiseks. Tootjate väitel on selliste lahenduste puhul võimalik saavutada kuni kilomeetrine tööraadius. Access Point 'e on sellistel juhtudel võimalik käitada kas relee või sillana.

Standardis IEEE 802.11 kasutatakse tähistus Independent Basic Service Set (IBSS) sidevõrkude puhul, mis töötavad Ad-hoc -režiimis ning tähistust Basic Service Set (BSS) infrastruktuuri-režiimis töötavate koosluste kohta, millel on oma Access Point . Mitut ühendatud BSSi nimetatakse ESSiks (Extended Service Set 'iks), ühendatud võrk kannab nimetust DS (Distribution System). Peaaegu kõikides Euroopa riikides kasutusse lubatud WLAN-süsteemid, mis vastavad standarditele IEEE 802.11, 802.11b ja 802.11g, kasutavad ISM-sagedusriba (Industrial-Scientific-Medical) vahemikus 2,4 ja 2,48 GHz, mida võib kasutada tasuta, ilma et oleks tarvis taotleda täiendavat luba. Saatja maksimaalne võimsus on piiratud 100 mW EIRP (Effective Isotropic Radiated Power) peale.
Süsteemid, mis vastavad standarditele IEEE 802.11a ja 802.11h, kasutavad 5 GHz sagedusala. Sagedusalas 5,15 kuni 5,35 GHz ning sagedusalas 5,47 kuni 5,725 GHz on Saksamaal lubatud piirangutega kasutada ühtekokku 19 kanalit, mille vahekaugused on 20 MHz. Kui kanali ribalaius on 20 MHz, siis lähedalolevaid teisi kanaleid sellega ei häirita. Sagedusalas 5 GHz töötavad ka sõjaväeja tsiviilotstarbelised radari- ja navigatsioonirakendused, ning siin tohib rakendada vaid selliseid süsteeme, mis toetavad dünaamilist sageduse valimist ja saatja edastusvõimuse reguleerimist.

Süsteemid, mis vastavad standardile IEEE 802.11, edastavad andmeid võimsusega 1 või 2 Mbit/s, kasutades spektrilaotuse meetodeid, ehk siis kas sagedushüpitamist (FHSSi) või otsejada (DSSSi). Täieliku loetelu mainimiseks olgu veel ka ära märgitud, et 802.11 defineerib lisaks ka veel infrapunal toimiva edastusmeetodi, kuid seni pole sellele parktikas märkimisväärset kasutust leitud. Süsteemid, mis vastavad standardile IEEE 802.11b, kasutavad DSSS-meetodit. Edastatavad andmed laotatakse laiali spetsiaalse kindla koodiga, eesmärgiga muuta

edastus kindlamaks igasuguste rikete suhtes. Juurdepääsu loomine sidekanaliga leiab, nagu kõikide 802.11 standardile vastavate süsteemide puhul, aset juhulikkuse printsiibil toimiva protseduuri kaudu, mis kannab nimetust Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). Andmeedastuse brutokiirus on IEEE 802.11b puhul maksimaalselt 11 Mbit/s. Nagu kõikide 802.11 standardite puhul, pole ka siin võimalik garanteerida püsivaid andmeedastuskiirusi, kuna need sõltuvad klientide arvust ja side edastuskanali kvaliteedist.

Süsteemid, mis vastavad standardile IEEE 802.11g, kasutavad edastustehnikana OFDMi (Orthogonal Frequency Division Multiplexing 'ut), mis vastab standardile IEEE 802.11a ning võimaldavad seetõttu andmeedastuskiirusi kuni 54 Mbit/s. 2,4 GHz sagedusalas on võimalik 802.11b standardile vastavaks sideedastuseks kasutada 13 sageduskanalit, mille sageduste omavaheline vahemik on 5 MHz. Kui kanalite ribalaiuseks on umbes 22 MHz, saab ilma kattumiseta korraga kasutada maksimaalselt siiski ainult 3 kanalit, nt kanaleid nr 2, nr ja nr 12. Süsteemid, mis vastavad standarditele IEEE 802.11a ja 802.11h, kasutavad 5 GHz sagedusala.

Ülevaade turvamehhanismidest

Kõikide 802.11 standardiga ühilduvate süsteemide turvamehhanismid on defineeritud standardis IEEE 802.11. Standardi täiendused, mis kannavad tähistusi a, b, g ja h, ei kajasta lisaturvamehhanisme Uusi turvamehhanisme defineerib vaid täiendus tähistusega i. Standardis IEEE 802.11 defineeritud mehhanismid on loodud eranditult vaid klientide ja Access Point 'ide vahelise sidekanali turvamiseks. Lisaks jätab sama standard ka vaba ruumi tootjapoolsetele laiendustele. Kõik standardi IEEE 802.11turvamehhanismid, mida järgnevalt esitletakse, on murtavad ning ei paku usaldusväärset kaitset konfidentsiaalse info edastamiseks.

Võrgu nimi (SSID)

- Standard pakub võimlaus anda võrgule nimi: ESSID või SSID (Extended) Service Set Identity). Selleks on võimalik kasutada kahte erinevat töörežiimi. Kui kasutaja määrab tunnuseks „Any“, aktsepteerib WLAN-komponent kõiki SSIDid. Muudel juhtudel kontrollitakse sisestatud nime ja võrguga võivad liituda vaid need osalejad, kellel on sama SSID. Ülekandes kahe naabruses oleva sideraku vahel kasutatakse SSIDd selleks, et leida üles järgmine Access Point . Kuna SSID saadetakse läbi võrgu loetava teksti kujul, saab potentsiaalne ründaja selle teada küllaltki lihtsate vahenditega teada. Mõningad Access Point 'id pakuvad võimalust siduda SSID edastamine Broadcast 'inguga. SSID sellise allasurumine ei vasta aga standardile.

WEP krüpteerimine, tervikluse kaitse ja autentimine

MAC-aadress

- Iga võrgukaart on varustatud konkreetse riistvara-aadressiga, niinimetatud MAC-aadressiga (Media Access Control -aadressiga). Põhimõtteliselt on ka WLANis võimalik defineerida vastavaid MAC-aadresse, millele lubatakse sideühendusi Access Point 'iga. Vajalikke aadressiloetelusid tuleb selle lahenduse puhul hallata „käsitsi“, mis on väga vaevarikas. Paljude kasutusvaldkondade puhul ei ole see isegi võimalik. MAC-aadresside filtreerimine ei kuulu standardi alla. Teiselt poolt jällegi on MAC-aadresside filtreerimine standardiga küllaltki kooskõlas, kuna filtreerimine ei mõjuta mitte mingil määral klientide koostalitlusvõimet.

- WLAN keskkonna konfidentsiaalsus, terviklus ja autentsus tuleks tagada WEP (Wired Equivalent Privacy) protokolliga. WEP-protokoll baseerub jadašifril RC4, millega töödeldakse loetaval kujul andmed sõltuvalt võtmest ja käivitusvektorist (IV) pakettide kaupa ümber šifreeritud andmeteks. Võtme moodustab siinjuures tähemärgijada, mille pikkuseks saab valida kas 40 või 104 bitti ja mis tuleb WLANis osalevatele klientidele ja Access Point 'ile juba eelnevalt kättesaadavaks teha. Antud lahenduse korral kasutatakse terve WLANi jaoks ühist võtit. IV valib andmete saatja ning iga edastatava andmepaketi jaoks tuleks see valida erinev. IV lisatakse krüpteeritud andmepaketile ette juurde ja edastatakse üle WLANi.
- WEP krüpteerib ainult edastatavad kasutajaandmed ja tervikluse kontrollsumma. Haldus- ja juhtsignaale (Management- und Control-Frame 'e) sideedastusliides ei krüpteeri.

Standardi IEEE 802.11i väljatöötamise käigus avaldas Wi-Fi Alliance, võttes aluseks IEEE 802.11i projekti nr 3.0, protokolli nimega WPA (Wi-Fi Protected Access). WPA sisaldab juba mõningaid turvamehhanismide parandusi ning kirjeldab ühelt poolt andmepakettide krüpteerimist peamiselt WEP'il (Wired Equivalent Protocol 'il) baseeruva TKIP (Temporary Key Integrity Protocol 'i) abil kombineerituna tervikluskontrolliprotseduuriga MICHAEL. MICHAEL lahendab WPA puuduliku tervikluskontrolli probleemi WEP. TKIP ja MICHAEL on siiski vaid ajutised lahendused, kuna TKIPd saab kasutada ainult valikuliselt ning WPA spetsifikatsioonid ei liigita seda kohustuslikuks.

Standard IEEE 802.11i, mis vastab väljaarvatud mõningate eranditega EAP-meetodite valikuvõimlaustes Wi-Fi Alliance'i WPA2'le, näeb kindlalt ette hoopis teistsuguse krüpteerimisprotseduuri kasutamist, milleks on CTR mode (Counter Mode) with CBC-MAC Protocol (Cipher Block Chaining Message Authentication Code, CCMP). Vastupidiselt RC4'le kasutab antud protseduur autentimis- ja kasutajaandmete krüpteerimiseks WEPis ja WPAs hoopis AESi (Advanced Encryption Standard 'it). Autentimisel ei krüpteerita AESiga mitte otse loetaval kujul olev tekst, vaid hoopis sümmeetrilisest võtmest tuletatud lugeja. Tegelik krüpteerimistulemus saavutatakse seeläbi, et loetaval kujul tekstiplokk seotakse AES-krüpteeringuga varustatud lugejaga vastava XOR-tehte abil. Lisaks kasutatakse CBCd (Cipher Block Chaining 'ut) ka veel andmete tervikluse tagamiseks. Võtmehalduse ja võtmete laialijagamise eelduseks on IEEE 802.1X. Standardis IEEE 802.11i kasutatava AES-võtme pikkus on 128 bitti. Nimetatud meetod on pikaajaliselt toimiv, kuid nõuab vastupidiselt TKIP-variandile uue riistvara kaasamist.

Autentimisel on võimaik täiendavaks kaitseks kasutada EAPd (Extensible Authentication Protocol 'i), mis vastab standardile IEEE 802.1X. EAP'd kirjeldab põhjalikult RFC 3748. Kasutaja logib ennast teatud autentimisinstantsi (nt RADIUS-serveri) juures sisse ning vastav instants kontrollib pääsuõigusi enne seansivõtmete vastastikust vahetamist. EAP toetab terve rea erinevate autentimismeetodite kasutamist, lubades rakendada nii sertifikaate kui ka kahefaktorilist autentimist.

Kontrollküsimused:

- Kas kasutajad ning ennekõike administraatorid on läbinud WLANi käsitsemist ja selle turvet kajastava koolituse?
- Kas kasutajaid on teavitatud tarkvaratööriistade turvamehhanismide olemasolust ning kas neid on koolitatud nende õige rakendamise vallas?

- Kas kõrge kaitsevajadusega turvatsoonides, mis vajavad LAN-i, toimub identifitseerimine ja autentimine MAC-aadressi abil?
- Kas WEP kasutamise korral, kui edastatakse andmepakette, valitakse alati erinev initsialiseerimisvektor?
- Kas WLAN-i kaitsmiseks kasutatakse pikaajaliselt turbestandardit WPA2?
- Kas autentimise täiendavaks kaitsmiseks kasutatakse Extensible Authentication Protocol'i (EAP)?

M 3.59 Traadita kohtvõrgu turvalise kasutamise koolitus

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: IT-juht, IT-turvaosakond, administraator

WLAN-komponentide käitamine eeldab laialdasi teadmisi selle tööpõhimõtetest, spetsiaalsetest tehnilistest eripäradest ning ka paljudest erinevatest turbeaspektidest. Seetõttu on ilmtingimata vajalik, et nii IT eest vastutavad töötajad kui ka IT-turvaosakond oleksid WLANi tööpõhimõtetest piisavalt informeeritud.

Administraatorite koolitus

WLAN-komponentide administraatoritel peaksid olema lisaks teoreetilistele teadmistele kindlasti ka praktilised oskused. Administraatoritele suunatud WLAN-koolitused peaksid muuhulgas kajastama järgmisi teemasid:

Ülevaade WLANi turbeaspektidest

- Tüüpilised ohud
- SSID, käitamisrežiimid, ühenduse loomine, aadresside filtreerimine, Spoofing 'u tõkestamine, MAC-aadresside filtreerimine

Sobilike turvamehhanismide väljavalimine, side autentimine ja turvamine

- WEP, WPA, WPA2, IEEE 802.11i, IEEE 802.1X
- Võtmehaldus TKIPs, CCMPs jne
- WLANi autentimismehhanismid nagu nt EAP, RADIUS
- WLANi tuvastamine
- WLANi käitamiseks vajalikud turbemeetmed
- Turvalisusega seotud WLANi konfigureerimisparameetrid

Süsteemihaldus

- Võrguanalüüsiprogrammid ja Wireless Intrusion Detection süsteemid
- VPNid WLANidele, IPSec, DHCP
- WLANide koostöö turvalüüsidega
- WLAN-komponentide kaitsmine volitamata juurdepääsu vastu

Kasutajate koolitus

Koolitada tuleb ka WLAN-komponentide kasutajaid, ennekõike WLAN-kliente. Kasutajad peaksid koolituste käigus selgeks saama WLAN-komponentide tööpõhimõtte ja nende turvalise kasutamise. Kasutajatele tuleb täpselt selgitada, mida tähendavad turvaseaded ning mille jaoks on need vajalikud. Lisaks tuleb kasutajaid informeerida ka ohtudest, mis kaasnevad neil juhtudel, kui kasutajad jätavad kas mugavusest või soovist saada vähem häirivaid veateateid turvaseaded kas tähelepanuta või koguni sisse lülitamata. WLAN-komponentide ja nende turvaseadete korrakohast kasutamist saab kasutajate hulgas saavutada kasutajate sihipärase teavitamisega.

Asutuse valvega tegeleva personali koolitamine

Võttes arvesse võimalikke *Wardriving* -ründeid, tuleks teavitustööd teha ka asutuse valvega tegeleva personali hulgas. Näiteks peaks valvega tegelev personal

suutma märgata ja näha ohtu ka selles, kui keegi võõras isik viibib pikemat aega kas sülearvutiga või koguni WLAN-antenniga ettevõtte hoone juures. Kahtluste korral tuleks olukorrast informeerida IT-turvaosakonda. Koolituste teemad tuleb alati viia kooskõlla kohapealsete kasutusvaldkondadega. Siinkohal võib mõelda ka veebipõhiste interaktiivsete koolitusprogrammide kasutamisele intraneti keskkonnas. Lisaks WLANi turvamehhanismide koolitusele tuleks töötajatele selgitada ka organisatsioonis kehtivad WLANi turvapoliitikat.

Täiendavad kontrollküsimused:

- Kas administraatorid on WLAN-komponentidega töötamiseks, eriti nende turbega seotud aspektide osas, piisavalt ette valmistatud?
- Kas kõik töötajad on kursis WLANi turvapoliitikaga?
- Kas kasutajad on WLAN-turvamehhanismidega kursis ning kas neid ka rakendatakse?
- Kas ka asutuse valvega tegelevat personali on koolitatud võimalike ohtude kohta?

M 3.60 Töötajate teadlikkuse tõstmine mobiilsete andmekandjate ja seadmete turvalise kasutamise kohta

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: IT-juht, IT-turvaosakond

Nii ettevõtetes kui ka ametiasutustes võetakse üha rohkem kasutusele kõikvõimalikke mobiilseid andmekandjaid. Lisaks suureneb ka selliste seadmete arv, mida on võimalik lisaks nende põhiotstarbele kasutada ka mobiilse andmekandjana. Selle kõigega seoses kasvavad ühelt poolt võimalused info levikuks, kuid teistelt poolt suureneb seeläbi ka potentsiaalsete turvalünkade arv. Teatud osa sellistest turvariskidest on küll võimalik tehniliste meetmetega minimeerida, kuid kui töötajatele ei õpetata kuidas mobiilseid andmekandjaid turvaliselt ja otstarbekalt kasutada, võib tekkida olukord, kus ettevõtted ja ametiasutused võivad olla teatud hetkel kõikvõimalikest tehniliste uuendustega liiga üle koormatud. Töötajatele tuleks selgitada mobiilsete andmekandjate ja seadete erinevaid kasutusvõimalusi. Siia alla kuulub ka informeerimine erinevatest seadmeliikidest ja nende variantidest, muuhulgas näiteks ka selle kohta, et ka MP3-pleier on mobiilne andmekandja. Lisaks tuleks töötajaid informeerida potentsiaalsetest ohtudest ja probleemidest seoses vastavate seadmete kasutamisega, samuti nende seadmete turvamehhanismide kasulikkusest ning kindlasti ka vastavate mehhanismide piiridest. Töötajatele tuleks regulaarselt selgitada uusi ohte, mis kaasnevad mobiilsete andekandjate ja seadete kasutamisega, näiteks panna intranetti üles vastavaid teemakohaseid artikleid või kasutada töötajatele suunatud uudiskirju.

Sihipärane kasutamine

Kasutajaid tuleb informeerida, et nad peaksid mobiilseid andmekandjaid ja seadmeid kasutama hoolikalt, et vältida nende kaotsiminekut ja vargusi ning tagada seadmete võimalikult pikk kasutusiga. Sel otstarbel võiks nt selgitada, kuidas tuleks seadmeid hoida väljaspool büroo- või eluruume ning milline on seadmete taluvus liiga kõrgete ja liiga madalate temperatuuride suhtes. Kahjudest ja kaotsiminekutest tuleks teavitada võimalikult kiiresti (M 2.306 Kahjudest teatamine). Lisaks tuleks kasutajate tähelepanu juhtida järgmistele täiendavatele aspektidele:

- millist liiki andmeid tohib ja milliseid ei tohi salvestada mobiilsetele andmekandjatele (vt M 2.217 Teabe, rakenduste ja süsteemide hoolikas liigitamine ja käitlus),
- kuidas kaitsta mobiilsetele andmekandjatele salvestatud andmeid volitamata juurdepääsu, manipuleerimise ja kaotsimineku vastu,
- kuidas mobiilsetesse andmekandjatesse salvestatud andmeid turvaliselt kustutada ning kuidas andmekandjaid korrektselt hävitada.

Täiendav kontrollküsimus:

- Kas töötajaid informeeritakse sellest, kuidas mobiilseid andmekandjaid ja seadmeid turvaliselt kasutada?

M 3.61w Sissejuhatus kataloogiteenuste põhialustesse

Algatamise eest vastutavad: IT-turvalisuse eest vastutav töötaja

Rakendamise eest vastutavad: IT-turvalisuse eest vastutav töötaja, spetsialist

Üha suurem hulk asutusi kasutab detsentraliseeritud, mitmeid riike hõlmavaid või lausa ülemaailmseid arvutivõrke, et vahetada tööprotsesside, eriülesannete või muude protseduuride jaoks vajalikku infot ja kasutada jagatud rakendusi. Seejuures tuleb kaitsta andmeid, samuti organisatsiooniväliseid ja -siseseid rakendusi kuritarvitamise eest. Sellistes võrkudes toimuva andmevahetuse jaoks on ülimalt oluline, et kasutajatel ja rakendustel, mis vajavad infot erinevate kommunikatsioonipartnerite, kasutajate ja võrguressursside kohta, oleks sellele infole juurdepääs. Seejuures tuleb tagada, et vastavat infot (näiteks sertifikaate, tooteomadusi jms) saaksid kasutada ainult volitatud kasutajad ja rakendused. Lisaks tuleb välistada infoga manipuleerimine ja selle võimalik kompromiteerimine. Ainult seeläbi saab tagada, et sideühendused luuakse eranditult usaldusväärsete partneritega ja et andmevahetus on piisavalt turvatud. Eriti siis, kui erinevate funktsioonide jaoks on kasutada suur kogus samalaadset infot, on väga oluline, et andmeid hallataks võimalikult tõhusalt ja kasutoovalt. Kui andmete kasutamine hõlmab endas peamiselt andmepäringuid ning andmeid muudetakse ainult harva, tuleks võrku integreerida kataloogiteenus, et tagada info ühtne organiseerimine ja võimaldada samal ajal rakendada selle kasutamiseks standardseid liideseid. Lisaks toetavad kataloogiteenused Single Sign-On meetodit, mille abil ei pea kasutaja pärast esmast autentimist muude võrgus leiduvate ressursside kasutamiseks ennast enam uuesti sisse logima.

Kataloogiteenuste ajalugu

Tänapäevaste kataloogiteenuste alguseks on Rahvusvahelise Telekommunikatsiooniühingu (ITU) kataloogiteenuste standard X.500. Standard X.500 kinnitati ka ISO 9594 standardina. Ajakohased kataloogiteenused kasutavad nime- ja failistruktuurides üldjoontes selle standardi sisemist ülesehitust. Standardi X.500 puuduseks on kataloogiteenuse keerukas juurdepääsuprotokoll, Directory Access Protocol (DAP), mis tugineb lisaks ka veel täielikul ISO/OSI protokollistikul. Praktilisema alternatiivina töötati välja Lightweight Directory Access Protocol (LDAP), mis lihtsustab juurdepääsu kataloogiteenustele, andes seega oma panuse nende populaarsuse kasvule. Võrreldes DAPiga rakendab LDAP palju vähem funktsioone ja andmetüüpe ning kasutab TCP/IP pinu. LDAP kaasaegne versioon LDAPv3 on saanud tööstusstandardiks ja RFC 4511 (endine RFC 2251) määratleb selle ka internetistandardina. Peaaegu kõik kataloogiteenused pakuvad tänapäeval võimalust kasutada LDAP-liidest, kuigi, lisaks sellele rakendatakse ka tootjate endi poolt arendatud protokolle ja liideseid. Vastava protokolli tõttu nimetatakse administratiivses keelekasutuses kataloogiteenuse servereid ka LDAP-serveriteks.

Kataloogiteenuste ülesehitus

Kataloogiteenuste ülesehitus meenutab hierarhilist andmebaasi. Objektide hierarhiliseks liigendamiseks kasutatakse puustruktuuri, sealjuures koosnevad kataloogipuu üksikud sõlmpunktid konteiner-objektidest, mis võivad omakorda sisaldada veel ka teisi objekte. Niinimetatud Leaf -objektid (lehed) on kataloogipuu lõpp-punktideks. Objektidest (sissekannetest, Entries) moodustub Directory Information Tree (DIT). Igal objektil on seejuures eraldi nimi, nn Distinguished Name (DN).

Näide

“cn=Max Mustermann, l=Bonn, ou=BSI, o=Bund, c=DE”

Ühe tasandi piires saab objekte eristada Relative Distinguished Name (RDN) abil, nt “cn=Max Mustermann”. Objektid sisaldavad omadusi (atribuute). Atribuutidele määratakse väärtused, näiteks: “mail: max.mustermann@bsi.bund.de”.

Directory Information Tree (DIT)

Igal Directory Information Tree (DIT) sissekanne liigitub vähemalt ühe objektiklassi (ObjectClass), nt “objectClass inetOrgPerson” alla. Eksisteerib objektiklasse, mis võivad olla edasiste sissekannete „konteineriteks“, ja selliseid, mis asuvad „lehtobjektidena“ DIT puustruktuuri okste lõpp-punktides. Directory Information Tree moodustab kataloogiteenuse struktuuri sees administraatorite mõjupiiri ja seega ka kataloogiteenuse enda piiri. Objektiklassides on defineeritud atribuudid, mis on saadaval vastavate sissekannete jaoks. Atribuutide liigitamine objektiklasside lõikes määrab selle, milliseid atribuute saab sissekannete jaoks kasutada. On atribuute, mis peavad sisaldama väärtust ja on selliseid, mis võivad jääda tühjaks. Näiteks objektiklassis ”inetOrgPerson"deklareeritav atribuut nimega “mail” võib jääda tühjaks. Objektiklasside vahel eksisteerivad sõltuvussidemed. Selleks, et kasutada levinud objektiklassi “inetOrgPerson”, tuleb esmalt deklareerida objektiklass “organizationalPerson”, see aga vajab objektiklassi “person” ja see veel omakorda objektiklassi “top”. RFC 2798 standardiga määratud objektiklass “inetOrgPerson” on üks enimkasutatavaid klasse, millega kuvatakse LDAPs isikuid nende organisatoorses keskkonnas.

Skeem (skeemifailid)

Objektiklasside definitsioonid on määratud nn skeemis. Skeem defineerib objektiklassid koos nende kohustuslike või täiendavate atribuutidega. Skeemid salvestatakse nn skeemifailidesse. Näiteks asub objektiklassi “inetOrgPerson” ja selle atribuutide kirjeldus failis “inetorgperson.schema”. Kataloogiteenuste paigalduspakettides on juba suur kogus skeemifaile juba olemas. Siiski on võimalik skeeme vajadusel ka täiendada või luua oma skeem. Kui üksikute objektiklasside definitsiooni on tarvis muuta, näiteks vastava atribuudikogumi täiendamisega, siis saab seda teha skeemi muutmise või täiendamise abil. Seega on skeemi muutmine teatud määral kõige tundlikum operatsioon, mida kataloogipuus üldse teha saab. Selline muudatus mõjutab kogu puud, mistõttu tuleb puu senine kontseptsioon uuesti põhjalikult läbi mõelda. Seetõttu nõuab kataloogiteenuse skeemi administreerimine põhjalikku kataloogiteenuse tundmist, samuti suuri teadmisi turvalisusest.

Hierarhilised vs relatsioonandmebaasid

Ka neil juhtudel, kui kataloogiteenuse andmed on salvestatud andmebaasi, on kataloogidel omadusi, mis eristavad neid muudest, eriti relatsioonandmebaasidest (vt B 5.7 Andmebaasid):

- Kataloogiteenused on organiseeritud hierarhiliselt, objektid koos atribuutidega on salvestatud neisse sissekannetena. Kataloogiteenuse objektid imiteerivad võrgu reaalseid objekte (nt kasutajaid või arvuteid). Objektide omavahelisi seoseid näitab nende sissekannete puustruktuur.
- Kataloogiteenused kasutavad teatud normeeritud struktuuri, mida saab vajadusel täiendada. Kasutatud skeem määrab kindlaks struktuuri. Skeem de-

fineerib objektiklassid koos nende kohustuslike või täiendavate atribuutidega. Vastavad atribuudid võivad olla mitme väärtusega.

- Kataloogiteenused pakuvad lihtsat ja kiiret võimalust lihtsastruktuuriliste otsingu- ja lugemispäringute jaoks. Kataloogiteenusega kontakteerumiseks kasutatakse võrguprotokolle. Suuremal osal kataloogiteenustest on selleks Lightweight Directory Access Protocol (LDAP) tugi, kuid sageli kasutatakse ka tootjate endi arendatud protokolle ja tarkvaraliideseid.
- Kataloogiteenustel on peenestruktuuriline turvamudel. Pääsuõigusi saab näiteks defineerida ühe sissekande jaoks ja siis võtta kasutusele kõikide teiste vastava sissekande alamsissekannete jaoks, mis kataloogipuus leiduvad.
- Kataloogiteenused on küll andmebaasid, aga need ei toeta jaotatud tehinguid või Rollback -operatsioone (taastamist). Parema käideldavuse tagamiseks jaotatud keskkonnas ei saa ei objekte ega ka atribuute muutmise ajaks lukustada. Seega tuleb leppida vähemalt ajaliste ebakõladega andmebaasi replikatsioonide vahel.

Võrreldes hierarhiliste andmebaasidega, nagu neid tavaliselt kataloogiteenustes kasutatakse, on relatsioonandmebaasidel muuhulgas järgnevad omadused:

- Päringute keeleks on SQL, mis võimaldab keerukamaid operatsioone, nt “Aggregation” loendamiseks ja “Join” ühendamiseks.
- Andmed on olemas tavakujul, puuduvad mitmeväärtuselised atribuudid.
- Relatsioonandmebaasid sobivad tänu oma lukustusmehhanismidele ja tehingutele nii koostöötavateks kui ka konkureerivateks kirjutusoperatsioonideks.

Kataloogiteenused on mõeldud lühikeste ühenduste jaoks ning lihtsateks päringuteks ressursside olemasolu kohta, atribuutide väärtuste olemasolu kohta või tervete objektide lugemiseks. Sellest võrdlusest selgub, et kataloogiteenuseid ei tohiks kasutada personali haldamiseks, olgugi et kataloogiteenus võimaldab asutusesiseselt kasutada mitmeid isikutega seotud atribuute. Nende alla kuuluvad näiteks kasutaja seostamine telefoninumbri, meiliaadressi ja ka sisselogimisnime, paroolide või sertifikaatidega. Muud omadused nagu palgatase, kontonumber, puhkusepäevad või tööaja lepingud on seevastu personaliosakonna andmed ning need ei tohiks olla osa kataloogiteenusest. Nii saab üksikuid, kataloogiteenuse jaoks olulisi andmeid hallata ka muude asutuses olevate relatsioonandmebaaside kaudu, nagu eelnevas näites toodud personaliandmete haldamise andmebaas. Seeläbi saab luua sõltuvusseoseid kataloogiteenuse andmebaasi ja teiste andmebaaside vahel. Andmevarunduse raames ja ka ootamatuste ennetamiseks tuleb jälgida, millistelt teistelt andmebaasidelt saab vastav kataloogiteenus oma sissekandeid.

Pääsuõigused ja õiguste pärimine

Kataloogiteenuse iga üksiku objekti ja iga objektiklassi lõikes saab objekti üksikutele atribuutidele kehtestada pääsuõigusi. Üksikasjalik õiguste määramine toimub seejuures õiguste omanike sissekandmisega pääsuloendisse Access Control

List (ACL). Võimalikud õigused ulatuvad seejuures Supervisor -tasemest, st täielikust administreerimisõigusest kuni sirvimisõiguseni, mis võimaldab vastava kataloogipuu lõiguga ainult tutvuda. Objektidele kehtestatud pääsuõigused päranduvad seejuures standardselt puu hierarhias ülevalt alla. Pärandamisprotsessi saab mõjutada filtritega, mis võivad automaatset pärandamist soovi korral takistada.

Reaalsed õigused

Kataloogiteenuste juurdepääsul rakenduvad lõppude lõpuks siiski kasutaja või kasutajate grupi reaalsed õigused. Reaalsed õigused arvutatakse seejuures igal kasutuskorral eraldi dünaamiliselt ning need põhinevad kasutajale ja kasutajate grupile antud õigustel.

Autentimine

Kasutajad pöörduvad kataloogiteenuse poole vastava klienditarkvara vahendusel. Kliendi juurdepääs kataloogiteenusele toimub tootjafirmade oma protokollide kaudu, seejuures edastab kataloogiteenus sisselogiva kasutaja privaatvõtme kliendile krüpteeritult. Krüpteerimisprotseduuri kaasatakse muuhulgas ka kasutaja parool. Kui kasutaja sisestab oma parooli, saab klient privaatvõtme lahti krüpteerida. Kliendi ja kataloogiteenuse serveri vahel leiab autentimiseks aset nn Challenge-Response -protseduur. Pärast edukat autentimist on kasutaja varustatud talle kataloogiteenuse kasutamiseks määratud pääsuõigustega.

LDAP-juurdepääs

Võrgurakendused ja internetikasutaja pöörduvad kataloogiteenuse poole tavaliselt LDAP-protokolli (Lightweight Directory Access Protocol) kaudu. Seejuures on olemas erinevaid ühendusliike, näiteks anonymous bind või proxy user anonymous bind. Eelseadistuse alusel antakse anonüümsele sisselogijale ka anonüümse kasutaja õigused. Standardina tähendab see piiramatuid lugemisõigusi, mis kehtivad kogu kataloogipuu ulatuses. Anonüümne sisselugemine ei nõua autentimist ning sellega tuleks edasise turvaanalüüsi juures arvestada. Parooliga autentimist saab konfigureerida selliselt, et parool edastatakse kas loetava teksti kujul või mitte. Paroole ei tohiks mitte kunagi edastada loetava teksti vormis. Turvalise ühenduse loomiseks Lightweight Directory Access Protocol i abil saab kasutada Secure Sockets Layer protokolli (SSL-protokolli) valikuliselt kas ühe- või kahepoolse autentimisega.

Sertifikaatide server

Sertifitseerimisserver on olulise tähtsusega õiguste määramisel ja seega süsteemi turvalisuse jaoks. Sertifikaadi haldamisest sõltuvad ka võrgus asetleidvad autentimised, samuti krüpteeritud kanali loomine (Secure Sockets Layer i, SSLi kaudu). Seetõttu nõuab sertifikaatide server eriti hoolikat administreerimist.

Partitsioonide loomine

Kataloogiteenuse skaleeritavuse ja jõudluse parandamiseks on soovitatav kataloogiandmebaas mitme serveri vahel partitsioonidena näol laiali jaotada. Partitsioonide loomisel tuleb arvestada mitme reegliga, näiteks M 2.409 Kataloogiteenuse partitsioonide loomise ja replikeerimise planeerimine kirjeldatutega .

Replikeerimine

Veatolerantsi ja süsteemijõudluse suurendamiseks võimaldavad kataloogiteenused kasutada erinevaid replikeerimisviise. Replikeerimise erinevaid aspekte kirjeldatakse ka meetmes M 2.409 Kataloogiteenuse partitsioonide loomise ja replikeerimise planeerimine .

M 3.62 Kataloogiteenuste administreerimise koolitus

Algatamise eest vastutavad: IT-juht, IT-turbespetsialist

Rakendamise eest vastutavad: IT-juht, administraator

Kataloogiteenuse administreerimine nõuab põhjalikke teadmisi tehnoloogiast, administreerimiskontseptsioonidest ning kasutatavast tootest. Puudulike teadmiste tagajärjel võib tekkida väärkonfiguratsioon, mis võib olulisel määral mõjutada institutsiooni turvalisust. Seega on vastavate administraatorite koolitamine antud valdkonnas kohustuslik.

Koolituse sisu

Sõltuvalt võrgu suurusest pole kataloogipuu administreerimine tavaliselt mitte ainult ühe vaid mitme administraatori ülesanne, kellest igal on oma eriülesanded ja tegevusvaldkonnad. Sellest tulenevalt ei vaja kõik kataloogi haldavad administraatorid ühesugust koolitust. Turvalise käitamise tagamiseks peab siiski iga administraator omama piisavaid põhiteadmisi käitamise aluseks oleva operatsioonisüsteemi kohta, et osata näha oma tegevust ka üldises kontekstis. Igal juhul peaksid koolitused käsitlema ja selgitama järgnevaid punkte. Kui sügavalt konkreetne administraator üksikuid aspekte tundma peab, sõltub tema hilisemast tegevusvaldkonnast ja kvalifikatsioonist.

Põhiteadmised autentimisest

- Ülevaade kataloogiteenustes vajaminevatest infoturbemõistetest, näiteks mida mõeldakse konfidentsiaalsuse, tervikluse ja käideldavuse all
- Identifitseerimis- ja autentimisprotseduurid, mõistete selgitused, näiteks teadmised, omand, omadus
- Teabe edastamine enamlevinud autentimisvõimaluste kohta, nt paroolide, ühekordsete paroolide, *Challenge-Response* -protseduuri, digitaalsete allkirjade jms kohta ning teadlikkuse tõstmine autentimistunnustega ümberkäimise suhtes
- Üldiste omandipõhiste autentimisvõimaluste, nt *token* ite, kiipkaartide, magnetribaga kaartide tutvustamine
- Võimalike biomeetriliste autentimismeetodite, nt sõrmejälgede, iirisetuvastuse, näotuvastuse jms demonstreerimine
- *Single-Sign-On* -toodete (SSO-toodete) eeliste ja puuduste tutvustamine
- SSO-toote kasutuskeskkonnale, näiteks administraatori töökohale seatud nõuete tutvustamine
- Ülevaade kasutatava SSO-toote turvafunktsioonidest
- Üldiste, kataloogiteenuste kasutamisega seotud andmekaitseaspektide tutvustamine, nt andmekaitseprobleemid, selges tekstivormis nimede avaldamine, kataloogiteenuste õiguslik liigitumine, töötajate andmed kataloogiteenustes
- Volituste halduse üldised aspektid ja juhised

Kataloogiteenuste põhitõed

- Kataloogiteenuse toimimisviisid
- Ülevaade üldiste kataloogiteenuste turvamehhanismidest ja turvahaldusest

- Puustruktuur ja nimeteisendus
- Pärimine kataloogipuu piires
- Autentimismeetodid kataloogiteenuse piires
- Kõikide kataloogiteenust pakkuvate serverite, kaasa arvatud replikatsioonide vajalik füüsiline kaitse

Kataloogiteenus

- Üldinfo: millega tuleb arvestada planeerimisel, paigaldamisel, administreerimisel?
- Skeemihaldus
- Partitsioonide loomine
- Replikeerimine, nt replikatsioonide tegemiseks kasutatavad meetodid, kataloogiteenuse sisu replikeerimiseks kasutatavad eelseadistusega parameetrid, kataloogiteenuse detsentraliseeritud administreerimise problemaatika seoses replikeerimiskonfliktidega
- Andmevarundus, nt kataloogiteenuste varukoopiate loomise problemaatika, andmete taastamine kataloogiteenust pakkuva serveri andmetest tehtud varukoopia abil, abimeetmed puustruktuuri defineerivate kataloogiteenuseserverite avarii korral
- Õiguste andmine, nt pääsuõiguste andmine kataloogiteenuste objektidele atribuutide tasandil, pääsuõiguste pärimine ja pärimise blokeerimine, reaalsed pääsuõigused, rollidel põhinev administreerimine, administratiivsete ülesannete delegeerimine
- Õiguste pärimine ja reaalsete õiguste arvutamine

Tootepõhiste / eritüüpi kataloogiteenuste põhitõed

- Kataloogiteenuse tootepõhine toimimisviis
- Kataloogiteenuse tootepõhised autentimismeetodid

Public Key infrastruktuur (PKI)

- PKI toimimisviis
- Sertifikaadid ja sertifikaatide erinevad tüübid
- Millega tuleb PKI planeerimisel arvestada?
- Suhtlemine PKI abil
- Sertifikaadiserveri administreerimine

Secure Sockets Layer (SSL)

- Põhiteadmised SSL-protokolli toimimisviisist
- SSLi konfigureerimine

Lightweight Directory Access Protocol (LDAP)

- LDAP-juurdepääs kataloogiteenusele
- Kasutajate võimalikud ühendamisviisid

Administreerimis- ja klienttarkvara

- Ülevaade administraatorite vastutusaladest, mis on vajalikud SSO-toote turvalise käitamise tagamiseks
- Ülevaade administraatorite jaoks olulistest võimalikest veateadetest
- Ülevaade administraatorite võimalikest privileegidest
- Administreerimis- ja klienttarkvara toimimisviis
- Administreerimis- ja klienttarkvara autentimine

Kui kataloogiteenuste planeerimisel langetatakse otsuseid rollidel põhineva administreerimise, samuti administreerimisülesannete delegeerimise kasuks, tuleb administraatoreid ka vastavalt nende ülesannetele koolitada. Erilist tähelepanu tuleb pöörata skeemiadministraatorite grupile, kuna neil on õigused muuta kogu kataloogipuu andmebaasi disaini. Kataloogiteenuse klienttarkvara ja LDAP-pääsuõiguste administreerimine eeldab põhjalikke teadmisi süsteemi konfigureerimisvõimaluste kohta. Seejuures on turvakeskkonna defineerimisel oluline roll kasutataval operatsioonisüsteemil, eriti oluline on see failisüsteemi turvalisuse jaoks.

Täiendavad kontrollküsimused:

- Kas kõik administraatorid on läbinud koolituse kataloogiteenuse käitamise aluseks oleva operatsioonisüsteemi turvafunktsioonide kohta?
- Kas kõik administraatoreid on läbinud koolituse kataloogiteenust puudutavate kliendi- ja serveripoolsete turvamehhanismide kohta?
- Kas kõiki administraatoreid koolitati rollipõhise halduse ja delegeerimise koolituse raames ka veel täiendavalt nende endi konkreetsete ülesannete osas?

M 3.63 Kasutajate koolitus autentimiseks kataloogiteenuste abil

Algatamise eest vastutavad: IT-juht, IT turbespetsialist

Rakendamise eest vastutavad: IT-juht, ülemused

Autentimine on kataloogiteenuste turvalises käitamises väga olulisel kohal. Autentimine peaks aset leidma niihästi suunal klient – kataloogiteenuse süsteem kui ka suunal kasutaja – klient. Teatud kataloogiteenuste kasutusvaldkondade puhul peaks vastastikuse usalduse loomise eesmärgil ennast autentima ka klient kasutaja suhtes ja server kliendi suhtes. Autentimise eduka läbimise korral saab kasutaja automaatse juurdepääsu kõikidele tema jaoks juurdepääsetavatele objektidele ja teenustele (background authentication). Sel moel toimib näiteks ainulogimisega pöördus (single sign-on, SSO). Kuna kataloogiteenusel baseeruv SSO on enamjaolt kasutuses koos volitustõendite, kiipkaartide, magnetribaga kaartide või sõrmejälje-, iirise- või näotuvastussüsteemidega, peaks järgnevad punktid andma ülevaate selleks vajalike koolituste sisust.

Järgnevad punktid on kokkuvõte kasutaja jaoks olulistest teemadest, mida tuleks käsitleda kataloogiteenuse abil turvalist autentimist tagavate koolituste raames:

- sissejuhatus turvalisust käsitlevasse identifitseerimise ja autentimise teemasse, nt selliste mõistete nagu teadmised, omand ja omadus selgitamine;
- kasutajate teadlikkuse tõstmine autentimistunnuste (nt paroolide ja PINide) kasutamisest;
- teiste võimalike olemasolevate autentimisvõimaluste õige kasutamine, näiteks volitustõendite, kiipkaartide, magnetribaga kaartide või autentimise biomeetriliste meetodite, nt sõrmejälje-, iirise-, näotuvastuse jms kasutamine;
- lugemis- või tuvastusseadmete kasutamine, nt kiipkaartide lugemisseadme turvatehniliste muudatuste tuvastamine;
- volituste halduse üldised aspektid ja juhised;
- ülevaade lõppkasutaja võimalikest privileegidest;
- üldiste, kataloogiteenuste kasutamisega seotud andmekaitseaspektide tutvustamine (nt andmekaitseprobleemid, selges tekstivormis nimede avaldamine, kataloogiteenuste õiguslik liigitumine, töötajate andmed kataloogiteenustes);
- kataloogiteenust võimaldava toote kasutuskeskkonnale, näiteks kasutajate töökohale seatud nõuete tutvustamine;
- ülevaate andmine kataloogiteenust võimaldava toote turvafunktsioonidest;
- ülevaade kasutajate vastutusaladest, mis on vajalikud kataloogiteenust võimaldava toote turvalise käitamise tagamiseks;
- ülevaade lõppkasutaja jaoks olulistest võimalikest veateadetest.

Seejuures tuleks tutvustada kontaktisikuid, kelle poole tuleb pöörduda asutuse kataloogiteenust puudutavate küsimustega. Lisaks tuleks kasutajaid informeerida võimalustest kataloogiteenuse sissekannet inspekteerida ja korrigeerida.

Kontrollküsimused:

- Kas kasutajad on läbinud kataloogiteenust käsitleva koolituse?

- Kui kasutajatele on antud volitused kataloogiteenuse all oma enda objektidele pääsuõiguste jagamiseks, siis kas neid on koolitatud vajalike kontseptsioonide ja mehhanismide teemal?
- Kas kasutajad on saanud koolituse turvamehhanismide ning rakendatud toodete ja tehnoloogiate kasutuskeskkonnale seatud nõuete teemal ja kas nad on läbinud nende toodete turvalise kasutamise koolituse?

M 3.64w Sissejuhatus Active Directory'sse

Algatamise eest vastutavad: IT-juht, IT-turbespetsialist

Rakendamise eest vastutavad: administraator

Active Directory on Windowsi serverioperatsioonisüsteemidel põhineva domeeni kõikide haldusandmete keskne andmebaas. Serveri-operatsioonisüsteemid koondatakse edaspidi ühismõiste „Windowsi server" alla. Abstraktselt vaadatuna moodustab Active Directory hierarhiliselt ja puustruktuuri abil organiseeritud objektpõhise andmebaasi. See tugineb kataloogiteenuse standardile X.500, millelt pärineb sisemine struktuur ja ülesehitus. Sellele vaatamata ei ühildu see kataloogiteenusega X.500.

Domeenid

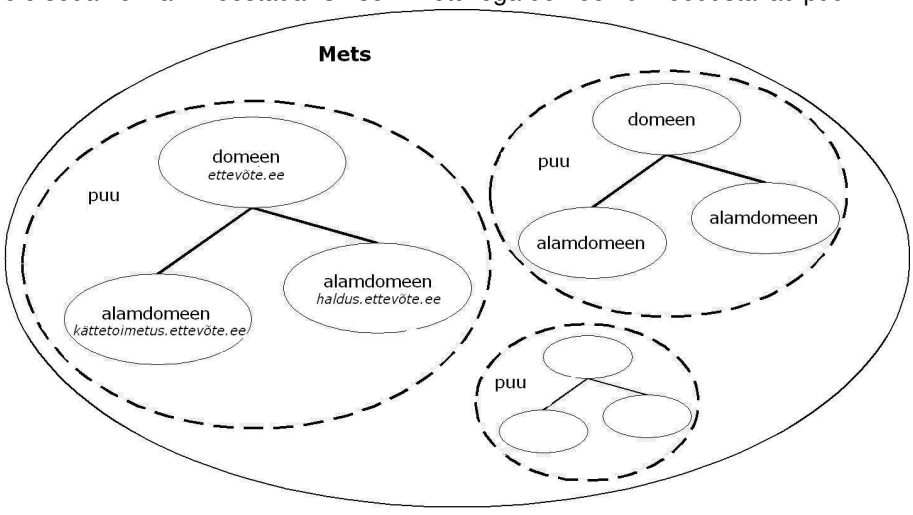
Windowsi serveri domeenikontseptsioon: arvuti ja kasutajad koondatakse domeeni alla ja domeeni administraator saab neid hallata. Domeeni piir moodustab üldjuhul ka administratiivse piiri ning piirab ka volituste mõjuala. Lisaks nimetatud kontseptsioonile pakuvad Windowsi serverid võimalust domeene üksteisega siduda puustruktuuri alusel, et luua domeenide vahel „vanem-laps" tüüpi seoseid. Laps-domeeni nimetatakse ka alamdomeeniks, kuna laps-domeeni nimi tuleneb kõrgemalseisva domeeni nimest – sellele nimele lisatakse punktiga eraldatud domeeni nimi.

Näide:

- vanem-domeeni nimi: ametiasutus.ee
- alamdomeeni nimi: haldus.ametiasutus.ee

Puu

Selliselt koostatud nimeruum on identne vastava DNS-i nimeruumiga ning teisiti ei ole seda võimalik koostada. Ühise nimetüvega domeenid moodustavad puu.



Mets

Erinevatesse puudesse kuuluvaid domeene – seega erinevatesse nimeruumidesse kuuluvad domeene – saab siiski ühiselt hallata. Selliselt kokku koondatud domeenipuud moodustavad metsa. Üksik domeen moodustab samuti puu ja samal ajal ka metsa.

Metsa juurdomeen

Metsas on alati üks eriline domeen, millel on teatud eristaatus. Tegu on esimesena loodud domeeniga, mida nimetatakse ka metsa juurdomeeniks. Eristaatus seisneb selles, et metsa juurdomeeni administraatorite volitused kehtivad kogu metsa ulatuses. Organisatsiooni administraatorirühma liikmete jaoks ei ole domeeni piirid administratiivseteks piirideks, sest neil on pääsuõigused kõikide domeenide jaoks. Windowsi domeenikogumi ülesehitamisel tuleb arvestada, et esimesena loodud domeen on alati metsa juurdomeen. Oluline on teada, et metsa juurdomeeni rolli ei saa hiljem mõnele teisele domeenile üle kanda, seega tuleb vajadusel kogu domeenistruktuur soovitud kujul uuesti luua.

Active Directory objektid

Active Directory koosneb erinevatest Active Directory objektidest (ADOdest). Igale objektile on määratud tüüp, nt kasutaja objekt või arvuti objekt, mis koosneb selle tüübi erinevatest atribuutidest. Erinevad objektiatribuudid võivad omada erinevaid väärtuseid, nt telefoninumbreid või IP-aadresse. Active Directory tunneb erinevaid eeldefineeritud objektitüüpe:- Domeeniobjekt: antud objekt on kõikide domeenis leiduvate Active Directory objektide juur ja sisaldab infot domeenide kohta, nt selle nime.

Domeeniobjektide alla võivad kuuluda täiendavad objektid:

- Rühmaobjektid: objektid teiste objektide rühmadesse liigitamiseks. Standardina on saadaval objekt „organiseerimisühik“ (Organizational Unit , OU). OU objekti alla võivad kuuluda edasised OU objektid, samuti arvuti, kasutaja ja kasutajarühmade objektid.
- Arvutiobjekt: antud objekt esindab Windows Client arvuteid. Arvutiobjekti alla ei saa liigitada täiendavaid objekte. Active Directory on mõeldud ainult Windowsiga arvutite haldamiseks, seega võivad arvutiobjektid esindada eranditult vaid Active Directoryga koostöötavaid Windowsi arvuteid.
- Kasutajaobjekt: antud objektiga esindatakse domeeni kasutajaid. Kasutajaobjekti alla ei saa kuuluda muid objekte.
- Kasutajagruppide objektid: need nn turvagrupid esindavad Windowsi gruppe.

On erinevaid grupitüüpe, mille erinevused seisnevad nende kehtivusalas (domeeni või kogu metsa piires) ja grupi võimalikes liikmetes (domeeni, metsa objektid). Siinkohal eristatakse kohalikke, domeenide kohalikke, globaalseid ja universaalseid gruppe. Turvagruppe kasutatakse volituste andmiseks.

Windowsi serveris arvestada suure gruppide arvuga (suuremate ettevõtete puhul mitmekümne tuhandega), mistõttu tuleb kaaluda programmitoega haldust. Halduse võib lahendada nii isekirjutatud skriptide kui ka teiste firmade toodete abil. Kas ja millised programmid on vajalikud, tuleb otsustada sõltuvalt konkreetsest olukorrast.

Active Directory üldist ülesehitust võib kirjeldada järgnevalt:

- Domeeni objekt moodustab domeeni kajastava Active Directory puu juure.

- Domeeni objekti alla luuakse OU-objektid, et arvuti, kasutaja ja kasutajagruppide objekte oleks võimalik struktureeritult kokku koondada. Kuna OU-objekte saab üksteise suhtes allutada, tekib organisatsiooni spetsiifikat järgiv puustruktuur.

Kohandamine administratiivsete oludega

Pärast standardset installeerimist on olemas lihtne ja tasapinnaline Active Directory struktuur, mille loob Windowsi server ja mida tuleb muuta vastavalt Active Directory planeerimise käigus väljatöötatud tingimustele. Kuna Active Directory on mõeldud peamiselt Windows-süsteemide haldamiseks, tuleb Active Directory struktuuri ülesehitamisel jälgida, et struktuur viidaks eelkõige vastavusse administratiivsete oludega. Kui selle asemel püütakse jäigalt iga pisidetailini taasluua asutuse organisatoorset struktuuri, võivad tagajärjeks olla haldusprobleemid.

Skeem

Niinimetatud Active Directory skeem kehtestab Active Directory objektide võimalikud kombinatsioonid, st määrab, milline objekt tohib teisi objekte sisaldada, millised on olemasolevad atribuudid ja millistest atribuutidest koosnevad objektid. Microsofti poolt etteantud Active Directory skeemi saab ka muuta. Kuid muutmise puhul on tegu tõsise sekkumisega Active Directory sse, mida tohib teha ainult hoolikalt ette planeerides. Skeemi muutmine mõjutab kõiki ühiselt hallatavaid domeene, st metsa (Forest). Kuna skeemi muutmine on kriitiline operatsioon, saab seda teha ainult ühes kindlas arvutis, nn Scheme Master is, kasutajagrupi Scheme Admins liikmete abil. Skeemimuudatuste tühistamine võib olla võimatu. Antud kasutajarühma kuulumist tuleb jagada ülimalt piiratult ning seda tuleb rangelt kontrollida.

Organisatsiooni administraatorid

Grupi „Organisatsiooni administraatorid“ liikmed, kelle hulka kuulub eelseadistuse puhul ka Forest-Root domeeni administraator, omavad erivolitusi võrgu kõikides domeenides. Neil on näiteks õigus lisada metsa uusi domeene ja neil on administraatoriõigused kõikides Active Directory domeenikontrollerites.

Domeeniadministraatorid

Konkreetse domeeni piires toimub administreerimine vastava (domeenispetsiifilise) grupi „Domeeniadministraatorid“ poolt. Sellel grupil on domeeni piires piiramatud administratiivsed volitused. Administratiivsete ülesannete täitmist on siiski võimalik lubada ka teiste kasutajakontode alt ning seeläbi administratiivseid ülesandeid delegeerida (vt M 2.230 Active Directory halduse planeerimine). Administratiivsete ülesannete delegeerimine domeeni piires võib toimuda ka selliselt, et delegeeritakse ainult teatud kindla osa kasutajakontode ja domeeni kuuluvate arvutite administreerimine. See on võimalik OUde piires, mis on mõeldud domeenis olevate kasutaja- ja arvutikontode grupeerimiseks.

Grupipoliitikad

Suur osa Windows-klient-konfiguratsiooniparameetritest on koondatud „grupipoliitikatesse“. Lisaks iga üksiku Windowsi klient-arvuti lokaalsetele grupipoliitikatele leidub ka grupipoliitikaid, mis on salvestatud Active Directory sse. See võimaldab arvuteid või kasutajakontosid tsentraalselt konfigureerida. Selliste, ADsse salvestatud grupipoliitikate mõjualaks võivad muuhulgas olla terved domeenid või

OUd. Siin rakendatakse OUsid samalaadselt konfigureeritud arvutite või kasutajakontode grupeerimiseks. Kuna OUsid on võimalik põimida ja ühe OUga võivad olla seotud mitmed grupipoliitikad, võivad üksikutele arvutitele korraga mõjuda mitmed erinevad grupipoliitikad (vt M 2.231 Windowsi grupipoliitika planeerimine ja M 2.326 Windows 7 grupeerimissuuniste planeerimine).

Jagatud andmebaas

Andmete salvestamiseks kasutatakse relatsioonilist, tehingutele suunatud andmebaasi. Vastav andmebaas jaotatakse spetsiaalsete serverite ehk domeenikontrollerite vahel. Domeenikontroller kasutab seejuures Active Directory t, et tagada domeeni piires kasutajate ja arvutite tsentraalne autentimine ja autoriseerimine.

Selleks kasutatakse järgnevaid protokolle:

- LDAPd (Lightweight Directory Access Protocol) Active Directory objektide ja atribuutide päringute jaoks
- Kerberost kasutajate ja arvutite autentimiseks
- CIFSi (Common Internet File System) arvutivõrgu andmeedastuseks
- DNSi (Domain Name System) võrgu arvutisüsteemide nimeteisenduseks.

Mõned erandid välja arvatud, sisaldab iga domeenikontroller ainult oma domeeni andmeid. Nimetatud erandid on järgnevad:

- Iga domeenikontroller sisaldab kogu metsa kajastavaid skeemi- ja konfiguratsiooniandmeid.
- Igas domeenis sisaldab vähemalt üks domeenikontroller lisaks ka veel "Global Catalog andmeid.

Global Catalog

Active Directory t hoitakse domeenikontrolleritel ja sünkroniseeritakse domeeni piires nendevahelise replikeerimise teel. Domeeni Active Directory sisaldab ainult domeeni puudutavat infot. Et leida metsas kiirelt infot kogu metsa kohta, moodustatakse nn Global Catalog (GC). See koosneb Active Directory objektide osainfost ja replikeeritakse kogu metsas selliselt, et domeeni Global Catalog i kaudu pääseks ligi teiste domeenide infole.

Sites

Lisaks kirjeldatud puulaadsetele ja hierarhilistele struktuuridele loob Windowsi server automaatselt ka täiendava ja ortogonaalse struktuuri. Ruumiliselt üksteisele lähedal asuvad arvutid – Windowsi server tuvastab seda võrguaegade abil – koondatakse kokku nn asukohtadeks (ingl Sites). Asukohtade abil juhitakse muuhulgas ka domeenikontrollerite replikeerimisstruktuuri. Ühe asukoha kohta peab olema vähemalt üks arvuti, mis sisaldab Global Catalog i koopiat. Kasutaja logimisprotsessi raames tuleb esitada päring Global Catalog ile, mis tähendab, et sisselogimisel peab alati mõni Global Catalog i server olema saadaval. Windowsi serveri poolt automaatselt koostatud asukohastruktuuri tuleks kohandada vastavalt ametiasutuse või ettevõtte sisestele oludele, nt asukohtadele erinevates linnades või riikides. Kuna see mõjutab Active Directory replikeerimissuhteid, tuleb selleks luua sobiv kontseptsioon.

Flexible Single Master Operations

Neid rolle nimetatakse Windowsi-serveri terminoloogias ka FSMO-rollideks (FSMO = Flexible Single Master Operations). Teatud muudatusi saab seega teha ainult arvutis, mis on seotud vastava rolliga. Andmete võrdlemine üksikute domeenikontrollerite vahel võib toimuda kahe erineva replikeerimismehhanismiga. Konfigureerida saab niihästi kasutatavat mehhanismi kui ka ajavahemikke, mille järel toimub replikeerimine. Jaotatud andmebaaside kontseptsiooniga saab saavutada Active Directory teatud tõrkekindluse, kuid probleemiks on seejuures FSMO-rollide omanikud.

Multi-Master -replikeerimine

Active Directory andmeid replikeeritakse organisatsiooni domeenikontrollerite vahel Multi-Master-replikeerimisprotseduuri abil. Igal domeenikontrolleril on seega olemas Active Directory replikatsioon, mida saab muuta ja mis võib olla tulevaste replikeerimiste aluseks. Kasutades asutuse raames korraga mitmeid domeenikontrollereid, tekitatakse sellega Active Directory liiased koopiad ning täieliku avarii tõenäosus väheneb.

M 3.65w Sissejuhatus VPNi põhimõistetesse

Algatamise eest vastutavad: IT-juht, IT-turbespetsialist

Rakendamise eest vastutavad: IT-turvaspetsialist, administraator

Virtuaalne privaatvõrk (VPN) võimaldab IT-süsteemide vahel luua juurdepääsukontrolli ja krüpteerimisega kaitstud turvalise sidekanali. Sobivate krüptograafiliste protseduuride valimise ja rakendamisega saab kaitsta edastatavate andmete terviklust ja konfidentsiaalsust. Samuti saab sobiva konfiguratsiooni puhul kommunikatsioonipartnereid turvaliselt autentida, seda ka siis, kui mitmed võrgud või arvutid on omavahel ühendatud renditud või avalike võrkude kaudu. VPNi saab luua peaaegu ükskõik millise kanali kaudu. VPNid võivad erineda oma juurutamisviisi, funktsioonide ja ka ISO/OSI-kihimudelist kasutatava kihi osas. Juba VPNi planeerimisel tuleks otsustada, kuidas VPNi hiljem käitada ja kas anda selle ülesehitamine või käitamine välise teenusepakkuja hoolde.

Järgnevalt kirjeldatakse mõningaid kasutusvaldkondasid, mis on VPNide puhul laialt levinud:

- Liikuvad töötajad: Liikuvad töötajad liiguvad erinevate töökohtade vahel ja erinevates keskkondades ning võivad seega vajada kaugpääsuõigusi asutusesiseses LANis hoitavatele andmetele ligipääsemiseks. Lisaks vastavate ühenduste kaitsmisele tuleb arvestada ka lõppseadme ning selle kasutuskeskkonna turvalisusega. Sõltuvalt ülesannetest võib juhtuda, et töötajad peavad ennast sisevõrku logima ka täiesti juhuslikest töökohtadest, näiteks hotellist või lennujaamast. Saavutamaks siinkohal sobivat, bürooga võrreldavat turvalisust, tuleb lisaks arvestada soovitustega moodulist B 2.10 Mobiilne töökoht . Töötajate lõppseadmeteks on tavaliselt sülearvutid või pihuarvutid. Ka siinkohal tuleb rakendada vastavaid IT-etalonturbe mooduleid, B 3.203 Sülearvuti ja B 3.405 Pihuarvuti (PDA) .
- Kaugtöökoht: Kaugtöökoha ühendamisel siseneb klientsüsteem väljaspool bürookeskkonda asuvast püsitöökohast asutuse sisevõrku. Kommunikatsioon kaugtöökoha ja LANi vahel leiab tavaliselt aset ebaturvaliste, avalike võrkude kaudu. Kaugtöökoha IT-süsteeme tuleks hallata tsentraalselt. Turvalisuse tagamist kaugtöökoha arvuti ühendamisel on kirjeldatud moodulis B 5.8 Kaugtöö .
- Kohapealsed võrguühendused: Kohapealsete võrguühenduste loomisel ühendatakse asutuse erinevates asukohtades olemasolevad osavõrgud. Seejuures ühendatakse usaldusväärsed, enda kontrolli all olevad LANid sageli ebaturvalise avaliku transportimisvõrgu abil. Eriti hoolikalt tuleb sellise kasutusvaldkonna puhul turvaliseks muuta kõnealune transportimiskanal. Lisaks tuleb asukohtade võrkusid ja klientsüsteeme kaitsta internetist tulevate rünnakute eest, rakendades selleks turvalüüse.
- Klientide ja partnerite ühendamine: Sageli on tarvis kliente või koostööpartnereid ühendada asutuse sisevõrguga. Teatud asutusesisest infot tuleb hoida selliselt, et vastavale infole pääseks ligi ka ainult piiratud usaldusväärsusega võrgust, st „väljast“. Usaldusväärsest võrgust, st „seest“, on tarvis saata päringuid välistesse andmebaasidesse, nt kaupade valimiseks ja tellimiseks. Sisesüsteemidel viiakse asutuseväliste firmade poolt läbi tarkvaraarendusi. Kuna kliendi või koostööpartneri IT-süsteemid pole asutuse kontrolli all, tuleb tagada, et juurdepääs oleks võimaldatud ainult ühiskasutusse antud ressurssidele. Näiteks võib kõiki IT-süsteeme, mida kliendid või koos-

tööpartnerid kasutada tohivad, käitada eraldi võrgus, mis on asutuse LANist eraldatud turvalüüsiga (vt B 3.301 Turvalüüs (tulemüür)).

- Kaughooldus: Kaughoolduse teostamiseks läheb sisesüsteemide puhul tarvis privilegeeritud administraator-pääsuõigusi. Sisesüsteemide kaughooldust (hooldust, tugiteenust ja käitamist) saavad osutada nii asutusesisesed kui ka asutusevälised töötajad. Mõlemal juhul kehtivad kõrged nõuded eemalasuva kasutaja autentimisele, andmevoo kontrollile ja ühenduse käideldavusele. Asutuseväliste töötajate palkamisel IT-süsteemide hooldamiseks tuleb arvestada soovitustega moodulist B 1.11 Väljasttellimine (Outsourcing) .

VPNe kasutatakse sageli ka selleks, et kaitsta üksikute protokollide ja rakenduste kommunikatsiooni. Näiteks kui olemasolevad traadita kohtvõrgu komponendid ei toeta turvalist krüpteerimist, saab kogu traadita kohtvõrgu kommunikatsiooni edastada krüpteeritult, kasutades traadita kohtvõrgust sõltumatut virtuaalset privaatvõrku. Samuti saab VPN-tunnelis siduda ja krüpteerida VoIP-ühenduse signaliseerimist ja meediatransporti.

VPN-lõpp-punktid

VPN-lõpp-punktide puhul eristatakse peamiselt VPN-serverit ja VPN-klienti. See lõpp-punkt, millega luuaks ühendus, toimib VPN-serverina. Ühendust algatavat lõpp-punkti nimetatakse VPN-kliendiks. VPN-lõpp-punkte saab luu nii tarkvara kui ka riistvara toel. Väljaspool asutust töötavate isikute puhul koosneb VPN-klient tavaliselt mobiilses IT-süsteemil asuvast tarkvararakendusest. Selline VPN-klient on sageli väga tugevalt seotud paigaldatud operatsioonisüsteemiga. Seega tuleks vältida mitme erineva VPN-kliendi paralleelset installeerimist ühele lõppseadmele. Üksikute VPN-lõpp-punktide omavaheline ühendamine peab toimuma vastavalt vajaduste analüüsi tulemustele (M 2.415 VPN vajaduste analüüs). VPN-lõpp-punktides tuleb vastavalt meetmes M 4.321 VPNi turvaline käitamine kirjeldatule tagada turvaline autentimine, et VPNi kaudu saaksid ennast sisse valida ainult volitatud kasutajad. Seejuures on sõltuvalt kasutusalast võimalik rakendada ka autentimisserverit, näiteks RADIUS-serverit.

Asukohtadevaheliste kommunikatsioonisuhete valimine

Kui on plaanis koondada mitu asukohta üheks LANiks, on oluline, milliste asukohtade vahel luuakse VPN-ühendus. Järgnevad topoloogiad või nende kombinatsioonid sobivad mitme asukoha võrkuühendamiseks:

- Tähtstruktuuriga võrk - Tähtvõrgu puhul valitakse välja mõni tsentraalne punkt (nt ettevõtte keskus), millega kõik teised hajali asukohad loovad iseseisva VPN-ühenduse. Info edastamiseks ühest hajaasukohast teise, peab info alati läbima ka keskuse. Tsentraalse asukoha avarii põhjustab seega kogu võrgustruktuuri katkemise. Probleemiks võivad olla ka pikemad ülekandeajad, eriti kui side leiab aset geograafiliselt lähestikku asuvate asukohtade vahel, kuid infot sunnitakse sellele vaatamata liikuma läbi vastava keskuse.
- Ringstruktuuriga võrk - Ringvõrgu puhul on iga asukoht ühendatud veel kahe teise asukohaga. Info, mis tuleb saata asukohta, millega puudub otseühendus, edastatakse adressaadile vahepeale jäävate asukohtade poolt.

Kui avarii esineb ainult ühes asukohas, saavad allesjäänud asukohad info siiski edasi toimetada. Kui avarii esineb rohkem kui kahes asukohas, on ohustatud kogu VPN-koosluse käideldavus.

- Puustruktuuriga võrk - Asukohtade erinevad VPN-lõpp-punktid on omavahel hierarhilises suhtes. Tsentraalne asukoht määratakse puustruktuuri „juureks“. Selle külge on ühendatud omakorda üks või mitu edasist VPN-ühendusega varustatud asukohta, mis on omakorda ühendatud edasiste asukohtadega. Täiendavaid asukohtasid saab puustruktuuriga võrku lisada probleemideta. Ükskõik millise tsentraalse süsteemi väljalangemise korral ei saa süsteemiga ühendatud VPN-segmendid enam VPN-koosluses suhelda.
- Täisseotisega võrk - Iga asukoht on ühendatud kõikide teiste asukohtadega eraldiseisva ühenduse kaudu. Kui mõni sidekanal katkeb, jätkub kommunikatsioon mõne teise allesoleva sidekanali kaudu. Otseühendus võimaldab vähendada ülekandele kuluvat aega. Nimetatud eelistele on vastukaaluks vastava topoloogia loomise suured kulud.

Nendest topoloogiatest või nende topoloogiate kombinatsioonidest tuleb valida enda jaoks sobiv. Saavutamaks kompromissi töökindluse ja kulude vahel, on praktikas kasulik rakendada topoloogiat, milles on mitu tsentraalset võrgujuurdepääsu, mille külge ühendatakse üksikud asukohad.

VPNi tüübid

VPNe saab kasutada, et koondada loogiliselt kaugelasetsevaid füüsilisi võrkusid üheks loogiliseks võrguks või selleks, et ühendada ebaturvalises võrgus asuvaid üksikuid lõppseadmeid turvalise kanali kaudu tsentraalse LANiga. Sõltuvalt sellest, millised süsteemid on VPN-ühenduse lõpp-punktideks, eristatakse Site-to-Site -, End-to-End - ja End-to-Site -VPNe.

- Site-to-Site -VPN - Site-to-Site -VPNidega ühendatakse võrkusid, et käitada või kasutada ühiseid rakendusi. Selleks on tarvis võrkudeüleseid juurdepääse. Transportimiskanalit turvatakse ühendatud võrkudes VPN-lüüsidega. Tüüpiline kasutusala LANide vaheliste ühenduste loomisel on institutsiooni harude või filiaalide ühendamine asutusesisese võrguga.
- End-to-End -VPN - End-to-End -VPNe kasutatakse tavaliselt üksikute rakenduste kasutamiseks. Ühendusi saab piirata konkreetsete süsteemide ja teenuste jaoks. End-to-End -VPNide tüüpilised kasutusalad on eriotstarbeliste, administraatori tasandi juurdepääsu nõudvate süsteemide kaughooldus; juurdepääsu võimaldamine üksikutele rakendustele või andmebaasidele. Selleks pole administraatori või süsteemi tasandi volitusi sageli üldse tarvis, juurdepääsu võimaldamine terminaliserverite kaudu. Kaugjuurdepääs eemalasuvale süsteemile võimaldab kasutada mitmeid sinna installeeritud rakendusi. Tavaliselt ei ole terminaliserveris selleks vaja ei administraatori ega ka süsteemi tasandi volitusi; Äripartnerite või klientide integreerimine asutuse tsentraalse andmevõrgu osadesse.
- End-to-Site -VPN (Remote-Access -VPN) - End-to-Site -VPNe nimetatakse ka Remote-Access -VPNideks (RAS-VPN). Selliseid VPNe kasutatakse kliendi juurdepääsuks mitmele rakendusele, mis asuvad asutuse LANi erinevates IT-süsteemides. Selleks on vaja juurdepääsu tervele võrgule, seega turvavad transpordikanalit tavaliselt klientsüsteemi VPN-tarkvara ja LANis olev VPN-lüüs. Kaugtöötajad ja mobiilsed kasutajad integreeritakse LANi alla tavaliselt End-to-Site -VPNidega.

VPNi variandid

Mõistet VPN kasutatakse sageli krüpteeritud ühenduste sünonüümina. VPNi variante nimetatakse sageli ka kasutatud VPN-protokolli järgi, näiteks TLS/SSL-VPN või IPSec-VPN. Transportimiskanali kaitsmiseks saab kasutada ka teisi meetodeid, näiteks rakendatava transportimisprotokolli erifunktsioone. Lisaks eristatakse veel kahte peamist VPNi varianti: Trusted -VPN ja Secure -VPN.

Trusted -VPN

VPNe nimetatakse Trusted -VPNideks, kui erinevate asukohtade vaheline VPN-ühendus tagatakse läbi usaldusväärsete väliste VPN-teenusepakkujate. Seejuures edastatakse usaldusväärsest võrgust pärinevad andmed tavaliselt krüpteerimata kujul eraldiseisva kommunikatsioonikanali kaudu teenusepakkuja lüüs-marsruuterisse. VPN moodustatakse VPN-andmevahetuse loogilise varjamisega ülejäänud andmevahetusest (nt Multiprotocol Label Switching u, MPLSi abil). Mobiilsete kasutajate jaoks pakuvad teenusepakkujad lisaks virtuaalseid privaatvõrke lüüs-marsruuteri kaudu, millele pääseb ligi ainult eriliste sissevalimissõlmede kaudu, mis on kaitstud volitamata ligipääsu eest. Kui Trusted -VPNiga varustamine usaldatakse välise teenusepakkuja kätte, tuleb lisaks arvestada mooduliga B 1.11 Väljasttellimine (Outsourcing) .Trusted -VPNid ei sobi konfidentsiaalsete andmete jaoks ilma täiendava, kasutuskihis toimuva krüpteerimiseta, kuna selliste ühenduste turvalisus on eranditult VPN-teenusepakkuja kätes. Seega ei paku Trusted -VPN kaitset teenusepakkuja enda siseringist pärit kuritarvitaja vastu. Konfidentsiaalse andmeside jaoks on seega soovitatav kasutada Secure -VPNi.

Secure -VPN

Konfidentsiaalsuse sõltuvust kolmandatest osapooltest saab vältida, kui sidet kaitstakse ühenduse lõpp-punktides krüpteerimisega, mis jääb VPNi kasutaja enda vastutusalasse. Seda lahendust nimetatakse ka Secure -VPNiks.

Eraldiseisvad Carrier -liinid

Kui VPNi teostamiseks kasutatakse eraldiseisvaid Carrier -liine, on tegu Trusted-VPNi erivormiga. Ka sel puhul tuleb konfidentsiaalseid andmeid kaitsta enne ülekandmist krüpteerimisega, mis jääb VPNi kasutaja enda vastutusalasse. Krüpteerimine võib toimuda transportimistasandil VPN-lõpp-punktides (Secure -VPN) või kasutajakihis.

VPN-seadmed

Tuleb otsustada, kas valitav VPN-toode peaks olema eraldiseisev VPN-seade, kombineeritud seade või tarkvarapõhine VPN-lahendus, mis töötab standardsetel IT-süsteemidel (näiteks Linuxil töötav IPSec):

- Eraldiseisvad VPN-lüüsid (Appliances): Need VPN-tooted on eranditult mõeldud VPN-ühenduste loomiseks ja ei paku täiendavaid funktsioone nagu nt sisu filtreerimist rakenduse tasandil. Eraldiseisvate VPN-lüüside eeliseks on, et need on optimeeritud VPN-kasutuseks ja nende turvaline konfigureerimine on lihtsustatud, kuna operatsioonisüsteem on juba karastatud.
- Kombineeritud seadmed: Integreeritud VPN-seadmed võivad olla näiteks marsruuterid ja teised turvalüüside komponendid (nt Application Level Gateway d, ALGd), mis on varustatud VPN-funktsioonidega või mida saab vastavalt täiendada. Kombineeritud seadmetel on lisaks finantsaspektidele sageli ka veel see eelis, et erinevaid funktsioone saab administreerida koos ühest kohast. Erinevate funktsioonide koondamine ühte seadmesse võib aga vähendada jõudlust. Intensiivse VPN-kasutuse puhul tuleb seega kontrollida, kas käideldavuse või jõudluse tagamiseks poleks parem eelis-

tada iseseisvaid VPN-komponente. Osadel kombineeritud seadmetel saab jõudluse suurendamiseks lisada spetsiaalseid riistvaral toimivaid krüpteerimismooduleid.

- Standardsetel IT-süsteemidel põhinevad VPNid: VPN-seadmeid saab tasuta või tasuliste tarkvarakomponentidega ka ise koostada. Neid komponente saab sageli paigaldada ka enamlevinud, standardsete operatsioonisüsteemidega varustatud riistvarale. Isekoostatud VPN-seadmed on paindlikumad ja neid saab edukalt kasutada mitmes erinevas kasutusolukorras.Vajalike komponentide paigaldamise ja integreerimise käigus võib siiski tekkida ka palju vigu. Seega võivad ise kokkupandud VPN-seadme kasutamisega kaasneda turvariskid. Täiendavaks puuduseks on asjaolu, et VPN-seadme erinevate komponentide (nt riistvara, operatsioonisüsteemi, VPN-tarkvara) tõttu tuleb abivajaduse puhul pöörduda erinevate kontaktisikute poole.

Järgnevasse tabelisse on koondatud erinevate koostevormide eelised ja puudused. (x) tähistab nõutud kriteeriumi täitmist, (-) tähistab kriteeriumi mittetäitmist.

Omadus	Eraldiseis-vad VPN-lüüsid	Kombinee-ritud seadmed	Standardsetel IT-süsteemidel põhinevad VPNid
VPN-komponentide (iseseisev) kaitse	-	x	-
Suur jõudlus	x	-	x
Madalad soetuskulud	-	-	x
Kasutuselevõtuks kulub vähe aega ja vaeva	x	x	-
Lihtne administreerida	x	x	-
Kergesti täiendatav	-	-	x
Know-How -jaotus	x	x	-
Tugiteenus saadav ühest allikast	x	x	-

Tabel 1: VPN-koostevormide võrdlus

Käesoleva tabeli sissekanded põhinevad praktikast tuletatud kogemustel ning nende vastavust tegelike tooteomadustega tuleb hinnata iga olukorra puhul eraldi.

M 3.66w Turvapaikade ja muudatuste halduse põhimõisted

Algatamise eest vastutavad: IT turvaspetsialist, IT-juht, muudatuste haldur

Rakendamise eest vastutavad: muudatuste haldur

Paikade ja muudatuste haldamise protsessi raames leiab tootmiskeskkonnas aset erinevate uuenduste ja täienduste ettevalmistamine, juhtimine ja haldamine. Selles valdkonnas on kasutusse võetud mitmeid asjakohaseid mõisteid. Protsessi teostuse eest vastutavad isikud peavad neid tundma. Versiooninimetuste tähistamiseks kasutatakse sageli väga erinevaid mõisteid. See tuleneb asjaolust, et mõistete definitsioonide kohta ei ole olemas ühtset, kohustuslikku ja kõikehõlmavat standardit. Loodavad tooted, näiteks riist- või tarkvara, läbivad erinevaid arengustaadiumeid. Ebatäpsete mõistete tõttu on soovitatav kasutada asutusesisest sõnastikku, et erialased mõisted oleksid kõigi jaoks ühtmoodi arusaadavad. Toote esimest töövõimelist versiooni nimetatakse tihti alfaversiooniks. Alfaversioon on sageli mõeldud asutusesiseseks kasutamiseks, et demonstreerida tarkvaraprojekti ellurakendamise võimalikkust. Üldjuhul on sellel olemas juba ka kõik olulisemad põhifunktsioonid. Beetaversioon on veel lõpetamata tooteversioon, mille arendaja avaldab eesmärgiga seda testida ja selle eelmüüki soodustada. Tootel on olulised funktsioon juba olemas, kuid nende põhjalik testimine pole veel lõpetatud. Beetaversioone jaotatakse nn beetatestijatele, kes kontrollivad toote funktsioone ja kasutuskõlblikkust ning teavitavad arendajaid vajaduse korral võimalikest vigadest. Tarkvaratoodete puhul leitakse selle meetodi abil tavaliselt mitmeid programmeerimisvigu. Lõpetamisjärgus olevat testversiooni tähistab tarkvaraarenduses mõiste kandidaatversioon (release candidate version, RC), mis sisaldab juba kõiki tarkvara lõppversiooni funktsioone. See versioon on mõeldud viimaseks süsteemi- või tootetestiks. Edaspidi avaldatakse RCsid ainult tõsiste kvaliteediprobleemide tuvastamisel.

Tarkvara lõpetatud ja avaldatud versiooni nimetatakse kandidaat- või stabiilseks versiooniks ning see märgistatakse tavaliselt versiooninumbriga. Kuna sel hetkel algab ka andmekandjate (CDde või DVDde) tootmine, kasutatakse siinkohal ka mõistet tootmiseks valmis (ready to manufacturing, RTM). Paljud tarkvaraarendajad on avaldanud mehhanisme tarkvarakorrektuuride haldamiseks. Siinkohal tuleb arvestada, et alljärgnevaid mõisteid ei kasutata sugugi alati järjepidevalt ühtemoodi. Siiski annavad nad üldjoontes vajaliku ülevaate valdkonda puudutavatest mõistetest. Tarkvarakorrektuure avalikustatakse eesmärgiga kõrvaldada vigu juba avaldatud tarkvaras. Paik (patch) on üldine tarkvaravärskendus (softwareupdate), mis kõrvaldab tarkvara vigased funktsioonid. Esmalt ei ole selline värskendus (update) ei kriitiline ega ka turvalisuse seisukohalt oluline. Kui täiend on tarkvara turvalisuse seisukohast oluline ja sulgeb turvaaugu, nimetatakse seda sageli turvapaigaks (security patch). Turvapaigale määratakse sageli olulisuse aste. See tähistab üldjuhul seda, kui tõsiseks peab tootja turvaauku, mida vastav turvapaik parandab. Kui täiendusega korrigeeritakse tarkvara olulist funktsiooni, mis ei ole ilmtingimata turvalisusega seotud, näiteks valet arvutust, siis nimetatakse seda kriitiliseks värskenduseks (critical update). Muud tootjapoolset väljundit, mis puudutab ainult konkreetseid kliendisituatsioone ja on sageli saadaval ainult kehtiva tugilepingu korral, või mis koostatakse alles tugipäringute alusel, nimetatakse kiirparanduseks (hotfix). Kiirparandus võib olla ühe või mitme failiga pakett, mis

kõrvaldab mõne tootes esineva probleemi. Hooldepaki (servicepack) puhul on tegu kogumiga kiirparandustest, kriitilistest värskendustest ja täiendustest, mis on avaldatud ja üldsusele kättesaadavaks tehtud alates toote turulejõudmisest. Hooldepakkide avaldamiseni kuluv aeg on tavaliselt väga pikk. Vahepeal avalikustatud tarkvarakorrektuuride hulgaga varustamiseks on mõnikord mõistlik kasutada kokkuvõtteid. Seepärast avaldavad osad tootjad vahepeal nn värskenduste vahepakke (update roll-ups). Täiendite vahepakid on kogumikud turvapaikadest, kriitilistest värskendustest, värskendustest ja kiirparandustest, mida pakutakse kuhjuvalt või mõne konkreetse tootekomponendi jaoks, näiteks veebiserverile. Pärast hooldepakkide avaldamist juhtub sageli, et hetkel saadaoleva tooteseeria numbrit tõstetakse komakoha juures ühe numbri võrra. See dokumenteerib, et tarkvaratootel on olemas kõik selle hetkeni saadaolevad korrektuurid. Mõned tootjad nimetavad seda ka integreeritud hooldepakiks (integrated servicepack). Kuna kliendid esitavad tootjale erinevaid nõudmisi, on tootjad sageli sunnitud tootesse integreerima uusi valikuid (features), mis täiendavad toote funktsioone. Neid funktsiooniuuendusi pakutakse tavaliselt funktsioonipakina (featurepack) kõikidele klientidele, kellel on olemas kehtiv leping tootjaga (tugileping, täiendite leping, tarkvarahoolduse leping vms). Uued valikud (features) muutuvad tavaliselt järgmise tooteversiooni koostisosaks.

Praktikas on tavaks kahte liiki IT-komponentide muudatused. Standardiseeritud muudatused ja muudatused, mis peavad läbima paikade ja muudatuste haldamise protsessi. Standardsed muudatused on rakenduste ja IT-süsteemide muudatused, mille jaoks on olemas täpsed protseduurijuhised ning mille on muudatuste haldur juba eelnevalt heaks kiitnud. Kirjeldatud protseduurijuhis peab tagama, et nimetatud muudatustega ei kaasne riske. Selle muudatuse võib sisse viia ka ilma täiendavalt muudatuste halduri poole pöördumata. See vähendab oluliselt protsessiga seotud isikute töökoormust.

Üks riist- või tarkvaramuudatuste põhjuseid on tõrked. Tõrge (incident) on IT-teenuse (service) kõrvalekalle tavapärasest tööst, mis kujutab endast teenuse kvaliteedi reaalset või potentsiaalset vähenemist või lausa teenuse katkemist. Kui tõrke põhjus pole nähtav, on tegu probleemiga, mis vajab lähemat uurimist. Mõistega probleem tähistatakse ITILis ühte või mitut samalaadset viga, mille põhjus pole teada. Kui põhjus tuvastatakse ja leitakse probleemi kõrvaldamise või sellest möödaminemise võimalus, muutub probleem tuntud veaks (known error). Lahendustee dokumenteeritakse muudatustaotluse (request for change, RfC) all ja viiakse ellu muudatuste halduri (change management) kontrolli all. Lisaks paikade ja muudatuste haldusega seotud mõistetekogumile (näiteks ITILile) peavad paikade ja muudatuste haldusega tegelevad isikud tundma ka infoturbega seotud mõisteid.

M 3.67 Töötajate koolitamine andmete kustutamise või hävitamise alal

Algatamise eest vastutavad: infoturbe spetsialist

Rakendamise eest vastutavad: infoturbe eest vastutav töötaja, juht

Töötajaid tuleb informeerida, milliste meetodite ja seadmete abil võib toimuda asutuses kasutatavate erinevate andmekandjate kustutamine või hävitamine ning millistele aspektidele tuleb seejuures tähelepanu pöörata. Selleks tuleb lisaks eeskirjadele avaldada regulaarselt nõuandeid intranetis. Ka printerite, koopiamasinate ja dokumendipurustite kõrvale üles riputatud informatsioonil on toetav funktsioon. Asutustes tuleb regulaarselt rakendada töötajate teadlikkust tõstvaid meetmeid (vt M 2.432z Eeskirjad informatsiooni kustutamiseks ja hävitamiseks). Eriti juhul, kui on toimunud muutused andmekandjate kustutamiseks või hävitamiseks kasutatavates meetodites, tuleb töötajaid sellest informeerida. Tähtis on anda teavet ka esinevate tüüpiliste vigade kohta. Nende hulka kuuluvad näiteks järgmised väärarusaamad:

Paberikorv büroos – tihti ei hävitata dokumente nende kaitsevajaduse kohaselt, vaid visatakse tavalisse paberikorvi. Sellele järgneval vanapaberi käitlemisel võivad volitamata isikud kõige lihtsamal viisil pääseda ligi konfidentsiaalsele informatsioonile (G 2.48 Andmekandjate ja dokumentide puudulik hävitamine). Nimetatud probleemi põhjuseks on, et töötajad ei tunne või ei järgi asutusesiseseid reegleid dokumentide hävitamiseks.

Operatsioonisüsteemi prügikast – tänapäevased operatsioonisüsteemid pakuvad kasutajatele kustutamisele minevate failide jaoks niinimetatud „prügikasti". See sarnaneb mitte ainult nime, vaid ka graafilise kujunduse ja kasutamise poolest klassikalise prügikastiga. Failid on lihtsalt võimalik paigutada prügikasti. Nagu klassikalise prügikastigi puhul, ei ole need failid veel hävitatud, vaid neid lihtsalt hoitakse seal. Kui need on sattunud prügikasti tahtmatult, on neid lihtne täielikult taastada, kuna need saadeti ju prügikasti oma originaalsalvestuskohast (vt M 4.56 Turvaline kustutus Windows operatsioonisüsteemides). Prügikasti tühjendamisel ei kustutata andmeid, vaid ainult viide informatsioonile operatsioonisüsteemi „sisukorras". Seega saaks neid andmeid ikka veel taastada, kuni need pole järgnevate kirjutusprotseduuride käigus üle kirjutatud. Tagamaks, et teavet ei saa taastada, tuleb see sihipäraselt üle kirjutada (vt M 2.167 Andmete kustutamiseks või hävitamiseks sobivate lahenduste valik).

Tekstikohtade mustaks tegemine – kolmandatele isikutele üleantavad dokumendid võivad üksikutes kohtades sisaldada informatsiooni, mida ei tohi levitada. See info tuleb enne dokumentide edasiandmist eemaldada. Põhiprobleemiks on kogu konfidentsiaalse teabe identifitseerimine, et seda oleks võimalik hoolikalt eemaldada. Ühelt poolt jäävad tundlikud andmed kergesti kahe silma vahele, teiselt poolt kasutatakse nende eemaldamiseks sobimatuid meetodeid. Paberdokumentidel tehakse tundlikku informatsiooni sisaldavad kohad tihti mustaga üle, et muuta need loetamatuks. See ei ole usaldusväärne meetod, kuna isegi

esialgse teksti koopiate puhul võivad ülevärvitud kohad olla tihti siiski loetavad. Ka elektroonilistel dokumentidel tehakse ikka ja jälle tekstiosad mustaks. See meetod on veelgi ebakindlam kui paberdokumentide puhul ning seetõttu tuleb selle kasutamisest loobuda (G 3.13 Väära või soovimatu andmekogumi saatmine). Selliselt muudetud dokumente ei tohi põhimõtteliselt edasi anda. Kui see on vältimatu, tuleb dokumendid pärast kriitilise informatsiooni eemaldamist uuesti klassifitseerida ja liigitada madalamasse turbeastmesse. Seejärel peavad need läbima uuesti ühiskasutusse andmise protseduurid. Selle vältimiseks peaksid dokumendid olema struktureeritud nii, et mitteavalikku teavet oleks võimalik eraldada, näiteks paigutada see lisasse.

Külastusalad – asutusesisestel aladel, mida saavad kasutada ka võõrad, tuleb eemaldada kogu materjal, mis võiks sisaldada tundlikku informatsiooni. Sellele tuleb erilist tähelepanu pöörata külastusaladel ja nõupidamisruumides, aga ka üldkasutatavates printimis- ja koopiaruumides. Koosolekuruumides tuleks pärast ürituse lõppemist kasutatud pabertahvli paber kaasa võtta ja tahvlid puhastada. Konfidentsiaalsete materjalide äraviskamiseks ei tohi sellistes ruumides kasutada paberikorve. Töötajad peaksid olema informeeritud, et see on nende, mitte koristajate või remonditööliste ülesanne.

Kontrollküsimused:

- Kas töötajad on teadlikud andmete kustutamiseks või hävitamiseks kasutatavatest meetoditest ja seadmetest?
- Kas tüüpilised vead on teada ja lahendusvõimalused läbi arutatud?

M 3.68 Samba-serveri administraatorite koolitus

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: infoturbespsetsialist

Samba-teenuste nõuetekohaseks haldamiseks tuleb vastutavatele administraatoritele korraldada koolitus. Väiksemadki konfiguratsioonivead võivad tekitada turvaauke. Võttes arvesse Unixi ja Windowsi failisüsteemide erinevusi, nõuab korrektne ligipääsupiirangute konfiguratsioon ja haldus häid teadmisi olemasolevatest võimalustest ja nende piiridest. Lähtuvalt tugevatest seostest samba turvamehhanismide ja aluseks oleva operatsioonisüsteemi vahel, peavad Sambaserveri administraatorid tundma ka operatsioonisüsteemi turvamehhanisme. See kehtib ka juhul, kui Samba-serveri administraatorid ei vastuta operatsioonisüsteemi halduse eest.

Peale üldise operatsioonisüsteemi turvalisuse peaks koolitus hõlmama ka järgmisi aspekte:

- Meetodid Samba teenuste installeerimiseks (installatsioon kasutatud distributsiooni pakihalduse kaudu, lähtekoodist kompileerimisel).
- Samba teenuse konfiguratsioonivõimalused, süntaks ja konfiguratsioonifailid.
- Samba teenuse kasutajate autentimise mehhanismid, kasutusalad, erinevate mehhanismide eelised ja puudused.
- Windowsi ja Unixi all kasutatavate failisüsteemide erinevus ja kuidas samba nende erinevustega toimib.
- Samba konfiguratsiooni ligipääsupiirangute ühilduvus ligipääsuõigustega failisüsteemi tasandil.
- Meetmed Samba-serveri kättesaadavuse kindlakstegemiseks.

Kontrollküsimused:

- Kas administraatorid tunnevad Samba-serveri turbeks olulisi aspekte, näiteks seda, et SMB protokoll ei toeta edastavate andmete krüpteerimist?
- Kas administraatorid on koolitatud käsitlemaks kasutatud operatsioonisüsteemi ja selle turbeks olulisi aspekte?
- Kas administraatorid teavad erinevaid Samba installeerimise ja konfigureerimise võimalusi?
- Kas administraatorid tunnevad Samba-serveri mehhanisme kasutaja autentimiseks?
- Kas administraator valdab protokolle, mida kasutatakse Active Directory domeenis ning kas nad tunnevad nende nõrku kohti?
- Kas administraatorid tunnevad Windowsi ja Unixi all kasutatavate failisüsteemide erinevusi ja kuidas Samba nende erinevustega toimib?
- Kas administraatorid mõistavad Samba konfiguratsiooni ligipääsuõiguste ja failisüsteemi tasandi ligipääsuõiguste kokkumängu?
- Kas administraatorid on tuttavad meetmetega Samba-serveri kättesaadavuse kindlustamiseks?

M 3.69w Sissejuhatus viirustest tulenevatesse ohtudesse

Algatamise eest vastutavad: infoturbespetsialist

Rakendamise eest vastutavad: infoturbespetsialist, spetsialist

Viirused on programmid, mis viivad arvutis ilma omaniku loa ja teadmiseta läbi kahjulikke toiminguid. Seejuures on viirused enamjaolt varjatud ja toimingud viiakse arvutis läbi salaja. Viirusi kasutatakse erinevate eesmärkide saavutamiseks, näiteks süsteemide kaugjuhtimiseks, paroolide tuvastamiseks, andmete kogumiseks, aga ka klaviatuurisisestuste salvestamiseks. Järgnevalt kasutatakse mõistet viirusetõrjeprogramm, selle all mõeldakse aga tarkvara viiruste avastamiseks arvutis.

Järgnevalt kirjeldatakse erinevaid viiruste liike. Need võivad sisaldada suurel hulgal kahjulikke tegureid, mida on rünnaku korral võimalik ka omavahel kombineerida.

Viirusi on järgmiste tunnuste abil võimalik jagada erinevatesse klassidesse:

Viirused

Viirus (ka arvutiviirus) ei ole iseseisev programmirutiin, see taastoodab ennast ise ja teostab süsteemis, teistes programmides või nende ümbruses kasutaja poolt kontrollimatuid manipulatsioone. Sellised programmi funktsiooni juhtimised võivad esineda nii tahtmatult kui ka tahtlikult. Suurimat kahju tekitab programmide ja andmete kadu või võltsimine. Taastootmise omadus sarnaneb bioloogilise prototüübiga ning sellest tuleneb ka nimetus „viirus“. Mõjutamise võimalused on väga mitmekesised. Eriti sagedane on andmete ülekirjutamine või viiruse koodi paigaldamine teistesse programmidesse ja operatsioonisüsteemi aladesse. Põhimõtteliselt esineb viirusi kõigis operatsioonisüsteemides. Tänu laiale levikule on enim ohustatud x86 arhitektuuriga personaalarvutid (PC). Eristatakse veel teisigi viiruste põhivorme, kusjuures need võivad esineda nii sega- kui ka erivormidena.

Buudiviirused

Buudiviirused paiknevad andmekandja, näiteks kõvaketta, buutsektoris või peabuutsektoris. Buutimisel teostatakse teiste hulgas programme, mis on küll iseseisvad, aga paiknevad andmekandja kataloogi nähtamatus ja ligipääsmatus sektoris. Buudiviirused kirjutavad need oma programmiga üle. Originaalsisu teisaldatakse andmekandjal mõnda teise kohta. Buudiviirus käivitub enne kui operatsioonisüsteem on täielikult laetud.

Failiviirused

Enamik andmeviirusi (failiviirusi) paiknevad täitmisprogrammides. Nakatunud programmi avamisel failiviirus käivitub ja levib. Järgnevalt avaneb ka täitmisprogramm ja kasutajale jääb mulje, nagu käivituks programm täiesti tavapäraselt. Teatakse ka algelisemaid viirusi, mis paiknevad programmi alguses ja seetõttu ei saa programm enam veatult töötada. Failiviirused võivad sisaldada erinevaid kahjulikke funktsioone, näiteks võivad nad faile kustutada või kõvaketta formaatida. Selle asemel, et mõne teise failiga ühineda, kopeerivad paljud failiviirused ennast operatsioonisüsteemi iseseisva failina. Manipuleerides operatsioonisüsteemi seadistusi (näiteks autostart sissekannete kaudu), kindlustavad failiviirused oma edasise käituse.

Makroviirused

Programmid võivad sisaldada ka makroviirusi. Makroviirused ei nakata rakendusprogrammi, vaid sellega loodud faile. See hõlmab ka kõiki rakendusprogramme, mille puhul ei saa loodud faili paigutada mitte ainult juhtmärke, vaid ka programme (näiteks Microsoft Office, StarOffice/OpenOffice). Mõned failivormingud võivad sisaldada objekte, mis omakorda võivad sisaldada programme. Selline sahtlisüsteem hõlbustab samuti viiruste pääsemist failidesse. Makrod on programmid, mille abiga on rakendusprogrammi võimalik laiendada lisafunktsioonidega, mis on loodud konkreetse kasutusjuhtumi tarvis (näiteks tekstivisandist puhtandi moodustamine). Makroviirused käivitatakse failidega töötamisel. Sageli levivad makroviirused e-kirja, interneti, aga ka CD ja USB pulga kaudu.

Skriptiviirused

Skript on tekitaja poolt teostatud programm. Tihtipeale kasutatakse skripte veebiserveritel või paigutatakse veebilehtedele (näiteks JavaScript). Neid skripte teostatakse enamasti märkamatult ja teatud juhtudel võivad ründajad kasutada neid kahjurvara laadimiseks IT-süsteemi.

Bottviirused

Bottviirus on programm, mis installeeritakse salaja, näiteks mõne nakatunud veebilehe külastamisel. Bottviirus võib saata salaja e-kirju, nuhkida failides või suhelda võrgu kaudu teiste bottviirustega, et viia läbi hajus ummistusrünne (DDoS – distributed denial-of-service). Paljud bottviirused tegutsevad alguses nii, et kasutajad ei märka midagi kahtlast. Ründajad saavad teadlikult kindlaid bottviiruseid „aktiveerida“ sellega, et saadavad nakatunud arvutile käsklusi. Nimetus „bott” tuleneb mõistest „robot”.

Peitviirused (stealth virus)

Peitviirusi kutsutakse ka nähtamatuteks viirusteks. Peitviirused üritavad oma avastamist takistada näiteks sellega, et tuvastavad viirusetõrjeprogrammid ja nakatunud faili skannimisel eemaldavad koodi failist ning lisavad selle pärast skannimist uuesti failile.

Polümorfsed viirused

Polümorfsed viirused kuuluvad kõige ohtlikumate viiruste hulka. Nad muudavad iga uue nakatamise ajal krüpteerimise või permutatsiooniga oma kuju ja on seetõttu viirusetõrjeprogrammidele raskesti leitavad. Üldjuhul krüpteerivad polümorfsed viirused oma viiruskoodi iga nakatumise ajal uuesti. Enamasti luuakse iga nakatumise ajal ka uus krüpteerimisvõti ja võtmegenereerimisprotseduur paigutatakse ka ise viiruse krüpteeritud koodi.

Retroviirused

Retroviirus kaitseb end viirusetõrjeprogrammi või tulemüüri avastamise vastu sellega, et üritab neid desaktiveerida või nendega manipuleerida. Desaktiveerimise tõttu võib hiljem süsteemi pääseda ka teistsugune kahjurvara.

Ussviirused

Ussviirused on süsteemis (eelkõige võrgus) levivad iseseisvad ja ise paljunevad programmid. Võrreldes viirustega ei vaja ussviirused hosti ehk „peremeest“.

Reeglina aeglustavad ussviirused arvutusaega või andmeside kvaliteeti. Seetõttu suudavad nad lühikese ajaga mõjutada paljusid arvuteid ja põhjustavad suurt majanduslikku või rahalist kahju.

Trooja hobused

Trooja hobune (nimetatakse lühendatult ka troojalaseks) on kahjustava toimega programm, mis on paigutatud teise programmi sisse. Trooja hobuseid levitatakse nii, et need integreeritakse võimalikult „atraktiivsetesse" programmidesse, mida pakutakse allalaadimiseks või lisatakse nad e-kirjale manusena. Trooja hobused ei pruugi põhjustada ainult otsest kahju, vaid võivad koguda ka informatsiooni üksikute arvutite ja lokaalse võrgu kohta.

Juurkratt (rootkit)

Unixi all tähendab root administraatorit, kellel on laialdased ligipääsuõigused. Rootkit ehk juurkratt on tööriistade kogum, mida kasutatakse kasutaja teadmata võimalikult laialdase ligipääsu saamiseks süsteemile. Kuigi mõiste rootkit on tekkinud Unixi maailmas, on tänapäeval olemas suur hulk Windowsi juurkratte. Nad muudavad näiteks süsteemifaile või võimaldavad ründajal saavutada kontrolli nakatunud süsteemi üle. Pärast seda võib ründaja nakatunud süsteemi kaudu saata edasi näiteks kahjurvara.

Tagauks (backdoor)

Backdoor on „tagauks", mis võimaldab ründajale ligipääsu arvutile või programmide funktsioonidele. Tagauks võib olla installeeritud kas operatsioonisüsteemi või rakendusprogrammi. Enamasti kasutatakse tagaust selleks, et viia arvutisse veel kahjurvara, näiteks Trooja hobune.

Nuhkvara

Nuhkvaraks nimetatakse programme, mis koguvad salaja ja ilma sellest teatamata informatsiooni kasutaja või arvuti kasutuse kohta ning saadavad selle informatsiooni hiljem edasi volitamata isikutele. Nuhkvara on tüütu, aga mitte nii ohtlik kui viirused, ussid ja Trooja hobused. Nuhkvara võib endast siiski kujutada turbeprobleemi, mis kajastub näiteks isikuandmete salajases edastamises, aga ka sellega seotud volitamata sisenemises IT-süsteemi. Teiste hulgas on võimalik muuta süsteemikonfiguratsiooni, näiteks Windows Registry, või on võimalik paigaldada käsukood, näiteks DLL, ActiveX Object / Java Object. Nuhkvara pääseb süsteemi paljudel juhtudel internetist volitamata allalaaditud tarkvara, uuenduste või teiste failide (muusika või kaheldavatest allikatest pärinevad dokumendid) kaudu. Nuhkvara võib sisaldada nn klahvinuhi (keylogger) programmi klaviatuurisisestuste salvestamiseks. Kõik klaviatuurisisestused salvestatakse ja saadetakse võimalikult märkamatult ründajale. Ründaja sorteerib välja tema jaoks olulise informatsiooni, näiteks registreerimisalase informatsiooni või krediitkaardinumbrid.

Valija (dialer)

Tasuliste internetiteenuste eest tasuti vanasti telefoniarve kaudu nii, et kasutajad suunati spetsiaalsete sissehelistamise programmidega tasulistele telefoninumbritele. Selleks kasutatud Dialer oli programm, mis lõi arvutile uue internetiühenduse. Pärast allalaadimist ja installeerimist ühendab Dialer end internetiga. Tavaliselt katkestatakse selleks ajaks olemasolev internetiühendus. (See toimib aga ainult tavalise telefoniühenduse korral, mitte aga DSL-i või teiste sarnaste

süsteemide puhul.) Pärast seda on uue ühenduse kaudu võimalik esitada päring tasulisele sisule. Tekkivate kulude suurus oleneb dialer'i valitud numbrist. DSL-i laia levikuga on Dialer paljuski oma tähenduse minetanud.

Hirmvara (scareware)

Scareware koosneb inglisekeelsest sõnast scare (hirm) ja software (tarkvara). Hirmvara esmane eesmärk on kasutajate ebakindlaks muutmine ja hirmutamine. Kasutajale kuvatakse veebilehe külastamisel teade, et tema arvuti on nakatunud viirusega. Samal ajal pakutakse talle viiruse eemaldamiseks tasuta viirusetõrjeprogrammi. See programm sisaldab aga tegelikku viirust. Või pakutakse kasutajale väidetava viiruse tõrjeks tasulist, kuid enamasti täiesti kasutut tarkvara.

Tähelepanu tuleb juhtida sellele, et ülal väljatoodud viiruste tunnused on ainult näited enimlevinud viirustest. Iga juhtum on erinev ja sellest tulenevalt võib viirusel olla ka teisi lisafunktsioone. Viimastel aastatel on uue kahjurvara üha keerukama leviku tõttu raske tõmmata kindlat piiri viiruste, usside ja Trooja hobuste vahele. Rünnaku korral kasutatakse tavaliselt erineva ülesehitusega programme kas üksteise järel või koos. Viirusetõrjeprogrammide tootjad kasutavad seetõttu sageli üldistavat mõistet kahjurvara (malicious software ehk malware).

M 3.70w Sissejuhatus virtualiseerimisse

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: IT-juht, administraator

Niinimetatud IT-süsteemide virtualiseerimisega saame oma käsutusse tehnoloogia ühe või mitme virtuaalse IT-süsteemi ühel füüsilisel arvutil käitamiseks. Ühte sellist füüsilist arvutit nimetatakse virtualiseerimisserveriks. Seda tehnoloogiat kasutati juba 1970. aastatel suurarvutitel (näiteks IBM zSeries), kuid keskmise suurusega serverite puhul on see laialdasemat kasutust leidnud alles 1990. aastate lõpust alates. IT-süsteemide virtualiseerimiseks mõeldud x86-arhitektuuriga tarkvaratoodete näideteks on Microsoft Virtual PC/Server, Parallels Virtuozzo, Sun VirtualBox, VMware Workstation/Server/ESX ja Xen, samuti SUN Solaris Zones, mis on saadaval SPARC- ja INTEL-platvormide jaoks. SUN-serveri ettevõtete seeria puhul on võimalik ka riistvaralise toega virtualiseerimine (siin nimetatakse seda partitsioneerimiseks) nn domeenide kaudu kasutamisega. zSeries-suurarvutite vallas saab virtualiseerimine toimuda näiteks loogiliste partitsioonide (LPAR, riistvaralise toega virtualiseerimine) või toote z/VM (tarkvaralise toega) abil (vt B 3.107 Suurarvutid S/390 ja zSeries).

Virtualiseerimistehnoloogia on väga kiiresti leidnud kasutust serverisüsteemide parema ärakasutamise ja konsolideerimise strateegilise vahendina, kuna ta võimaldab kontsentreerida paljud teenused ühele füüsilisele serverisüsteemile, ilma et tuleks loobuda teenuste üksikutele IT-süsteemidele jaotamisest. Nii kasutatakse füüsilise serveri ressursse paremini ja serveri töö saab muuta märkimisväärselt säästlikumaks mitte ainult kasutatavate füüsiliste IT-süsteemide vähenemise, vaid ka elektrikulude, serveriruumide ja arvutuskeskuste ning kliimaseadmete osas. Peale selle on virtualiseerimise abil võimalik kiirendada uute serverite kasutuselevõttu, näiteks seetõttu, et iga uue serverisüsteemi puhul ei ole tarvis hanget korraldada. Mõnede virtualiseerimislahenduste puhul saab virtuaalseid IT-süsteeme kopeerida (mis aitab virtualiseerimislahendusi lihtsustada) või luua nn virtuaalsete IT-süsteemide snapshot 'e, mille abil saab vigase konfiguratsioonimuutuse puhul kiiresti algseisundi taastada.

Peale selle saab mitu virtualiseerimisserverit ühendada üheks nn virtuaalseks taristuks. Sellise virtuaalse infosüsteemi puhul hallatakse mitut virtualiseerimisserverit ühiselt koos neil jooksvate virtuaalsete IT-süsteemidega, mis võimaldab kasutada lisafunktsioone. Näiteks saab virtuaalseid IT-süsteeme ühelt virtualiseerimisserverilt teisele liigutada. See on osaliselt võimalik ka siis, kui kasutatakse virtuaalset IT-süsteemi (Live Migration). Peale selle avanevad võimalused suurendada virtuaalsete IT-süsteemide käideldavust. Nii saab Live Migration 'i abil virtuaalse süsteemi viia alati virtuaalse süsteemi käitamiseks parajasti parimat jõudlust pakkuvale virtualiseerimisserverile. Veel üks võimalus on käivitada virtuaalsed IT-süsteemid automaatselt teisel virtualiseerimisserveril, kui algne virtualiseerimisserver on näiteks riistvararikke tõttu välja langenud.

Rikkalikud võimalused virtuaalsete IT-süsteemide manipuleerimiseks virtualiseerimistarkvara abil demonstreerivad virtualiseerimisserveri erilist sobivust test- ja arenduskeskkondade ülesehitamiseks. Virtualiseerimise abil on võimalik valmistada kiiresti IT-süsteeme testimise ja arenduse jaoks ning ehitada kiiresti ja tõhusalt üles keerukaid keskkondi. Peale selle saab tegelikke virtuaalseid IT-süsteeme test- ja arenduskeskkonna jaoks kopeerida, et testida uuendusi ja muudatusi ilma tegelikku tööd häirimata.

Eeldused virtuaalsete IT-süsteemide käitamiseks ühel virtualiseerimisserveril

Erinevate virtuaalsete IT-süsteemide ühel virtualiseerimisserveril korraga käitamiseks peab virtualiseerimistarkvara täitma teatud eeldused.

Virtualiseerimistarkvara peab hoolitsema selle eest, et:

- iga virtuaalne IT-süsteem kujutaks endast selles töötava tarkvara jaoks praktiliselt iseseisvat füüsilist arvutit (kapseldus),
- üksikud virtuaalsed IT-süsteemid oleksid üksteisest isoleeritud ja saaksid suhelda ainult kindlaksmääratud teid kaudu (isolatsioon),
- üksikud virtuaalsed IT-süsteemid pääseksid riistvararessurssidele juurde ettenähtud viisil.

Sõltuvalt sellest, kuidas ressursside virtualiseerimine on realiseeritud, võidakse neid virtualiseerimiskihi funktsioone täita ainult piiratult. Nii on näiteks lahendusi, mille puhul operatsioonisüsteemi tarkvara tuleb enne virtuaalsel IT-süsteemil käitamist veidi kohandada.

Teine näide virtualiseerimisepiirangute kohta on lahendused

Mille puhul kõik virtuaalsed IT-süsteemid peavad kasutama ühel virtualiseerimisserveril sama operatsioonisüsteemi erinevaid instantse. Virtualiseerimiskiht ei pea olema tingimata puhtas tarkvarakomponent. Mõningate platvormide puhul toetab ressursside virtualiseerimist ka riist- või püsivara. Virtualiseerimiskiht annab virtuaalsete IT-süsteemide käsutusse tavaliselt konfigureeritavaid juurdepääsuvõimalusi lokaalsetele seadmetele ja võrguühendustele. See võimaldab virtuaalsetel IT-süsteemidel omavahel ja võõraste IT-süsteemidega suhelda.

Praktikas eristatakse kaht liiki virtualiseerimistarkvara – serveri virtualiseerimist ja operatsioonisüsteemi virtualiseerimist.

Serveri virtualiseerimine

Serveri virtualiseerimine moodustab aluse virtualiseerimisserverist abstraheeritud, virtualiseeritud ja iseseisva riistvarakeskkonnaga virtuaalsetele IT-süsteemidele. Sellesse virtuaalsesse riistvarakeskkonda installeeritakse täielik operatsioonisüsteem, millel saab hakata rakendusi harjunud viisil käitama. Tavaliselt on see operatsioonisüsteem, mille saab virtuaalsele IT-süsteemile installeerida, täiesti sõltumatu operatsioonisüsteemist, mille all töötab virtualiseerimistarkvara.

Virtuaalse IT-süsteemi juurdepääsu virtualiseerimisserveri ressurssidele (protsessor, töömälu, massimälu, võrk) juhitakse virtualiseerimistarkvara kaudu. Selleks sisaldab iga virtuaalne IT-süsteem virtualiseerimisserveri sellele ressursile juurdepääsu võimaldavaid seadmeid. Need seadmed kas emuleeritakse täielikult või antakse füüsilised seadmed virtuaalse IT-süsteemi käsutusse virtualiseerimistarkvara abil. Igal juhul hoolitseb virtualiseerimistarkvara selle eest, et virtuaalsed IT-süsteemid kasutaks füüsilisi seadmeid ettenähtud viisil, nii et nad saaks üksteist võimalikult vähe mõjutada. Draiverid virtuaalsete IT-süsteemide virtualiseerimisserveri riistvarakomponentidele juurdepääsuks installeeritaks tavaliselt pärast operatsioonisüsteemi virtuaalses IT-süsteemis installeerimist.

Serveri virtualiseerimise puhul eristatakse nn hüperviisoripõhiseid (tüüp 1-) ja hostipõhiseid (tüüp 2-) virtualiseerimistooteid. Hüperviisoripõhiste virtualiseerimistoodete puhul installeeritakse füüsilisele riistvarale ainult üks virtualiseerimisele spetsialiseerunud põhioperatsioonisüsteem ehk nn hüperviisor, mis loob virtuaalsete IT-süsteemide tööks vajaliku keskkonna ja juhib virtuaalsete IT-süsteemide juurdepääsu füüsilistele ressurssidele. Hostipõhiste virtualiseerimistoodete puhul installeeritakse hüperviisor teenusena täielikult varustatud ja kasutusotstarbe jaoks optimeerimata operatsioonisüsteemis.

Operatsioonisüsteemi virtualiseerimine

Operatsioonisüsteemi virtualiseerimine erineb serveri virtualiseerimisest väga oluliselt selle poolest, kuidas virtuaalsed IT-süsteemid luuakse. Serveri virtualiseerimise puhul on virtuaalsete IT-süsteemide käsutuses iseseisev riistvarakeskkond. Operatsioonisüsteemi virtualiseerimine kujutab endast aga lahendust, mille puhul antakse virtuaalsete IT-süsteemide käsutusseoperatsioonisüsteemi isoleeritud instantsid, millele on installeeritud virtualiseerimistoode.

Seetõttu ei vajata näiteks füüsiliste süsteemide riistvarakomponentidele juurdepääsuks tavaliselt spetsiaalset draiverit, kuna riistvarakomponendid antakse virtuaalsele IT-süsteemi käsutusse muutmata kujul. Virtualiseerimistarkvara juhib siin ainult juurdepääsu, et virtuaalsed IT-süsteemid üksteist ei mõjutaks. Sellist tüüpi virtualiseerimise tõttu esinevad virtualiseerimislahenduse abil käitatavate virtuaalsete IT-süsteemide puhul teatud piirangud. Tavaliselt ei ole võimalik erinevaid operatsioonisüsteeme ühel virtualiseerimisserveril töötaval IT-süsteemil kasutada, kuna virtualiseerimisserver peab operatsioonisüsteemi üle võtma. Mõnede toodete puhul saab aga ühel virtualiseerimisserveril kasutada sama operatsioonisüsteemi erinevaid tuumaversioone. Mõlema virtualiseerimistehnoloogia puhul on virtualiseerimisserveri, hüperviisori ja virtuaalsete IT-süsteemide haldamiseks saadaval haldustarkvara, milleks võib olla veebipõhine haldusliides, spetsiaalne haldustarkvara või ka käsuridadepõhine kasutajaliides. Mõnede 1. tüübi serveri virtualiseerimistoodete puhul realiseeritakse see haldusliides hüperviisori täieliku kontrolli all oleva virtuaalse IT-süsteemina.

Serveri ja operatsioonisüsteemi virtualiseerimise võrdlus

Operatsioonisüsteemi virtualiseerimise suur eelis seisneb selles, et virtualiseerimisserveril ei vajata praktiliselt üldse ressursse virtuaalse tarkvara

emuleerimiseks nagu serveri virtualiseerimise puhul. Seetõttu saab operatsioonisüsteemi virtualiseerimise puhul käitada ühel süsteemil märksa rohkem virtuaalseid IT-süsteeme kui serveri virtualiseerimise puhul. See võimaldab suuremat pakkimisastet ja seega virtualiseerimisserveri ja füüsiliste IT-süsteemide kõrgemat suhet. Operatsioonisüsteemi virtualiseerimise olulised puudused on aga väiksem paindlikkus erinevate operatsioonisüsteemide kasutamise puhul, samuti virtuaalsete IT-süsteemide nõrgem kapseldatus. Erinevate rakenduste kasutamisel virtuaalses IT-süsteemis võib seetõttu esineda piiranguid. See sõltub suuresti asjaolust, et virtuaalsete IT-süsteemide ja virtualiseerimisserveri vastastikmõju on tugevam kui serveri virtualiseerimise puhul. Operatsioonisüsteemi virtualiseerimise puhul kasutatakse paljusid virtualiseerimisserveri operatsioonisüsteemi osi koos virtuaalsete IT-süsteemidega. Seega on enamasti kasutusel samad tarkvarateegid ja operatsioonisüsteemi komponendid, mõnede virtualiseerimistoodete puhul hoitakse näiteks tarkvarateeke füüsilise süsteemi töömälus ainult ühekordselt ja neid kasutavad kõik virtuaalsed IT-süsteemid. Seetõttu on virtuaalsete IT-süsteemide kapseldus operatsioonisüsteemi virtualiseerimise puhul vähem ilmne kui serveri virtualiseerimise puhul. Selle tulemusena võib ka virtuaalsete IT-süsteemide isolatsioon nii omavahel kui virtualiseerimisserveri suhtes nõrgem olla.

Serveri virtualiseerimise puhul on virtualiseerimisserveri ressursivajadus ühe virtuaalse IT-süsteemi kohta tavaliselt suurem kui operatsioonisüsteemi virtualiseerimise puhul. Virtuaalsete IT-süsteemide teenindamine ja hooldamine (näide: tarkvarauuenduste installeerimine) on samuti kulukam, kuna see toimub tugevama kapseldumise tõttu sageli iga virtuaalse IT-süsteemi puhul eraldi. Operatsioonisüsteemi virtualiseerimise puhul saab selliseid tarkvarauuendusi osaliselt installeerida turvapaikade virtualiseerimisserverile installeerimise käigus kõigis virtuaalsetes IT-süsteemides korraga. Peale selle saavutatakse serveri virtualiseerimise lahenduste puhul suurem paindlikkus suurema keerukusastme hinnaga. Suurem keerukus tuleneb virtualiseerimisserveri IT-koosluse taristu integreerimisega seotud mõningal määral suurematest kuludest. Nende süsteemide võrkudesse ja salvestusvõrkudesse integreerimise protseduur on tavaliselt keerukam. Peale selle võib osutuda vajalikuks käimasolevaid protsesse uute IT-süsteemide käitamiseks kohandada. Seetõttu sobib operatsioonisüsteemi virtualiseerimine eriti hästi siis, kui vajatakse suurt hulka samasuguseid virtuaalseid IT-süsteeme, näiteks ühteviisi või sarnaselt konfigureeritud veebiservereid.

Serveri virtualiseerimise eelised tulevad esile siis, kui on vaja käitada paljusid erinevaid virtuaalseid IT-süsteeme. Heterogeensete serverimaastike virtualiseerimise vajaduse korral pole serveri virtualiseerimisele sageli alternatiivi.

Virtualiseerimisserverite ja virtuaalsete IT-süsteemide võrku integreerimine Erinevate virtualiseerimislahenduste puhul on virtuaalsetele IT-süsteemidele IT-koosluse võrkudele juurdepääsu võimaldamiseks palju erinevaid meetodeid.

Põhijoontes saab nende võrguühenduste realiseerimise puhul eristada kaht põhimõtet:

- Virtuaalsetele IT-süsteemidele allutatakse otseselt virtualiseerimisserveri füüsilised võrguliidesed. Seejuures on virtuaalsed IT-süsteemid on seotud otse võrguga, millega on seotud virtualiseerimisserver ise.
- Füüsilised võrguliidesed seotakse kaudselt virtuaalsete IT-süsteemidega, kusjuures hüperviisori abil luuakse virtuaalne kommutaator, millega on seotud virtuaalsete IT-süsteemide virtuaalsed võrguliidesed. Selle virtuaalse kommutaatori saab omakorda siduda virtualiseerimisserveri füüsilise võrguliidese kaudu füüsilise võrguga. Selle tehnoloogia abil on samuti võimalik defineerida virtuaalseid kommutaatoreid ja võrke, millel puudub ühendus IT-koosluse füüsilise võrguga.

Need kaks erilaadset võrguintegratsioonitehnoloogiat mõjutavad erinevalt seda, kuidas toimub virtuaalsete IT-süsteemide ja virtualiseerimisserverite integratsioon IT-koosluse võrku. Eriti teise variandi puhul saab erinevatele kaitsevajaduse nõuetele paindlikult reageerida.

Külalistööriistad

Paljud tootjad annavad virtuaalsete IT-süsteemide käsutusse nn külalistööriistad, mille abil virtualiseerimistarkvara saab virtuaalseid IT-süsteeme hõlpsasti juhtida. Need tööriistad võimaldavad näiteks virtuaalseid IT-süsteeme virtualiseerimistarkvara kaudu välja lülitada, ilma et peaks virtuaalse süsteemiga otse suhtlema. Lisafunktsioonid on näiteks lõikelaua vahetamine virtuaalse IT-süsteemi ja virtuaalse IT-süsteemi kasutaja arvuti vahel või lihtsustatud juurdepääs andmekandjatele nagu virtualiseerimisserveri või virtuaalse IT-süsteemi kasutaja arvuti draividesse sisestatavad CD- või DVD-ROMid. Draiverid juurdepääsuks virtualiseeritud riistvarale ja tööriistad virtuaalsete IT-süsteemide juhtimiseks on sageli saadaval integreeritud installatsioonipaketina.

M 3.71 Virtuaalkeskkondade administraatorite koolitamine

Algatamise eest vastutavad: asutuse/ettevõtte juhtkond, infoturbespetsialist

Rakendamise eest vastutavad: infoturbespetsialist, IT-juht

Virtuaalsed taristud kujutavad endast arvutuskeskuse olulist taristuelementi. Nad on traditsiooniliste serveristruktuuriga võrreldes märkimisväärse kokkuhoiupotentsiaaliga ning leiavad arvutuskeskustes laialdast kasutust. Seetõttu tuleb tagada, et kõigil virtualiseerimiskomponentide haldamisega tegelevatel isikutel oleks virtuaalse infosüsteemi aluseks olevate toodete kohta piisavalt teadmisi. Virtualiseerimisserverid on väga keerukad. Lisaks virtuaalsetele IT-süsteemidele sisaldavad nad ka hüperviisorit ja võrgukomponente nagu näiteks virtuaalsed kommutaatorid ja eraldi teenused. Kuna konfiguratsioonivigadel on virtualiseerimisserveril käitatavate virtuaalsete IT-süsteemide jaoks sageli tõsised tagajärjed, esitatakse virtualiseerimiskeskkonna administraatoritele kõrgemaid nõudeid. Seetõttu on oluline, et administraatorid oleks probleemide ennetamise, tehniliste probleemide õigeaegse äratundmise ja kõrvaldamise, samuti virtualiseerimistööriistade funktsioonide ja turvafunktsioonide optimaalseks kasutamiseks piisavalt koolitatud. Neil peab olema võimalik kontrollida konkreetse virtualiseerimistoote funktsioone kontrollida ja hinnata konfiguratsioonimuutuste tagajärgi.

Koolitused peavad andma piisavalt teadmisi valitud virtualiseerimistoote planeerimiseks, ülesehitamiseks ja kasutamiseks. Ka administraatorirollide jaotamisel (vt M 2.446 Haldustoimingute jaotus virtualiseerimisserverite puhul) peavad kõik administraatorid valdama valitud virtualiseerimistehnoloogia aluseid, kuna senine vahetegemine eri valdkondade vahel nagu serveri-, võrgu- ja mälukasutus on kadunud. Juba virtualiseerimiskeskkonna planeerimisel tuleb arvestada piisava koolituseelarvega. Samuti tuleb varakult planeerida koolitused personalialase ressursinappuse vältimiseks. IT-süsteemide virtualiseerimise koolitused peavad sisaldama vähemalt järgmisi elemente:

- Konkreetse virtualiseerimissüsteemi alused ja kontseptsioonid
- Arvutuskeskuse töö sise-eeskirjade ja -reeglite koostamine ja rakendamine
- Konkreetsete komponentide käskude või kasutajaliidese tundmine.
- Virtualiseerimiskeskkonna planeerimine võrgu dimensioneerimise ja turvamise seisukohalt
- Riistvara dimensioneerimine protsessori-, muutmälu-, võrgu- ja salvestusvõrguressursside jaoks
- Virtualiseerimisserveri operatsioonisüsteemi ettevalmistamine
- Virtualiseerimissüsteemi installeerimine ja konfigureerimine
- Operatsioonisüsteemide installeerimine virtuaalses IT-süsteemis
- Virtuaalse IT-süsteemi võrgukonfiguratsioon
- Käitamine
- Kontroll, haldamine
- Protokollimine
- Konfiguratsioonide turvamine ja haldamine
- Virtuaalmasinate turvamine
- Automatiseerimisprotsessid

- Analüüs ja veaotsing

Tuleb jälgida, et koolitus sisaldaks lisaks teooriale ka piisavalt praktilisi osi.

Täiendavad kontrollküsimused:

- Kas koolitusmeetmete jaoks on kasutada piisav eelarve?
- Kas virtuaalsete keskkondade administraatorite koolitus viiakse läbi soovitatava miinimumsisuga?
- Kas virtualiseerimiskeskkonna administraatorid on probleemide vältimise, tehniliste probleemide õigeaegseks äratundmise ja virtualiseerimistööriistade turvafunktsioonide optimaalse ärakasutamise jaoks piisavalt koolitatud?

M 3.72w Virtualiseerimistehnika põhimõisted

Algatamise eest vastutavad: asutuse/ettevõtte juhtkond, IT-turvaosakond

Rakendamise eest vastutavad: infoturbespetsialist, IT-juht

Mõistet „virtuaalsus” ja sellest tuletatud omadussõna „virtuaalne” kasutatakse arvutitehnoloogias juba kaua aega ja väga erinevates kasutuskontekstides. Enamikes stsenaariumites tähistatakse objekt omadusega „virtuaalne”, kui seda ei ole küll füüsiliselt olemas, aga selle mõju ikkagi eksisteerib. Virtuaalsel objektil võivad seega olla ikkagi reaalsed mõjud ehk ta võib reaalsust muuta või seda mõjutada. Seetõttu ei saab mõisteid „virtuaalsus” ja „reaalsus” vaadelda vastanditena.

„**Virtualiseerimiseks**” nimetatakse ka protsessi, mille korral objekt teisaldatakse reaalsest virtuaalsesse olekusse või kui see antakse juba algusest peale kasutusse virtuaalsel kujul. Eriti infotehnoloogias kasutatakse objektide virtualiseerimist tehnikana nende objektide asendamiseks (millegi samaväärsega või samasuguse mõjuga). Näiteks kui IT-süsteemi reaalne põhimälu asendatakse virtuaalse põhimäluga (samaväärne asendus), võib seda kasutada samamoodi nagu reaalset, kuigi ta paikneb näiteks süsteemi kõvakettal ainult failina. Kuigi see fail ei ole tegelikult reaalne põhimälu, on selle mõju sarnane põhimälu omale. Seda tehnikat kasutatakse selleks, et kasutada rohkem põhimälu, kui seda tegelikult olemas on. Virtuaalse põhimälu kasutamisega võib aga kaasneda süsteemi jõudluse vähenemine. On olemas veel palju näiteid ressursside virtualiseerimise kohta, näiteks VLAN-id, VPN-id ja ka virtuaalsed protsessorid (Intel Hyperthreading).

Nagu eelmisest lõigust näha, kasutati minevikus virtualiseerimist põhiliselt kallite ja vähe kättesaadavate ressursside asendamiseks laialdaselt kättesaadavate ja odavate ressurssidega. Praeguseks on arvutitehnika ja eelkõige arvutite jõudlus arenenud nii kaugele, et virtualiseerimise kontseptsiooni laiendatakse ka teistele kasutusaladele. Arvutit saab vastava virtualiseerimistarkvara abiga kasutada universaalse tööriistana objektide virtualiseerimiseks ja eelkõige arvuti enda virtualiseerimiseks.

Eraldamine ja isolatsioon

Eraldamine ja isolatsioon on virtualiseeritud lahenduse kaks kõige olulisemat turbenõuet. Isolatsioon tähendab selles kontekstis, et kaks ühel virtualiseerimisserveril paiknevat virtuaalset IT-süsteemi saavad omavahel suhelda ainult selleks ettenähtud mehhanismide kaudu. Isolatsioon takistab, et ühelt virtuaalselt IT-süsteemilt on volitamata võimalik ligi pääseda mõne teise virtuaalse IT-süsteemi andmetele. Virtualiseerimise kontekstis tähendab eraldamine seda, et virtuaalne IT-süsteem saab suhelda ainult nende ressurssidega, mis on selleks vabastatud. Nendeks ressurssideks võivad olla näiteks riistvarakomponendid, võrguühendused või protsessid, mis jooksevad otse virtualiseerimisserveril. Eraldamine ei kaitse virtuaalseid IT-süsteeme mitte ainult volitamata ligipääsu eest, vaid takistab ka

virtuaalsete IT-süsteemide volitamata ligipääsu ressurssidele. Peale selle kasutatakse eraldatust ka virtuaalsete IT-süsteemide teisaldamiseks. Isolatsioon ja eraldamine on väga sarnased turbemehhanismid, mis tehnilisel tasandil saavutatakse sarnaste mehhanismidega. Praktikas aga neid kahte aspekti tihti ei eristata.

Süsteemi virtualiseerimine

Kaasaegsete arvutisüsteemide suure jõudluse tõttu, mida ei ole võimalik tavaliste operatsioonisüsteemidega ja rakendustega enam ära kasutada, tekib soov neid jõudlusreserve efektiivselt ära kasutada. Seda võiks teostada näiteks rakenduste koondamisega vähem koormatud arvutisüsteemile. Sellise efektiivsemaks muutmise strateegia keelamisel on aga head põhjused (vt M 4.97z Ainult üks teenus serveri kohta). Kuna rakendused võivad üksteist ettenägematul moel mõjutada, oleks selline süsteem arvutisüsteemile installeerituna peaaegu täiesti kontrollimatu.

Kui neid käitatakse eraldi, siis selliseid mõjutusi ei tekigi. Operatsioonisüsteemis tehtud muudatusi (näiteks uuendused või turvapaigad) ei tule kontrollida paljude rakenduste suhtes, vaid ainult ühe rakenduse suhtes. Lisaks on enamjaolt välistatud, et ühe rakenduse uuendamine mõjutaks mingil moel teisi rakendusi.

Kuid nüüd hoolitsetakse sobiva tehnikaga selle eest, et:

- arvutisüsteemis loomulikult olemas olev ühine operatsioonisüsteemi ja rakenduste eraldatus ning
- mitmel arvutisüsteemil tekkiv operatsioonisüsteemi ja rakenduste isolatsioon nendel arvutitel püsima jääb, kui neid andmekeskusi käitatakse virtuaalsete süsteemidena ühel andmekeskusel, jääb alles üksikuteks arvutisüsteemideks jaotamise eelis. Seevastu arvutiressursside kasutamist aga parandatakse. Arvutisüsteemi virtualiseerimisega on võimalik jõudlusreserve paremini ära kasutada, ilma et oleks vaja loobuda rakenduste ja teenuste ülevaatlikkusest üksikutel serverisüsteemidel. See arvutisüsteemi mitmeks virtuaalseks instantsiks jagamise kontseptsioon viidi esmalt sisse suurarvutite maailmas. Siinjuures jaotati suurarvuti nn jaotustehnikaga paljudeks väikesteks arvutiteks (loogiline jaotus, näiteks IBM LPAR z-Series i) juures omaenda operatsioonisüsteemi ja rakendustega. Et ühel riistvaraplatvormil kasutada suuremat arvutite hulka, kanti jõudluse kasvades see tehnika hiljem üle ka keskmise jõudlusega serveritele ja serverisüsteemidel, mis põhinesid x86 või x64 arhitektuuril. Järgnevalt kirjeldatakse, kuidas on virtualiseerimistehnika arenenud x86 või x64 arhitektuuril põhinevatel serverisüsteemidel ja millised baastehnikad ning riistvaraeeldused selleks loodi. Järgnevalt tutvustatakse mõningaid virtualiseerimistehnika rakendusi.

Täielik süsteemiemulatsioon

Virtualiseerimistehnika juurutati algselt puhtakujulise tarkvaralahendusena. See tähendab, et virtualiseerimistarkvara kaudu ei esitatud virtuaalsele süsteemile mitte kunagi emuleeritud riistvarakeskkonda. Virtuaalse IT-süsteemi arvutikomponendid nagu protsessor, põhimälu ja massmälu ning võrguliides emuleeriti ja kujundati tarkvaras järgi. Seeläbi on sellise virtuaalse süsteemi jõudlus piiratud. Samas võimaldab ta protsessoriemulatsiooni tõttu väga paindlike võimalusi, kuna siinjuures

on võimalik kogu IT-süsteemi platvormi virtualiseerida. Selliste täielike arvutivirtualiseerimistega on näiteks (siin Microsoft Virtual PC for Mac 7) võimalik teostada operatsioonisüsteemi nagu PowerPC-l põhineval arvutil, mille operatsioonisüsteemiks on Mac OS X 10.4, kuna x86 protsessor kujundatakse täielikult tarkvara poolt järgi. Selline arvuti virtualiseerimine on aga ülimalt ebaefektiivne, kuna protsessoriarhitektuuri ja teiste riistvarakomponentide täielik emulatsioon nõuab väga palju ressursse ja virtuaalne IT-süsteem saab kasutada ainult murdosa füüsilise süsteemi jõudlusest.

Serveri virtualiseerimine

Täielikust ja kogu platvormi virtualiseerimisest on oluliselt efektiivsem lahendus spetsiifilise platvormi virtualiseerimistehnika. Siin ei tule täieliku arvutikeskkonda järele kujundada (protsessor, põhimälu, kõvakettas jne). Virtualiseerimistarkvara tuleb kujundada nii, et vastava virtuaalse instantsi riistvaraarhitektuuri sisene eraldatus ja isolatsioon oleksid sarnased füüsilise süsteemi omale. Sellisel juhul ei ole enam vajalik riistvarakomponentide täielik emulatsioon. Virtuaalsete süsteemide juhtimist ja riistvarakeskkonda simuleerivat tarkvara nimetatakse Hypervisor iks.

Virtualiseerimistarkvaral (Hypervisor) on põhimõtteliselt ainult järgnevad ülesanded:

- Eraldatud ja isoleeritud käituskeskkonna võimaldamine üksikutele virtuaalsetele instantsidele ja
- virtuaalse süsteemi ligipääsu juhtimine füüsilise süsteemi riistvarakomponentidele.

Seda siin kirjeldatud platvormispetsiifilist virtualiseerimistehnikat nimetatakse Hypervisoril põhinevaks serveri virtualiseerimiseks. Serveri virtualiseerimises eristatakse ikka veel Hypervisor 'il põhinevat lahendust (tüüp 1) ja hostil põhinevat lahendust (tüüp 2). Hostil põhineva virtualiseerimislahenduse korral installeeritakse virtualiseerimistarkvara otse standardoperatsioonisüsteemile nagu Unix või Microsoft Windows Server. Hypervisor 'il põhineva lahenduse korral (tüüp 1) installeeritakse füüsilisele riistvarale ainult Hypervisor. See Hypervisor kujutab endast siis virtualiseerimisele spetsialiseerunud minimaalset operatsioonisüsteemi. 1. tüübi virtualiseerimistarkvara nimetatakse mõnikord ka Bare Metal Virtualization.

Serveri virtualiseerimistehnikat kasutavad tooted on näiteks:

- Microsoft Hyper-V (tüüp 1), Microsoft VirtualPC (tüüp 2) või Microsoft
- /VirtualServer ">VirtualServer (tüüp 2)
- QEMU (Tüüp 2 Märkus: QEMU-t saab kasutada täielikuks süsteemi emulatsiooniks)
- Sun /VirtualBox ">VirtualBox (Tüüp 2)
- VMware Server (Tüüp 2) ja VMware Workstation (Tüüp 2)
- VMware vSphere või VMware ESX (Tüüp 1),
- Xen'il põhinevad tooted nagu Citrix /XenServer ">XenServer, Sun OpenVM (Tüüp 1)

Serveri virtualiseerimisel luuakse reeglina virtuaalne arvuti, mis koosneb virtuaalsetest riistvarakomponentidest. Need riistvarakomponendid esitatakse

virtuaalse süsteemi operatsioonisüsteemile. Virtualiseerimistarkvara saab nüüd kõik virtuaalse IT-süsteemi operatsioonisüsteemi ligipääsu- ja juhtimiskäsud virtuaalsele ristvarale teisendada füüsilise riistvara käskudeks. See teostus on tunduvalt efektiivsem kui ülevalpool kirjeldatud riistvarakomponentide täielik emulatsioon. Seda tehnikat nimetatakse nn Täisvirtualiseerimiseks Jõudluse veelkordset tõusu on võimalik saavutada nn paravirtualiseerimise kasutamise kaudu. Siinjuures teostatakse Hypervisor i kontrolli all virtuaalses IT-süsteemis spetsiaalselt kohandatud operatsioonisüsteem. See on nii modifitseeritud, et virtuaalse IT-süsteemi operatsioonisüsteemi kernel ei sisalda enam riistvaralähedasi süsteemikäske.

Neid süsteemikäske nimetatakse tihti ka “Ring 0 käsk” või “Dom0 käsk”. Virtuaalne IT-süsteem teostatakse siis kas “Ring 1” või “DomU”. Kui virtualiseerimisserveri protsessor ei toeta paravirtualiseerimist (näiteks AMD-V ja Intel VT), võib sobitatud operatsioonisüsteemist loobuda. Seda võimalust kasutab näiteks XEN 3.0.

Operatsioonisüsteemi virtualiseerimine

Virtualiseerimistarkvara efektiivsust on võimalik veel tõsta, kui kõigil süsteemidel ei ole mitte ainult ühine riistvara platvorm, vaid ka operatsioonisüsteem. Selliseid virtualiseerimistehnikaid nimetatakse operatsioonisüsteemi virtualiseerimiseks. Virtuaalsete IT-süsteemide riistvaraligipääsu on võimalik ülimalt lihtsustada, kuna siinjuures ei ole vaja mitte ühtegi virtuaalset riistvarakomponenti.

Virtuaalsel süsteemil on sama operatsioonisüsteem mis füüsilisel süsteemil, millel seda käitatakse, ja seetõttu saab kasutada samasid riistvaradraivereid. Sellisel juhul muutub teisaldamine virtuaalse ja füüsilise riistvara vahel üleliigseks. Virtuaalsete IT-süsteemide eraldamine ei ole siinjuures aga operatsioonisüsteemile enam suuresti märgatav, kuna kõik virtuaalsed instantsid kasutavad sama (mitte ühte ja sama!) operatsioonisüsteemi. Virtualiseerimistarkvara kindlustab ainult erinevate virtuaalsete instantside eraldatuse.

Näited selliste operatsioonisüsteemi virtualiseerimise lahenduste kohta on:

- Sun Solaris Containers
- BSDjails
- Parallels Virtuozzo
- User Mode Linux

Võrreldes serveri virtualiseerimisega on operatsioonisüsteemi virtualiseerimisel põhinevate toodete eeliseks virtuaalsete instantside suur jõudlus ja suhteliselt väike jõudluskulu virtualiseerimisserveril. Seeläbi on saavutatav väga suur tihendus

(virtualiseerimisserverite suhe virtuaalsete süsteemidega). Mõnede operatsioonisüsteemi virtualiseerimislahendustega on võimalik keskmise jõudlusega virtualiseerimisserveril käitada kuni 200 virtuaalset IT-süsteemi. Sama koormusega serveril, mis kasutab serveri virtualiseerimislahendust, on enamasti võimalik kasutada 10 kuni 15 virtuaalset süsteemi. Operatsioonisüsteemi virtualiseerimislahenduse puuduseks on aga operatsioonisüsteemi ja rakenduste nõrk eraldatus virtualiseerimisserveril.

See nõrk eraldatus viib selleni, et erinevaturbevajadusega

virtuaalseid IT-süsteeme ei saa ilma lisameetmeteta koos ühel virtualiseerimisserveril käitada. See on serveri virtualiseerimisel põhineva virtualiseerimislahenduse korral reeglina teisiti, kuna virtuaalsete süsteemide eraldatus on tugevam. Kas erineva turbevajadusega virtuaalseid IT-süsteeme on aga võimalik koos ühel virtualiseerimisserveril käitada, sõltub peale kasutatud toote ka organisatsioonipoolsest või virtuaalse IT-süsteemi turbevajaduse määramisest.

Virtualiseerimistehnika kasutamine

Virtualiseerimistehnika vahenditega on võimalik luua mõningaid rakendusi, mida on füüsilistel süsteemidel võimalik realiseerida ainult ebaproportsionaalselt suurte jõupingutustega. Tavaliselt põhinevad need rakendused olukorral, kus virtualiseerimistarkvaral on otsene kontroll virtuaalse IT-süsteemi protsesside, põhimälu ja massmälu üle. Ta saab otseselt mõjutada, kuidas virtuaalne süsteem ressursse kasutab. Seega saab virtualiseerimistarkvara iga kell analüüsida näiteks virtuaalse IT-süsteemi protsessori või põhimälu olekut. Neid võimalusi saab kasutada selleks, et virtuaalne IT-süsteem teadmata ajaks külmutada. Peale selle on võimalik protsessorisse või põhimällu laadida eelnevalt salvestatud sisu. Eelnevalt virtualiseerimisserveri kõvakettal salvestatud protsessori ja põhimälu olek laetakse pärast käituse katkestust uuesti ja virtuaalse süsteemi käitus jätkub täpselt sealt, kus süsteem külmutati.

Virtuaalse IT-süsteemi külmutamise võimalust kasutatakse nn snapshot'ide tegemiseks jooksva käituse ajal.

Snapshot

Enamik virtualiseerimislahendusi võimaldab suvalisel ajahetkel virtuaalse IT-süsteemi oleku säilitamist, ilma et see mõjutaks mingil viisil virtuaalse IT-süsteemi teostust. Snapshot'i loomisel virtuaalne kõvaketas külmutatakse ja edasised ligipääsud edastatakse eraldi failile. Aktiivsete snapshot'idega masina hetkeolek tuleneb snapshot'ide ühendamisest baasfailidega. Snapshot'e võib luua nii koos kui ka ilma virtuaalse IT-süsteemi põhimälu sisuta. Ilma töömälu sisuta snapshot'id peegeldavad enamasti IT-süsteemi olekut, mida ei suletud vaid mis lülitati välja jooksva käituse ajal. Töömälu sisuga snapshot'id võimaldavad IT-süsteemi varustada just selle olekuga, milles ta oli snapshot'i tegemise ajahetkel, tähendab on võimalik tagasiminek jooksvasse, avatud rakendustega operatsioonisüsteemi. Niikaua kui snapshot'i ei kustutata, leiab snapshot'i ajahetke mäluseisu enamasti faili vormingus virtuaalse IT-süsteemi kataloogist.

Virtuaalsete IT-süsteemide Live Migration

Tehnikad nagu Live Migration XEN-i jaoks, Citrix /XenMotion ">XenMotion ja Microsoft HyperV server 2008 R2 või VMotion VMware jaoks lubavad virtuaalsete IT-süsteemide ülekandmise teistele füüsilistele virtualiseerimisserveritele jooksva

käituse ajal. Kasutaja vaatepunktist ning ka virtuaalse IT-süsteemi vaatepunktist toimub see katkestusteta. Seeläbi muutub näiteks võimalikuks virtualiseerimisserveri riistvara laiendamise või väljavahetamise, virtualiseerimisserverite koormuse teadliku ümberjaotamise ning teatud teenuste või rakenduste ümberpaigutamise teistele virtualiseerimisserveritele. Nii enne migratsiooni, selle ajal kui ka pärast migratsiooni peab olema kindlustatud virtuaalse IT-süsteemi ligipääs teatud failisüsteemidele.

Siinkohal tulevad kõne alla salvestusvõrgud (SAN Storage System) Fiber Channel i kaudu või iSCSI ja võrguandmesüsteemid nagu NFS. See tehnika toimib põhimõtteliselt nii, et esmalt kantakse virtuaalse IT-süsteemi snapshot allikas virtualiseerimisserverilt siht-virtualiseerimisserverile. Sihtserver laeb nüüd edastatava virtuaalse IT-süsteemi põhimälu oma mällu. Kuna süsteem jookseb algserveril edasi, muutus vahepeal ka virtuaalse süsteemi mälu. Need muudatused edastatakse nüüd jooksvalt ja seetõttu toimub allikassüsteemi ja sihtsüsteemi sünkroniseerimine. Kui sünkroonsus on saavutatud, peatatakse allikaserver, protsessoriolek edastatakse sihtserverile ja virtuaalne IT-süsteem jätkab sihtserveril edastatud protsessoriolekuga tööd. See toimub virtuaalse IT-süsteemi jaoks täiesti transparentselt. Live Migration it saab kasutada jõudlusega seotud kitsaskohtade ennetamiseks. Seda protsessi on võimalik automatiseerida, nii et virtuaalsel IT-süsteemil oleks alati maksimaalne jõudlus.

Põhimälu ülebroneerimine

Mõnede virtualiseerimislahenduste korral saab virtuaalsete IT-süsteemide käsutusse anda rohkem põhimälu kui virtualiseerimisserveril reaalselt olemas on. Üksiku virtuaalse IT-süsteemi käsutusse ei saa aga anda rohkem mälu kui on Hypervisori kasutada. Virtualiseerimisserveri põhimälu suuruseks on näiteks kaks gigabaiti. Sellel käitatakse kolme virtuaalset serverit, millest igaühel on üks gigabait, ühesõnaga kokku kolm gigabaiti põhimälu. Sellise ülebroneerimise võimaldamiseks ei anta mitte kõike põhimälu mahust virtuaalse IT-süsteemi käsutusse.

Selle asemel antakse füüsiline mäluosa üksiku virtuaalse IT-süsteemi käsutusse ainult siis, kui virtuaalne süsteem seda ka tegelikult vajab. Virtuaalse IT-süsteemi poolt nõutud mälu ei ole Hypervisor i kaudu põhimõtteliselt enam võimalik tagasi nõuda. Nii tõuseb virtuaalse IT-süsteemi mäluvajadus järkjärgult kuni konfiguratsioonipiirini. Kuna võib lähtuda sellest, et virtuaalse IT-süsteemi operatsioonisüsteem kasutab aja jooksul kogu talle antud mälumahtu, peab olema võimalus, kuidas virtualiseerimisserveril ressursitäiendusega ümber käia. Üht sellist võimalust näidatakse järgmistes lõikudes ühe näite põhjal.

Näiteks võimaldab firma VMware ESX server kolme erinevat, üksteisega kombineeritavat võimalust põhimälu ülebroneerimiseks:

- Transparent Memory Sharing - Hypervisor monitoorib kõikide virtuaalsete

IT-süsteemide lehekülgi. Kui Hypervisor tuvastab kaks ühesugust lehekülge, siis edastatakse need ainult üks kord virtualiseerimisserveri füüsilisele põhimälule. Kui üks virtuaalne IT-süsteem muudab neid lehekülgi, kopeeritakse see selle süsteemi tarvis ja teised virtuaalsed IT-süsteemid kasutavad edasi muutmata lehekülge. See tehnika võimaldab mälu oluliselt kokku hoida, kuna näiteks paljudel virtuaalsetel IT-süsteemidel kasutatakse samu operatsioonisüsteemituumasid või tarkvararaamatukogusid. Nende tuumade või kogude mälupilt peab ainult üks kord olema virtualiseerimisserveri füüsilises mälus talletatud.

- Ballooning - Sõltuvalt kogu süsteemi põhimälu kasutusest võib virtuaalse põhimälu jaotus üksikutele virtuaalsetele süsteemidele dünaamiliselt sobitada. Selle teeb võimalikuks draiver virtuaalses süsteemis, mis hõivab sihilikult mälu (Ballooning) ja sunnib nii virtuaalse IT-süsteemi operatsioonisüsteemi salvestama põhimälu sisu tema virtuaalsele kõvakettale. ESX server tunneb Ballooning- draiveri poolt hõivatud mälu ära ja seda on võimalik jagada teistele virtuaalsetele IT-süsteemidele. Selle meetodi abiga on ajutiselt võimalik kompenseerida mäluga seotud kitsaskohti. Kuna virtuaalse IT-süsteemi operatsioonisüsteem kontrollib, milliseid protsesse väljastpoolt sisse tuuakse, on selle negatiivne mõju jõudlusele lühiajaliselt vastuvõetav.
- Paging - Kui virtuaalse IT-süsteemi mälu ei ole võimalik vabastata ei virtualiseerimisserveri Transparent Memory Sharing kaudu ega Ballooningu kaudu, edastatakse teiste mitte aktiivsete virtuaalsete IT-süsteemide mälu Hypervisori poolt ESX-serveri kõvakettale. Selle juhtudes vähendatakse märgatavalt virtuaalsete IT-süsteemide jõudlust, kuna Hypervisor ei arvesta väliste virtuaalsete IT-süsteemide operatsioonisüsteemide protsessidega.

Samuti on võimalik üle täita virtualiseerimisserveri kõvakettaruumi. Siinjuures antakse virtuaalsete IT-süsteemide käsutusse rohkem kõvakettaruumi, kui seda tegelikult olemas on. Seejuures jagatakse kasutada olev kõvakettaruum nii, et virtuaalne masin tunneb ära näiteks kümne gigabaidi suuruse ajami ja saab siis luua täpselt nii suure failisüsteemi. Virtualiseerimisserveri kõvakettal hõivab virtuaalne IT-süsteem konteinerfailis ainult tegelikult vajamineva ruumi, mis kasvab dünaamiliselt koos vajamineva mälumahuga. Niipea kui virtuaalne IT-süsteem kasutab lisaruumi, hõivatakse see ka virtualiseerimisserveri füüsilisel kõvakettal.

Virtuaalse IT-süsteemi poolt vabastatud mälumahtu ei vabastata füüsilisel kettal tavaliselt automaatselt. Lisaks tuleb jälgida, et virtuaalsed IT-süsteemid satuvad veasituatsiooni, kui füüsilisest mälust enam ei piisa, et edasisi mälunõudmisi täita: Virtuaalsed IT-süsteemid ei „tea” mälu ülebroneerimisest midagi ja üritavad edasi oma virtuaalsetele kõvaketastele kirjutada. Virtuaalses IT-süsteemis tekivad kirjutusvead ja selle tulemusena failisüsteemi lekked.

Riistvarakomponentide veatolerants

Mõned virtuaalsed IT-süsteemid saavad tolerantsmehhanismide virtualiseerimistoodetest riistvaravigade korral kasu. Kuna virtualiseerimistarkvara juhib näiteks virtuaalse ja füüsilise võrguliidese jaotust, võib algse võrguliidese vea korral virtuaalse IT-süsteemi kommunikatsiooni ümber juhtida mõnele teisele võrguliidesele. Kui ühes virtualiseerimisserveri on kasutada mitu redundantset komponenti,

hoolitseb virtualiseerimistarkvara selle eest, et ühe komponendi rivist väljalangemisel võetakse kasutusele veel töökorras komponent.

Virtuaalsete IT-süsteemide veatolerants

Virtualiseerimistoodetel Citrix /XenServer“>XenServer (Marathon /EverRun”>EverRun) ja VMware vSphere (Fault Tolerance) on näiteks olemas mehhanismid, et virtualiseerimisserveri rivist väljalangemise juhuks luua veatolerantsed virtuaalsed IT-süsteemid.

Et seda virtuaalse IT-süsteemi veatolerantsi saavutada, luuakse ühel teisel virtualiseerimisserveril selle virtuaalse IT-süsteemi koopia. Seda koopiat sünkroniseeritakse jooksvalt originaaliga ja see ei ole nii kaua võrguga ühendatud, kui originaal toimib. Kui virtualiseerimisserver, millel originaali käitatakse, langeb rivist välja, saab koopia kohe võrguga ühendada ja kõik originaalfunktsioonid kiiresti üle võtta. Seejärel luuakse uuel virtualiseerimisserveril kohe jälle virtuaalse IT-süsteemi uus koopia.

M 3.73 DNS-serveri administraatorite koolitamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: infoturbespetsialist

DNS-serveri korrektse ja turvalise haldamise tagamisel on vastutavate administraatorite koolitamine möödapääsmatu. Ka kõige pisemad konfiguratsioonivead võivad viia turvaaukude tekkimiseni. Eriti põhjalikke ja erialaseid teadmisi eeldab DNS-serveri kasutamise hoolikas planeerimine ja kommunikatsiooni piiramine volitatud kasutajatele.

Peale operatsioonisüsteemi üldise turvalisuse, mida kirjeldatakse näiteks moodulis B 3.102 Server Unixi all , on olulised ka järgmised punktid:

- DNS-serveri installimine;
- DNS-serveri integreerimine operatsioonisüsteemi käivitusprotsessiga;
- ohtude selgitamine, et luua arusaam erinevatest võimalikest rünnetest;
- õiguste kontseptsiooni loomine nii administraatorite (seoses konfigureerimisega) kui ka DNS-serveri protsesside jaoks;
- Advertisingu ja Resolvingu DNS-serveri erinevus;
- DNS-serveri konfigureerimise võimalused;
- päringute kaitsemehhanismid;
- tsooniedastuste kaitsemehhanismid;
- dünaamiliste värskenduste kaitsemehhanismid (kui neid kasutatakse);
- DNSSEC kasutusvõimalused ja konfigureerimine;
- DNS-serverite käideldavust tagavad mehhanismid;
- tsooniinfo kaitsemehhanismid.
- vajaliku eelarve olemasolu?

Kontrollküsimused:

- Kas administraatoreid on piisavalt koolitatud, et nad oskaksid DNS-serverit käsitseda ja tunneksid selle turbeaspekte?
- Kas koolituse jaoks on olemas vajalik eelarve?

M 3.74 Rühmatarkvarasüsteemide süsteemiarhitektuuri ja turbe koolitus administraatoritele

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: infoturbespetsialist, IT-juht

Rühmatarkvarasüsteemi õigeks ja turvaliseks haldamiseks on vastutavate administraatorite koolitamine vältimatu. Isegi väike konfigureerimisviga võib süsteemi turvalisust mõjutada. Seetõttu tuleb administraatoreid süsteemiarhitektuuri ja eriti kasutatava rühmatarkvara konkreetsete turvamehhanismide suhtes piisavalt koolitada. Rühmatarkvarasüsteemide kasutamine on keerukas ning selles osalevad paljud osapooled. Seetõttu tuleb silmas pidada, et teenindaval personalil oleks oma tegevuse jaoks vajalik väljaõpe. Selleks tuleb järgida M 3.11 Hooldus- ja halduspersonali väljaõpe toodud soovitusi. Lisaks tuleb administraatorite nõuetekohaseks väljakoolitamiseks (et nad oskaksid oma ülesandeid täita) kasutada selliseid meetmeid nagu seminarid ja kasutajate koosolekud. Tuleb kaaluda koolitusplaani koostamist.

Administraatorid peavad saama väljaõppe rühmatarkvarasüsteemide turbe seisukohast olulistes valdkondades, kuhu kuuluvad peale rühmatarkvara komponentide turvafunktsioonide ülevaate järgmised aspektid:

- Rühmatarkvarasüsteemide aktuaalsed ohud nagu Denial-of-Service-ründed, kahjurvara , ohuallikas „vaikeseaded ” jne.
- Ülevaade SMTP-turbest.
- Kahjurvara ja rämpsposti tõrje (rämpsposti- ja viirusetõrje lahenduste ülesehitamine ja integreerimine).
- Ülevaade rühmatarkvara haldamise vastavatest õiguslikest aspektidest (näiteks andmekaitse).
- Rühmatarkvarakomponentide turvamehhanismidega ümberkäimine.
- Pääsuõiguste määramine ja operatsioonisüsteemi pääsuõigustesse integreerimine, autentimismehhanismid.
- Ülevaade mitmesugustest sõnumiturbe lahendustest nagu krüpteerimine, digiallkiri, VPN-id.
- Logimine.
- Konfiguratsiooniandmete turvamine ja haldamine.
- Andmevarundus.
- Intsidentidega tegelemise ja süsteemi avariijärgse taastamise meetmed.

Lisaks eeldab rühmatarkvarakomponentide haldamine teadmisi kasutatavate serveri-, kliendi- ja andmebaasiplatvormide konfigureerimisvõimalustest. Kõigil administraatoritel peavad olema üldised põhiteadmised , millest lähtudes saab üksikuid raskuspunkte sihipäraselt üles ehitada ja hooldada.

Kontrollküsimus:

- Kas administraatoreid on kõigi rühmatarkvarasüsteemis ette tulevate tööde jaoks piisavalt koolitatud ?

M 3.75 Rühmatarkvaraklientide turvamehhanismide koolitus kasutajatele

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: infoturbespetsialist, IT-juht

Rühmatarkvarasüsteemid on üldiselt sedavõrd keerukad, et vale kasutuse või konfiguratsiooni puhul võib tekkida ootamatuid turvaauke. Eriti kehtib see siis, kui kasutaja ei ole rühmatarkvarasüsteemi kohta piisavat väljaõpet saanud . Süsteem konfigureeritakse küll tavapäraselt, nii et kasutaja saab seda muuta vaid piiratud ulatuses, kuid teadmatus kasutaja käsutuses olevatest turvamehhanismidest ja -seadistustest võib teha süsteemi kasutamise ebaturvaliseks. Seetõttu tuleb kõiki kasutajaid koolitada, et nad oskaksid rühmatarkvarakliendiga ümber käia. Klienditarkvara kasutamise kõrval on vaja kasutajatele selgeks teha ka rühmatarkvarasüsteemide põhifunktsioonid. Eriti tuleb kasutajatele selgitada, millised turvamehhanismid nende käsutuses on , et nad suudaksid neid õigesti ja arukalt kasutada. Töötajaid teavitatakse rühmatarkvara- ja meiliklientide kasutajatega seotud ohtudest näiteks lühiõppuse või infolehe abil . Nende tähelepanu juhitakse sellele, et suhtlustarkvara ebaharilikku käitumist ei tohi enda teada jätta. Eriti tuleb kasutajatele selgitada, millised turvamehhanismid nende käsutuses on , et nad suudaksid neid õigesti ja arukalt kasutada .

Täiendavad kontrollküsimused:

- Kas kõik kasutajad on saanud koolituse rühmatarkvarakliendiga töötamise kohta ?
- Kas kasutajatele on selgitatud rühmatarkvara kõigi turvamehhanismidega ümberkäimist ?

M 3.76 Rühmatarkvara ja meili kasutajate koolitus

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: kasutaja

Enne suhtlusteenuste ja rühmatarkvararakenduste (näiteks e-post) kasutuselevõttu tuleb kasutajatele tutvustada teenindusvigade vältimist ja asutuse eeskirjadest kinnipidamist. Eriti tuleb kasutajate tähelepanu juhtida võimalikele ohtudele ja turvameetmetele, mis on seotud meilide saatmise ja vastuvõtmisega. Samuti tuleb neile selgeks teha, et suhtlustarkvara ebaharilikku käitumist ei tohi enda teada jätta. Kasutajaid tuleb teavitada, et ebahariliku sisuga faile ei tohi edasi saata, infoserveritele salvestada ega avada.

Peale selle tuleb suhtlusteenuste kasutamisel neile südamele panna, et nad pööraksid tähelepanu järgmistele aspektidele:

- Iga hinna eest tuleb vältida hooletut või lausa kavatsuslikku jooksva töö katkestamist. Eriti tuleb vältida igasuguseid volitamata juurdepääsukatseid võrguteenustele, kui nende katsete eesmärk on võrgus ligipääsetava info muutmine, võrgukasutaja individuaalsesse töökeskkonda sekkumine või arvuti ja isiku kohta kogemata saadud andmete edastamine.
- Tuleb vältida avalikkuse jaoks ebaolulise info levitamist, samuti võrgu koormamist ebasihipärase ja üleliigse info levitamisega.
- Tuleb vältida liigset infolevikut.

Lisaks tuleb kasutajaid teavitada järgmistest asjaoludest:

- Kui meil saadetakse mitmele vastuvõtjale, kantakse aadressid sageli To - või CC -väljale. Eeliseks on see, et ühte meili peab saatma ainult korra ja iga vastuvõtja näeb ka teisi saajaid. Sageli pole aga vaja, et iga vastuvõtja kogu saajate nimekirja näeks. See pole mitte ainult vastuvõtjale koormav, vaid võib olla andmekaitse seisukohast soovimatu ja tekitada rämpsposti. Suuremate saajanimekirjade puhul tuleb meiliaadressid kanda CC asemel BCC alla või kasutada meililiste. BBC tähendab meili pimekoopiat (Blind Carbon Copy) ning sellele väljale sisestatud aadresse teistele vastuvõtjatele ei näidata.
- Meililistide õigsust ja aktuaalsust tuleb regulaarselt kontrollida, et meilid ei satuks vigase või vananenud nimekirja tõttu valele vastuvõtjale.
- Kasutajad peavad tundma asutuse kõiki eeskirju, mis kehtivad suhtluse, rühmatarkvara ja meili kohta (näiteks millal ja millises vormingus signatuurid (saatjaandmed) meilile lisatakse).
- Meilitsi liigub palju kahjurvara. Kasutajaid tuleb kahjurvarast ja selle levimisteedest teavitada. Samuti peavad nad teadma, et kõigist turvameetmetest hoolimata võib juhtuda, et asutusse sissetulevad meilid või manused sisaldavad kahjurvara ja seetõttu ei tohi mingil põhjusel kahtlasena tunduvaid meile ega manuseid (näiteks ootamatuid manuseid) avada.
- Meilisüsteemi ülekoormuse vältimiseks tuleb töötajatele tutvustada võimalikku väärkäitumist. Seejuures tuleb neid hoiatada kettkirjades osalemise ja mahukate meililistide tellimise eest.

Enamiku rühmatarkvarasüsteemide puhul edastatakse infot avalike liinide kaudu krüpteerimata kujul. Nii saab seda enne vastuvõtjani jõudmist mitmesugustesse vahearvutitesse salvestada ja tee peal kergesti manipuleerida. Aga ka meili saatja saab enamasti sisestada suvalise aadressi (From), nii et saatja autentsuses võib olla kindel ainult päringu või digiallkirja kasutamise puhul. Kahtluse puhul tuleb saatja ehtsust kontrollida päringu, või veel parem, krüpteerimise ja/või digiallkirja abil. Põhimõtteliselt ei tohiks meilisaatja ehtsuse suhtes saatja andmetele lootma jääda. Meilide puhul oodatakse kiiret reageerimisaega, mistõttu tuleb sissetulevat posti kontrollida mitu korda päevas. Pikema eemaloleku puhul tuleb rakendada esinduseeskirju, näiteks võib sissetulevad meilid edastada oma esindajale (vt M 2.274 Asendamise korraldamine meilivahetuse alal). Kuna paljudel juhtudel ei saa ennustada, milline meiliklient millist meilisaajat kasutab või millist tarkvara ning operatsioonisüsteeme tee peal kasutatakse, peab kasutaja teadma, et nii ülekandmisel kui ka sõnumite ja manuste kuvamisel võib saaja juures probleeme esineda. Seda eriti ebatavaliste märgistike või failivormingute ja vananenud meilitarkvara kasutamise puhul. Samuti peavad kasutajad teadma, et meilid ei jõua alati vastuvõtjani. Eelkõige just pakiliste või oluliste meilide puhul ei tohi saatja lootma jääda vastuvõtja automaatsele kinnitusele – pigem peaks järgnema sõltumatu tagasiside, näiteks lühike meil saaja sõnastatud kinnitusega.

Meilide kustutamine

Kasutajaid tuleb teavitada, et meilirakenduse kaudu kustutatud meilid ei kao enamasti pöördumatult. Paljud meiliprogrammid ei kustuta meili, vaid saadavad erilisse kataloogi. Kasutajatele tuleb selgitada, et klientide meile saab täielikult kustutada. Lisaks võivad meilid pärast kliendi juurest kustutamist meiliserveritesse alles jääda. Paljud internetiteenuse pakkujad ja administraatorid arhiveerivad sissetulevaid ja väljaminevaid meile. Paljud meilirakendused ei kustuta meile, vaid sadavad prügikasti, mida tuleb omakorda tühjendada. Kasutajad peavad teadma, et meili konfidentsiaalsust ei saa tagada vaid krüpteerimise teel. Lootma ei saa jääda ka sellele, et meilid kustutatakse pärast vastuvõtmist kiiresti. See kehtib teistegi rühmatarkvararakenduste, nt kalendri puhul.

Eeskirjade avalikustamine

Kõik rühmatarkvara kasutamist puudutavad eeskirjad ja teenindusjuhendid peavad töötajatele alati kättesaadavad olema (näiteks sisevõrgus).

Kontrollküsimus:

- Kas kasutajaid on rühmatarkvara kasutamisel tekkivatest ohtudest ja vastavatest turvameetmetest teavitatud?

M 3.77 Interneti kasutamisega seotud teadlikkuse suurendamine

Algatamise eest vastutavad: infoturbespetsialist, personalijuht, ülemused

Rakendamise eest vastutavad: infoturbespetsialist, personaliosakond

Internetti saab ettevõtetes ja ametiasutustes kasutada mitmel otstarbel ja erinevate teenustega. Võimaluste hulka kuuluvad klientidega meili teel suhtlemine, kiirsõnumite kaudu suhtlemine, foorumid ja blogid, organisatsiooni isiklikud veebilehed või info otsimine. Selleks, et interneti kasutamine oleks organisatsiooni jaoks ohutu, saab teatud teenuste või veebilehtede kasutamist keelata või piirata. Kuna kõikide soovimatute teenuste kasutamist ei saa tehnilistel põhjustel keelata, muu hulgas pidevalt uute lisanduvate lehekülgede ja teenuste tõttu, on mõistlik töötajaid koolitada, et nad oskaksid internetti kasutada turvaliselt ja otstarbekalt. Töötajatele tuleb ka selgitada, kuidas vältida õigesti käitudes ja internetirakenduste, nt brauseri optimaalse seadistamisega soovimatute andmejälgede jätmist internetti. Töötajad peavad mõistma, millised on interneti kasutamise võimalikud ohud ja vajalikud turbemeetmed. Eriti peavad nad mõistma:

- organisatsioonisiseseid interneti kasutamise reegleid (on võimalik, et lisaks interneti kasutamise reeglistikule on olemas eraldi reeglistik meilide, blogide jms kasutamise kohta);
- allalaaditud failide käsitlemist ning internetist pärit tarkvara ja pluginate installimise reegleid;
- interneti kasutamise võimalikke ohtusid ja nendevastaste turbemeetmete tõhusust;
- aktiivsisu, nt Java aplette, ActiveX-i komponente ja JavaScripti, ning organisatsiooni otsust aktiivsisu kasutamise kohta;
- organisatsiooni inforeeglistikku, st millist infot ei tohi internetti edastada (nt kui see on konfidentsiaalne või avaldamiseks sobimatu);
- õiget käitumist internetiteenuste kasutamisel, sest töötajad tegutsevad ametiasutuse/ettevõtte nimel;
- rämpsposti vältimise strateegiaid;
- õigusnõudeid (autoriõigust, nt seoses internetist võetud materjali kasutamisega, illegaalse, põhiseadusevastase või äärmusliku sisu, pornograafia jms käsitlemist);
- krüpteerimise ja digiallkirjade põhiteadmisi, et osata SSL-i ja krüpteerimisprogramme õigesti kasutada;
- fakti, et internetist leitud info ja pakkumised pärinevad – nii nagu paljud teised infokanalid – erineva usaldusväärsusega allikatest ja et nende kasutamisel tuleb olla kriitiline ning vajaduse korral allikat kontrollida.

Ei piisa, kui töötajatele selgitatakse interneti turvalist kasutamist vaid ühe korra – seda tuleb teha korduvalt, lähtudes uusimatest muudatustest. Tavapäraste koolituste kõrval tuleks kasutada ka intranetti riputatud veebipõhiseid interaktiivseid programme ja juhiseid. Uusimad muudatused selles vallas võib edastada ka uudiskirjades ja teatistes, samuti regulaarsete ürituste ajal, nt osakonna koosolekutel.

Täiendav lontrollküsimus:

- Kas töötajatele on selgitatud interneti kasutamisega seotud ohtusid ja nende turbemeetmeid?

M 3.78w Korrektne käitumine internetis

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: kasutajad

Internetiteenuste ametialasel kasutamisel tehtud väljaütlemisi peetakse tavaliselt organisatsiooni, mitte eraisiku seisukohaks. Seega tuleb töötajatele selgitada, kuidas internetti kasutades õigesti käituda ja millist käitumist tuleb kindlasti vältida. Infot tohiks internetis avaldada alles pärast hoolikat kaalumist, olgu siis avaldamise kohaks internetiportaalid, organisatsiooni enda veebilehed, meililistid või blogid. Ka lühikest aega tähelepanu saav info, näiteks foorumipostitus, mis on suunatud vaid väiksele hulgale lugejatele, võib olenevalt olukorrast jääda väga kauaks internetis kättesaadavaks. Otsingutega, nt otsingumootorites või suhtlusvõrgustikes, saab koguda infot väga erinevatest valdkondadest. Vältimaks olukorda, kus konkreetset isikut või organisatsiooni teatud valdkonda puudutava info sihilik kasutamine põhjustab ebameeldivusi, peavad internetikasutajad pidama kinni alljärgnevatest reeglitest:

- Võimalikult vähe andmeid. Kasutaja peab alati enne info edastamist või avaldamist internetis hoolikalt järele mõtlema, millise mulje võib see info jätta temast ja organisatsioonist, kus ta töötab, ning kas selle info edastamine on kindlasti vajalik. Isiklikku või organisatsiooni tegevuse jaoks olulist infot tohiks edastada võimalikult napilt. Lähtuda tuleb põhimõttest, et avaldada tohib ainult selliseid asju, mida kõlbaks avaldada oma nime all ka mõnes ajakirjas.
- Ainult vajalik (*need-to-know*). Infot tuleks edastada ainult neile, kes seda ka tõesti teadma peavad. Näiteks võib andmete edastamiseks kasutada suletud foorumeid või muid kaitstud alasid.
- Blogisid, foorumeid, meililiste jms rakendusi tuleb kasutada nii, et eraviisilisi väljaütlemisi ei saaks segi ajada ametialastega, samuti ei tohi olla võimalik neid valesti tõlgendada.
- Failide metaandmetest tuleb eemaldada liigne lisainfo (vt M 4.64 Ülekantavate andmete kontrollimine enne edastamist/peidetud info kõrvaldamine). Pildifailid võivad sisaldada rohkem infot, kui on avaldatud pildil näha.

Iga kasutaja peab internetis sobivalt käituma, st jälgima netiketti. Netiketiks (neti etikett) nimetatakse viisakusreegleid ja käitumissoovitusi, mis on aja jooksul interneti kasutamisel tavaks saanud ja mille järgimine peaks tagama, et igaüks saab internetti kasutada tõhusalt ja kedagi häirimata. Selle alla kuuluvad näiteks järgmised soovitused:

- Internetis tuleb jälgida, et jutu stiil ja sisu vastaksid sihtgrupile. Organisatsioonide töötajad peavad alati jälgima, et nad väljendaksid end ainult sellisel viisil, et nende väljaöeldut ei saaks tõlgendada nende endi või organisatsiooni suhtes negatiivselt. Suhtlusstiil peaks alati jääma asjalikuks. Oma avalduste puhul tuleb alati mõelda, kas neid kõlbaks sellises sõnastuses ka

trükituna avaldada. Need ei tohi olla ülbed, diskrimineerivad ega solvavad ja ka sellise mulje tahtmatu jätmine pole hea.

- Uudiste kujundamisel saab määravaks internetirakendus, mille kaudu uudis avaldatakse. Tuleb järgida põhimõtet, et info antaks edasi selliselt, et seda oleks võimalikult kerge lugeda ja töödelda. See puudutab õiget lauseehitust ja veatut õigekirja, suur- ja väiketähe ortograafiat ning tavapäraseid viisakusreegleid. Uudised ei tohi olla ülemäära pikad.
- Info edastamisel tuleb alati arvestada ka kehtivate seadustega. Enne andmete (tekstide, fotode jms) edastamist kolmandatele isikutele või nende kaudu, tuleb muu hulgas kontrollida autoriõigust, üldist isikukaitseseadust (õigused omaenda pildile) ning asjassepuutuvaid seaduseid, mis käsitlevad isiklike ja äriandmete kaitset.

Internetiteenuste kasutamise käitumissoovitused tuleb avaldada intranetis või mõnel muul sobival viisil mis on kasutajatele kättesaadav.

Täiendav kontrollküsimus:

- Kas töötajatele on selgitatud, kuidas internetis käituda ja millist käitumist tuleb kindlasti vältida?

M 3.79w Sissejuhatus Bluetooth'i põhimõistetesse ja tööpõhimõtetesse

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator, infoturbespetsialist, IT-juht

Bluetooth on raadiolevil põhinev tehnoloogia, mis leiab rakendust ennekõike lähiümbruses. See meede annab ülevaate vastava andmeedastuse tehnilistest põhimõtetest ning selgitab mõisteid ja funktsioone, mille tundmine on Bluetooth'i rakendamiseks hädavajalik.

Andmeedastuse tehnilised põhimõtted

Bluetooth töötab 2,4-GHz-ISM-sagedusribal, 79 kanalil, sagedusalas 2400–2483,5 MHz. Kanalite vahemaa on 1 MHz, sagedusriba piirivahemikes on 2 ja 3,5 MHz vabaks jäetud, et vältida ligistikku töötavate süsteemide vastastikust segamist. Andmepakettide edastamist juhitakse ajapiludega (TDD, Time Division Duplex) ja sagedushüpitamisega (FHSS, Frequency Hopping Spread Spectrum). Selle eesmärgiks on vähendada tundlikkust kõikvõimalike tõrgete suhtes. Reeglina toimub sagedushüpe pärast iga andmepaketi edastust. Hüpitamise sagedus läbib lühikeste ajavahemike jooksul ühtlaselt kõik 79 kanalit ning kordub alles pärast mitme tunni möödumist. Bluetooth'i spetsifikatsiooni 1.2 rakendavates seadmetes kasutatakse adaptiivset sagedushüpitamise meetodit (AFH, Adaptive Frequency Hopping), mis piirab sagedushüpitamisega hõivatud kanalite töö segamata, st vabade sageduste peale. Sellega soovitakse tagada tõrkevaba paralleelkasutus teistele, samas sagedusalas töötavatele raadioleviteenustele, eriti WLAN-ile. Modulatsiooniprotseduurina kasutatakse sagedus- ehk faasimodulatsiooni. Selle käigus toimub sagedushüpitamine reeglina üks kord ühe mikrosekundi jooksul, mida kirjeldatakse sümbolikiirusena 1 megasümbol sekundi kohta. Saavutatav andmekiirus sõltub rakendatavast modulatsiooniprotseduurist, mis määrab ära ühe sümboli kohta edastatavate bittide arvu. Bluetooth eristab kolme protseduuri:

- esimene protseduur on binaarne sagedusmodulatsioon, mis kannab nimetust „Basic Rate“ ning mille puhul edastatakse üks bitt iga sümboli kohta. sellega saavutatakse andmekiirus 1 Mbit/s. See protseduur on alates versioonist 1.1 Bluetooth-spetsifikatsiooni kindel koostisosa. Kõik Bluetooth-lahendused peavad seda protseduuri toetama.

- Teine protseduur on neljaväärtuseline faasimodulatsioon, mille puhul edastatakse kaks bitti sümboli kohta. Selle protseduuriga saavutatakse andmekiiruseks 2 Mbit/s ning see kannab nimetust „Enhanced Data Rate“ (EDR). Protseduuri definitsioon kajastub Bluetooth'i versioonis 2.0 + EDR.

- Kolmas protseduur on kaheksaväärtuseline faasimodulatsioon, mille puhul edastatakse kolm bitti sümboli kohta. Andmekiiruseks, mille nimetus on samuti „Enhanced Data Rate“, saavutatakse siinjuures 3 Mbit/s. Ka selle protseduuri definitsiooni leiab Bluetooth'i versioonist 2.0 + EDR.

Erinevaid Bluetoothi spetsifikatsioone järgivate seadmete koostalitlusvõime tagatakse sellega, et iga andmepaketi ees olevad protokolliandmed saadetakse väl-

ja reeglina andmekiirusega „Basic Rate“. Ümberlülitus mõnele EDRi variandile toimub alles kasutajaandmete edastamisel, seda muidugi juhul, kui ka vastasseade seda toetab. Seda, kas seade toetab „Enhanced Data Rate“ andmekiirust või mitte, saab välja lugeda Bluetoothi spetsifikatsiooninumbrist, kus seda tähistatakse lühendiga „EDR“. Bluetooth kasutab andmeedastuse käigus reeglina kahte töörežiimi:

- asünkroonset ühendusevaba ülekannet (ACL, Asynchronous Connectionless Link),
- sünkroonset, ühendusele orienteeritud ülekannet (SCO, Synchronous Connection Oriented).

Asünkroonset ühendusevaba ülekannet rakendatakse peamiselt andmeedastuseks ning sünkroonset, ühendusele orienteeritud ülekannet ennekõike kõne edastamiseks. Asünkroonne edastus on WLAN-tüüpi võrkude edastus, sünkroonne vastab telefonivõrgu liinipõhisele edastusele. Asünkroonse andmeedastuse maksimaalne andmekiirus on 723 kbit/s ja 58 kbit/s (asümmeetriline) ning 434 kbit/s (sümmeetriline). EDRiga on võimalik seda väärtust kaheksaväärtuselise faasimodulatsiooniga maksimaalselt kolmekordistada.

Bluetooth’i liigitus leviulatuse põhjal

Bluetooth-jaamasid liigitatakse vastavalt nende saatjavõimsusele. Saatjate võimsus on siinkohal otseses seoses Bluetooth-raadiolainete levialaga. Eristatakse järgnevat kolme klassi:

Bluetoothi klass	max saatjavõimsus	max leviala
1. klass	100 millivatti	u 100 meeter
2. klass	2,5 millivatti	u 10 meeter
3. klass	1 millivatt	u 1 meeter

Tabel: Bluetooth’i liigitus saatjavõimsuse põhjal

Reaalne leviala sõltub muidugi paljudest ümbritsevat keskkonda puudutavatest tingimustest ning tabelis loetletud väärtused on saavutatavad ideaaljuhtudel. Leviala võivad pärssida välised tõkked nagu nt hoonete konstruktsioonid ja teised raadiolevi kasutavad tehnoloogiad, nt WLAN-id. Elektritarbimise piiramiseks on välja töötatud erinevad säästurežiimid (Sniff-, Park- ja Hold-Mode) ja saatjavõimsuse piirang (Power Control).

Rakendusprofiilid

Erinevate seadmete omavahelise koostalitlusvõime tagamiseks, ilma et neisse oleks tarvis paigaldada kõiki eksisteerivaid protokolle, on Bluetooth SIG välja töötanud nn rakendusprofiilid. Järgnevalt kirjeldame mõningaid sagedamini kasutatavaid profiile.

- Generic Access Profile (GAP): GAP on peamine profiil, mida kasutatakse erinevate tootjate Bluetooth-seadmete omavaheliseks kommunikatsiooniks. GAP kirjeldab Bluetooth-seadmete tuvastamiseks ja nendevahelise ühenduse loomiseks vajalikke protseduure rakenduse vaatevinklist. Rakendusprofiilide kasutamise eelduseks on GAP-s kirjeldatud protseduurid.

- Serial Port Profile: Bluetoothiga asendatakse tihti kahe seadme ühendamiseks kasutatavaid jadakaableid (RS-232). Kommunikatsiooni otstarbel kasutatakse sellistel juhtudel protokolli RFCOMM (Radio Frequency Communication). Serial Port Profile teeb rakendusprogrammid kättesaadavaks virtuaalsele jadaliidesele. Kuna Bluetooth-lahendused on teistest raadiosidetehnoloogiatest soodsamad, kasutatakse seda sageli kaablite asendamiseks tootvas tööstuses, kus kaablitele langeks osaks tavapärasest suurem koormus (pidev liigutamine, mustus jne).

- Headset Profile ja Handsfree Profile: need kaks profiili kirjeldavad funktsioone, mida läheb tarvis mobiiltelefonides seoses vabakäeseadete kasutamisega. Lisaks tavapärasele kõneedastusele mõlemas suunas mängib Handsfree Profile'i puhul rolli ka telefoni kaugjuhtimine.

- Advanced Audio Distribution Profile (A2DP): see profiil kirjeldab kõrgekvaliteediliste digitaalsete audioandmete edastamist käsitlevaid funktsioone. Rakenduseks on nt kõrgekvaliteediliste stereokõrvaklappide traadita ühendamine pleieritega.

- Human Interface Device Profile (HID Profile): see profiil kirjeldab protokolle ja funktsioone, mida läheb tarvis juhtmevabade klaviatuuride, hiirte ja muude kursoriseadmete ühendamiseks arvutiga. HID-Profile asendab vastavaid kaablipõhiseid Universal System Bus (USB) funktsioone.

- Dialup Network Profile (DUN Profile) ja Fax Profile: need profiilid kirjeldavad protokolle ja funktsioone, mida on tarvis modemite ja mobiiltelefonide juhtmevabaks ühendamiseks arvutiga, kui soovitakse luua sissevalimisega ühendusi kas andmete või fakside edastamiseks.

- File Transfer, Object Push ja Synchronization Profile: neid profiile kasutab Bluetooth failivahetuseks. Olulisemateks rakendusteks on kontaktide, kalendrisissekannete, ülesannete ja meilide sünkroniseerimine kaasaskantavate seadmete (Personal Information Manager, PIM) ja serverite vahel. Profiilid kasutavad OBEX protokolli (OBject Exchange).

- Audio/Video Remote Control Profile (AVRCP): see profiil kirjeldab protokolle ja funktsioone, mis hoolitsevad kaugjuhtimispuldi ja pleieri vahelise ühenduse eest.

- SIM Access Profile (SAP): See profiil toetab juurdepääsu SIM-kaardile. Sellega saab Bluetooth-seade luua ligipääsu andmetele, mis on salvestatud mõne teise seadme, enamasti mobiiltelefoni SIM-kaardile. Tüüpiliseks kasutusvaldkonnaks on statsionaarselt autodesse sisseehitatud autotelefonid, millel ei ole oma SIM-kaarti. Oma kaardi asemel loob see ühenduse autojuhi telefoniga ja logib ennast selle andmetega (ja selle kulul) mobiilivõrku.

Ühenduste loomine ja võrkude topoloogiad

Selleks, et iga Bluetooth-seade oleks üheselt kommunikatsioonipartnerina identifitseeritud, on igal seadmel 48 biti pikkune avalik ning ülemaailmselt kordumatu seadmeaadress, nn Bluetooth Device Address. Ühenduse loomise aluseks on funktsioonid Inquiry ja Paging. Inquiry funktsiooniga saab Bluetooth-seade tuvastada, kas tema levialas asub teisi seadmeid, eeldusel, et need seadmed on konfigureeritud nähtavaks (discoverable). Alates Bluetooth'i spetsifikatsioonist 2.1+ EDR toetavad seadmed ka laiendatud Inquiry -funktsiooni, mis tuvastab lisaks seadme aadressile veel ka seadme nime ja selle poolt toetatavad rakendusprofiilid. Paging -funktsiooniga saab kahe Bluetooth-seadme vahel ainult ühendusi luua. Seade, mis ühendust luua püüab, kannab nimetust Master ning teine seade on vastavalt Slave . Paging -funktsioonile järgnevad reeglina veel täiendavad sammud, enne kui kommunikatsioon võib edukalt toimima hakata. Paljud rakendusprofiilid loovad näiteks nn ühendusvõtme (Link Key) vahetamise teel kahe seadme vahel paarisühenduse. Seda protsessi tähistatakse GAP-s Generic Access Profile) lisaks ka mõistega Bonding. Lisaks kahe Bluetooth-seadme vahel toimivale punktist-punkti-ühendusele näeb Bluetooth'i spetsifikatsioon ette veel ka võimaluse kasutada punktist-mitmikupunkti-ühendust. Selle puhul on võimalik ühe Bluetooth'i Master -seadmega ühendada nn Piconet-võrku kuni 255 Slave -seadet. Ühe Piconet-tüüpi võrgu piirides saavad korraga Master-seadmega sideühenduses olla kuni seitse Slave- seadet. Kõik Piconet võrku kuuluvad seadmed lähtuvad Master -seadme kanalihüpitamissagedusest (Channel Hopping Sequence) ja ajamääratlusest. Bluetooth näeb ette isegi võimaluse, et seade võib olla korraga isegi mitme Piconet-tüüpi võrgu liige. Sellisel juhul tekib nn Scatternet . Scatternet 'ide moodustamiseks ja nende andmesideks läheb siiski tarvis täiendavaid protokolle, mille kohta on hetkel olemas vaid ideed, kuid puuduvad reaalsed lahendused.

Bluetooth'i turvamehhanismid

Järgnevalt selgitatakse mõningaid Bluetoothi olulisemaid turvamehhanisme.

Krüptograafilised turvamehhanismid

Kuna Bluetooth'i näol on tegemist raadiolevilahendusega, on alati oht, et võõrad, ilma volituseta Bluetooth'i toega seadmed võivad Bluetooth-sidet pealt kuulata või aktiivsete liikmetena ennast sidesse juurde lülitada. Bluetoothi spetsifikatsioonides ette nähtud krüptograafilised turvamehhanismid püüavad mõlemat nimetatud ohtu tõrjuda. Turvafunktsioonid on tööle rakendatud juba kiibi tasandil ja on Link -kihis võrdselt saadaval. Kõikide rakendatavate krüptograafiliste turvameetmete aluseks on ühenduste võtmed (Link Keys), mis lepitakse kahe Bluetooth-seadme vahel kokku paaristamisprotsessi käigus.

Paaristamine (Pairing) ja ühenduse võti

Kahe Bluetooth-seadme paaristamisprotsessi käigus koostatakse reeglina vaid nende kahe seadme ühendamiseks kasutatav 128 bitine kombinatsioonivõti (Combination Key), mis salvestatakse mõlemasse seadmesse tulevase kasutuse tarbeks ühenduse võtmena (Link Key, LK). Kombinatsioonivõtme koostamisel võetakse mõlemast seadmest nende seadmeaadressid ja mõlemast ka üks juhuslikult koostatud arv. Juhuslikkuse põhimõttel koostatud arvude turvaliseks edastamiseks kasutatakse lähtestamisvõtit, mis koosneb täiendavast (avalikust) juhuarvust, seadme aadressist ja PIN-koodist, mis on enamasti konfigureeritav. Selleks tuleb mõlemasse seadmesse sisestada PIN-koodid. PIN-koodi saab kasutaja kas ise konfigureerida võis siis on tegu muutumatu koodiga. Juhtudel, kus kahest seadmest ühes on muutumatu PIN-kood, tuleb see kood sisestada teise seadmesse. Kahte muutumatu PIN-koodiga seadet paaristada ei õnnestu.

Muutumatud PIN-koodid on nt peakomplektidel ja teistel sarnastel lihtsamatel seadmetel. Pika PIN-koodi sisestamisel kahte seadmesse võib kergesti tekkida vigu ning võib tekkida ka konflikt paaristamisfunktsioonile ette nähtud ajalise limiidiga. Selle probleemi vältimiseks nägi juba Bluetoothi spetsifikatsioon 2.0 + EDR ette ka alternatiivse võimaluse, mille korral toimub kahe seadme vaheline kokkuleppeprotsess automaatselt, kasutades nt Diffie-Hellmann- võtme kokkuleppimise protokolli. Protseduuri reaalne rakendus kaasnes aga alles spetsifikatsiooniga 2.1 + EDR, kandes nime Secure Simple Pairing. Lisaks kombinatsioonivõtmetele lubab see standard ühendusevõtmetele (Link Keys) ka täiendavaid võimalusi:

- seadmevõtmeid (Unit Keys) saab kasutada Link Key funktsioonides Seadmevõti koostatakse Bluetooth-seadme esmakordsel kasutamisel ning tavaliselt seda hiljem ei muudeta. Bluetooth'i spetsifikatsioonid ei soovita seadmevõtmeid enam kasutada, kuna need kujutavad endast turvariski.

- Mitmete seadmete vahel toimiva Bluetooth-seansi jaoks võib kokku leppida (ajutiste) Master -võtmete (Master Keys) kasutamise, juhul, kui Master soovib ühe ja sama krüpteerimisvõtmega kontakti astuda mitme erineva seadmega. Master- võtmeid kasutatakse vaid punktist-mitmikpunkti-ühenduste korral ning nende ülekannet Master -seadmetelt Slave-seadmetele turvatakse kehtivate ühendusvõtmetega (Link Keys).

Bluetoothi spetsifikatsioon eristab ajutisi ja poolpüsivaid ühendusevõtmeid. Ajutised ühendusevõtmed on teatud mõttes ühekordsed võtmed, st iga uue ühenduse jaoks koostatakse uus ühendusevõti (iga ühenduse kohta viiakse läbi paaristamine). Poolpüsivad ühendusevõtmed seevastu salvestatakse pärast sides osalevate Bluetooth-seadmete paaristamist ja autentimist nende püsimällu. Poolpüsivate ühendusevõtmete rakendamine võimaldab kaht seadet omavahel uuesti ühendada, ilma et oleks tarvis neid korduvalt autentida. Sellisel juhul ei pea kasutaja ühenduse loomise käigus enam uuesti PIN-koodi sisestama. Sellega vähenevad turvariskid, mis on seotud ühenduse loomisprotsessi pealtkuulamise ning võimalike nõrkade PIN-koodide äraarvamisega.

Secure Simple Pairing (SSP)

SSP-protseduur (Secure Simple Pairing) juurutati Bluetooth'i spetsifikatsiooniga 2.1+EDR. SSP tekitab ühenduse loomise protsessi käigus turvalise kanali, läbi mille seadmed oma ühendusevõtmes kokku lepivad. Selleks otstarbeks kasutatakse elliptiliste kõveratega Diffie-Hellman-protseduuri, mis on tuntud kui vähest arvutusvõimsust eeldav meetod. Vältimaks Diffie-Hellman-võtmekokkuleppe käigus esineda võivaid Man-in-the-Middle -tüüpi ründeid, leiab aset Bluetooth-seadmete vastastikune autentimine. Autentimisel saab SSP korral valida nelja erineva assotsieerimismudeli vahel:

- Numeric Comparison - Selle mudeli korral peab mõlemal seadmel olema ekraan, kuhu saab kuvada vähemalt kuuekohalist näitu ning võimalus, et

kasutaja saaks valida vastuste „ei“ ja „jah“ vahel. Sellise mudel kasutusnäiteks võiksid olla mobiiltelefon ja sülearvuti. Mõlemas seadmes kuvatakse autentimisprotsessi raames ühte ja sama kuuekohalist arvu. Kasutajad peavad arvu kokkulangemist kinnitama mõlemas seadmes, vastates „jah“.

- Just Work - See mudel on mõeldud seadmetele, mis ei suuda kuvada numbreid ning millel puuduvad võimalused andmete sisestamiseks, nagu see on nt tavaliste kõrvaklappide puhul. Just Works ei suuda pakkuda kaitset autentimise raames toime pandavate Man-in-the-Middle -rünnete vastu, kuid ühenduse loomise protsessi seevastu suudab see väga hästi kaitsta nt passiivse pealtkuulamise vastu, nagu ka kõik teised SSP mudelid.

- Out of Band (OOB) - See mudel põhineb lahendusel, mis loob enne Bluetooth'ide reaalset ühendamist kahe ühendamist ootava seadme vahel mõne muu meediumiga vastava kanali. Läbi vastava Out-of-Band -kanali saavad seadmed üksteist tuvastada, ilma et neid oleks tarvis Bluetoothi Inquiry -funktsiooniga otsida. Kanalit kasutatakse kõikidel juhtudel eesmärgiga, vahetada autentimiseks vajalikku infot. Kasutaja vaatevinklist sarnaneb Out of Band mudeliga Just Works , kuna kumbki ei eelda kasutaja sekkumist. Erinevus seisneb siiski selles, et teine, Bluetooth'ist sõltumatu kanal võimaldab tuvastada võtmevahetusprotsessi suhtes toimepandavaid Man-in-the-Middle -ründeid. Eelduseks on see, et kanali loomiseks tuleb kasutada tehnoloogiat, mis on sellist tüüpi rünnete suhtes immuunne. Out-of-Band -kanali loomiseks saab kasutada nt lähiväljasidet NFC (Near Field Communication). Eduka ühenduse loomiseks NFC-ga tuleb mõlemad seadmed paigutada teineteisele võimalikult lähedale ehk kuni mõne sentimeetri kaugusele.

- Passkey Entry - Selle lahenduse korral on ühel seadmel olemas ekraan, teisel seadmel on olemas nii ekraan kui ka võimalus arvude või märkide sisestamiseks. Seda mudelit saab kasutada nt Bluetooth-klaviatuuri ühendamiseks arvutiga. Ekraaniga varustatud seadmest tuleb autentimiseks välja lugeda kuuekohaline arv ning sisestada see teise seadmesse. Võimalik on ka variant, et mõlemasse seadmesse tuleb sisestada kuuekohaline Passkey .

- Juhtudel, kus Out-of-Band -kanali loomine ei ole võimalik, rakenduvad tavapärased funktsioonid Inquiry ja Paging . Sellistel juhtudel saab autentimine toimuda ainult kolme järgneva mudeliga: Numeric Comparison , Just Works ja Passkey Entry . Juhul kui Out-of-Band -kanali loomine on võimalik, rakendatakse seda esmalt sidepartnerite tuvastamiseks, asendades tavapärase Inquiry -funktsiooni. Seejärel saab autentimiseks kasutada üht neljast võimalikust assotsieerimismudelist.

Protsess nimega Secure Simple Pairing koosneb ühtekokku järgnevast viiest faasist:

- Faas nr 1: Avalike võtmete vahetamine - Iga Bluetooth-seade koostab võtmepaari, mis koosneb avalikust ja privaatvõtmest ning mõlemad seadmed edastavad enda avaliku võtme oma sidepartnerile. Edastamiseks kasutavad

nad reeglina Pairing-funktsiooni raames loodud Bluetooth-kanalit. See protsess tuleb igas seadmes läbi teha põhimõtteliselt ainult üks kord. Bluetooth'i spetsifikatsioon jätab tootjale vabaduse, mis lubab koostada ükskõik millal uue võtmepaari.

- Faas nr 2: Autentimine 1. astmes - Teises faasis kontrollitakse, kas seadmetesse nende sidepartneritelt laekunud avalikud võtmed pärinevad nende õigetelt sidepartneritelt. Selles faasis tuvastatakse Man-in-the-Middle - ründed. Selle tagamiseks kasutatakse kõigi kolme ehk Numeric Comparison , Passkey Entry ja Out of Band meetodi puhul erinevaid protokolle. Just Works kasutab sama protokolli nagu Numeric Comparison.

- Faas nr 3: Autentimine 2. astmes - Selles astmes leiab aset kinnitus, et autentimine ja sellega seotud Pairing-funktsioon on kulgenud edukalt. Selles faasis täidetakse oluline osa Out of Band assotsieerimismudelist. Juhul kahest seadmest ühel on võimalik passiivse kiibiga kasutada lähiväljasidet (NFC, Near Field Communication), saab see seade Out-of-Band -kanalis andmeid küll edastada, aga mitte vastu võtta. Selline seade ei saa seega mitte mingisugust infot selle kohta, kas autentimine läks korda või ebaõnnestus. Sellistes olukordades kontrollitakse Bluetooth-kanalis uuesti, kas autentimine ja paaristamine toimusid edukalt.

- Faas nr 4: arvutamine Link Key - Kahe seadme vahel vahetatud andmetest ja Diffie-Hellman-meetodiga koostatud sümmeetrilisest võtmest koostatakse krüptograafilise funktsiooniga vastav Link Key . Sellesse funktsiooni lisandub täiendav, vaid selleks otstarbeks koostatud juhuarvude paar, mis kindlustab selle, et Link Key koostataks alati teistsugune, ilma et Diffie-Hellman-võtmepaari tuleks iga ühenduse loomise käigus uuesti genereerida. Täiendavalt lisanduvad Link Key arvutamisse veel ka seadmete aadressid ja üks konstantne arvujada.

- Faas nr 5: Krüpteerimise läbiviimine - Lõpetuseks koostavad mõlemad seadmed sümmeetrilise Link Key protseduuriga krüpteerimisvõtme, mis on andmevoo krüpteerimise aluseks. Faas nr 2 toimub iga nelja võimaliku assotsieerimismudeli korral erinevalt. Kõik ülejäänud faasid on mudelist sõltumatud.

Turvalised käitusrežiimid

Bluetooth'i GAP (Generic Access Profile) näeb seadmetele ette neli turvarežiimi. Turvarežiimi nr 4 rakendatakse alates toodetest, mis vastavad Bluetooth'i spetsifikatsioonile 2.1 + EDR, millega juurutati paaristamisfunktsioon Secure Simple Pairing.

- Turvarežiim nr 1 (non-secure): Bluetooth-seade ei lülita omaalgatuslikult tööle mitte ühtki spetsiaalset turvamehhanismi, kuid reageerib teiste seadmete autentimispäringutele.

- Turvarežiim nr 2 (service level enforced security): Turvamehhanismide valikul ja kasutamisel on määravaks Bluetooth-seadme tüüp (trusted või non-trusted) ning rakendusetasandi teenus, st valiku määrav Bluetooth-profiil. Seade lülitab turvamehhanismid tööle alles siis, kui on saanud ühenduse loomise päringu.

- Turvarežiim nr 3 (link level enforced security): iga ühenduse loomine eeldab autentimisprotsessi läbimist. Edastatavate andmete krüpteerimist saab valida.

- Turvarežiim nr 4 (service level enforced security): üldjoontes sarnaneb see turvarežiim režiimile nr 2. Rakenduse tasandi teenus määrab, millist liiki Link Key' d on tarvis Secure Simple Pairing protsessi raames seadmete vahel vahetada. Turvarežiimis nr 4 eristatakse kolme atribuuti.

Bluetooth'i spetsifikatsioon 2.1+EDR nõuab, et kasutatakse turvarežiimi nr 4. Ühilduvuse tagamiseks vanemate Bluetooth-seadmetega võidakse kasutada ka turvarežiimi nr 2. Kasutatava turvarežiimi valib välja rakendus. Näide: SIM Access Profile'i spetsifikatsioon, st kõige kõrgemate turvanõuetega Bluetooth'i profiil nõuab alati nii autentimist kui ka krüpteerimist. Nende nõuete täitmiseks peavad seadmed kasutama kas turvarežiimi nr 2 või nr 3, kui need vastavad Bluetooth'i spetsifikatsioonile 2.0 + EDR või 1.x. Seadmed, mis vastavad spetsifikatsioonile 2.1+EDR või 3.0 +HS, peavad kasutama turvarežiimi nr 4. Lisaks turvarežiimidele sätestab GAP ka seda, kuidas on võimalik juhtida Bluetooth-seadmete käitumist ühenduste loomisel:

- Tuvastatavus: selle režiimiga juhitakse seda, kas seade vastab Inquiry funktsioonile või mitte? Lisaks mittetuvastamisrežiimile „non-discoverable mode“ (seade ei vasta Inquiry päringutele) ning üldisele tuvastamisrežiimile „general discoverable mode“ (seade vastab alati kõikidele Inquiry päringutele), on veel ette nähtud ka piiratud tuvastusrežiim „limited discoverable mode“, mille puhul muutub seade tuvastatavaks kas ainult teatud ajaks või teatud seadmeseisundi tagajärjel.

- Ühenduse loomise võimalus: see režiim juhib Bluetooth-seadmete võimet vastata ühenduse loomise päringutele Paging -funktsiooniga. Seade töötab kas ühendusvõimelises režiimis „connectable mode“ või ühendust vältivas režiimis „non-connectable mode“.

- Seadmete paarisühenduse võimalus: selle all peetakse silmas seadmete võimet paaristamisfunktsiooni käigus teineteist vastastikku autentida ja omavahel paarisvõtit (Link Key 'd) vahetada (bondable mode). Juhul kui seade töötab režiimil „non-bondable mode“, ei ole krüpteeritud andmeside jaoks paarisühendust luua võimalik. Vanemas Bluetoothi spetsifikatsioonis tähistati nimetatud funktsioone mõistega „pairable“.

Autentimine

Autentimiseks kasutatakse Challenge-Response -protseduuri, mis põhineb omakorda sümmeetrilisel šifreerimisprotseduuril. Reeglina kasutatakse vastastikust autentimist, st seade (Claimant) autendib ennast teise seadme (Verifier) ees. Juhtudel, kus mõlemad seadmed soovivad teineteist vastastikku autentida, korratakse autentimisprotseduuri vahetatud rollidega.

Krüpteerimine

Krüpteerimist saab valida juhul, kui kahest andmesides osalevast seadmest vähemalt üks on ennast teise suhtes autentinud. Krüpteerimissoovi võib esitada nii Master - kui ka Slave -funktsioonis töötav seade. Krüpteerimisprotseduur algatatakse siiski alati Master -seadme poolt ning pärast seda, kui Master -seade on vajalikud parameetrid Slave -seadmega kokku leppinud. Kokkuleppe saavutamiseks peavad seadmed esmalt jõudma ühisele arusaamale võtme pikkuse kohta. Seejärel käivitab Master -seade krüpteerimisprotseduuri, saates Slave -seadmele juhuslikkuse põhimõttel koostatud arvu. Krüpteerimisprotseduur võib aset leida kahes töörežiimis: punktist-punkti krüpteerimisrežiimis ja punktist-mitmikpunkti krüpteerimisrežiimis. Punktist-punkti krüpteerimisrežiimis tuleb autentimisprotokolli Authenticated Cipher Offset 'il täita Cipher Offset'i funktsioone. Punktist-mitmikpunkti krüpteerimisrežiimis kasutatakse Cipher Offset 'i funktsioonides seevastu Masterseadme seadmeaadressi. Lisaks tuleb enne krüpteerimisega alustamist ühendusevõti asendada Master -võtmega. Punktist-mitmikpunkti krüpteerimist kasutatakse nt Piconeti keskkonnas, kui Master -seade tahab üht ja sama sõnumit saata korraga mitmele Slave -seadmele (Multicast).

Bluetooth IEEE 802.11 WLAN vahendusel

Bluetooth'i spetsifikatsioonist 3.0+HS leiab alternatiivse raadiosidetehnoloogia kirjelduse, mis kannab nimetust Alternate MAC/PHY (AMP). WLANi füüsilist liidest kasutades suudab Bluetooth vastavalt standardile IEEE 802.11 võimaldada senisest suuremaid andmekiiruseid. Selleks otstarbeks täiendati L2CAP protokolli (Logical Link Control and Adaption Layer Protocol) funktsioone, mis võimaldavad valida raadiolevitehnoloogiate ja vastavate kontrollerite vahel. On olemas isegi funktsioonid, mis võimaldavad raadiolevitehnoloogiad vahetada ka töösolevate ühenduste korral. Mõiste APM, mis tähistab tehnoloogiaülest valikut, lubab oletada, et tuleviks lisandub Bluetooth'i jaoks ka veel teisi raadiolevisüsteeme. Spetsifikatsiooni tuumiku moodustab nn 802.11 Protocol Adaption Layer (802.11 PAL). Tegu on ühenduslüliga Bluetoothi Host-Controller-liidese (HCI) ja WLANi MAC-liidese vahel. 802.11 PAL suudab muuhulgas järgnevat:

- füüsikaliste ühenduste ülesehitamine vastavalt HCI nõuetele.
- WLAN-pakettidel põhinev andmeedastus.
- Interferentside vältimine WLANi ja Bluetooth'i vahel 2,4-GHz-ribas. PAL hoolitseb selle eest, et ühendusele orienteeritud andmeliiklust (SCO), mille toimimise eest hoolitseb Bluetooth Control, ei saadetaks WLANi kontrollerisse samaaegselt ühendusevabade andmepakettidega (ACL).

M 3.80 Bluetooth'i kasutamise teadlikkuse tõstmine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator, infoturbespetsialist, IT-juht

Juhtudel, kus organisatsioonis kasutatakse Bluetooth-liidestega seadmeid, peaksid ka IT eest vastutav töötaja ja turvaosakond ennast Bluetooth'i põhitõdedega kurssi viima. Ülevaate Bluetooth'i käsitlevatest põhimõistete kohta leiate M 3.79 Sissejuhatus Bluetooth'i põhimõistetesse ja tööpõhimõtetesse .

Administraatorite koolitus

Bluetooth-liidestega seadmete administraatoritel peaks lisaks teoreetilistele teadmistele olema kindlasti ka praktilised oskused. Administraatorite koolitus peaks hõlmama muuhulgas järgmisi valdkondi:

- Bluetoothi turbeaspektide ülevaade
- Bluetooth-seadmete tüüpilised ohud
- töörežiimid, ühenduste loomine, autentimine ja Bluetooth-andmeside turve
- Bluetoothi kasutamiseks sobilike turvamehhanismide valimine
- Bluetooth-seadmeosade konfigureerimine ja testimine
- turbe seisukohast olulised Bluetooth'i konfigureerimisparameetrid

Kasutajate teadlikkuse tõstmine

Ka Bluetooth-liidestega varustatud seadmete kasutajad peaksid teadma, kuidas Bluetooth-seadmeosad töötavad ning kuidas nendega turvaliselt ümber käia. Kasutajatele tuleb täpselt selgitada, mida tähendavad turvaseaded ning mille jaoks on need vajalikud. Lisaks tuleb kasutajaid informeerida ka ohtudest, mis kaasnevad juhtudel, kus kasutajad jätavad kas mugavusest või soovist saada vähem häirivaid veateateid turvaseaded kas tähelepanuta või koguni sisselülitamata. Bluetooth-seadmeosade ja nende turvaseadete korrektse kasutamise tagamiseks tuleb kasutajaid sihipäraselt teavitada. Bluetoothi kasutamispraktika kõige suuremaks kitsaskohaks on autentimis- ja krüpteerimisotstarbeliste PIN-koodide õige rakendamine. Paljud senised ründed on toimunud just kasutajate tüüpiliste harjumuste tõttu seoses PIN-koodide valimisega. Selle vastu aitab *Secure Simple Pairing*. Bluetoothi turvalist kasutamist võimaldab eriti *Numeric Comparison*, kuna see meetod ei eelda kasutajatelt enda valitud tugevate paroolide sisestamist. Bluetooth-andmesidet ei ole võimalik tehniliste lahendustega kohustuslikus korras turvata, st ka praeguste turbevõimaluste juures on ja jääb turbemeetmete rakendamine eeskätt siiski kasutaja enda mureks. Oluline on saavutada turvaline konfiguratsioon ja õppida seda tehnoloogiat mõistlikult kasutama. Koolituste teemad tuleb alati viia kooskõlla kohapealsete kasutusvaldkondadega. Siinkohal võib mõelda ka veebipõhiste interaktiivsete koolitusprogrammide kasutamisele intraneti keskkonnas. Lisaks Bluetooth'i turvamehhanismide koolitusele tuleks töötajatele selgitada ka organisatsioonis kehtivat Bluetooth'i turvapoliitikat.

Täiendavad kontrollküsimused:

- Kas administraatorid on Bluetooth-seadmeosadega töötamiseks, eriti nende turbega seotud aspektide osas, piisavalt ette valmistatud?
- Kas kasutajad on Bluetoothi turvamehhanismidega kursis?

M 3.81 Koolitamine terminaliserveri turvaliseks kasutamiseks

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: tehnilise osakonna juht, IT-juht

Terminaliserveri infrastruktuuri haldamine on administraatorite jaoks kompleksne. Ilma eelteadmisteta kasutajatele tuleb mõningaid punkte selgitada. Kõiki isikuid, kes töötavad terminaliserveri süsteemiga, tuleb koolitada. Eelkõige kehtib see administraatorite kohta.

Administraatorite koolituse sisu

Administraatorite jaoks vajatakse detailseid teadmisi kasutatavast rakendusserveritehnikast ja selle taga paiknevatest haldustööriistadest ja teenustest. Lisaks sellele on vaja kogemusi seoses operatsioonisüsteemiga, mis moodustab valitud lahenduse baasi. Terminaliserveri arhitektuur eristab üksteisest sisendit, väljundit ja programmiteostust. Tänu sellele abstraktsioonile on võimalik, et terminal ja server ei põhine ühel ja samal operatsioonisüsteemil. Sellisel juhul on vajalik vastutavate isikute poolne erialateadmine klientsüsteemide kohta. Vastasel juhul võib see viia väärkonfiguratsioonideni, mis võivad põhjustada turbetehnilisi probleeme. Seepärast on administraatorite koolitamine selles valdkonnas ja eriti terminaliserveri keskkonna turbemehhanismide suhtes olulise tähtsusega. Koolituse sisu tuleb vastavusse viia koolitatavate isikute kasutusalaga. Tekitamaks kasutajates teatud tundlikkust turvaliseks terminaliserveriga töötamiseks, peaks osa koolitusest kindlasti käsitlema turbe seisukohast olulisi teemasid. Teatud ajavahede tagant on soovitatav teadlikust turvalisuse suhtes värskendada *(Security Awareness Programm*) ja juhtida tähelepanu uutele või muudetud situatsioonidele, mehhanismidele või meetoditele. Selles raamistikus tuleks käsitleda institutsioonis kehtivaid infoturbedirektiive, värskendada terminaliserveri spetsiifilisi teemasid ning kõrvaldada ka kõik tekkinud arusaamatused.

Kasutajate koolituse sisu

Kasutajate koolitusele tuleb esitada teised nõudmised. Kasutajatele on esmase tähtsusega teadmised kaugkasutajaseansside eripära ja turbeaspektide kohta. Vead terminaliserveri kasutamisel võivad eelkõige tekkida siis, kui puuduvad varasemad kogemused terminaliserveri tehnoloogia kasutamisel. Nii võib iseseisva operatsioonisüsteemiga klientidel olla failirada või printeri nimetus teistsugune kui terminaliserveri kliendil. Lisaks võib segadust tekitada kliendist erinev eemal asuva kasutajaliidese käitumine. Isikuid, kes kasutavad terminaliserverit, tuleks informeerida vähemalt järgmistest punktidest:

- Kasutatavate turbemeetmete selgitamine, koos selgesõnalise keeluga neid deaktiveerida või neist mööda hiilida.
- Lubatud ligipääsuvõimalused ja lõppseadmed
- Rajad ja ajamiühendused failisalvestuseks ja printimiseks
- Lubatud informatsioonivahetusvõimalused kliendi operatsioonisüsteemi ja terminaliserveri vahel.
- Käitumine võrguühenduse katkemisel
- Juhised väljalogimiseks kasutusaja lõppedes
- Juhised kliendi lukustamiseks ruumist lahkudes

- Lubatud terminaliserverid, millega kasutajad ennast terminaltarkvara kasutades ühendada võivad
- Konfiguratsiooniandmete kasutamise keeld (näiteks .RDP või.ICA failid)
- Käitumisjuhised kahtlase käitumise korral (näiteks iseenesest liikuv hiire kursor).

Kui kasutada on kergesti mõistetav koolitusmaterjal terminaliserverite kohta, võib koolituse asemel anda käsu materjal ise läbi töötada. Eelduseks siinjuures on piisav aeg materjalide läbitöötamiseks.

Täiendavad kontrollküsimused:

- Kas kõiki kasutajaid ja eelkõige vastutavaid administraatoreid koolitati terminaliserveriga töötama ning kas koolitusmaterjal kohandati koolitatavate isikutega?
- Kas kajastati kõiki terminaliserveri turbemehhanismide käsitlemist?
- Kas kasutajaid koolitati kasutama eemal teostatavaid terminaliserveril paiknevaid rakendusi?

M 3.82 Kodukeskjaama turvalise kasutamise koolitus

Algatamise eest vastutavad: infoturbespetsialist, IT-juht, personalijuht

Rakendamise eest vastutavad: infoturbespetsialist, IT-juht

Kodukeskjaamaga seotud seadmete ja teenuste korrektseks ja eesmärgistatud kasutamiseks tuleb kasutajad selleks eelnevalt ette valmistada. Lisaks tuleb kasutajatele anda kõik keskjaama lõppseadmetega seotud vajalikud kasutusjuhendid, nagu nt telefoni kasutusjuhend. Vähene kasutuskindlus võib ohustada konfidentsiaalsust ja integreeritust, samas viia ka selleni, et kõigi olemasolevate võimaluste mittetundmise tõttu ei kasutata keskjaama plaanipäraselt. Seepärast on otstarbekas määrata vastavad kontaktisikud ja vastutajad. Oluline on nõuda kodukeskjaama kasutamise juhenditest ja reeglitest kinnipidamist. Lisaks peavad kõik (tavapärase) keskjaama kasutajad teadma tavaliste hoiatusmärkide, -toonide ja -sümbolite tähendust. Siia kuuluvad esmajoones:

- otsesele kõnelemisele viitav toon,
- ühendamise hoiatustoon,
- vabakäefunktsiooni märguanne,
- märguanne otseseks aktiveeritud kõnelemiseks,
- märguanne automaatseks tagasihelistamiseks ja
- kolme kõnelejaga kõne sisselülitamise märguanne.

Niipea, kui keegi kasutab keskjaamas ebatavalisi rakendusi, peavad hoiatustähised sellest üheselt märku andma. Mittelubatud rakenduste kasutamine (nt tunnistaja lülitumine kõnesse) võib ohustada infoturvet. Seepärast peaksid töötajad just neid hoiatustähiseid ja -toone hästi tundma. Nii näiteks on oluline ära tunda hoiatussignaal juhul, kui kahe isiku vahel peetavasse kõnesse lülitub kolmas isik. Igast keskjaama väärkasutuse kahtlusest tuleks teavitada vastavat vastutavat töötajat ning kahtluse korral kasutada kuni asjaolude selgumiseni võimalusel alternatiivseid sidekanaleid. Keskjaama manipuleerimiskahtluste korral tuleks pöörduda IT-turbespetsialisti või andmekaitse eest vastutava töötaja poole. Samuti on oluline töötajatele selgitada lõppseadmete kaitsmise vajadust paroolide ja PIN-idega, et takistada kõrvaliste isikute juurdepääsu lõppseadmetele salvestatud konfidentsiaalsele infole. Paljudel lõppseadmetel on tootja seadistatud standardparoolid, mille kasutaja peab enne seadme kasutuselevõttu ära muutma. Olenevalt töötajate kuuluvusest ühte või teise kasutajagruppi tuleb neid erinevalt koolitada. Administraatorid peaksid saama teistsuguseid teadmisi kui tavakasutajad. Igal juhul tuleb eesmärgistatult toetada koolitusel saadavate teadmiste turvalist kasutamist. Selleks sobivad muuhulgas sissekanded intranetti, infoüritused, telefonikasutamise flaierid, valvepersonali juhendamine või kontrollnimestikud administraatoritele. Taolised abimaterjalid tuleks koostada juba koolituse alguseks ja koolituse ajal neid eesmärgistatult kasutada. Lisaks tavapärastele koolitustele võiks mõelda ka koolitustele, kus kasutatakse internetipõhiseid interaktiivseid programme. Valdkonna uudistest võiks lisaks teada anda ka uudis- või ringkirjadega, samuti jagada töötajatele infot regulaarselt toimuvatel osakonna koosolekutel.

Täiendavad kontrollküsimused.

- Kas kodukeskjaama lõppseadmed on konfigureeritud nii, et kahtlaste ilmingute korral antakse sellest selgelt teada?
- Kas kõik töötajad tunnevad ära keskjaama hoiatustähised, -toonid ja -sümbolid?
- Kas töötajaid on teavitatud keskjaama kasutamisega kaasnevatest ohtudest?
- Kas kõigi keskjaama lõppseadmete kohta on olemas vastavad kasutusjuhendid?

M 3.83z Personaliga seotud turbefaktorite analüüs

Algatamise eest vastutavad: infoturbespetsialist, personalijuht

Rakendamise eest vastutavad: ülemused, personaliosakond

Institutsiooni infoturbe ühed olulisemad alustalad on kindlasti ka selle töötajad. Kogemused on näidanud, et ka kõige keerukamatest tehnilistest turbemeetmetest pole kasu, kui töötajad neid ei rakenda. Määrav on siinkohal see, et töötajad mõistaksid infoturbe olulisust institutsiooni ja selle tööprotsesside toimimises ning oskaksid kaitstava infoga õigesti ümber käia. Seetõttu tuleb institutsiooni jaoks turbemeetmeid valides lähtuda alati töötajatest. Arvesse tuleb võtta töötajate teadmisi, kuidas teabe ja IT-ga ümber käia, ja sellega seotud oskusi. Seetõttu oleks esmalt mõttekas analüüsida erinevaid tegureid, mis mõjutavad töötajate turbekäitumist. Seejärel saab välja selgitada valdkonnad, kus oleks võimalik turvet nii töötajate kui ka organisatsiooni juhtimise tasandil veelgi tõhusamaks muuta, nt suurendades töötajate infoturbeteadlikkust ja korraldades asjakohaseid koolitusi. Analüüsida tuleks alljärgnevaid valdkondi.

Turbekultuur

Terminiga „turbekultuur" tähistatakse institutsiooni ja selle töötajaskonna turbeseisukohti, -väärtusi ja -põhimõtteid. Turbekultuuri all mõistetakse ka seda, kui avatult või suletult tegeldakse institutsioonis infoturvet käsitlevate küsimustega. Näiteks on turvaintsidentide efektiivseks lahendamiseks tarvis, et institutsiooni töötajad usaldaksid üksteist ja suhtleks omavahel avatult, sest nii ei jää esmane teave turvaintsidendi kohta kuhugi toppama ja vastumeetmed võetakse võimalikult kiiresti.

- Kuidas käiakse ametiasutuses või ettevõttes üleüldiselt ümber tööprotsesse kajastava teabe ja riskidega? Kas institutsioon keskendub pigem tekkinud riskidele või püüab riske ennetada? Kas teave liigub edasi pigem takistusteta või edastatakse seda ainult piiratud mahus?
- Millised nõuded on kehtestatud täpsusele ja korrektsusele? Kas näiteks väiksemad vead tekstides on talutavad, sest tekstid läbivad niikuinii veel mitmeid kooskõlastusprotsesse? Kas sisestamisel tehtud üksainus viga võib põhjustada suurt kahju?
- Millised on käideldavusnõuded? Kas on palju lähestikku kuhjuvaid tähtaegasid? Kas päringute ja tööprotsesside töötlemiseks kuluvat aega on võimalik määrata paindlikult? Kas väiksem tähtaegade ületamine või tähtaegade muutmine on talutav või on sellel rasked tagajärjed?

Turbekultuuri mõjutab suuresti institutsiooni töövaldkond. Suurt turvalisust nõudvates töökeskkondades käiakse teabega kindlasti palju ettevaatlikumalt ümber kui teaduslikes uurimiskeskustes.

Teadmised ja oskused

- Kui hästi oskavad töötajad IT vahenditega ümber käia? Kas IT ja interneti kasutamine on töötajatele pigem segav lisakohustus, mis ei lase neil varasemaga võrreldes efektiivsemalt töötada, või ei suuda nad oma elu ja tööd ilma IT ja internetita enam ettegi kujutada?

- Millised on töötajate teadmised infoturbest ja andmekaitsest? Kui hästi oskavad töötajad kasutada IT-põhiseid turbemeetmeid, nt krüpteerimist? Kas töötajate teadmised on institutsiooni erinevates osakondades erinevad?
- Kuidas käiakse igapäevatöös ümber infoturvet ja andmekaitset puudutavate küsimustega? Milline on töötajate seisukoht küsimuses, kas infot on tarvis muudatuste või volitamata edasiandmise eest kaitsta? Kas töötajatele on antud võimalus kaasata infoturbega seotud ideid ja ettekujutusi turbeprotsessi?

Turvapoliitika

- Kas institutsiooni turvapoliitika sobib kokku reaalsete tööprotsesside ja turbekultuuriga? Kas turvapoliitikat on lihtne rakendada? Kas see on kasutajasõbralik ja kas see on kohandatud kasutusvaldkonnaga? Kas see takistab tööprotsesse? Kas see toetab soovitud käitumist?

Rakendused ja IT

- Kas olemasolevad IT-komponendid suudavad tagada tööprotsessides kajastuva teabe piisava kaitse, st kehtestatud turbenõuete täitmise?

Juhtkond

- Milline on juhtkonna seisukoht seoses infoturbega? Kas juhtkond on eeskujuks? Kas juhtkonnal on soove, kuidas turbeprotsesse paremaks muuta?

Kultuuritaustast tingitud eripärad

- Kaitstava infoga ümberkäimist ja üldiselt turbenõuete täitmist võib mõjutada ka töötajate kultuuritaust. Seetõttu tuleks analüüsida, kas infoturbenõuete täitmisel on mingeid regionaalseid või rahvuslikke eripärasid. Eelkõige tuleks välja selgitada, kas infoturbenõuete täitmisel esineb erinevusi institutsiooni valdkondade vahel. Ka näiteks ühe osakonna piires võivad tööprotsesside seisukohast olulise infoga ümberkäimisel kehtida üldnõuetest erinevad reeglid.

Muudatused

- Mis tahes suuremad muudatused tööprotsessides võivad mõjutada seda, kuidas töötajad andmete ja IT-ga ümber käivad ning oma tööd teevad. Muudatuste alla kuuluvad näiteks restruktureerimised, vallandamised, tööülesannete muutmine ja ülemuste vahetumine.

Kui analüüsi käigus peaks selguma, et töötajate käitumine ei ole turbe seisukohast mõistlik, tuleks otsida erinevaid lahendusi, kuidas olukorda parandada. Näiteks võib proovida käitumist muuta (vt B 1.13 Infoturbe teadlikkus ja -koolitus). Teisalt võib sageli olla hoopis lihtsam korraldada ümber turbenõuded ja tööprotsessid, sest töötajate käitumise muutmine on väga pikaajaline protsess.

Kontrollküsimus:

- Kas turvakontseptsioonis on võetud arvesse ka personaliga seotud turbefaktoreid, nt institutsiooni turbekultuuri?

M 3.84w Sissejuhatus Exchange'i süsteemidesse

Algatamise eest vastutab: IT-juht

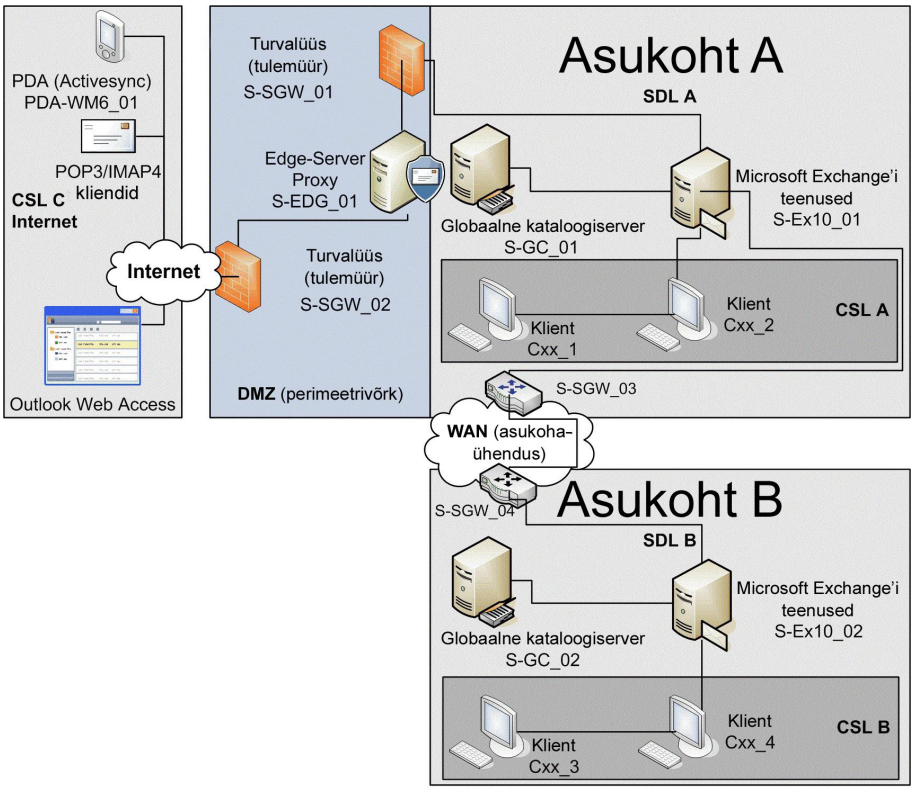
Rakendamise eest vastutavad: administraator, kasutaja, IT-juht

Rühmatarkvara keskendub rühmade koostööle, aitab kokku leppida ja muuta tähtaegasid ning tagab igapäevase kommunikatsiooni. Microsofti rühmatarkvaralahendus koosneb Microsoft Exchange Serverist ja Microsoft Outlookist. Exchange Server on haldussüsteem, millega hallatakse teateid ja toetatakse seeläbi workflow -funktsioone. Muu hulgas on see mõeldud keskmise suurusega ja suurtele ametiasutustele ja ettevõtetele teadete, nt meilide vahetamiseks nii institutsiooni sees kui ka väljaspool. Exchange'iga saab teateid hallata, kätte toimetada, filtreerida ja välja saata. Samuti võimaldab Exchange kasutada ja hallata selliseid tüüpilisi siderakendusi nagu uudistegrupid, kalender, tööülesannete loetelud ja Unified Messaging. Microsoft Outlook on Microsoft Office'i paketti kuuluv Groupware Client. Meilifunktsiooni kõrval pakub see ka mitmeid lisafunktsioone, nt kommunikatsiooni ja kiirsõnumivahetust, mis peaksid lihtsustama ametiasutuste ja ettevõtete tööprotsesse. Microsoft Exchange'i süsteemi all peetakse järgnevas tekstis silmas ühe Exchange'i serveri ja selle külge ühendatud Outlooki kliendi kombinatsiooni. Kirjeldamisel keskendutakse tüüpilistele ja väga sageli kasutatavatele installatsioonidele.

Exchange'i arhitektuur

Tüüpilise Microsoft Exchange'i süsteemi struktuur ja topoloogiline ülesehitus sõltuvad suurel määral selle kasutusvaldkonnast: alustades väikeste ettevõtete ja ametiasutustega, mis kasutavad ainult ühte serverit, kus pannakse tööle kõik funktsioonid, ning lõpetades suurte ettevõtete ja ametiasutustega, mis kasutavad tihti eraldi servereid nii erinevate funktsioonide kui ka harukontorite jaoks.

Erinevad eeltingimused kajastuvad ka Active Directory asukohapõhises topoloogias:
Microsoft Exchange'i süsteem integreerib endaga Microsofti kataloogiteenuse Active Directory (vt B 5.16 Active Directory). Integreerituse aste muutub iga uue Microsoft Exchange'i versiooniga aina suuremaks. Kataloogiteenust on võimalik laiali jaotada mitme (globaalse) kataloogiserveri peale.



Joonis 1. Tüüpiline Exchange'i süsteem

Microsoft Exchange'i süsteemi puhul on teenuse kasutamist võimaldav koht ja teenuse kasutamise koht erinevad: teenuse kasutamist võimaldav koht (Service Delivery Location – SDL) on füüsiline koht, kus paiknevad Microsoft Exchange'i server ja teised serverid. SDL peab võimaldama ka kõiki teisi teenuseid, mida Microsoft Exchange oma tööks vajab. Peale lokaalse võrguinfrastruktuuri (Local Area Network – LAN) kuuluvad asukohaga seotud vältimatute tegurite hulka ka DNS-iga (Domain Name System) nimeteisendus ja Active Directory domeenikontrolleritega või globaalsete kataloogiserverite kataloogiteenused. Joonisel 1 osutavad DNSteenust ning võimaldavad domeenikontrollerite ja kataloogiteenuste funktsioone globaalsed kataloogiserverid S-GC_01 ja S-GC_02. SDL-id võivad vajaduse korral sisaldada ka avalikke väliseid võrguühendusi ja demilitariseeritud tsoone (Demilitarized Zones – DMZ) või perimeetrivõrkusid. SDL võib koosneda ühest või ka mitmest alamvõrgust ning ühest või mitmest Active Directory asukohast. SDL langeb kokku kas hoonega või eraldatud keskkonnaga, milles on üldine Backbonevõrk.

SDL-id on üksteisest alati eraldatudWAN-ühendusega (Wide Area Network). Joonisel 1 on seda ühendust kujutatud asukohaühendusena: joonisel on asukoht A ja asukoht B (mõlema puhul on tegemist eraldi Exchange'iga) teineteisest täien-

dava perimeetrivõrguga lahutatud. SDL-i saab kasutada klientide rühm, mis on seotud asukohaga (Client Service Location – CSL). CSL võib paikneda SDL-iga samas või SDL-ist eraldatud kohas. CSL hõlmab sealjuures ka neid seadmeid, mis kasutavad läbi avaliku võrgu mõnda levinud klient-pöördusprotokolli (POP3, SMTP, IMAP).

Microsoft Exchange Server

Peale tavapärase meiliteenuse võimaldamise kuuluvad Microsoft Exchange'i süsteemi tüüpiliste funktsioonide hulka SDL-is ka kalendrisse sisestatud kohtumiste haldamine, samuti tööülesannete, kontaktide ja aadresside haldamine ning märkmete ja dokumentatsiooni talletamine. Neid funktsioone saab CLS-is paiknev klient kasutada Microsoft Outlooki või Outlook Web Accessiga. Ent Outlook Web Accessiga ei saa kasutada kõiki funktsioone. Enim levinud meilikliendid on piiratud, st oskavad kasutada ainult Exchange'i serveri meilifunktsioone. Meiliprotokollide täpsemad kirjeldused leiate soovi korral IETF-i (Internet Engineering Task Force) RFC-dokumentidest. Kaasaskantavate seadmete jaoks on Microsoft Exchange'i süsteemis olemas laialdaselt kasutatav ActiveSynci protokoll. Turvafunktsioone, mis puudutavad nt konfidentsiaalsust ja terviklust, võimaldab Exchange kasutada koos sertifikaadipõhise autentimise ja krüpteerimisega läbi PKI, S/MIME toega, Sender ID E-Maili autentimisprotokolli toega ning liini krüpteerimisega kliendi ja serveri vahel. Peale Anti-Spam-filtri saab hallata ka lubatud ja keelatud nimekirju (White-/Blacklists). Et tagada Microsoft Exchange'i koostalitlus teiste firmade toodetega, kasutatakse nn konnektoreid ja teisi transpordiprotokolle.

Microsoft Exchange'i süsteemide geograafilise määratluse kõrval arvestatakse ka füüsikaliste topoloogiatega. Kui on vaja kirjeldada võrku ning selle serveriteenuste ja -rollide jaotumist füüsikaliste elementide vahel, võib alustada SDL-idest, kus töötab ainult üks server, jätkata mitme serveriga ja lõpetada mitmete asukohtadega. Serveriteenused võivad seejuures olla nii tsentraliseeritud kui ka laiali jagatud.

Microsoft Outlook

Microsoft Outlook on rakendus, mida kasutatakse meilikliendi, suhtlustööriista ja isikliku infohaldurina (Personal Information Manager – PIM). Apple Mac OS-i jaoks on Microsoftil olemas sarnaste funktsioonidega rakendus Entourage. Koostöös Microsoft Exchange'i serveriga saab Outlook kasutada kõiki funktsioone: töökohtumiste märkmiku haldamist, koosolekute kokkuleppimist, osalejate, ressursside ja ruumide haldamist. Microsoft Outlook koondab kontaktandmebaaside ning märkmete ja tööülesannete haldamise ühte kasutajaliidesesse. Ent Outlooki saab siiski kasutada ka ilma Microsoft Exchange'i serverita, sest meilifunktsiooni jaoks on sellel olemas levinuimate internetiprotokollide tugi (POP3, IMAPv4 ja SMTP).

Väljaanded Standard ja Enterprise Edition

Microsoft Exchange'i süsteemide väljaanded ja versioonid võivad olla kohati väga erinevad. Microsoft Exchange Server tarnitakse kas väljaandes Standard või Enterprise Edition. Erinevad väljaanded (editions) sisaldavad erinevaid funktsioone, mille kasutamist juhitakse litsentsidega. Erinevused seisnevad peamiselt sel-

les, milline on salvestusgruppide arv, kas hallata saab ühte või mitut andmebaasi, milline on andmebasside maksimaalne suurus ja kõrgkäideldavuse funktsioonid, nt Clustering. Arhitektuuri- jt arendustööde tulemusel on olemas ka Microsoft Exchange Serveri ja Microsoft Office'i 64-bitised versioonid, mida saab käitada Microsofti 64-bitistes operatsioonisüsteemides. Seevastu 32-bitisest versioonist ei ole võimalik värskendusega (update) teha 64-bitist versiooni.

Järgmises näites esitatud konkreetsed väljaanded käivad versiooni 2010 kohta.

- Microsoft käitab ise ka arvutuskeskuseid, mis pakuvad Exchange Online'i teenust. Ent optimeerimisvõimalused on nii head, et on premises 'i installatsioone saab käitada ka koos Exchange Online'iga, ning see muudab eraldiseisvate Exchange'i koosluste integreerimise ja skaleerimise ülimalt paindlikuks, st tarvis on vaid Exchange Online'i teenused juurde osta. Märkimisväärsete tootefunktsioonide hulka kuulub ka meilide arhiveerimine. Sellega tagatakse andmete täiesti ühtlane kaitse ja meiliarhiivile esitatavate nõuete täitmine. See uus funktsioon ja Exchange'i intuitiivne kasutajaliides lihtsustavad meilide salvestamist ja nende hilisemat ülesleidmist ettevõttes või ametiasutuse suurest andmekooslusest.

Joonis 2. Microsoft Exchange Serveri andmemälu edasiarendused

Andmebaaside puhul, mis peavad haldama Microsoft Exchange Serveri andmemälu, on muudetud pöörduse protsesse. Varasemates versioonides kasutati kõvaketaste sisend-/väljundprotsessides kulukat random access -pöördust. Sellist liiki pöörduste rakendamiseks oli ilmtingimata tarvis kõrgkäideldavaid ja usaldusväärseid kõvakettakooslusi. Nüüdseks saab andmemälu jaoks kasutada ka soodsamaid SATA-kõvakettaid, sest andmete haldamiseks kasutatakse järjestikpöördust. Tervikluse ja käideldavuse tagamise eest hoolitseb Microsoft Exchange'i arhitektuuri tuum: katastroofijärgsed taastamisfunktsioonid ja kõrgkäideldavuse lahendused on CCR-i ja SCR-iga saadud kogemuste põhjal koondatud kokku üheks lahenduseks. Sellega seoses muutuvad LCR, SCC ja postkastiserverite klasterdamine üleliigseks. Serverirollide jaotuses aset leidnud paradigmavahetus on järjekindlalt edasi kandunud ka andmebaasidesse: üksikuid postkastiservereid on võimalik kokku liita andmebaaside käideldavusgruppideks (Data Availability Groups – DAG). Need võimaldavad nüüd andmeid taastada varasema füüsilise serveritasandi asemel loogilise postkasti tasandil. Selle tagajärjel pole enam salvestusrühmade kontseptsiooni tarvis, sest postkastiandmebaasid ei ole seotud Microsoft Windows Serveri süsteemiga ja neid saab hallata sõltumatult. Need uuendused ei puuduta avalike kaustade andmemälu.

Olulised muudatused on tehtud ka transportimis- ja marsruutimisfunktsioonides: workflow -kinnitamisprotsesse saab nüüd kasutada ka meilirakenduses. Teadete transportimiseks rakendatud Shadow Redundancy kontseptsioon takistab teadete kaotsiminekut marsruutimise käigus. Selleks jäetakse saatja serverisse väljasaadetavatest teadetest alles koopiad, mida hoitakse alles seni, kuni adressaat kinnitab teate kättesaamist. Marsruutimisfunktsioonid võimaldavad omavahel ühendada mitut Exchange'i on premise 'i installatsiooni (cross premises) ja Exchange Online'i teenuseid. Marsruutimist reguleerivad funktsioonid, nt teadete edasisaatmise tõkestamine ja teadete sisu krüpteerimine, pannakse tööle asjakohaste reeglitega (Rights Management Services – RMS). Reeglite asemel saab neid funktsioone rakendada ka Exchange'i organisatsiooni haldustasandil või SDL-iga. Hästi on välja arendatud ka veebikasutuse tugi, milleks on Outlook Web Access: veebilehitsejate, nt Safari ja Firefoxi tugi on õnnestunud saavutada Microsofti kesksete aktiivsisu ja laienduste järjekindla vältimisega. Lisaks on võimalik haldustegevusteks (Exchange Control Panel – ECP) kasutada juba OutlookWeb Accessi tuttavat veebiliidest. Töörollide ja ülesannete jaotamiseks erinevate administraatorite vahel ja kasutajate haldustegevuseks, nt uue töötaja kasutajakonto loomiseks või jaotusloendite haldamiseks, saab rakendada rollipõhist pääsukontrolli (Role Based Access Control – RBAC). Outlook Web Accessi kasutajaliidese funktsioonid lähtuvad varasemaga võrreldes palju rohkem otseselt Outlooki tarkvaraklientidest.

Microsoft Outlook 2010 on eelkäijatest kasutusmugavam ja võimaldab erinevaid kommunikatsioonivõimalusi paremini integreerida: kõneposti saabunud teated muudetakse loetavaks tekstiks ja kuvatakse sisse tulnud kirjade eelvaates. Teiste Office'i rakenduste kasutamiseks on Outlookiga nüüd integreeritud ribbon - kasutajaliides. Uus funktsioon MailTips tõkestab ebavajalike meilide väljasaatmist ja hoiatab võimalike eksimuste eest, mis on seotud meilide saatmisega suurtesse jaotusloenditesse või süsteemivälistele adressaatidele.

Funktsioonidega Clean Up ja Ignore saab sisse tulnud posti hulgas kasutada Threadiga loodud meilikokkuvõtteid ja ignoreerida soovimatuid vestlusi.

M 3.85w Sissejuhatus OpenLDAP-sse

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

OpenLDAP on kataloogiteenus, mis sai alguse Michigani Ülikooli LDAP-projektist. Projekti algne eesmärk oli välja töötada Directory Access Protocoli (DAP) vaste, mis põhineb kataloogiteenuse standardil X.500. DAP oli koostatud OSI-pinu jaoks, samas kui LDAP ehk Lightweight DAP ehk DAP n-ö kõhnem versioon kasutas TCP/IP-pinu. Tootenimes kasutatud omadussõna „ light ” viitab muu hulgas sellele, et LDAP ei suuda rakendada kõiki X.500 DAP funktsioone. Michigani Ülikool töötas välja ka serveri, mis selle protokolliga eriti hästi kokku sobib. Antud kontekstis räägitakse sel juhul LDAP-serverist, kuigi LDAP on tegelikult siisk ainult protokolli nimi. Sellised serverid on hierarhilise andmebaasi ülesehitusega ja toetavad väga hästi LDAP-protokolli tööd, võimaldades efektiivselt salvestada protokolliga liigutatavaid andmeid.

Open Source Software

OpenLDAP on avatud lähtekoodiga tarkvara (Open Source Software). OpenLDAP arendajad töötasid Michigani Ülikooli projektist pärit serveri kallal edasi ja nende töö tulemus, k.a lähtetekst, on internetis kõigile tasuta kättesaadav. OpenLDAP-d kasutatakse kõige enam Unixi ja Linuxi operatsioonisüsteemis, kuid seda saab sama edukalt kasutada ka Microsoft Windowsis ja z/OS-is. OpenLDAP arendajad panevad suurt rõhku sellele, et tarkvara vastaks LDAP-standardile. Kui jätta kõrvale erinevad teostused (nt Active Directory) või sihipäraselt mugandatud LDAP-protokolli vormid (nt Novell eDirectory), järgib OpenLDAP praegune värske versioon 3 (LDAPv3) LDAP-standardit väga rangelt. See väljendub muu hulgas selles, et OpenLDAP kasutab konfiguratsioonifailide jaoks ning failide importimiseks ja eksportimiseks LDIF-failivormingut (LDAP Data Interchange Format). Sel põhjusel nimetatakse OpenLDAP-d ka LDAPv3 referentsteostuseks. OpenLDAP toetab LDAPv3 kõrval ka LDAP-standardi versiooni 2 (LDAPv2), kuid selle puhul ei garanteerita standardi ranget järgimist. Esialgse X.500 DAP jaoks liidesed puuduvad. Põhimõtteliselt on andmevahetus ka LDAP-serverite ja X.500 DAP Directory System Agentite vahel küll võimalik, kuid OpenLDAP-s vastavaid funktsioone ei ole. OpenLDAP toetab iseseisvalt ka IPv4, samuti IPv6 protokolli ning lisaks Unixi internetiprotsessi kommunikatsiooni (IPC).

Tööpõhimõte

Nagu iga LDAP server, nii salvestab ka OpenLDAP server andmed eelmääratletud hierarhilisse puustruktuuri – Directory Information Treesse (DIT). Enim levinud struktuuri kirjelduse ja kasutatud terminid leiate meetmest M 1.1 Vastavus normidele ja eeskirjadele . OpenLDAP võimaldab oma andmeid kasutada klient-server-taristuga ja seansipõhiselt, st iga kataloogiteenuse kasutaja rakendab serveriga ühenduse loomiseks klientrakendusi. Kasutaja algatab klientprogrammi vahendusel erinevaid operatsioone, nagu otsing telefoniraamatu sissekannetes või enda parooli muutmine. Server vastab kasutaja algatatud tegevustele näiteks sellega, et edastab kasutajale otsitava sissekande või kinnitab, et parooli muutmine õnnestus. Kui selle käigus loetakse või muudetakse atribuutide väärtusi, tuleb eristada, kas tegu on tavaliste atribuutide või nn tegumiatribuutidega, mida OpenLDAP kasutab enda sisemiseks haldamiseks. Viimaste hulka kuuluvad ka näiteks objekti looja Dinstinguished Name (DN) ja ajatemplid, mis on olulised replikatsiooni puhul. Pärast seda, kui kasutaja on kõik operatsioonid ära teinud, ühendus serveriga lõpetatakse (unbind , seansi lõpetamiseks).

OpenLDAP arhitektuur

OpenLDAP LDAP server on slapd-server (Stand-alone LDAP Daemon). LDAP teekide kõrval, mida IT-süsteemil läheb tarvis LDAP funktsioonide kasutamiseks, on LDAP server OpenLDAP tarkvara üks olulisimaid komponente. slapd-server ei salvesta kataloogiteenuse andmeid ise, vaid kasutab selleks andmebaasi haldussüsteemi (DBMS), mis ei ole OpenLDAP tarkvara koosteosa.

Tagaprogrammid ja andmebaasid

Tagaprogramm (backend) on OpenLDAP osakomponent. slapd-server ei suhtle DBMS-iga otse, vaid kasutab selleks tagaprogrammi funktsioone. Tagaprogrammid kannavad nime „back-*". Suuresti üldistades võib eristada järgmisi tagaprogramme:

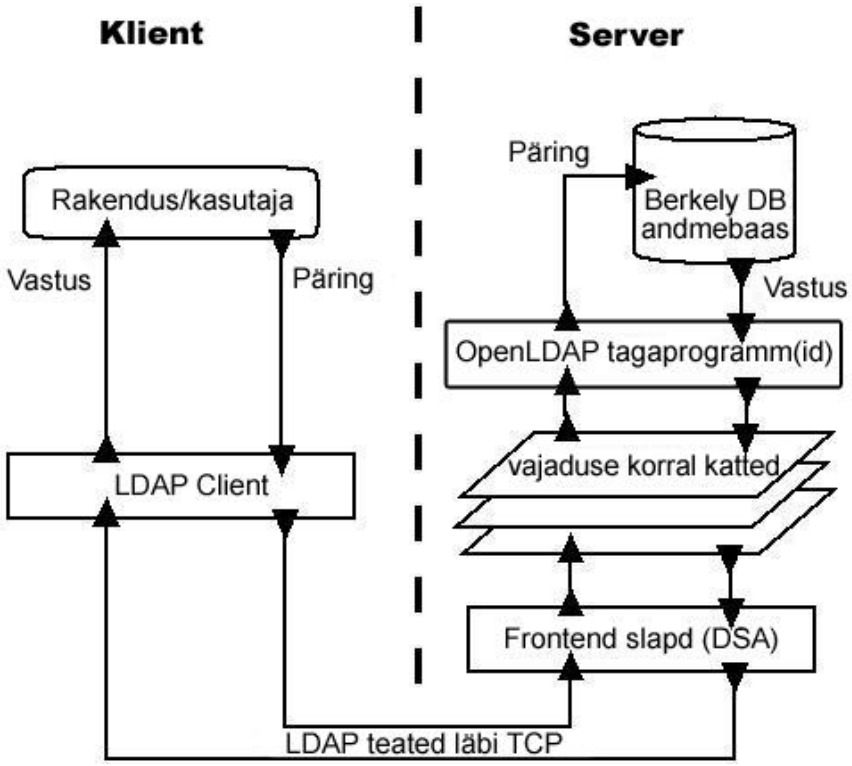
- tagaprogrammid, mis tegelevad andmete salvestamisega (nt „back-hdb" tagab juurdepääsu Berkeley DB-le);
- tagaprogrammid, mis teevad proksi-pöördusi teistesse andmemäludesse (nt „back-ldap" võimaldab kasutada teisi kataloogiteenuseid);
- tagaprogrammid, mis tegelevad andmete dünaamilise genereerimisega (nt „back-monitor" kuvab OpenLDAP praegust seisundit).

Nende põhimõtteliste erinevuste tundmine on oluline eelkõige komponentide planeerimisel, kuid konfigureerimise ja käitamise jaoks enam mitte. Andmebaasi all mõistetakse OpenLDAP puhul backend 'i, nt andmebaasi, millesse on salvestatud osakataloog „OU=BSI, O=Bund, C=DE" (Bund – riigiasutus). Ühe tagaprogrammi puhul saab enamasti korraga kasutada selle mitut instantsi, nt võib alamkataloogi „l=Bonn, OU=BSI, O=Bund, C=DE" jaoks eksisteerida oma andmebaas ja „l=Berliin, OU=BSI, O=Bund, C=DE" alamkataloogi jaoks oma. Mõne tagaprogrammi puhul on võimalik kasutada siiski ka ainult ühte instantsi, nt töö ajal on ainult üks „back monitor"-instants. Praktikas ja OpenLDAP-d kajastavas kirjanduses kasutatakse termineid „ backend " ja „andmebaas" väga sageli sünonüümidena. Siinkohal tuleks aga siiski arvestada, et andmebaase kui backend 'i andmekoosluse üht loogilist osa ei aetaks segamini DBMS-i kui eraldi tarkvarakomponendiga.

Kate (overlay)

Katteid kasutatakse tagaprogrammide töö mõjutamiseks juhtudel, kus muidu tuleks hakata backend 'i ennast kohandama või seda uuesti kirjutama. Katted lülitatakse slapd-serveri ette ning selle tulemusel saabuvad teated serverisse filtreeritult ja väljuvad sealt muudetud kujul. Suur osa katteid on mõeldud kasutamiseks andmebaasi tasandil, kuid sageli ei ole need piiratud ühe tagaprogrammi tüübiga.

OpenLDAP arhitektuurist annab ülevaate järgmine joonis.



OpenLDAP arhitektuur

Backend 'ide või andmebaaside ja katete kasutamiseks on vajalikud järgmised sammud: esmalt peavad tagaprogrammid (backends) ja katted (overlays) OpenLDAP-d tõlkides ka lähteteksti ära tõlkima (vt M 4.383 OpenLDAP turvaline installimine), seejärel tuleb tagaprogrammid ja katted konfiguratsiooniga ka käivitada (vt M 4.384 OpenLDAP turvaline konfiguratsioon). Tagaprogramme ja katteid on võimalik tõlkida ka dünaamiliste moodulitena.

Tarkvaratööriistad

Teekide ja slapd-serveri kõrval hõlmab OpenLDAP ka mitmeid tarkvaratööriistu (tools). Need tööriistad on jaotatud ldap*- ja slap*-tööriistadeks.

ldap*-tööriistad on järgmised:

- ldapadd: sissekannete tegemiseks kataloogiteenuses;
- ldapauth: enda autentimiseks kataloogiteenuses;
- ldapdelete: sissekannete eemaldamiseks kataloogiteenusest;
- ldapmodify: kataloogiteenuses olemas olevate sissekannete muutmiseks;
- ldapmodrdn: sissekande Distinguished Name'i (DN) muutmiseks;
- ldappasswd: isik-objekti parooli muutmiseks kataloogiteenuses;
- ldapsearch: sissekannete otsimiseks kataloogis;
- ldapwhoami: enda identiteedi avaldamiseks seansi raames.

ldap*-tööriistad kasutavad LDAP-protokolli ja teevad töötavas kataloogiteenuses oma tööoperatsioone alati klientidena. Sealjuures ei sõltu need slapd-serveri

tüübist, st need tööriistad suudavad suhelda teiste LDAP serveritega ja nende funktsioone saab kasutada ka teiste, st mitte ainult OpenLDAP tarkvaratööriistadega. Praktikas on väga levinud graafilised tarkvaratööriistad.

slap*-tööriistad on järgmised:

- slapacl: pääsuõiguste toimimise kontrollimiseks;
- ldapadd: sissekannete tegemiseks kataloogiteenuses;
- slapauth: SASL-identiteedi kontrollimiseks kataloogiteenuses;
- slapcat: kataloogiteenuse objektide eksportimiseks;
- slapdn: Distinguished Name'i (DN) usaldusväärsuse kontrollimiseks kataloogiteenuses;
- slapindex: atribuutide (uuesti) indekseerimiseks;
- slappasswd: parooli räsiväärtuse genereerimiseks;
- slaptest: konfiguratsiooni süntaksi kontrollimiseks.

slap*-tarkvaratööriistad ei kasuta LDAP-protokolli. Need tarkvaratööriistad töötavad slapd-serverist sõltumatult, st lähevad sellest mööda ja pöörduvad muu hulgas otse konfiguratsioonifailide või andmebaaside failide poole. slap*-tarkvaratööriistad on kohandatud slapd-serveri ja Berkeley DB jaoks. Range reeglina kehtib nõue, et slapd-server peab alati töötama siis, kui kasutatakse ldap*-tööriistu, ja see ei tohi mitte kunagi töötada ajal, mil kasutatakse slap*-tööriistu.

OpenLDAP kohandamine

OpenLDAP on detailselt dokumenteeritud. Sisemised seosed ja töötlemisetapid on lähteteksti kättesaadavuse tõttu teada. Seega on väga lihtne koostada ja rakendada haldamist lihtsustavaid abivahendeid, nt skripte. Samuti on võimalik muuta ja ise tõlkida lähteteksti. Lisaks on olemas geneeriline programmiliides (Application Programming Interface – API), mille kaudu saab OpenLDAP-d muutmata koostada ja rakendada isegi enda tagaprogramme ja katteid.

Lisateave

IT-etalonturbe kataloogides antakse OpenLDAP-st ainult lühike ülevaade ja keskendutakse ennekõike turbeaspektidele. Kõik muud aspektid, nt jõudlust parandavad seadistused, jäävad käsitlusest välja, olgugi et planeerimisel ja installimisel on need vägagi olulised. OpenLDAP kohta avaldatud erialakirjanduse kõrval on väga hea teabeallikas ka arendajate poolt tasuta kättesaadavaks tehtud dokumentatsioon. Põhidokument on OpenLDAP Administrator's Guide (http://www.openldap.org/doc), mis kuulub kasutatavate versioonide juurde. Korduma kippuvaid küsimusi (Frequently Asked Questions – FAQ) ja nende vastuseid kogutakse aadressil http://www.openldap.org/faq. Samas tuleb arvestada, et FAQ-de hulgas leidub ka palju sellist teavet, mis kehtib ainult OpenLDAP vanemate, mitte praegu kasutatavate versioonide kohta. Laialdast teavet seadistamise ja parameetrite kohta annavad nn juhendilehed (Manpages ehk Manual Pages). OpenLDAP juhendilehed installitakse tavaliselt koos OpenLDAP-ga, kuid need on kättesaadavad ka internetis (http://www.openldap.org/software/man.cgi). Samas jällegi pole kõikide tarkvarakomponentide, eriti uute tagaprogrammide ja katete jaoks veel piisavalt ja piisava kvaliteediga juhendilehti. Üksikasjalikuma teabe saamiseks ja probleemidele lahendusi otsides on soovitatav heita pilk ka selle projekti

avalikesse meililistidesse aadressil http://www.openldap.org/lists. Listiga on võimalik liituda, vanemad postitused on samal leheküljel ka arhiivis kättesaadavad.

M 3.86 OpenLDAP administraatorite koolitus

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator, IT-juht

OpenLDAP turvaline sisseseadmine ja käitamine eeldavad põhjalikke teadmisi OpenLDAP-st ja selle kontseptsioonidest. Seetõttu on administraatorite koolitamine nii OpenLDAP kui ka selle turbe valdkonnas kindlasti vältimatu.

Koolituse sisu

See, kui üksikasjalikult peab administraator erinevaid aspekte tundma, sõltub tema tegevusvaldkonnast. Üldteavet kataloogiteenuste kohta leiate M 1.1 Vastavus normidele ja eeskirjadele . OpenLDAP koolitused peaksid ilmtingimata sisaldama ja selgitama järgmisi punkte:

Põhitõed

- OpenLDAP ülesehituse ülevaade, tagaprogrammide (*backends*) ja katete (*overlays*) funktsioon
- Planeerimine, kasutuselevõtt ja konfiguratsioon („slapd.conf" ja „slapd-config")
- Algtõed, mis võimaldavad rakenduse installimist lähtetekstist.
- Teadmised Open Source Software'i erinevate andmeallikate kasutamise kohta
- LDAP Data Interchange Formats (LDIF)
- Objektiklassid ja operatsioonide atribuudid
- OpenLDAP tarkvaratööriistad ning ldap*- ja slap*-tarkvaratööriistade süstemaatilised erinevused

Skeemihaldus

- Skeemi muutmisega seotud probleemid ja nende tagajärjed
- Atribuutide piiramine skeemide sees katetega (*overlays*)
- Tavaliste atribuutide ja operatsiooniatribuutide eristamine

Replikeerimine

- OpenLDAP replikeerimise mehhanismid („refreshOnly" ja „refreshAndPersist")
- Otsingufiltrid ja operatsiooniatribuudid
- Delta-replikatsiooni ülevaade
- Multi Masteri ja Mirror Mode'i ülevaade seoses replikeerimiskonfliktidega

Andmevarundus

- OpenLDAP andmetest varukoopiate tegemisega kaasnevad probleemid
- Mõlema konfiguratsioonirežiimi konfiguratsiooni varundamine
- Andmete taastamine varukoopiatest slapadd'iga

Pääsuõiguste andmine

- Kataloogiteenuse objektide pääsuõiguste andmine
- Globaalsete ja andmebaasispetsiifiliste ACL-ide koostöö
- Võimalikud pääsuõigused

Autentimine

- *Hash* -algoritmid
- Kerberos
- SASL
- SSL/TLS-sertifikaadid

Täiendav kontrollküsimus:

- Kas administraatoreid on koolitatud, kuidas OpenLDAP-d ja selle turvamehhanisme kasutada?

M 3.87w Sissejuhatus Lotus Notesi/Dominosse

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: infoturbespetsialist, erialaspetsialist

Lotus Notesi/Domino platvormi terminid ja ajalooline areng

Lotus Notes/Domino kuulub IBM-i Lotuse tarkvaraperekonda. Alguses arendas seda küll Iris Associates, kuid rühmatarkvara platvormina sai see edukaks tooteks siiski Lotus Software Corporationi käes ning nüüdseks on see olnud juba aastakümneid domineeriv platvorm koostöö ja kommunikatsiooni vallas (Communication Platform). Microsoft Exchange'i ja Outlooki turuletulekuga sai Lotus Notes/Domino endale ärikasutajate hulgas tugevad konkurendid, mis on samuti haaranud enda kätte märkimisväärse turuosa. Ent leidub ka mitmeid avatud lähtekoodiga tooteid, millega saab samuti mõlema platvormi funktsioonid üles ehitada, kuid nendest on suur turuosa vaid üksikutel komponentidel (nt Apache Webserver). IBM tegi Workplace'i kontseptsiooniga (Lotus Notesiga paralleelne tootearendus, millel on Groupware'i ja Office'i funktsioonid ning mis kasutab tehnoloogilise baasina Open Office'it ja WebSphere'i platvormi) Lotuse tootevalikus suuri strateegilisi ja tehnilisi muudatusi ning määratles Lotus Notes Full Clienti kui universaalse kliendi. Universaalse kliendi kontseptsioon näeb ette, et erinevatele rakendustele juurdepääsuks kasutatakse ühtainsat klienti, ning see kehtestab põhimõtteliselt ka nõude, et suure arvu veebirakenduste jaoks tuleb kasutada ainult üht brauserit – see kõik kokku on uus peatükk valdkonnas Fat ehk Full Clients. Tootjad, kes pakuvad suurt hulka rakendusi, saavad ühe standardiseeritud (Full) Clienti rakendamisega võimaldada varasemast palju suuremat sünergiat, sest selliste klientidega saab kõikide rakenduste puhul kasutada brauseritega võrreldes palju laialdasemaid kliendifunktsioone. Lotus Notesi/Domino tootjakeskset maailma täiendab ja osaliselt ka asendab aina suurenev hulk avatud standardeid. Seetõttu rõhutab Lotus oma Notesi/Domino puhul aina rohkem selle staatust platvormina. Selle alla kuuluvad näiteks suur valik baasteenuseid, nagu e-post, kalender / töökohtumiste planeerija, veebikasutus, Presence ja Instant Messaging ning laialdane tugi sellele platvormile mõeldud rakenduste arendamisel. Baasteenuseid on võimalik ise edasi arendada ja neid seeläbi ettevõtte vajadustega kohandada, nt saab töötähtaegade planeerimisega liita funktsiooni, mis võtab arvesse ettevõtte ressursiandmebaasi. Samas on võimalik arendada ka enamjaolt sõltumatuid rakendusi, nt tegutsemismudeli rakendusi projektipõhise ärimudeli jaoks. Siia lisanduvad veel laialdased võimalused Lotus Notesi/Domino platvormi integreerimiseks teiste platvormidega, avatud standardid ja suur valik lisatooteid nii platvormi enda kui ka teistelt tootjatelt. Järgnevas tekstis kasutatakse terminit „Lotus Notesi/Domino platvorm" saadaolevate, st institutsioonis kasutusele võetud Lotus Notesi/Domino komponentide summa kohta, mis vastab mõnele määratletud redaktsioonile (release), ja termini „Lotus Notesi/Domino keskkond" all mõeldakse konkreetset instantsi (installatsiooni) koos määratletud funktsioonidega, nt institutsiooni sees Lotus Domino teenuste ja Notesi klientide baasil üles ehitatud intranetti. Ühes institutsioonis võidakse kasutada mitut Lotuse/Domino keskkonda, kuid välistatud ei ole ka mitu platvormi (kui paralleelselt kasutatakse Lotus Notesi/Domino mitut erinevat redaktsiooni).

Lotus Notesi/Domino platvorm sisaldab nii serveri- kui ka kliendikomponente, mis hoolitsevad kommunikatsiooni, andmetalletuse ja -töötluse eest.

Lotus Domino on serveri funktsioonides installeeritava baaskomponendi nimi ja Lotus Notes vastava kliendi baaskomponendi nimi. Põhimõtteliselt on võimalik ka-

sutada eraldi ka ainult serveri- või kliendikomponente. Enamasti sisaldab Lotus Notesi/Domino keskkond siiski mõlemaid, st nii serveri- kui ka kliendikomponente. Kui alguses oli Lotus Notes/Domino ainult tootja enda tehnoloogia jaoks mõeldud klassikaline klient-server-rakendus, mille puhul lähtuti Fat Clienti kontseptsioonist, siis nüüd on selles tehtud põhimõttelisi muudatusi. Praegu saab klientidena kasutada juba ka brauseripõhiseid kliente (iNotes) või kaasaskantavatele seadmetele, nt pihuarvutitele, nutitelefonidele jms mõeldud kliente. Nende kõrval pakutakse jätkuvalt ka nn klassikalist klienti tootjakeskses versioonis (Basic Client) ja Eclipse'i platvormi standardil põhinevat varianti (Standard või Full Client). Võõraste meiliklientide kasutamine POP3 ja IMAP-standarditega on samuti võimalik. Serveri poole pealt on suurendatud Domino serveriga pakutavate teenuste arvu ja tagatud on parem ühilduvus uute Web 2.0 internetistandarditega. Notesi/Domino kasutusvaldkond võib tänapäeval olla väga erinev. Näiteks võivad kõne alla tulla lihtsad meilisüsteemid koos neid täiendavate Workgroupi funktsioonidega, aga ka suur hulk võrku ühendatud teenuseid, mis on tööle pandud erinevate Domino serveritega ja mida käitatakse kas ettevõtte sisevõrgus, erinevates välisvõrkudes või internetiliidesena. Teenuseid on võimalik kasutada erinevat versiooni klientidega, kusjuures Notesi/Dominot saab kasutada integreeriva platvormina nii serverite kui ka klientide jaoks, nt SAP-süsteemide kasutamiseks. Sel põhjusel ei käsitleta siinkohal mitte intraneti ega ka interneti arhitektuuri, vaid keskendutakse Notesi/Domino keskkonnas töötavate teenuste turvamisele, võttes arvesse nende kasutusvaldkonda.

Lotus Notesi/Domino platvormi turbeareng

Lotus Notesi/Domino platvormi praegused redaktsioonid 8.0.x ja 8.5.x on oma funktsioonide ja neis rakendatava tehnoloogia poolest tugevalt edasi arenenud. See puudutab nii pakutavate Domino teenuste arvu ja nende funktsioone kui ka võimalike Domino klientide arvu ja funktsioone ning platvormi kasutusvaldkondi üldiselt. Notesi/Domino platvormi turbe tagamiseks on olulised eelkõige järgmised arengusuundumused:

- Elektroonilise kommunikatsiooni ja koostöö osatähtsus aina suureneb. Peaaegu kõikide tööprotsesside kaasamisega Lotus Notesi suurenevad ka selles kasutatavate teenuste, nt meiliteenuse ning sise- ja välisvõrgu juurdepääsu turbevajadused. See omakorda suurendab terve Lotus Notesi/Domino platvormi turbevajadust.
- Uuemate internetiteenuste, nt Presence'i ja Instant Messagingi potentsiaalsete ohtude kohta on seni veel väga vähe käsitlusi ja seetõttu ei osata nendega seotud IT-ohte endale veel piisavalt teadvustada.
- Platvormi arhitektuur muutub pidevalt. Puhta klient-server-arhitektuuri ja Fat Clienti põhjal on Lotus Notesi/Domino platvormi puhul praegu tegemist teenusepõhise platvormiga. See sisaldab erineval moel konfigureeritavaid serverikomponente ja teenuseid, keerukat arenduskeskkonda ja mitmeid kliente, mida saab kasutada kas kogu platvormi teenuste rakendamiseks või ainult valikuliselt, defineeritud teenustega (nt POP3 ja IMAP-kliendid meilide jaoks).
- Uued võimalused tootja enda edukate platvormide ühendamiseks ja erinevate standardite kasutamiseks (DB2 DBMS-i jaoks, Eclipse, WebSphere'i tehnoloogia, W3C standardid) muudavad tarkvara üha keerulisemaks, mis aga suurendab märkimisväärselt potentsiaalsete turvaaukude ohtu ja muu-

dab ülevaate saamise varasemast raskemaks: arhitektuuri, liideseid ja kriitilisi komponente on turbestrateegia alusel üha keerulisem hinnata.
- Uute tehnoloogiaplatvormide ühendamisega tekkinud koodibaaside heterogeensus (klientide jaoks Eclipse, serveri jaoks WebSphere'i tehnoloogia, Web 2.0 standardid) eeldab Lotus Notesi/Domino platvormi turbe tagamisel ka varasemast põhjalikumat oskusteavet erinevate tehnoloogiate kohta.

Notesi platvormi laialdased integreerimise võimalused, eriti Alloy komponent SAP integreerimiseks, aga ka teised serverite ja klientide integreerimise võimalused võivad teatud liiki kasutuse korral Lotus Notesi/Domino komponentide turbevajadust märkimisväärselt suurendada (nt klientide puhul, kui rakendatakse Universal Clienti strateegiat).

Universal Client

Olgugi et veebibrauserid on end rakenduste eeskomponentidena juba hästi tõestanud, on keerulisemate rakenduste jaoks olemas siiski ka veel nn klassikaline klient, mis võimaldab kasutada palju rohkem funktsioone kui n-ö tavaline veebibrauser. Browser Plugini või Ajaxi Frameworkiga saab brauseripõhise kliendi funktsioone küll laiendada, kuid komponentide turve ja hooldamine muutuvad seeläbi keerulisemaks. Suured tarkvaratootjad loodavad, et universaalse kliendi kontseptsioon lihtsustab ühelt poolt klassikaliste klientide arendamist pakutavate rakenduste tarbeks ning teisalt vähendab kliendi (tarkvara soetaja) juures tehtavate installimis- ja haldustööde mahtu. IBM-i senine enda välja arendatud Notes Client on väga tunnustatud toode, millega saab kasutada Lotus Notesi/Domino platvormi laialdast funktsioonivalikut, mistõttu kasutavad paljud kliendid seda ka Clienti funktsioonides enda tarkvaraarenduste tegemiseks Lotus Notesi/Domino keskkonnas. Eclipse Framework on Lotus Notesi/Domino platvormile nii arendustegevuse raamistik kui ka Runtime'i raamistik Full Clienti jaoks. Sellel raamistikul on IBM-i tugi ning kuna tegemist on vaba platvormiga, aktsepteerib see laialdaselt ka Javat. Notes Clienti kohandamisega Eclipse'i platvormi jaoks versioonis Notes 8 (Standard ehk Full Client) ja Eclipse'i baasil loodud Lotus Notesi/Domino arenduskeskkonna Domino Designer kasutuselevõtuga on IBM loonud kõik eeldused selleks, et Notes Client kui universaalne klient sobiks peale enda tooteperekonna ka Java baasil loodud rakendustele. Universaalse kliendi mõju infoturbele võib olla ütlemata suur, seepärast tuleb enne päris sissejuhatuseni jõudmist esmalt tutvuda kontseptsioonidega. Eriti tuleks võtta arvesse järgmisi aspekte:

- Erinevate rakenduste liigitamine turbeklassidesse muutub universaalset klienti rakendades lihtsamaks, sest kliendi turvamehhanismide puhul piisab nende ühekordsest hindamisest.
- Klientide turbevajadus suureneb klientprogrammi kasutavate rakenduste maksimaalse arvu suurenemise ja kumulatsiooni tõttu ning see mõjutab nii käideldavust, konfidentsiaalsust kui ka terviklust.
- Kuna Lotus Notes Client muutub struktuurilt üha keerukamaks, on ka selle turbe tagamine aina raskem. Turvet mõjutab ka asjaolu, et Full Client pärineb arenduskeskkonnast, mille kontseptsioon on palju avatum (ja seetõttu ka kergemini rünnatav) kui puhtalt ühe tootja rakenduste jaoks mõeldud klientide, nt Basic Clienti puhul.

Rakenduste integreerimine Lotus Notesi/Dominoga

Tootja ise määratleb Lotus Notesi/Domino platvormi aina enam kui rakenduste integreerimiseks loodud platvormi. Tehniliselt lahendatakse see avatud standardeid kasutavate liidestega ja tootjapõhise Lotuse tehnoloogia rakendamisega WebSphere'i platvormi ja Eclipse'i raamistiku abil.

Rakenduste integreerimine Lotus Notes Clientitega

Full Clienti kontseptsioon ja Lotus Notesi klientide rakendamine universaalse kliendina pakub lisaeelisena võimalust integreerida rakendusi kliendis (kasutades nt Web Servicesi lahendust). Rakenduste integreerimine kliendis on sageli lihtsam ja kiirem kui serveris, sest integreeritava rakenduse tööprotsessidesse ei ole kas üldse tarvis sekkuda või tuleb seda teha väga vähe.

Rakenduste integreerimine Lotus Domino serveriga

Serveri pakutavate integreerimisvõimaluste tõttu, nt DB2 andmebaaside ühendamine Domino Application Serveriga või Lotus Enterprise Integrator for Dominoga (täiendav litsentseeritud toode tootevalikust Lotus Extended Products) võib Lotus Notesi/Domino platvormi pidada alternatiiviks tootele, mida rakendusetootjad on rakenduste integreerimiseks loonud. Koostöös SAP-ga väljaarendatud tooted (nt Alloy) võimaldavad Lotus Notes Clientil teha pöördusi SAP-süsteemidesse ja tugevdavad nii selle positsiooni universaalse kliendina, seejuures Domino Server ja SAP Application Server suhtlevad omavahel vastavate pluginatega. Samamoodi nagu universaalse kliendi puhul, suureneb juhtudel, kus rakenduste integreerimiseks kasutatakse Lotus Notesi/Domino platvormi, nii kliendipoolsete Notesi komponentide kui ka integreerimiseks serveris kasutatud Domino komponentide turbevajadus. Selle tagajärjel võivad vajalikud turbemeetmed osutuda palju keerukamaks kui siis, kui kasutatakse üksnes Lotus Notesi/Domino funktsioone ja Lotus Notesi/Domino platvormi jaoks koostatud enda tarkvaraarendusi.

M 3.88 Lotus Notesi/Domino sihtrühmade koolitused

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: infoturbespetsialist

Lotus Notes/Domino on ülimalt kompleksne platvorm. Olenevalt ettevõttes või ametiasutuses rakendatava Lotus Notesi/Domino keskkonna (või keskkondade) suurusest ja keerukusest ning rakendatud funktsioonide ja teenuste arvust eeldab selle käitamine ka suuri teadmisi nii Lotus Notesi/Domino käitamise eest vastutavatelt töötajatelt kui ka selle kasutajatelt. Seetõttu tuleb korraldada sobivaid, st sihtrühmade vajadustest lähtuvaid koolitusi, mis tagaksid piisava kompetentsuse platvormi arhitektuuri ja turbearhitektuuri valdkonnas, õpetaksid seda õigesti konfigureerima ja pöörama tähelepanu käitamise eripäradele ning edastaksid vajaduse korral teavet Lotus Notesi/Domino platvormi rakenduste arendamise kohta ja rakenduste integreerimise kohta Lotus Notesi/Domino platvormiga. Järgnevalt on esitatud Lotus Notesi/Domino koolituste põhiteemad sihtrühmade kaupa:

- juhttöötajad (koolituse sisu: ülevaatekoolitus);
- infoturbehaldus (koolituse sisu: Lotus Notesi/Domino turbearhitektuuri ja turvamehhanismide eripära);
- administraatorid (koolituse sisu: Lotus Notesi/Domino arhitektuuri, käitamise, parameetrite ning andmevarunduse ja andmete taastamise põhitõed);
- süsteemi- ja tarkvaraarhitektid, süsteemi integreerijad (koolituse sisu: Lotus Notesi/Domino keskkonna arhitektuurid ja Lotus Notesi/Domino liidesed);
- arendusjuhid, tarkvaraarendajad (koolituse sisu: Lotus Notesi/Domino spetsiifilised arendustööriistad (*designers*) ja Lotus Notesi/Domino keskkonnas rakenduste arendamisel häid tulemusi andnud protseduurid nii tootjakeskse Notesi kui ka Eclipse'i baasil arenduste jaoks);
- Lotus Notesi/Domino kasutajate üldkoolitus (koolituse sisu: uute Lotus Notesi versioonide muudatused, tootlikkust suurendavad koolitused, kasutajate turberolli selgitamine).

Täiendav kontrollküsimus:

- Kas Lotus Notesi/Domino jaoks on määratud kindlaks erinevate sihtrühmade vajadusi arvestavad koolitused ning kas neid koolitusi planeeritakse ja korraldatakse?

M 3.89 Logimisprotsessi haldamise koolitus

Algatamise eest vastutavad: infoturbespetsialist, ülemused
Rakendamise eest vastutavad: ülemused, infoturbespetsialist
Kõikide logimisprotsessi funktsioonide ja omaduste optimaalseks kasutamiseks on oluline, et administraatorid saaksid asjakohase koolituse. Koolitustel tuleks käsitleda logiserveri komponentide juurutamist, käitamist ja haldamist. Siia kuulub ka asutuses või ettevõttes logimiseks rakendatavate erinevate toodete tootjaspetsiifiliste aspektide tutvustamine.

Operatsioonisüsteemi üldise turvalisuse kõrval, mida kirjeldatakse näiteks moodulis B 3.102 Server Unixi all , on olulised ka järgmised punktid:

- logiserveri konfigureerimine ja installimine;
- administreerimise põhitõed ja kontseptsioonid;
- juurutamist, käitamist, hooldust ja veaotsingut võimaldavate käskude tundmine;
- andmekaitseaspektid (vt M 2.110 Andmeprivaatsuse suunised logimisprotseduurides).

Logifailide hoolika analüüsi tagamiseks tuleks koolitustel edastada ka teavet võimalike ründestsenaariumite kohta. Samuti oleks mõttekas käsitleda Intrusion Detectioni / Intrusion Preventioni (IDS/IPS) valdkonna põhitõdesid. Lisaks tuleks sellistel koolitustel käsitleda tsentraalse logiserveri rakendamist ja andmekaitseaspekte. Koolitusmeetmete eelarvet tuleks hakata planeerima ja administraatorite koolituskava koostama juba IT-komponentide soetamisel.

Kontrollküsimused:

- Kas tsentraalse logimise jaoks on välja töötatud koolituste kontseptsioon?
- Kas administraatoreid koolitatakse piisavalt, kuidas logiserveri komponente juurutada ja käitada, ning kas seda tehakse ka tsentraalse logiserveri rakendamisel?

M 3.90w Tsentraalse logimise põhitõed

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

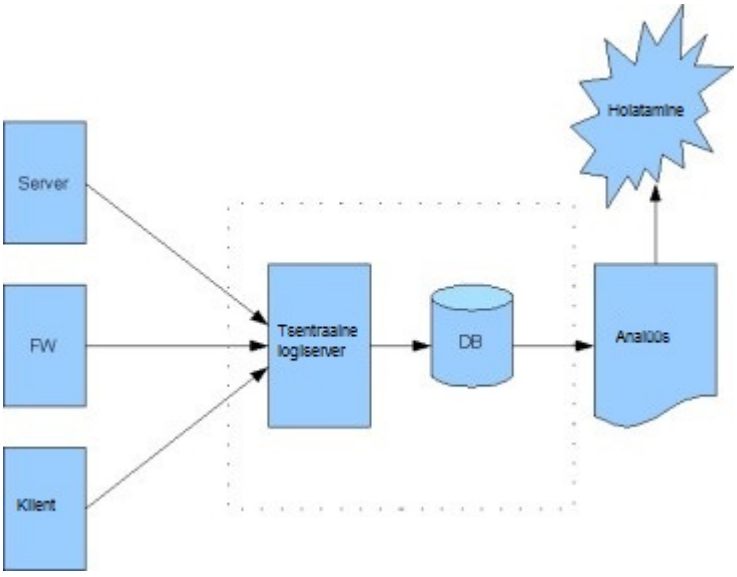
Suurt osa infokooslusse kuuluvatest IT-süsteemidest on võimalik konfigureerida selliselt, et need koostaksid erinevate sündmuste, nt failidele tehtud pöörduste kohta logiandmeid. Logiandmed sisaldavad olulist teavet, mis võib aidata tuvastada nii riist- kui ka tarkvaraprobleeme ning aidata välja selgitada nende asukohta. Lisaks kasutatakse logiandmeid turvaprobleemide ja rünnete tuvastamiseks. Infokooslusest tervikliku ülevaate saamiseks võib kasutada tsentraalselt töötavat logiserverit, mis koondab erinevad logiandmed kokku, analüüsib ja valvab neid.

Logiandmete ülesehitus

Iga logifail sisaldab alati kajastatud sündmuste kõrval ka kuupäeva ja kellaaega. Olenevalt logifaili koostavast süsteemist võib nende andmete struktuur olla erinev. Kellaaeg ja kuupäev on tsentraalse logimise jaoks väga olulised (vt M 4.227 Lokaalse NTP -serveri kasutamine aja sünkroniseerimiseks).

Tsentraliseerimine

Ülevaatlikkuse suurendamiseks ja logitud andmete töötluse lihtsustamiseks saadetakse kõikide logimisprotsessi kaasatud komponentide logiandmed sageli läbi turvalise kanali mõnda tsentraalsesse serverisse. Kui kasutatakse tsentraalset logiserverit, peab selles olema piisavalt mäluruumi, et kogu infokoosluse suure andmehulgaga toime tulla.



Joonis. Tsentraalse logimise põhimõtteline ülesehitus

Serverite ja võrgukomponentide seisundi-, vea-, hoiatusteadete ja teiste teadete edastamiseks logiserverisse võib kasutada näiteks syslogi. syslog tähistab ühelt poolt protokolli, kuid teisalt ka programmi, millega saab genereerida, vastu võtta, edasi saata ja salvestada sündmusi kajastavaid teateid. syslog-teated edastatakse loetava teksti kujul. Logiandmete saatmiseks krüpteeritult tuleb võrgus kasutada tunneldamist SSL-i või SSH-ga. Logimisel ei ole ilmtingimata tarvis koguda ega

ka hiljem analüüsida kõiki võimalikke logiteateid. Erinevad logifailid võivad sageli sisaldada identset teavet ja seetõttu kajastavad need lõppkokkuvõttes ikkagi ainult üht konkreetset sündmust, mille põhjal järeldusi teha. Et vältida logiandmete kuhjumist, kogutakse liiasusega andmed kokku üheks andmepaketiks (aggregation). Sellise liitmisprotsessi muudab raskeks asjaolu, et erinevad andmevormingud, milles logiandmeid kogutakse, tuleb esmalt ilmtingimata ühtlustada.

Normeerimine

Kokkukogutud erinevad teated tuleb hilisema analüüsi tarbeks viia ühte andmevormingusse (normeerida), sest vormingu ja edastusprotokolli jaoks puudub ühtne standard. Normeerimisega on võimalik logide erinevaid andmevorminguid, nt syslog, Microsoft Eventlog, SNMP, Netflow ja IPFIX, üksteise suhtes kohandada ja seejärel koos analüüsida. Normeerida saab nt lihtsate skriptidega, kuid selleks on olemas ka komplekssseid rakendusi.

Kokkukogumine (aggregation)

Ettevalmistuse järgmine samm on kokkukogumine. Selles etapis kogutakse identse sisuga logiteated kokku üheks andmepaketiks. Üks ja sama süsteem võib väga sageli üksteise järel genereerida mitmeid identseid logiteateid, mis tähendab, et nendele teadetele järgnevates teadetes muutub uue teabe hulk järjest väiksemaks. Seetõttu kaasatakse andmetöötlusesse ainult esimene logifail. Siiski peab peale esimese teate kajastuma info hulgas ka see, kui palju tekkis selle järel liiasusega teateid, et oleks võimalik kindlaks teha selliste identsete teadete tekkimise sagedus.

Filtreerimine

Normeerimise ja kokkukogumise kõrval tuleb tsentraalse logimise mõistlikuks kasutamiseks rakendada ka filtreerimisfunktsiooni. Filtreerimisega saab logiandmete analüüsimisest juba võimalikult varajases etapis välja arvata vastava kasutusvaldkonna jaoks ebaolulised andmed. Keskenduda tuleks ennekõike turbe tagamiseks oluliste IT-süsteemide logiandmetele. Alles seejärel tuleks ette võtta logiandmed, mis kajastavad rakenduste nõuetekohast kasutamist. Seevastu käideldavuse puhul on olulised just nimelt regulaarselt koostatavad ja süsteemide käitamist kajastavad seireandmed. Siia alla kuuluvad näiteks süsteemide käideldavus võrgus ja operatsioonisüsteemide veateated, mis võivad viidata probleemidele.

Analüüsimine

Logiandmete analüüsimise eesmärk on tuvastada kiiresti IT-süsteemide käitamisel tekkinud probleemid ja võimalikud ründed. Selleks peab komponentide seire toimima reaalajas. Analüüs ei tuvasta mitte ainult turbega seotud sündmusi ja vigu, vaid annab ka infot hetkekoormuse kohta. Logiandmete analüüsimisel tuleks tagada, et selle tulemused oleksid selgesti mõistetavad ja kajastuksid piisava võimsusega kasutajaliideses ning et süsteemiga saaks koostada ka aruandeid. Paljud süsteemid tuvastavad sündmusi sageli automaatselt, kuid seda, kas tegemist on tõepoolest ründega või mitte, peaks kinnitama administraator. Selleks peavad administraatorid olema piisavalt koolitatud ja nende tööd peaksid toetama mõistlikud analüüsisüsteemid.

Hoiatamine

Kogutud logiandmed võivad toetada IT-hoiatussüsteemi tööd tööprotsesside ja andmevoogude seire valdkonnas. Olulisi sündmusi kajastava hoiatuse puhul tuleks kasutada korraga mitut teavituskanalit, nt meili ja SMS-i. Et hoiatussüsteemi oleks võimalik mõistlikult kasutada, ei tohi hoiatavate teadete hulk paisuda liiga

suureks. Siinkohal on oluline lävendiväärtuste realistlik seadistus, mis arvestaks infokoosluse eripäradega.

Arhiveerimine

Logiandmete salvestamisel pikaks ajaks tuleb kontrollida, millised on seadustest ja lepingutest tulenevad säilitustähtajad. Sündmuste tagamaade väljaselgitamiseks võib olla andmetele kehtestatud minimaalne säilitusaeg, andmekaitsenõuete tõttu võib aga kehtida ka andmete kustutamise kohustus (vt M 2.110 Andmeprivaatsuse suunised logimisprotseduurides).

M 3.92w Salvestisüsteemide kasutamise põhiterminid

Algatamise eest vastutavad: asutuse/ettevõtte juhtkond, infoturbeametnik

Rakendamise eest vastutavad: infoturbeametnik, IT-juht

Asutuste tööprotsessid on tänapäeval suures osas infotehnoloogiaga läbi põimunud. Tähtsad andmed nagu sideandmed, ettekanded, reklaammaterjalid või konstruktsiooniplaanid eksisteerivad paljudel juhtudel üksnes digitaalsel kujul. Ettevõtete ja ametiasutuste jaoks on nendel andmetel suur tähendus. Samuti on nõuded, mida asutused esitavad oma salvestisüsteemile, minevikus pidevalt kasvanud. Samal ajal laiendavad uued arendused salvestisüsteemis võimalikke kasutusvaldkondi, toovad aga sellega koos kaasa uued ohud. Seetõttu kasvab hoolika planeerimise tähtsus seoses salvestisüsteemide kasutamisega.

Eduka planeerimise eeldus on muuhulgas kõikide vastutavate isikute ühine arusaam põhilistest mõistetest, mida salvestisüsteemi rakendamisel vajatakse. Alljärgnevalt on toodud salvestisüsteemi mõistete selgitused, mis hõlmavad kõiki asjakohaseid aspekte.

Salvestilahendus

Salvestilahendus koosneb ühest või mitmest salvestivõrgust ja ühest või mitmest salvestisüsteemist. Seega kirjeldab salvestilahenduse mõiste kõikide komponentide kogumit, mis on vajalikud andmete salvestamiseks ja nende andmiseks juurdepääsu omavate süsteemide käsutusse.

Salvestisüsteem

Keskset instantsi, mis annab teiste süsteemide käsutusse salvestiruumi, nimetatakse salvestisüsteemiks. Samas võimaldab salvestisüsteem paljudel teistel süsteemidel (nt virtuaalsetel ja füüsilistel serveritel, klientidel) kasutada üheaegselt olemasolevat salvestiruumi. Salvestisüsteem koosneb paljudest komponentidest, mida kirjeldatakse lähemalt allpool.

Andmekandjad

Salvestisüsteem sisaldab üht või enamat andmekandjat, mis võimaldab andmete salvestamist ja hilisemat kuvamist. Andmekandjad võib seejuures jaotada näiteks elektroonilisteks andmekandjateks (nt välkmälud), magnetilisteks andmekandjateks (nt kõvakettad või magnetribad) või optilisteks andmekandjateks (nt optilised lindid).

Salvestikorpus

Tavaliselt asuvad andmekandjad eraldi salvestikorpuses. Väiksemate salvestisüsteemide korral võivad andmekandjad olla paigaldatud ka koos salvesti kontrolleritega või NAS-kontrolleritega ühisesse korpusesse.

Salvesti kontroller

Salvestisüsteem võib olla varustatud ühe või mitme liiaselt varustatud salvesti kontrolleriga. Salvesti kontroller koosneb seejuures tavaliselt järgmistest kompo-

nentidest:

- Frontend-Port'id (Fibre Channel + Ethernet)
- salvestiprotsessor(id) ja sinna juurde kuuluv RAM
- salvesti vahemälu
- Backend-Port'id salvestikorpustele (SAS, FC)

Salvesti kontroller võimaldab salvestisüsteemi konfigureerimist ja kujutab endast seega keskset komponenti salvestisüsteemi sees. Salvesti kontrolleri ülesanne on seega konfigureeritud andmekandjate andmine salvestivõrgu käsutusse.

NAS-kontroller

Salvestisüsteem võib olla varustatud ühe või enama liiaselt projekteeritud NAS-kontrolleriga. NAS-kontroller võimaldab NFS-i (Network File System) või CIFS-i (Common Internet File System) kasutamise abil juurdepääsu salvestisüsteemidele. Peamine kasutusvaldkond on failiserveri teenuste osutamine. NAS-kontroller võib ühelt poolt olla paigaldatud salvesti kontrolleriga ühendatult, teisalt aga olla koos salvesti kontrolleriga paigaldatud ühte korpusesse.
Võimalikud juurdepääsumeetodid salvestisüsteemidele

Salvestisüsteeme võib eristada nende juurdepääsumeetodite järgi. Alljärgnevalt on esitatud salvestisüsteemide tavalised variandid.

- Plokipõhised salvestisüsteemid: juurdepääs salvestisüsteemile toimub üksnes plokipõhiselt. NAS-kontrollerit ei kasutata.
- Failipõhised salvestisüsteemid: juurdepääs salvestisüsteemile toimub üksnes failipõhiselt. Kasutatakse NAS-kontrollerit.
- Ühendatud salvestisüsteemid (faili- ja plokipõhised): juurdepääs salvestisüsteemile toimub nii ploki- kui ka failipõhiliselt.

Salvestivõrk

Salvestivõrgud võimaldavad ühelt poolt pääseda juurde salvestisüsteemidele ning teisalt replikeerida andmeid erinevate salvestisüsteemide vahel. Salvestisüsteemi sees kasutatakse erinevaid protokolle. Seetõttu eksisteerivad, eriti plokipõhise juurdepääsu korral, spetsiaalsed võrgukomponendid, mis laiendavad salvestivõrku erifunktsioonidega.

Protokollid

Juurdepääs salvestisüsteemidele toimub salvestivõrkude abil. Põhimõtteliselt tuleb siin nagu ka salvestisüsteemide puhul eristada IP-põhist failijuurdepääsu (nt

CIFS), IP-põhist plokijuurdepääsu (nt iSCSI) ja puhtalt plokipõhist juurdepääsu (nt FC). Olenevalt juurdepääsuvormist kasutatakse alati erinevaid protokolle.

IP-põhise juurdepääsu korral saab kasutada järgmisi protokolle:

- NFS (Network File System)
- CIFS (Common Internet File System), SMB (Server Message Block) laiendus
- HTTP (Hypertext Transfer Protocol),
- WebDav (Web-based Distributed Authoring and Versioning),
- REST (Representational State Transfer), on tihedalt seotud HTTP-ga,
- SOAP (Simple Object Access Protocol).

Plokipõhise juurdepääsu korral saab kasutada järgmisi protokolle:

- FC (Fibre Channel)
- FCoE (Fibre Channel over Ethernet)
- iSCSI (internet Small Computer System Interface)

Kui kasutatakse iSCSI-d, tuleks siin kasutusse anda eraldi võrk. Seetõttu toimub siin administratsioonivõrgu, rakenduste ja kasutajate tootmisvõrgu ning iSCSI-võrgu eraldamine. See toiming on end praktikas hea tavana tõestanud. Eraldi võrkudega saab vea ilmnemisel leida põhjuse kiiremini ja hõlpsamalt ja selle kõrvaldada. Lisaks mõjutavad rikked samaaegselt ainult võrku ja mitte kõiki rakendusi.

FC-SAN-kommutaatorid

FC-SAN-kommutaatorid kujutavad endast FC-plokipõhise juurdepääsu korral juurdepääsu omava serveri jaoks ühenduskohta salvestivõrgus. Tänu sellele võimaldavad need paljude serverite samaaegset juurdepääsu salvestisüsteemidele.

Tänapäeval on olemas järgmised kommutaatoritehnoloogiad:

- FC-SAN-kommutaatorid, mis kasutavad FC-d kui ainsat protokolli
- Unified-Fabric-kommutaatorid, mida kasutatakse vastavalt konfiguratsioonile ja asetusele samaaegselt kui LAN-, FC- ja FCoE-kommutaatorit

Replikeerimine

Replikeerimise all mõeldakse salvestisüsteemi andmete mitmekordset salvestamist ja nende andmeallikate sünkroniseerimist. Replikeerimine võib seejuures toimuda tuletõkke tsoonis, sellest väljaspool või isegi väljaspool arvutuskeskust või riigist väljaspool. Praktikas eristatakse kaht replikeerimisviisi.

Sünkroonne replikeerimine võimaldab täielikult liiasusega varustatud andmetalletust, mille korral peegeldatakse salvestisüsteemi andmed reaalajas eraldatud

süsteemi. Seejuures tagatakse, et andmeid sünkroniseeritakse nende asukohtades pidevalt. Sünkroonse replikatsiooniga on tegemist siis, kui andmeobjekti muutmistoimingu saab üksnes siis edukalt lõpetada, kui see on ka replikaatidel läbi viidud (vastuvõtukinnitus).

Sünkroonse replikeerimise eelis on see, et mõlemad andmeplokid sünkroniseeritakse igal ajal täielikult. Usaldusväärne võrk ja eelkõige lühikesed vastuse ootamise ajad on sünkroonse replikeerimise eeldus. See tähendab, et ülekande ulatus on selle tehnoloogia kasutamisel piiratud. Piirang tuleneb seejuurees kas tootja spetsifikatsioonidest või põhineb maksimaalsel tootjapõhisel vastuse ootamise ajal.

Kuni kauguseni 10 km ei ole sünkroonse andmete peegeldamisega täiendavaid meetmeid rakendamata tavaliselt mingit probleemi. Kaugustel üle 10 km tuleb erilist tähelepanu pöörata andmeühenduse kvaliteedile. Üle 10 km klaaskiuühenduste korral tuleb Fibre-Channel-kommutaatorites Short-Wave-Port-moodulite asemel kasutada Long-Wave-Port-mooduleid. Arvutuskeskuste ühendamisel, mis asuvad üksteisest rohkem kui 10 km kaugusel, kasutatakse ka tehnoloogiaid nagu DWDM (Dense Wavelength Division Multiplexing) või CWDM (Coarse Wavelength Division Multiplexing). Siin on ühendusliinide absoluutne latentsusaeg sünkroonse peegelduse realiseerimiseks oluline.

Vastupidiselt sünkroonsele replikeerimisele ei replitseerita andmeid asünkroonse replikeerimise korral reaalajas, vaid ajalise viivitusega. Asünkroonseid replikeerimisi kasutatakse sageli IP-ühenduste korral erinevate asukohtade vahel. Ülekande ulatus võib sellisel juhul ulatuda üle kontinentide.

Salvestilahenduste virtualiseerimine

Salvestilahenduste virtualiseerimise korral lisatakse salvestivõrku uus virtuaalne kiht, mis seob salvestiruumi kasutusse andmise lahti füüsilistest oludest. Salvestilahenduste virtualiseerimise kasutamine pakub asutusele terve rea lisaväärtusi:

- suurenenud paindlikkus salvestilahenduse ehitamisel, planeerimisel ja laiendamisel;
- salvestihalduse ühtlustamine;
- sõltumatus salvestisüsteemide valikul;
- praktikas sageli esinevad salvestilahenduste teostused.

Network Attached Storage (NAS)

Network-Attached-Storage-süsteemid koosnevad tavaliselt vähemalt ühest NAS-kontrollerist ja ühest või mitmest salvestikorpusest. NAS-i peamine kasutusvaldkond on failiserveri teenuste osutamine IP-võrgu kaudu. Seetõttu kasutavad teenuseosutajad nende süsteemide puhul ka terminit filer.

Storage Area Network (SAN)
Storage Area Network'i (SAN) lahenduse puhul luuakse tavaliselt salvestisüsteemide ja serverite või lõppseadmete vahele eraldi salvestivõrk. SAN-süsteemid töötati välja suurte andmehulkade pidevaks ja kiireks jadaandmeedastuseks. Tänapäeval kujutavad need endast suure käideldavuse ja suure jõudlusega installatsioone, mis kasutavad kas Fibre-Channel- või IP-protokolli (iSCSI).

Hybrid-Storage või Unified Storage
Salvestilahendusi, mis kujutavad endast NAS-i ja SAN-i kombinatsiooni, nimetatakse sageli hybrid-storage-salvestisüsteemideks või ka kombineeritud salvestisüsteemideks (unified storage). Teenuste osutamisel võib seda käitada nii NAS- kui ka SAN-süsteemina. Kombineeritud käitamine on võimalik tänu vastavatele süsteemikomponentidele ja nende konfiguratsioonile.
Nii on võimalik, et üks ja sama salvestisüsteem suudab pakkuda teatud rakendustele juurdepääsu läbi Ethernet-ühenduse, töötades nn filer-ina ja osutada seeläbi failiteenuseid CIFS- ja NFS-protokolliga ja pakkuda läbi Fibre Channel'i või iSCSI teistele serveritele ka salvestimahtusid.

Object storage
Object storage (sageli ka object based storage) võimaldab traditsiooniliste plokija failipõhiste juurdepääsude kõrval rakendada andmete suhtes ka objektipõhist juurdepääsu.

Objektikesksed salvestilahendused salvestavad andmeid andmekandjatele koos nende juurde kuuluvate metaandmetega mitte failide, vaid objektidena. Objekti saab eksimatult identifitseerida objekti ID (räsiväärtus) põhjal, mis sisaldab muu hulgas ka objekti metaandmeid. Juurdepääs objektipõhisele mälule toimub läbi juhtiva rakenduse. Rakendus pääseb objektipõhisesse salvestisüsteemi kas spetsiaalse API (IP) ja selle võimalike käskudega või otse IP-ga. Juhtudel, kus juurdepääsuks kasutatakse API-d, peab vastav rakendus toetama objektipõhise salvestisüsteemi tootjapõhist API-d.

M 3.93 Teavitus- ja koolitusprogrammide sihtrühmade analüüs

Algatamise eest vastutab: infoturbeametnik

Rakendamise eest vastutavad: infoturbeametnik, ülemused

Kui asutuse jaoks koostatakse teavitus- ja koolitusprogramm (vt ka M 2.312 Infoturbealase koolitus- ja teavitusprogrammi kavandamine), tuleb selle kavandamise käigus määratleda vastavad sihtrühmad. Selleks tuleb läbi viia üksikasjalik sihtrühma analüüs, et meetmed saaks suunata spetsiaalsetele nõuetele ja erinevatele taustadele.

Ühte sihtrühma võivad olla suunatud näiteks võrreldava erialase tausta, teadmiste või ülesannetega töötajad. Teostatav lahendus on ka sihtrühmade loomine organisatsiooni üksuste põhjal. Tavaliselt tuleb siin lähtuda sellest, et töötajad töötavad analoogse tehnika ja sarnaste nõuete alusel.

Järgmine kriteerium on sündmused, mis töötaja karjääri jooksul esinevad. Siia kuuluvad nt töölevõtmine, ülesannete või osakonna vahetumine, asukohavahetus, tehnika vahetus, muudatused organisatsioonis või asutusest lahkumine.

Võimalike sihtrühmade näited ja nende tunnused on järgmised:

Juhatus

- Juhatuse liikmetel on töötajate jaoks eeskuju funktsioon. Üldiselt on neil sageli ka vähe aega, nii et teavitus- ja koolitusmeetmed peavad olema struktureeritud ja konkreetsed.

Töötajad

- Selle sihtrühma käitumisel igapäevatöös on kõige tugevamad otsesed mõjud asutuse infoturbele. Siinkohal tuleb arvestada, et teadmiste tase võib töörühma sees olla väga erinev. Näiteks on tarkvara-arendajatel teistsugune IT-varustus ning muud ülesanded ja teadmised kui personalihalduse töötajatel. Need rühmad vajavad seega erineva sisuga infoturbealaseid koolitusi.

Administraatorid

- Administraatoritel ja tehnilise toe personalil peavad olema põhjalikud erialased teadmised nende hallatavatest IT-süsteemidest ja rakendustest, et nad suudaksid tuvastada, kõrvaldada ja ka ennetada turvaprobleeme.

Personaliosakond

- Selle osakonna töötajatel on suur teabevajadus andmekaitsenõuetest.

Asutusevälised projektijuhid

- Paljudel juhtudel on ka asutusevälistel isikutel, kes on asutusega tihedalt seotud või isegi seal tegevad, juurdepääs asutusesisestele andmetele, rakendustele ja süsteemidele. See sihtrühm peab samuti toetama asutuse infoturbealaseid eesmärke ja reegleid ning nad peavad olema selleks samamoodi kohustatud nagu asutuse töötajad. See nõuab vastavaid koolitusmeetmeid, nt juhised, mille teatavaksvõtmine on kirjalikult kinnitatud. Need meetmed peaks väline asutus ellu viima oma asutusega kokkulepitud nõuete kohaselt.

Uued töötajad

- Sellel sihtrühmal ei ole seni olnud kokkupuudet asutusesise infoturbega.

Kontrollküsimused:

- Kas infoturbealane teavitus- ja koolitusmeetmete vajadus on määratletud sihtrühmade kohaselt?

M 3.94 Õpitulemuste edukuse mõõtmine ja hindamine

Algatamise eest vastutavad: infoturbeametnik, personaliosakond

Rakendamise eest vastutavad: personaliosakond, ülemused

Õpitulemuste edukust tuleks infoturbe valdkonnas mõõta ja hinnata sihtrühmade põhiselt, et teha kindlaks, mil määral on saavutatud teavitus- ja koolitusprogrammides kirjeldatud eesmärgid (vt M 2.312 Infoturbealase koolitus- ja teavitusprogrammi kavandamine ja M 2.557 Infoturbealase koolitusprogrammi kontseptsioon). Seeläbi on võimalik saada üksikasjalik üldpilt ja võtta täpsed parandusmeetmed, kui üksikud eesmärgid ei ole saavutatud.

Personaliosakonnal on sageli head kogemused koolitusmeetmete hindamisel. Seepärast on soovitatav orienteeruda sellele meetodile ja see personaliosakonnaga kooskõlastada. Õpitulemuste edukuse testimiseks võib kasutada alljärgnevaid võimalusi.

Läbiviidud teavitus- ja koolitusmeetmete dokumenteerimine

Kõikide meetmete dokumenteerimine, sh sisude ja läbiviimise tsüklite lühikirjeldus, annab esimese ülevaate koolituse ulatusest ja läbiviidud tegevustesse kaasatud sihtrühmadest.

Teavitus- või koolitusmeetmetest osavõtnute arvude dokumenteerimine

Koolitustest osavõtjate arvu või nende töötajate arvu dokumentatsioon osakonna, valdkonna, asukoha jne kohta, kelleni teavitusmeetmed on jõudnud, annavad teavet meetmete läbipõimumise soovitud taseme kohta asutuses.

Turbealaste küsimuste arv kontaktisikutele (vt M 3.46 Kontaktisik turvalisuse alal)

Kui pärast koolitus- või teavitusmeetmeid tõuseb turbeküsimuste kontaktisikute poole pöördumiste arv, võib see olla märk sellest, et töötajate teadlikkus on tõusnud, aga ka sellest, et asutuse tundmine on suurenenud.

Koolituste hindamine

Esimese kvalitatiivse ülevaate koolituse edukusest annavad standardsed koolituse hindamislehed, mille osalejad täidavad tavaliselt pärast koolituse lõppu. Lisaks küsimustele, mis puudutavad koolituse kulgu, ürituste korraldamist või esineja õpetamismeetodit, võib siia lisada ka küsimused osalejate hinnangu kohta koolituse kasulikkusest.

Koolituse lõputest

Koolituse ajal või lõpus läbiviidavad teadmiste testid on praktikas järeleproovitud meetod õpitulemuste edukuse kontrollimiseks. Sobitatuna konkreetsete koolituse sisudega võivad aluseks olla küsimused õpitud teadmiste kohta, aga ka küsimused kirjeldatud olukordade hindamiseks.

Teadmiste kontroll teatud ajavahemiku järel

Selleks, et teha kindlaks teadmiste taseme liikumist, võib pärast koolituse lõppu viia teatud ajahetkedel läbi täiendavaid teste. Kuna siin puudub otsene seos kindla koolitusega, võib olla raske motiveerida osalejaid küsimustele vastama. Selle vältimiseks võib selle testi viia läbi ka mälumängu vormis, nt andes osalejatele auhinnad.

Töötajate ankeedid
Vestlustel töötajatega standardsete ankeetide abil saab koguda teavet selle kohta, kas ka koolitusvälised teavitusmeetmed on tõhusad.

Reeglite vastu eksimiste arv
Teine võimalus, et hinnata, kas meede oli edukas, on lugeda kokku reeglite vastu eksimiste arv enne ja pärast teavitusmeetme läbiviimist. Selleks võivad vastutavad isikud kohaldada ka teadlikult ja kontrollitult turvaauke ja seejärel jälgida, kuidas töötajad neid käsitlevad.

Siia sobivad järgmised näited:

- ilma töötõendita võõrad isikud, kes liiguvad asutuses ringi ilma saatjata,
- DVD-d, CD-d või USB mälupulgad, mis on asutuses igale poole välja pandud,
- e-kirjad, mis on töötajatele laiali saadetud manusena või linkidega tundmatutele veebilehtedele, millel on aga tuttavalt kõlavad saatja aadressid või
- ukse sulgemise funktsioonid, mis blokeeritakse.

Siinjuures on oluline, et tulemusi ei esitataks üksikute töötajate vale käitumise, vaid rühmade tulemusena.

Social-penetration-testid / social-engineering-auditid
Selleks, et kontrollida õpitulemuste edukust social-engineering-ennetuse raames, soovitatakse läbi viia social-penetration-testid või social-engineering-auditid. Siinjuures üritatakse välise ründe toimepanija rollis kasutada ära töötajate valet käitumist ja hankida teavet, mille abiga saavutab testija ründe ettenähtud eesmärgid.

Seda tüüpi auditid on siiski alati vaieldavad, sest töötajad, kes valiti ilma nende teadmata ründeobjektiks, võivad näha hindamises pärast edukat rünnet reetmist või paljastamist. Teisest küljest annavad sellised auditid häid vihjeid, kui kaugele on infoturbega tegelikult jõutud. Seetõttu tuleb selle meetodi kasutamist kontrollida iga juhtumi puhul eraldi ning kaaluda koos personali esindajate ja juhtkonnaga.

Praktilised harjutused
Alternatiivina kirjeldatud social-penetration-testidele võib kasutada ka praktilisi harjutusi. Siin on võimalikud erinevad variandid, mis annavad ülevaate teavitus- ja koolitustasemest. Pärast koolitust võib luua harjutuste seeriad, milles on mänguliselt kujutatud erinevaid olukordi, nt social-engineering-tüüpi rünnet. Rühma vabatahtlike osalejate ülesanne seisneks selles, et reageerida sellele ründele. Harjutuse anonüümne hindamine seminari juhataja poolt annab ülevaate eelnevate meetmete õpitulemuste edukuse kohta.

Vahendid ja mängud
Igat liiki õppemängud või -vahendid pakuvad paljudel juhtudel samuti võimalust mängijate tulemuste või tulemuste arengu hindamiseks.

Kontrollküsimused:

- Kas teavitus- ja koolitusprogrammide õpitulemuste edukust hinnatakse kvantitatiivselt ja kvalitatiivselt?

M 3.95z Õppematerjali kinnistamine

Algatamise eest vastutab: infoturbeametnik

Rakendamise eest vastutavad: infoturbeametnik, ülemused

Infoturbealaste teavitus- ja koolitusprogrammide kontseptsiooni puhul on õppematerjali kinnistamine väga oluline, sest ainult pidevalt olemasolevad teadmised toovad kaasa soovitud muudatused käitumises. Pärast teavitus- ja koolitustegevusi on osalistel tavaliselt palju uusi teadmisi ja oskusi. Kui nad neid teadmisi pärast koolitust üle ei loe või ei kasuta, on olemas oht, et need ununevad täiesti või osaliselt. Selleks, et töötajate teadlikkus infoturbest paraneks jätkuvalt, tuleks teavitus- ja koolitusmeetmete teemasid regulaarselt korrata või kasutada. Sellele aitab kaasa õppematerjalide kinnistamine, mida viiakse läbi nii koolituse ajal, pärast koolituse lõppemist kui ka ajavahemikul selle järel. Meetmete valik, mis õppematerjalide kinnistamise alla kuulub, tuleb sobitada konkreetse asutuse kultuuri ja suurusega.

Õppematerjali kinnistamise meetmete näited on järgmised:

- kirjalikud või suulised testid koolituse ajal ja/või pärast lõpetamist,
- koolitusteemadega viktoriini stiilis küsitluslehed võiduvõimalustega,
- intranetil põhinevad küsitlused läbiviidud koolituste teemade kohta,
- meeskonnavestluste kasutamine jne, et viia läbi arutelu infoturbe asjakohaste aspektide kohta,
- infoturvet kajastavate tegevus- ja rollimängude läbiviimine (vt M 3.47z IT-turbealased tegevus- ja rollimängud),
- seminaride regulaarne kordamine,
- lühikesed juhised intranetis,
- täiendavad lühiettekanded, nt asutusesiseste ürituste raames.

Kontrollküsimused:

- Kas asutuses on võetud meetmeid õppematerjalide kinnistamiseks?

M 3.96 Juhatuse tugi teavitusele ja koolitusele

Algatamise eest vastutavad: infoturbeametnik, asutuse/ettevõtte juhtkond

Rakendamise eest vastutab: infoturbeametnik

Selleks, et luua asutuses edukas infoturve, on tingimata vaja teadlikke ja koolitatud töötajaid. Asutuse vajaduste kohane ja sobivalt koostatud teavitus- ja koolitusprogramm on seega oluline edufaktor, et luua asutuses jätkusuutlikult infoturbealased juhised ja meetmed ning tagada nende tõhusus. Selle rakendamiseks peab juhtkond olema ka ise teadlik (vt M 3.44 Juhtkonna teadlikkuse tõstmine infoturbe alal) ja toetama aktiivselt programmi selle kasutusaja jooksul nõuetekohaste meetmetega.

Algatamine

Enne infoturbealase teavitus- ja koolitusprogrammi väljatöötamist peaks juhtkond väljastama täpse korralduse. Seda tuleb levitada asutuse sees. Selle kaudu kinnitatakse vastutavad isikud ja toetatakse neid nähtavalt. Lisaks sellele mõistavad töötajad teemat ja saavad aru selle tähendusest.

Planeerimine

Infoturbealase teavitus- ja koolitusprogrammi plaan tuleks esitada juhtkonnale, kes selle vastu võtab. Korraldusega võtta programm kasutusse võib juhtkond anda märku oma edasisest toetusest ja anda kasutada vajalikud ressursid.

Rakendamine ja loomine

Sel ajal, kui asutuses juurutatakse ja luuakse rakendatavaid programme, peab juhtkond olema nähtavalt kaasatud, sest tänu sellele mõjutatakse oluliselt töötajate positiivset vastuvõttu. Juhtivtöötajad peaksid infoturbealaste teavitus- ja koolitusmeetmete läbiviimisel aktiivselt osalema, nt

- omapoolse panusega asutuse meedias,
- erinevate ürituste korraldamisel,
- eeskuju andva käitumisega,
- töötajatele piisavate ressursside andmisega.

Nii rõhutavad nad, kui tähtsad on need meetmed nende endi jaoks. Lisaks muutub teema töötajate jaoks arusaadavaks ja usutavaks. Nad mõistavad ja aktsepteerivad, et asjakohane infoturve on üha vajalikum ja moodustab enesestmõistetava osa nende igapäevatööst.

Edukuse kontroll ja uuendamine

Regulaarselt tuleb kontrollida, kas loodud teavitus- ja koolitusmeetmed on endiselt tõhusad ja vajaduse korral tuleb neid kohandada. See peab toimuma ka siis, kui asutuse raamtingimused on muutunud (vt lisaks M 3.83z Personaliga seotud turbefaktorite analüüs , M 3.94 Õpitulemuste edukuse mõõtmine ja hindamine ja M 3.95z Õppematerjali kinnistamine).

Siinjuures saab juhtkond väärtuslikult panustada, nt

- saab juhtkond vahendada erinevate huvirühmade vahel sageli raskeks osutuvat kooskõlastamist õpitulemuste edukuse mõõtmise ja määramise puhul;

- saavad nad hoolitseda selle eest, et infoturbealast teavet edastatakse avatult ja usaldusväärselt. Nii aktsepteerivad töötajad seda rohkem ja on valmis kõrvaldama olemasolevaid nõrku kohti;
- kui teavitus- ja koolitusmeetmeid tuleb kohandada või uuesti välja töötada, peaks juhtkond reageerima õigel ajal ja andma nõusoleku näiteks vajalike ressursside kasutamiseks.

Kontrollküsimused:

- Kas juhtkond toetab infoturbealaste teavitus- ja koolitusmeetmete elluviimist piisavalt?

M 3.97 Projektimeeskonna koolitamine tarkvaraarenduse jaoks

Algatamise eest vastutavad: infoturbeametnik, IT-juht

Rakendamise eest vastutavad: IT-juht, infoturbeametnik

Arendusmeeskonna suurem teadlikkus infoturbest mängib turvaliste IT-süsteemide loomisel otsustavat rolli. Seejuures peab see turvalisusega seotud teadlikkus olemas olema mitte üksnes rakendusetapis, vaid tarkvaraarenduse kogu kasutusaja jooksul.

Üldised teemad projektimeeskonna koolitamiseks turvalisema tarkvaraarenduse jaoks

Nõuete analüüs

Nõuete analüüs ja standard on tarkvaraarenduse edu tagamisel otsustava tähtsustega. Seejuures tuleb kindlaks teha, et kliendi ja osakonna nõuded määratletakse ja dokumenteeritakse täielikult, üheselt, terviklikult ja arusaadavalt. Nõuete analüüs paneb aluse süsteemi hilisemale vastuvõtmisele ja seetõttu peavad nõuded olema kontrollitavad.

Projektihaldus üldiselt ja konkreetselt süsteemiarenduse korral

Projektihaldus määrab ära arendusprojekti edu või ebaedu. Projektijuhil peavad seetõttu olema vajalikud teadmised ja oskused, et nt motiveerida projektis osalevaid töötajaid, edendada meeskonna koostööd ja rakendada õigesti kavandamist ja kontrollimist.

Riskihaldus tarkvaraarenduses

Selle valdkonna asjakohased teemad moodustavad riskihalduses tarkvaraarendusprojektide, tarkvaraarenduse riskide, riskide tuvastamise meetodite, analüüsi, hindamise ja käsitlemise aluse. Siinjuures on eriti oluline tunda tarkvaraarenduse tavalisi riske ja nende võimalikke mõjusid ning riskide käsitlemise meetmeid ja järelevalvet tarkvaraarenduses.

Kvaliteedihaldus

Asjakohaste teemade hulka kuuluvad kvaliteedihalduse meetodid ja normid (mh ISO standardid seeriast 9000 jj) ning praktilised teadmised kvaliteedi planeerimise, tagamise ja juhtimise rakendamiseks.

Kvaliteedi tagamine

Arvestades selle punkti tähtsust süsteemiarenduses ja suurt meetodite valikut, tuleks seda punkti süvendada vähemalt testimismeeskonna jaoks. Võimalike teemade hulka kuuluvad siin kvaliteedi tagamise meetodid, planeerimine ja hindamine, integreeritud tarkvara ja testimise arendamise meetodid ning kulutuste hindamise meetodid testimisel. Testimismeeskond peaks olema kursis järgmiste kvaliteedi tagamise meetoditega:

- staatiline katsemeetod (nt koodi ülevaatus),
- dünaamiline katsemeetod (nt Blackbox-testi meetod, nagu vastavusklasside moodustamine, piirväärtuse analüüs, oleku test ja Whitebox-testi meetod, nt nõuete, harude ja failiteede kattuvus, tingimuste testimine).

Mudelid ja meetodid tarkvaraarenduse jaoks

Arendusmeeskond peaks olema kursis tarkvaraarenduse tuntud meetodite, standardite ja ajakohase tehnika taseme ning heade tavadega.

Muudatuste haldus

Nii tarkvaraarenduse projektijuht kui ka arendusmeeskonna liikmed peavad mõistma muudatuste halduse tähendust ning tundma ja oskama kasutada muudatuste halduse põhikontseptsioone ja tööriistu. Muudatuste halduse kokkupuutepunktid muude tarkvaraarenduse tegevustega tuleb õigesti määratleda (nt kvaliteedi tagamiseks ja konfiguratsioonihalduseks), vajaduse korral tuleb siin arvesse võtta erinevate standardite nõudeid muudatuste haldusele.

Infoturve

Turvalisemate toodete arendamise jaoks on tingimata vajalik turbega seotud teadlikkus. Seetõttu tuleks projekti meeskonnale anda teadmisi üldiste turbega seotud teemade suhtes, nt

- tavapärased turvariskid sarnaste süsteemide korral (tavapärased ründestsenaariumid, tüüpilised turvaaugud, tavalised süsteemirikked ja nendega seotud kahjustused)
- standardsed turvameetmed turvaliseks tarkvaraarenduseks
- üldised teadmised infoturbest.

Turvanõuded asutuses

Tarkvaraarenduse korral tuleb järgida asutuse turvapoliitikat ja teisi turvasuuniseid. See eeldab loomulikult, et projekti meeskond tunneb kõiki sellele vastavaid nõudeid.

Turvalisuse aspektid konkreetsetes valdkondades

Lähtudes arendatava tarkvara rakendusalast, tuleks arendajaid koolitada spetsiifiliste aspektide suhtes. Siia kuuluvad näiteks võrgu- ja sideprotokollid ning -teenused, autentimine ja juurdepääsukontroll, andmebaasid, krüptograafilised meetodid, krüptovõtmete ja sertifikaatide haldus jne.

Arendajate koolitusteemad turvalisemaks programmeerimiseks

Esmajoones on oluline, et arendusmeeskond tunneks kasutatavaid meetodeid, programmeerimiskeeli, arenduskeskkonda, konfiguratsioonihalduse tööriistu ja kõiki muid tööriistu, mida kasutatakse tarkvaraarenduses. Seetõttu tuleks tegeleda ka järgmiste täiendavate valdkondadega.

Turvaaukude vältimine süsteemis:

- suurema osa programmide turvaaukudest põhjustavad ühesuguste vigade liigid. Tõsiste turvaprobleemide korral, millest CERT-d teavitavad, on üks põhjus ikka ja jälle nt buffer overflow. Süstemaatilise vigade kõrvaldamisega (exception handling) koodis saab paljusid turvaauke vältida, lastes süsteemil kontrollida kasutatavate andmete (andmevaldkond, andmestruktuur) õigsust ja saades valed andmed kätte.

Koodi konventsioonide kasutamise ja programmeerimistehnoloogiatega saab programmikoodi kvaliteeti tunduvalt parandada. Koodi konventsioonid on eeskirjad, mis võimaldavad ühtset ja ülevaatlikku programmikoodi loomist, nt failide ja kataloogide ülesehituse eeskirjade, koodi kommentaaride, nimeandmisega jms ning sellega hõlbustatakse programmikoodi analüüsi, hooldust ja taaskasutamist.

Samamoodi on tähtis ka programmisuuniste kasutamine, nagu näiteks erandite käsitlemine, eeskirjade määratlemine konstantide kasutamiseks ja viitamiseks jne. Tavaliselt on kõikide tavapäraste programmeerimiskeelte jaoks olemas tarkvaratööriistad, mis toetavad valdavalt koodi konventsioonidest ja programmeerimissuunistest kinnipidamise kontrollimist.

Sisestuse kehtivuse kontrollimine (sisestuse valideerimine) on tingimata vajalik, et tuvastada võimalikult palju rünnete liike. See peab toimuma süsteemi kõikides vastavates liidestes. Näiteks kliendi-serveri-keskkonnas ei tuleks sisestust kontrollida üksnes süsteemi kliendi poolel, vaid ka serveri poolel. Vastasel korral on süsteem vastuvõtlik Man-in-the-Middle-tüüpi rünnetele. Kui ründe toimepanija saab kätte kliendilt serverile suunduva andmevoo ja seda muudab, ei ole kaitse enam võimalik. Seetõttu on tingimata vajalik sisestuste kontrollimine pikkuse, väärtusskaala ja vormingu suhtes.

Tüüpseadistused peaksid süsteemile pakkuma võimalikult suurt kaitset. Pidades silmas ka pakutavaid liideseid, teenuseid või avatud porte, tuleks arvestada sellega, et süsteemis oleks võimalikult väike rünnatav ala.

Nii arendajate kui ka administraatorite ja kasutajate puhul tuleks järgida minimaalsete volituste andmise põhimõtet. Selle jaoks on vajalik autentimise ja volituste kontseptsioon ning see tuleb koostada juba projekteerimise etapis. Soovitatav on määratleda rollid erinevate juurdepääsude jaoks ja piirata pääsuõigusi süsteemitasandil nii palju kui võimalik. Seejuures on oluline kasutada asjakohaseid autentimise ja volituste protseduure. Vaadeldavate protseduuride hulka kuuluvad kahefaktoriline autentimine, kasutajakontode lukustusfunktsioonid, tugevate paroolide nõue, paroolide aegumistähtajad jne.

Süsteemirikkeid, tõrkeid ja vigu ei ole alati võimalik vältida. Seetõttu tuleb tähelepanu pöörata sellele, et

- iga rikke korral jääks süsteem turvaliseks
- süsteemi ja andmete sisu jääks pärast riket või viga alles

- veateated või süsteemi käitumine ei reedaks sellistel juhtudel konfidentsiaalseid andmeid ega pakuks ründevõimalusi
- vea põhjuste väljaselgitamiseks protokollitakse vajalikud andmed.

Alati tuleks vältida programmisiseste andmete väljastamist kasutajaliidesel. See tähendab näiteks, et veateated ei tohi kasutajale avaldada siseinfot programmi, süsteemi ega võrgu kohta.

Eriti veebirakenduste puhul tuleb tähelepanu pöörata sellele, et internetiaadressi (URL) kaudu ei avaldataks konfidentsiaalseid andmeid ja et ei toimuks URL-i kahjustamist.

Konfidentsiaalseid andmeid tuleb edastamisel ja salvestamisel piisavalt kaitsta. Selleks tuleb rakendada hinnatud ja asjakohaseid krüptograafilisi meetodeid. Näiteks ei tohiks paroole edastada loetava tekstina ja need tuleb salvestada kaitstult. Selleks, et vältida uutel toodetel võimalikult hästi turvaauke, peaksid kõik arendajad ennetamiseks tutvuma infoturbe ja turvalise arendamise põhimõtetega. Eriti tuleks arendajaid koolitada tavapäraste vigade ja turvaaukude vältimise protseduuride suhtes kasutatava programmeerimiskeele ja arendatava süsteemi jaoks (nt Buffer Owerflows'i vältimine). Kõik arendajad peavad olema teadlikud oma vastutusest seoses uue süsteemi turvalisusega.

Kontrollküsimused:

- Kas arendajaid on koolitatud turvalisuse aspektide suhtes?

M 3.98 Töötajate õpetamine, kuidas kasutada autentimisprotseduure ja -mehhanisme

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, personalijuht

Rakendamise eest vastutavad: personaliosakond, ülemused

Kõiki töötajaid tuleb õpetada, kuidas kasutada asutuses rakendatavaid autentimismeetodeid ja -mehhanisme turvaliselt. Peale selle tuleb kõiki töötajaid teavitada suuniste ja kasutusjuhendite kohta autentimisprotseduuride ja -mehhanismide kasutamiseks (vt nt M 2.11 Paroolide kasutamise reeglid). Eriti oluline on seejuures selgitada töötajatele, miks on suunised vajalikud ja asjakohased. Nii on nad paremini motiveeritud nõuetest kinni pidama. Suunised peavad olema töötajate jaoks arusaadavad ja need tohivad sisaldada üksnes selliseid eeskirju, mida ka kasutatakse. Need peaksid olema sõnastatud võimalikult positiivses toonis.

Õpetus peaks sisaldama vähemalt järgmisi punkte:

- milleks kasutatakse autentimist
- identifitseerimise ja autentimise põhimõtted, mõistete selgitused, näiteks teadmised, omand, omadus
- suunised kasutatavate autentimisprotseduuride ja -mehhanismide käsitlemiseks (nt autentimislubade säilitamine)
- nõuded paroolide valimiseks ja kasutamiseks (nt paroolide üleskirjutamise ja edasiandmise keeld, paroolid ei tohi olla liiga tavalised, neil peab olema teatud pikkus ja keerukus, vt M 2.11 Paroolide kasutamise reeglid).
- Volituste kasutamine: asutuse volituste kontseptsiooni ülevaade, volituste andmise korraldamine
- identiteedi- ja volituste halduseks kasutatava toote turvafunktsioonide ülevaade
- kirjeldus, kuidas toimib (korduv-) väljastuse protsess kasutajatunnuste lukustamise korral
- ülevaade erinevatest ülesannetest ja rollidest identiteetide, kasutajatunnuste ja volituste haldamisel, kontaktisikute määramine.

Kontrollküsimused:

- Kas kõiki töötajaid on õpetatud autentimisprotseduure õigesti kasutama?
- Kas autentimisprotseduuride kasutamiseks on olemas arusaadavad suunised?
- Kas kõiki töötajaid on teavitatud vastavatest autentimise eeskirjadest?

M 3.E2 Töötajate koolitus ID-kaardi/PKI lahenduste kasutamise osas

Algatamise eest vastutavad: turvajuht

Rakendamise eest vastutavad: turvajuht, tema poolt määratud isik või subjekt, väline ekspert

Kõik asutuse töötajad, kellel on tööalaselt kokkupuudet ID-kaardi/PKI süsteemide komponentidega – ID-kaart, digi-ID, mobiil-ID, turvaline autentimine, digiallkirjade andmine ja verifitseerimine, digitembeldamine ja templite verifitseerimine vms – peavad läbima vastava koolituse. Koolituse läbiviimise eest vastutab turvajuht.

Koolitusel osalejatele tuleb tutvustada kõiki neid süsteeme ja nende häid toimimistavasid, millega nad tööalaselt kokku puutuvad. Muuhulgas tuleb koolituse käigus põgusalt käsitleda ka PIN-koodide ja paroolide häid kasutustavasid ning enamlevinud ründeid, mida ID-kaardi/PKI lahenduste ja komponentide vastu võib korraldada. Mõistlik oleks koolitus siduda asutusesisese üldise turvakoolitusega – vt M 3.5 Turvameetmete koolitus , samas võib ta olla ka eraldiseisev moodul.

Turvajuhi või tema poolt määratud isiku kohustuseks jääb ka nn “pidev koolitus” – töötajate ID-kaardi/PKI vahendite ja nende turvalise kasutamise alane nõustamine süsteemselt korraldatud koolitusürituste vahelistel aegadel.

Kontrollküsimused:

- Kas töötajad saavad kõikide nende poolt kasutatud ID-kaardi/PKI komponentide kohta koolitusel piisava tasemega teavet?
- Kas koolitaja erialane kompetents seesuguse koolituse läbiviimiseks on piisav?

M4: Riistvara ja tarkvara

Meetmete nimekiri

M 4.1 IT-süsteemide paroolkaitse

Algatamise eest vastutavad: IT-juht, IT turvaosakond

Rakendamise eest vastutavad: kasutajad

IT-süsteemi paroolikaitse peab tagama, et andmetele ja IT-rakendustele pääseksid ligi ainult vastavate volitustega kasutajad. Volituste tõendamine peab toimuma vahetult pärast IT-süsteemi sisselülitamist. Kui kasutaja ei suuda vastavate volituste olemasolu tõendada, ei lase paroolkaitse teda IT-süsteemile ligi.

IT-süsteemi paroolkaitset saab rakendada mitmel viisil:

- Suurem osa BIOS-variantidest pakuvad buutimisparooli paigaldamise võimalust. Vale sisestuse korral buutimist ei toimu. BIOS-paroolist möödapääsemine ei ole raske, kuid see kaitseb siiski juhuslike ründekatsete eest, seega tuleks seda kasutada kõikjal, kus paremad kaitsemehhanismid puuduvad (vt lisaks: M 4.84 BIOSi turvamehhanismide kasutamine).
- Headel operatsioonisüsteemidel on pääsuõiguste kontrollimise funktsioonid juba olemas. Tavaliselt tuleb need aga ka veel eraldi aktiveerida, nt määrates kõikidele kasutajatele paroolid. Lisainfot selle teema kohta leiate operatsioonisüsteeme puudutavatest moodulitest.
- Installeeritakse täiendav riistvara või tarkvara, mis küsib enne arvuti tegelikku käivitamist parooli ja takistab vale parooli korral IT-süsteemi kasutamise.

Paroolide kasutamisel tuleb arvestada juhistega meetmes M 2.11 Paroolide kasutamise reeglid , eriti oluline on parooli regulaarne muutmine.

Kontrollküsimused:

- Kas asjassepuutuvatesse arvutitesse on paroolkaitse installeeritud?
- Millised BIOS-turvamehhanismid on aktiveeritud?

M 4.2 Ekraanilukk

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: kasutajad

Ekraanilukk võimaldab varjata hetkel ekraanil olevat. Ekraaniluku desaktiveerimine peaks olema võimalik ainult pärast edukat autentimist, nt parooli sisestamist, et tagada IT-süsteemi pääsukaitse ka IT-kasutaja lühiajalise eemalviibimise ajal. Ekraaniluku peaks saama aktiveerida käsitsi, samuti peab see teatud aja jooksul ise tööle hakkama, pärast seda, kui kasutaja pole süsteemi enam aktiivselt kasutanud. Kõikidele kasutajatele tuleb selgitada, et nad aktiveeriksid lühiajaliselt töökohalt lahkudes ekraaniluku. Pikema eemaloleku korral peaks kasutaja ennast süsteemist välja logima.

Automaatne lukustus, kui kasutaja sisestused puuduvad

Aeg, mille möödudes ekraanilukk puuduvate sisestuste tõttu aktiveerub, ei tohi olla ei liiga lühike ega liiga pikk. Aeg ei tohi olla nii lühike, et ekraanilukk aktiveerub juba lühikese mõttepausi järel. Samas ei tohi aeg olla nii pikk, et kasutaja eemalolek annaks kolmandale isikule võimaluse olukorda ära kasutada. Mõistlik pikkus on 15 minutit. IT-turvaosakonna meeskond peaks ooteaega seadistama, lähtudes seejuures vastava IT-süsteemi ja kasutuskeskkonna eripäradest.

Parooli küsimise sisselülitamine

Suuremal osal operatsioonisüsteemidest on ekraanilukud juba integreeritud. Nende kasutamisel peab jälgima, et oleks aktiveeritud ka parooli küsimine. MS-Windows 3.x pakub paroolitoega ekraanilukku ekraanisäästurina. Asjakohases dokumentatsioonis on aga kirjas järgnev: „Kui avatud rakendus pole Windowsi rakendus, siis ekraanisäästur automaatselt ei käivitu, sõltumatult sellest, kas rakendus on käivitatud aknas, MS-DOSi käsurealt või sümboli kaudu.“ Windows 95 all aktiveerub ekraanisäästja ka DOSi rakenduste puhul. Lisaks MS-Windowsile leidub veel ka teisi tooteid, mis pakuvad paroolitoega ekraanisäästureid. Enne selliste toodete kasutamist tuleb kontrollida, kas ekraanilukk töötab kõikide rakenduste korral.

Unixi all saab ekraanilukku kasutada programmidega nagu *lock* või X-Window keskkonnas vastavalt *lockscreen* .

Täiendavad kontrollküsimused:

- Kas arvutitesse, kus on selle järgi vajadus, on installeeritud ekraanilukk?
- Kas ekraanilukku kasutatakse järjepidevalt?

M 4.3 Viirusetõrjeprogrammide kasutamine

Algatamise eest vastutavad: infoturbeametnik, IT-juht

Rakendamise eest vastutavad: administraator, kasutaja

Kahjurvaraprogrammide vastast kaitset saab üles ehitada erinevatele põhimõtetele. Tõhusaim meetod on kasutada programme, mis otsivad IT-süsteemidest teadaolevaid kahjurvaraprogramme. Meetmes M 2.157 Sobiva viiruseskanneri valimine kirjeldatud nõuete järgi tuleks seega kasutada viirusetõrjeprogramme. Kaasaskantavate seadmete, nagu nutitelefonide, tahvel- või pihuarvutite korral tuleb lisaks järgida meedet M 4.466 Viirusetõrjeprogrammide kasutamine nutitelefonides ning tahvel- ja pihuarvutites .

Internetiteenuste kaitse

Kesksel e-posti-lüüsil tuleks kasutada viirusetõrjeprogrammi, mis kontrollib sissetulevaid ja väljaminevaid e-kirju. Kõik ülejäänud internetiteenused (HTTP, FTP jms) peaksid samuti olema kaitstud spetsiaalse kaitsetarkvaraga. Kui see ei oleks näiteks jõudlusprobleemide tõttu võimalik, tuleb vähemalt aktiivsete sisude teostus mitteusaldusväärsetelt lehekülgedelt tehniliselt lahutada.

Kogu andmehulga regulaarne analüüs

Ka siis, kui viirusetõrjeprogramm teostab igakordsel andmetele juurdepääsul kontrolli kahjurvarade suhtes, on asjakohane analüüsida regulaarselt kõikide klientide ja andmeserverite andmeid. Nii on võimalik leida kahjurvaraprogrammid, mille kohta ei olnud nende salvestamise ajal veel olemas tuvastussignatuuri. Sellistel juhtudel tuleb näiteks uurida, kas kahjurvaraprogramm on juba enne oma avastamist kogunud konfidentsiaalseid andmeid, lülitanud välja kaitsefunktsioone või laadinud internetist alla koodi. Jõudlusest tulenevatel põhjustel tuleks andmekogu täielik kontrollimine viia läbi aegadel, mil IT-ressursside vajadus ei ole väga suur. Ideaaljuhul valvab tarkvara arvuti koormust ja kasutab selle „tööpause" automaatselt kontrollimiseks. Töökoha arvutitel võiks viirusetõrjeprogramm olla ühendatud nt ekraanisäästja käivitusega.

Andmevahetus ja andmete edastamine

Andmed, mida on vaja laiali saata, tuleb vahetult enne saatmist kontrollida üle seoses kahjurvaraprogrammidega. Analoogselt tuleb ka vastuvõetud andmed vahetult pärast kättesaamist seoses kahjurvaraga üle kontrollida. Need kontrollimised on nõutavad nii juurdepääsul andmekandjatele kui ka andmete ülekandmisel sideühenduste kaudu. Need kontrollimised peaksid olema võimalikult suurel määral automatiseeritud. Täiendava meetmena võivad väljast tulevate programmide ja andmete jaoks olla sisse seatud kontrollikohad. Kontrollikohad on eraldi IT-süsteemid, mis ei ole integreeritud kohalikku võrku. Viirusetõrjeprogrammide abil testitakse kontrollikohtadel kõiki väljast tulevaid programme ja andmeid ning antakse luba nende kasutamiseks. See protseduur võib olla näiteks vajalik juhul, kui turbealased nõuded on väga kõrged või kui liikvel on eriti ohtlik kahjurvaraprogramm.

Vastastikused mõjutused krüpteerimistehnoloogiatega

Krüpteerimistehnoloogiate kasutamisel tuleb arvestada nende võimalike mõjudega kaitsele kahjurvaraprogrammide eest. Kui andmed krüpteeritakse, ei pääse süsteemi komponendid või rakendused nendele andmetele ligi, kui neil ei ole vas-

tavat võtit. See tähendab, et viirusetõrjeprogramm peab töötama kas kasutaja kontekstis või tuleb varustada vastavate krüptograafiliste võtmetega, et see suudaks ka krüpteeritud faile kahjurvaraprogrammide suhtes läbi kontrollida. Kui aga varustada kasutajatunnus, mille all viirusetõrjeprogramm töötab, vastavate krüptograafiliste võtmetega, tekivad selle tagajärjel turvariskid, mida tuleks vältida. Seega on soovitatav kasutada taustal töötavat viirusetõrjeprogrammi, mis kontrollib kahjurvaraprogramme kasutajast lähtuvalt iga failipöörduse korral.

Kaitse volitamata inaktiveerimise või muudatuse eest

Klientide ja lõppseadmete viirusetõrjeprogrammid peavad olema konfigureeritud nii, et kasutajad ei saaks ette võtta viirusetõrjeprogrammide turvalisusega seotud muudatusi ja seadistusi. Eriti kindel peab olema see, et kasutajad ei saa viirusetõrjeprogramme välja lülitada.

Kontrollküsimused:

- Kas viirusetõrjeprogrammid on installeeritud kõikidele IT-süsteemidele, millel see on turvakontseptsiooni kohaselt nõutav?
- Kas tehakse kindlaks, et nii skaneerimisprogramm kui ka allkirjad on alati kõige ajakohasemas olekus?
- Kas kasutajad tunnevad skaneerimisprogrammi, eriti nõudmisel skaneerimise (on-demand-scan) võimalust?
- Kas keskne e-posti lüüs on kaitstud viirusetõrjeprogrammiga?
- Kas kasutatavatele internetiteenustele on tagatud piisav kaitse kahjurvaraprogrammide vastu?
- Kas andmekogule teostatakse regulaarset analüüsi kahjurvaraprogrammide suhtes?
- Kas kahjurvaraprogrammi leidmisel uuritakse, kas leitud kahjurvaraprogramm on juba enne oma avastamist kogunud konfidentsiaalseid andmeid, lülitanud välja kaitsefunktsioone või laadinud internetist alla koodi?
- Kas andmevahetusel ja andmete edastamisel viiakse läbi kahjurvaraprogrammide otsing?
- Kas ka krüpteeritud andmetele on tagatud piisav kaitse kahjurvaraprogrammide vastu?
- Kas on kindlaks tehtud, et kasutajad ei saa teostada viirusetõrjeprogrammide seadistustes turvalisusega seotud muudatusi?

M 4.4 Eemaldatavate andmekandjate draivipilude ja väliste andmekandjate nõuetele vastav kasutamine

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: Kasutajad, administraator

Tänapäeval kaubanduses müüdavad PC-d on tavaliselt varustatud CD-/DVDROM-draivi või CD-/DVD-kirjutajaga. Lisaks sellele on võimalik liideseid kasutades arvutiga väliseid salvestuskandjaid ühendada, mida uuemad operatsioonisüsteemid tunnevad automaatselt ära. Näideteks on siinkohal USB-mälupulgad, mis pistetakse USBliidesesse, ja Firewire -kõvakettad.

Selliste vahetatavatele meediumidele mõeldud draivide ja eksternsete andmesalvestite kasutamisest tulenevad järgmised potentsiaalsed turvaprobleemid:

- PC-d saab selliste draivide abil kontrollimatult buutida.
- Selliste draivide abil saab kontrollimatult tarkvara arvutisse installeerida.
- Andmeid saab vahetatavatele meediumidele kopeerida, omamata selleks õigust.

Vahetatavate meediumide buutimisel või võõra tarkvara installeerimisel on võimalik mitte ainult turvaseadeid välja lülitada, vaid ka personaalarvutit nakatada arvutiviiruste ja muude pahatahtlikke programmidega.

Nende ohtude vastu tuleb vastavaid organisatsioonilisi või tehnilisi turvameetmeid rakendades võidelda. Selleks on olemas mitmesugused võimalused, mille **spetsiifilisi eeliseid ja puudusi alljärgnevalt lühidalt tutvustatakse**:

- Draivide väljamonteerimine - Vahetatavatele meediumidele mõeldud draivide väljamonteerimine (ka nendest loobumine arvuti soetamisel) pakub küll kõige kindlamat kaitset ülalmainitud ohtude eest, on aga enamasti seotud suurte kulutustega. Lisaks tuleb arvestada sellega, et teatavail juhtudel takistab draivide väljamonteerimine IT-süsteemi administreerimist ja hooldamist. Seda lahendust tuleks kasutada siis, kui on tegemist eriliste turvanõuetega.
- Draivide lukustamine - Mõnede draiviliikide jaoks on olemas lukustatavad sisselükatavad seadised, mille abil saab kontrollimatut kasutamist takistada. Seadmete soetamisel tuleks jälgida, et draivilukud sobiksid olemasolevatele draividele ja ei vigastaks neid. Samuti tuleks pöörata tähelepanu sellele, et lukkudel oleks tootja poolt piisav arv erinevaid võtmeid kaasas. Puudusteks on draivilukkude soetamisega seotud kulutused ja kulutused võtmete haldamisele. Seetõttu on see lahendus mõttekas vaid suurema turvavajaduse või eriliste turvanõuete korral.
- Deaktiveerimine BIOSis ehk operatsioonisüsteemis - Enamik PC-sid pakub BIOSis võimalusi seadistada, milliseid draive saab buutimiseks kasutada. Seoses BIOSi seadistuste kaitsmisega parooli abil (vt M 4.84 BIOSi turvamehhanismide kasutamine) saab sel moel takistada vahetatavate meediumide ja mobiilsete andmekandjate kontrollimata buutimist. Peale selle on

moodsate operatsioonisüsteemide puhul võimalik olemasolevaid draive ja liideseid üksikult desaktiveerida. See raskendab volitamata kasutamist, näit. võõra tarkvara installeerimist või andmete kopeerimist vahetatavatele meediumidele. Draivide deaktiveerimisel BIOSis ehk operatsioonisüsteemis on see eelis, et ei ole vaja riistvara muuta. Vastavaid seadistusi operatsioonisüsteemis saab vajadusel isegi tsentraalselt teha. Selleks, et see tegutsemisviis oleks efektiivne, peab olema garanteeritud, et kasutajatel ei ole õigust operatsioonisüsteemi kasutada, et draivide deaktiveerimist tühistada.

- Liideste kasutamise kontroll - Selliste eksternsete salvestuskandjate nagu USB-mälupulkade kasutamist on väga raske takistada, kui kasutatavat liidest kasutatakse muude (lubatud) lisaseadmete jaoks. Nii näiteks tarnitakse sülearvuteid, millel on hiire ühendamiseks ainult USB-liides. Seepärast ei ole tavaliselt mõttekas “USB-lukku” kasutada või liidest muid mehhaanilisi meetmeid rakendades desaktiveerida. Seetõttu tuleks liideste kasutamist operatsioonisüsteemi tasemel vastavaid õigusi väljastades või lisaprogrammide abil reguleerida. Mõnede lisaprogrammide puhul, mida kasutatakse USB- või Firewire -liidestega, on ka võimalik kindlaks määrata, et eksternsetelt andmekandjatelt saab andmeid ainult lugeda. Alternatiivina võib seadmete lisamist kontrollida. Andmekandjate ühendamisel eksternsete liidestega laaditakse sageli operatsioonisüsteemist draivereid või operatsioonisüsteemi tuuma mooduleid või tehakse sisestusi konfiguratsioonifailidesse (näit. Windows-Registry), mida on võimalik avastada. Üksikasjad tulenevad toote ja operatsioonisüsteemi spetsiifikast ning neid kirjeldatakse eraldi meetme all (vaata ka M 4.200z USB-salvestuskandjatega ümberkäimine).
- Krüpteerimine - On olemas tooted, mis hoolitsevad selle eest, et on võimalik ainult nendele mobiilsetele andmekandjatele juurde pääseda, millele on juurdepääs lubatud. Üks lahendus on näiteks see, et ainult neid andmekandjaid saab lugeda ja nendele salvestada, mis on teatud krüptograafiliste võtmete abil krüpteeritud. See kaitseb mitte ainult volitamata juurdepääsu eest manipuleeritud mobiilsete andmekandjate kaudu, vaid kaitseb ka mobiilsetele andmekandjatele salvestatud andmeid kaotsimineku ja varguse eest.
- Kasutamiseeskirjad - Paljudel juhtudel tohivad kasutajad vahetatavatele meediumidele mõeldud sisseehitatud draive või eksternsete liidestega ühendatud salvestuskandjaid täiesti kasutada, kuid kasutamine on siiski vastavate juhenditega reglementeeritud. Tehnilisel tasandil tuleks siis ainult vahetatavate meediumide buutimine BIOSis desaktiveerida. Draivide väljamonteerimine, lukustamine või desaktiveerimine operatsioonisüsteemis ei tule kõne alla. Sel juhul tuleks draivide ja salvestuskandjate kasutusjuhised sõnastada nii selgesti kui võimalik. Näiteks võib kehtestada üldise keelu , nii et ainult avalike tekstidokumentide kopeerimine on lubatud. Juhiseid tuleb kõikidele kasutajatele tutvustada ja nendest kinnipidamist peab kontrollima.

Nende programmide installeerimine ja käivitamine, mis on salvestatud vahetatavatelt meediumidelt, tuleks keelata ja kui võimalik, siis ka tehniliselt võimatuks muuta (vaata ka M 2.9 Aktsepteerimata riist- ja tarkvara kasutuse keeld). See puhtorganisatoorne lahendus tuleks valida ainult siis, kui kasutajad peavad aegajalt või regulaarselt draive kasutama. Muidu tuleks juurdepääsu tehniliste meetmete abil tõkestada nii, nagu on eespool kirjeldatud. Sobivat tegutsemisviisi valides peab alati kõiki vahetatavate meediumide draive silmas pidama, samuti kõiki võimalusi võrgu, seega eelkõige meili teel ja internetiühenduse kaudu andmeid

vahetada. Kui personaalarvutil on internetiühendus, ei piisa üksnes sellest, kui desaktiveeritakse või monteeritakse välja kõik vahetatavate meediumide draivid. Erilist tähelepanu tuleb pöörata arvuti kaitsmisele pahatahtlike programmide, näit. arvutiviiruste või trooja hobuste eest (vaata ka M 4.3 Viirusetõrjeprogrammide kasutamine). Selleks, et turvameetmeid aktsepteeritaks ja järgitaks, tuleb kasutajaid vahetatavate meediumide draivide kasutamisest tulenevatest ohtudest informeerida, et nad oskaksid neid ära tunda.

Kontrollküsimused:

- Kas juurdepääs vahetatavatele meediumidele on tõkestatud või reglementeeritud?
- Kas kasutajaid on kõikidest vahetatavate meediumide draivide ja väliste andmesalvestitega ümberkäimise eeskirjadest informeeritud?
- Kas on garanteeritud, et personaalarvuteid ei ole võimalik vahetatavaid meediume kasutades kontrollimata buutida?

M 4.5 Kodukeskjaama (PBX) haldustööde logi

Algatamise eest vastutavad: andmekaitsetöötaja, kodukeskjaama eest vastutav töötaja, infoturbespetsialist

Rakendamise eest vastutavad: administraator

Tavaliselt on kõiki kodukeskjaama kaudu tehtud sisestusi võimalik logida. Nii näiteks saab logida seda, kes on kasutanud telefoni või faksi või kandnud üle andmeid, ja kes on kellega suhelnud. Taolisest infost saab teha kokkuvõtteid, seda saab töödelda ning seejärel salvestada. Sageli kasutatakse neid andmeid arvete ja tõendusmaterjali esitamiseks. Logitud info sisaldab muuhulgas järgmisi sissekandeid:

- kõne või ühenduse kuupäev ja kellaaeg,
- helistaja ja helistatava telefoninumbrid,
- kõne kestus.

Andmeid võib töödelda ja analüüsida integreeritult asutuse sees või kanda need üle vastavatesse välistesse süsteemidesse. Kuna tegemist on salajase teabega, tuleb kaitsta kõikide süsteemide andmeid ka nende ülekandmisel. Konfidentsiaalsuse ja integreerituse kaitsmiseks tuleb rakendada vastavaid ettevaatusabinõusid. Nii näiteks võiks teavet edastada selleks ettenähtud andmevõrkudes või krüpteeritult LAN-võrgus. Lisaks tuleks tagada, et kaitstud andmetele oleks juurdepääs vaid selleks õigust omavatel töötajatel. Selleks tuleks kindlaks määrata, mis ametikoha töötajatel on kõneandmetele juurdepääs. Logida tuleks lisaks kõiki programmimuutusi sisaldavaid süsteemtehnilisi sekkumisi, aga ka töötlemisi, andmeülekandeid ja juurdepääse andmetele.

Haldustööd

Kõik kodukeskjaama haldustööd tuleb logida, et hiljem oleks võimalik järele vaadata, kes või kuidas on seadistusi muutnud. Seepärast oleks autentimisel otstarbekas logida kasutajatunnus, kuupäev ja kellaeg, samuti toimunud ühendus. Toimunud juurdepääsul tuleks lisaks autentimisandmetele logida ka juurdepääsu liik (lugedes, kirjutades), aga ka läbiviidud haldustööd. Logi peab olema ülevaatlik, täielik ja korrektne. Kõrvalistel isikutel ei tohi olla võimalik logifunktsiooni desaktiveerida ning seda ei tohi olla võimalik hiljem muuta. Samuti peab olema välistatud logiandmete muutmine. Logitud infot tuleb regulaarselt kontrollida. Sagedasi katseid juurdepääsu väärkasutada tuleks eesmärgistatult uurida. Kui kahtlused tekivad ka edukal sisselogimistel, tuleb neid võrrelda läbiviidud konfiguratsiooni- ja hooldusmeetmete dokumentatsiooniga. Silmatorkavate erinevuste korral tuleks vastavalt kehtivatele IT-reeglitele kohe oletatava turvarikkumise kohaselt tegutseda ja seda senikaua, kuni ründekahtlus on üheselt ümber lükatud. Kuna logiandmed sisaldavad enamasti isikuandmeid, tuleb kindlustada, et neid andmeid kasutataks ainult andmekaitse kontrolli, andmevarunduse või reeglipärase käituse jaoks (vt M 2.110 Andmeprivaatsuse suunised logimisprotseduurides). Logimise ulatuse ja selle hindamiskriteeriumid tuleks dokumenteerida ja majasiseselt kooskõlastada. Vajadusel tuleb kooskõlastamisse varakult kaasata ka pädevad toimkonnad.

Täiendavad kontrollküsimused.

- Kas dokumenteeritakse see, millistel isikutel on juurdepääs keskjaama maksuandmetele?
- Kas keskjaama infole on juurdepääs ainult selleks õigust omavatel isikutel?
- Kas kõik keskjaama hooldusliidese kaudu tehtud sisestused ja vastavad kontod logitakse automaatselt?
- Kas keskjaama logiandmeid kontrollitakse regulaarselt?

M 4.6 Kodukeskjaama (PBX) konfiguratsiooni läbivaatus

Algatamise eest vastutavad: kodukeskjaama eest vastutav töötaja, infoturbespetsialist

Rakendamise eest vastutavad: infoturbespetsialist, revident

Kodukeskjaama turvalisuse tagamiseks tuleks regulaarsete ajavahemike järel läbi viia keskjaama seadmete konfiguratsiooni revisjon. Revisjon peaks hõlmama süsteemihaldust, hoolduspersonali, keskjaama tegelikku olukorda ja andmekaitse reeglitest kinnipidamise kontrolli. Iga konfiguratsioonimuudatus, näiteks kasutajale pääsuõiguste andmine, tuleks kanda hetkeseisu kajastavasse loendisse. Taolist loendit võib pidada nii käsitsi kui ka arvutis. Regulaarsete vahemike tagant, näiteks iga kuue kuu järel, tuleks seda hetkeseisu loendit vähemalt pisteliselt tegelikkusega võrrelda. Hetkeseisu loendi regulaarse revisjoniga saab tagada soovitud turva- ja andmekaitsetaseme. Ebakõlade põhjused tuleb selgitada logide abil.

Näiteks tuleks kontrollida, kas:

- kõik jagamata jäänud telefoninumbrid on ka tegelikult mittekasutatavad
- telefoninumbrid vastavalt täielikult kasutajatele
- keelatud volitused on tõesti välja jagamata,
- desaktiveeritud rakendused ja sideliidesed on tõesti desaktiveeritud,
- desaktiveeritud sissehelistamisfunktsioonid on tõesti desaktiveeritud.

Kui sõltumatu revidendi ametikohta ei soovita moodustada või kui see ei ole võimalik, võib logiandmeid analüüsida ka administraator. Tuleks aga jälgida, et see ei muudaks võimatuks administraatori enda tegevuse kontrollimist. Lisaks oleks administraatoril sel juhul võimalus tutvuda kaitstud andmetega (kõnelogid) (vt M 2.110 Andmeprivaatsuse suunised logimisprotseduurides). Analüüsi tulemused tuleks seepärast esitada vähemalt ka IT-turbespetsialistile, vastutavale IT-töötajale või mõnele teisele otsustusõigust omale töötajale.

Kontrollküsimused:

- Kas on olemas reeglid kodukeskjaama regulaarseks kontrollimiseks?
- Kas kodukeskjaama süsteemiga seotud konfiguratsiooni ja rakenduste muudatused dokumenteeritakse nii, et nendega oleks võimalik hiljem tutvuda?
- Kas on olemas reeglid kodukeskjaama regulaarse kontrolli tulemusel saadud andmete ja mahu sätestamiseks?

M 4.7 Algparoolide muutmine

Algatamise eest vastutavad: kodukeskjaama eest vastutav töötaja, IT turvaosakond, IT-juht
Rakendamise eest vastutavad: administraator, kasutaja

Paljudes IT-süsteemides, kodukeskjaamades ja võruühenduselementides (nt ISDN-marsruuterites, keeleandmete multiplekserites jne) on pärast tarnimist kasutusel veel eelseadistatud standardsed paroolid. Tootjate või administraatorite eelseadistatud paroolid tuleb muuta vahetult pärast installeerimist, kuid hiljemalt riist- või tarkvara esmakordsel kasutuselevõtul. Seejuures tuleb kinni pidada paroolireeglitest (vt M 2.11 Paroolide kasutamise reeglid).

Tähelepanu!

Teatud kodukeskjaamade puhul salvestatakse konfiguratsioonimuudatused ainult RAM-mällu. See kehtib ka paroolide muutmise kohta. Seetõttu tuleb pärast selliseid operatsioone alati andmed varundada, et tagada värske varukoopia olemasolu. Kui seda ei tehta, kehtib pärast süsteemi taaskäivitamist jälle standardparool. Lisaks tuleks kontrollida, kas pärast uue parooli määramist kaotas standardparool tõesti oma kehtivuse, st veenduda, et seda ei saa süsteemile ligipääsemiseks enam kasutada.

Kontrollküsimused:

- Kas süsteemis kehtib veel standardparool?
- Kas pärast individuaalse parooli määramist ja salvestamist (nt kodukeskjaamades) tehti varukoopiad?
- Kas pärast uue parooli määramist on süsteemile ligipääs standardparooliga välistatud?
- Kas paroolireegleid järgitakse?

M 4.9 X Windowsi turvamehhanismid

Algatamise eest vastutavad: IT-turvaosakond, administraator
Rakendamise eest vastutavad: administraator

X-Window tarkvara 5. redaktsioon pakub vaid mõningaid väheseid meetmeid, mis aitavad suurendada turvalisust andmete edastamisel X-serveri ja X-kliendi vahel, mistõttu on soovitatav X-Window tarkvara kasutada ainult turvalises keskkonnas.

Käsk xhost

- Arvutipõhiline juurdepääsu kontroll: Igal X-serveril on loend lubatud arvutitest, mida saab muuta käsuga xhost . See loend peab igal juhul piirduma arvutitega, mis vajavad juurdepääsu X-serverile. Mitte mingil juhul ei tohi võimaldada globaalset juurdepääsu käsuga xhost + . Seda on võimalik tagada, kui kanda xhost -tabelisse vaid konkreetsed arvutid. Lisaks tuleb arvestada, et igal kasutajal, kes töötab lubatud arvutil, on piiramatu ligipääs X-serverile. Sellist pääsukontrolli saab seega soovitada ainult neil juhtudel, kui mõjuval põhjusel ei saa kasutada ühtki järgnevatest mehhanismidest.

MIT-MAGIC-COOKIE NIS-autentimine

- - Kasutajapõhine juurdepääsu kontroll: X-serveri protsessi saab konfigureerida selliselt, et sisselogimisel (nt xdm 'i abil) luuakse võti, mida kasutatakse autentimiseks kliendi ja serveri vahel toimuva ülekande puhul. Vastav võti (MAGIC COOKIE) salvestatakse kasutaja isiklik kataloogi alla faili nimega .Xauthority ning X-kliendile saab seda edastada käsuga xauth . Kuigi MIT-MAGIC-COOKIE -mehhanism on ainult üks teatud liiki parool, mille ülekannet saab pealt kuulata, pakub see mehhanism koos NIS- võimalustega ja DES-krüpteeringuga rohkem turvalisust, mistõttu tuleks seda eelistada.

Turvatud kanal

- Juurdepääsu kontroll Secure Shell 'i kaudu: Side X-kliendi ja X-serveri vahel võib toimuda ka ssh -ühenduse turvatud kanali kaudu (vt M 5.64 Secure Shell (SSH)). Seejuures leiab aset nii arvutipõhine kui ka kasutajapõhine juurdepääsu kontroll. Autentimis- ja kasutajaandmed krüpteeritakse. X-Window tarkvara turvaliseks käitamiseks soovitatakse seetõttu kasutada Secure Shell' i.

Klaviatuurisisestuste pealtkuulamine

Lisaprogrammiga saab X-Window all muuta eemalasuva arvuti klahvivajutusi tekstiks ja seda lugeda. Klahvivajutuste pealtkuulamist saab takistada programmiga xterm , mis takistab asetleidnud KeyPress -sündmuste edastamist teistele programmidele. Selleks tuleb xterm -menüüs sisse lülitada valik secure keyboard -, et vastaval aknal oleks klaviatuurile ainuõiguslik juurdepääs.

Täiendav kontrollküsimus:

- Kas kasutajate jaoks on võimalus käsuga xhost + arvutipõhist juurdepääsu kontrolli välja lülitada takistatud?

M 4.10 Kodukeskjaama (PBX) terminalide paroolikaitse

Algatamise eest vastutavad: kodukeskjaama eest vastutav töötaja, IT- turbespetsialist
Rakendamise eest vastutavad: kasutaja, IT-turbespetsialist

Kodukeskjaamadel on mitmeid lõppseadmerakendusi ja -liideseid. Olenevalt keskjaamast võivad need rakendused või liidesed esineda erinevas vormis või erinevate nimetuste all. Mõne kindla rakenduse kasutusluba peab olema antud kodukeskjaamast, teised seadistatakse vastavatel lõppseadmetel.
Nii nagu keskjaamadel, võib ka lõppseadmetel lisaks telefonikaabliga ühendusvõimalusele olla ka muid liideseid. Siia kuulub näiteks Bluetooth, mis võimaldab kasutada vabakäesüsteemi, või traadita kohtvõrk, millega ühendatakse VoIP-i traadita telefonid LAN-iga ja otse kodukeskjaamaga. Mittekasutatavad liidesed ja rakendused tuleb desaktiveerida. Liideste kasutamisel tuleb need kõrvalistele isikutele ligipääsu vältimiseks juba varem autentimisega kaitsta. Kättesaadavate rakenduste arv peaks piirduma hädavajaliku miinimumiga ning põhimõtteliselt peaks olema võimalik kasutada vaid tööks vajalikke rakendusi. Nii välditakse seda, et kodukeskjaam satuks ilmaaegu oma rakenduste kaudu võimalike rünnakute objektiks. Võib olla, et mõnda kindlat rakendust rünnatakse eesmärgistatult, eriti seoses nende salajasuse ja kättesaadavusega. Keskjaama omanikule võib taoline väärkasutus aga tähendada lisaks ka täiendavaid kulutusi.

Lõppseadmete võimaliku väärkasutamisega seotud rakendused on näiteks:

- nn otse kõnelemine või automaatne kõne vastuvõtmine, kuna telefoni seda funktsiooni saab kasutada ruumis toimuva vestluse pealtkuulamiseks,
- kergesti juurdepääsetavate telefoniaparaatide väärkasutus, kuna kõrvalistel isikutel on võimalus asutuse kulul kõnesid pidada,
- kõne ümbersuunamine, kuna nt tahtmatu või tahtliku väärkasutuse tagajärjel ei ole telefoniühenduse kasutaja kättesaadav,
- ümberlülitamine, mis võimaldab helistajal toimuvat vestlust pealt kuulata,
- sissehelistamisega konverentsilülitus, kuna sel juhul võivad osalejad valida ise sellise lülituse, mida teised osalejad ei märka, ning nii on kõrvalisel isikul võimalus vestlust pealt kuulata ja
- erinevad ekspordiks ette nähtud rakendused (nt tunnistajate lülitamine kõnesse või pealtkuulamine), kuna neid on võimalik kasutada konfidentsiaalsuse printsiibi rikkumiseks.

Lõppseadmed tuleb etteantud võimaluste piires nii konfigureerida, et neid saaks turvakriitiliste asjaolude ilmnedes kohe hooldada. Mittekasutatavad või oma väärkasutuspotentsiaali tõttu kriitiliseks hinnatud rakendused tuleb kesksest seadmest nii kaugelt kui võimalik välja lülitada. Kui see võimalus on piiratud või kui võimalused ei ole piisavalt diferentseeritud, võib kesksed seadistused koos vastavate tõkestusseadistustega kombineerida lõppseadmele. Lõppseadmetele salvestatud ja vajadusel kasutatavad salajased andmed, nagu kontaktandmed või majasisesed telefoniraamatud, peavad olema turvatud lisakaitsemeetmetega. See kehtib

eriti mittekaitstud alal, nagu nt koosolekuruumis või allmaagaraažis paiknevate lõppseadmete kohta. Mõningal juhul on ka võimalik, et keskjaama kaudu lubatakse juurdepääs vastavatele lõppseadmeühendustele. Selleks, et ära hoida vabalt juurdepääsetavas kohas asuvate lõppseadmete omavolilisi konfiguratsioonimuudatusi, peavad need seadmed olema kaitstud parooli või PIN-iga.

Tehases varustatakse paljud lõppseadmed juba standardparooli või PIN-iga. Need standardparoolid tuleb kindlasti enne esmakordset kasutuselevõttu ümber muuta. Üldiselt peaks selliseid rakendusi nagu kõne ümbersuunamine, teistele aparaatidele tulnud kõnede vastuvõtmine ja muu sarnane, olema võimalik kasutada alles pärast autentimistunnuse sisestamist. Selleks, et hoida ära lõppseadme funktsioonide väärkasutust, tuleks kasutada paroolikaitse võimalust.
Kuna lõppseadme ja selle konfiguratsiooni eest vastutab kasutaja ise, on oluline, et kasutaja oleks sellest teadlik ja et ta oleks saanud vastava koolituse (vt M 3.82 Kodukeskjaama turvalise kasutamise koolitus).

Kontrollküsimused:

- Kas kodukeskjaama mittekasutatavatele ja seega tõenäoliselt mittevajalikele rakendustele on juurdepääs tõkestatud?
- Kas kodukeskjaama kõik mittekasutatavad liidesed on desaktiveeritud?
- Kas kodukeskjaamal rakendatakse paroolikaitset?

M 4.11 Kodukeskjaama (PBX) liideste turve

Algatamise eest vastutavad: kodukeskjaama eest vastutav töötaja, IT-turbespetsialist
Rakendamise eest vastutavad: administraator

Kodukeskjaama liidesed, mille kaudu süsteemi hallatakse, kujutavad endast kaitsmist vajavaid punkte. Seepärast tuleb neid eriliselt turvata. Mittekasutatavate või mittekaitstud liideste kaudu võib kõrvaline isik näiteks sülearvuti abil süsteemi manipuleerida. Sellisel juhul ei annaks paroolikaitse kasutamine kodukeskjaamas või pääslarakendusel tulemust. Eesmärgiks on ära hoida süsteemimanipulatsioon või vähemalt saada aru süsteemi manipuleerimise katsetest. Seepärast peavad kasutatavad liidesed olema hästi suletud ja vajadusel ka plommitud. Kasutamata liideseid võib kaitsta suletavate ja plommitavate katetega.

Täiendav kontrollküsimus:

- Kas kodukeskjaama mittevajalikke liideseid kaitstakse füüsiliste kaitsemehhanismidega?

M 4.13 Identifikaatorite hoolikas jaotamine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: administraator

Unix-süsteemides toimub protsesside ja failide kasutaja- ja grupitunnuste alusel muuhulgas ka aktsioonide põhjustajate tuvastamine ja volituste määramine. Seetõttu on oluline olla nende tunnuste määramisel võimalikult hoolikas. Iga Login -nimi, iga kasutaja-ID (UID) ja iga grupi-ID (GID) tohib esineda ainult korra. Ka pärast kasutaja või grupi kustutamist ei tohiks nende Login -nime ja UIDd / GIDd mõnda aega uuesti kasutada. Võrguühendusega süsteemide puhul tuleb süsteemideüleselt jälgida, et kasutajanimesid ja IDsid ei määrataks mitmekordselt. See on eriti oluline NFSi kasutamisel UIDde rakendamise pärast, et vältida andmete volitamata lugemist.

Iga kasutaja peab olema vähemalt ühe grupi liige. Iga failis /etc/passwd esinev GID peab olema defineeritud failis /etc/group. Iga grupp peab sisaldama ainult neid kasutajaid, kes on hädavajalikud. See on eriti oluline süsteemigruppide puhul (nt root, sys, bin, adm, news, uucp, nuucp või daemon).

UID 0 (Super-User) Login tohib lisaks süsteemiadministraatori root 'ile määrata ainult administratiivsete Login 'ide jaoks vastavalt eelnevalt kehtestatud reeglitele (vt M 2.33 Unixi ülemarollide jagamine).

Login -nimede ja UIDde/GIDde jaoks tuleks määrata nimeandmiskontseptsioonid. Lisaks tuleks regulaarselt kontrollida, kas kõik UIDd on korrektsed. Näiteks peavad need koosnema ainult numbritest, ega tohi sisaldada kehtetuid kombinatsioone nagu 00 või 000.

Faile /etc/passwd ja /etc/group ei tohi töödelda redaktoritega, kuna vead võivad oluliselt mõjutada süsteemi turvalisust. Kasutada tuleks eranditult vastavaid administreerimistööriistu, kuid need on väga süsteemispetsiifilised.

Kontrollküsimused:

- Milliste reeglite järgi määratakse IDd?
- Kas failide /etc/passwd ja /etc/group sisu kontrollitakse regulaarselt?
- Kas /etc/passwd UID-väli koosneb ainult numbritest?
- Kas kõik UIDd on korrektsed?

M 4.14 Kohustuslik paroolkaitse Unixi all

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: administraator

Unix-arvuti iga konto paroolkaitse tagab, et oma Login -nimega saab sisse logida ainult volitatud kasutaja, kuna pärast Login -nime sisestamist leiab aset parooli sisestamine autentimise eesmärgil.

Password sobiva versiooni kasutamine

Rakendades kasutajate ja gruppide jaoks paroole, tuleb järgida meetmes M 2.11 Paroolide kasutamise reeglid toodud juhiseid Tuleb arvestada, et teatud süsteemides kaasatakse paroolide kontrollimisse mitte kogu parool, vaid ainult piiratud arv selle tähemärke. Nende meetmete rakendamiseks tuleks kasutada ainult selliseid passwd versioone, mis tagavad kehtestatud reeglite järgimise, või rakendada administratiivseid meetmeid, nt Shell-skripte ja vastavaid cron -sissekandeid. Üheks täiendavaks võimaluseks on asendada Unixi standardkäsk passwd mõne teise parooliprogrammiga, millel on rohkem funktsioone. Nende hulka kuuluvad avalikud Public-Domain -programmid anlpasswd, npasswd ja passwd+ , mis kontrollivad uue parooli kvaliteeti juba kasutajapoolse paroolimuudatuse käigus ja keelduvad selle kasutuselevõtust, kui see peaks olema liiga lihtne. Neid on võimalik hankida nt FTP-serverist ftp://ftp.cert.dfn.de/pub/tools/password/. Paroolid ei tohi asetseda üldloetavas failis /etc/passwd, vaid kasutaja jaoks loetamatus shadow -paroolifailis. Igas uuemas Unix-süsteemis on vastav shadow -võimalus olemas, kuid ei ole pärast esmakordset installeerimist alati aktiivne (nt tuleb RedHat Linuxi all pärast standardset installeerimist aktiveerida shadow -paroolifaili kasutamine käsuga pwconv).

Paroolita kasutajatunnuste sulgemine

Faili /etc/passwd tuleb regulaarselt kontrollida, et seal ei leiduks kasutajatunnuseid, millel puudub parool. Sellise kasutajatunnuse leidmise korral tuleb vastav kasutaja sulgeda. Kui gruppidele on kehtestatud paroolikohustus, tuleb kontrollida faili /etc/group. Siiski on soovitav hoiduda paroolide kehtestamisest tervetele gruppidele ning igasse gruppi tuleks kanda võimalikult vähe kasutajaid. Grupikuuluvuse vahetamine erinevate gruppide vahel, kuhu kasutaja on sisse kantud, muutub seeläbi kergemaks ja volitamata vahetamine, st vastavate programmide abil erinevate paroolide läbiproovimine on võimatu. Kõiki Login 'e eriti neid, millel on UID 0, tuleb regulaarselt testida paroolide olemasolu ja paroolide kvaliteedi osas (vt lisaks M 2.11 Paroolide kasutamise reeglid ja M 4.26 Regulaarne turvakontroll Unix-süsteemis). Lisaks meetmes M 4.26 Regulaarne turvakontroll Unix-süsteemis kirjeldatud programmidele saab vastavaid Login 'e tuvastada ka järgnevate programmidega:

awk -F: '{if ($3=="0") print $1}' /etc/passwd
awk -F: '{if ($2=="") print $1}' /etc/passwd
Kontrollküsimused:

- Kas paroolide kasutamist kontrollitakse regulaarselt?
- Kas kasutajaid takistatakse nõrkade paroolide valimisel (nt anlpasswd abil)?

- Kui kaua paroolid kehtivad?

M 4.15 Turvaline sisselogimine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: administraator

Sisselogimisel tuleks kasutada Login -programmi või aktiveerida selline seadistus, mis lubaks rakendada järgnevaid meetmeid:

- Iga kasutaja peab saama isikliku tunnuse ja isikliku parooli. Ilma tunnuse või paroolita ei tohi juurdepääsu võimaldada. Parooli asemel võib kasutajat identifitseerida ka elektroonilise allkirja, paroolipiletite vms abil.
- Ebaõnnestunud Login -katsete arv peab olema piiratud. Pärast igat edutut sisselogimiskatset suureneb ooteaeg kuni järgmise sisselogimisvõimaluseni. Teatud arvu ebaõnnestunud katsete järel suletakse vastav kasutajatunnus ja/või terminal. Seejuures ei tohi vastav sulgemine takistada administraatori juurdepääsu, st administraatorile peab konsoolis pääsuvõimalus alles jääma.
- Kasutajale näidatakse sisselogimisel eelmise eduka sisselogimise kellaaega.
- Sisselogimisel teavitatakse kasutajat ebaõnnestunud sisselogimiskatsetest. Vajadusel tuleks seda teadet korrata ka veel mitme järgneva sisselogimise juures.
- Kasutajale näidatakse sisselogimisel eelmise väljalogimise aega. Seejuures eristatakse väljalogimisi, mis olid interaktiivsed ja selliseid, mis ei olnud interaktiivsed (taustprotsessidest väljalogimised).
- Sisselogimiseks võrkude kaudu, kus paroolid edastatakse ilma neid krüpteerimata, tasub kasutada ühekordseid paroole (vt ka M 5.34 Ühekordsed paroolid).

z/OS

Spetsiaalsed juhised sisselogimise turvamiseks z/OS all leiate meetmest M 4.213 Logimisprotsessi kaitse z/OS all all.

Täiendavad kontrollküsimused:

- Kas kasutajate tähelepanu on juhitud sellele, et nad peaksid kontrollima oma viimase eduka sisselogimise aega ja tegema kindlaks, kas see on loogiline?
- Kui sageli teavitatakse kasutajaid nende ebaõnnestunud sisselogimiskatsetest?

M 4.16 Konto- ja/või terminalipääsu piirangud

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator

Piirang väljaspool tööaega

Kasutaja konto ja/või terminal tuleks töövälisеks ajaks sulgeda. Kui sellega kaasneks liiga suur töömaht (nt väga ebaregulaarsete või sageli muutuvate tööaegade tõttu), tuleks vastav piirang kehtestada vähemalt neil aegadel, mis jäävad selgelt väljapoole tööaega.

Piirdumine teatud kindlate IT-süsteemidega

Kui töötaja kasutab võrgus ainult teatud kindlat terminali või IT-süsteemi, peaks kasutajatunnuse ja vastava parooli kasutamine piirduma vaid selle arvutiga, et vältida sisselogimist mõnest teisest arvutist. Eriti just administraator peaks ennast võimalusel ainult konsooli kaudu sisse logima. Seda saab sundida ka tehniliste meetmetega (vt M 4.21 Ülemaõiguste volitamatu võtu vältimine).

Atribuutide määramine seadmefailidele

Unixi all tuleb terminalide puhul määrata seadmedraiveri omanikuks vastav kasutaja. Niipea kui kasutaja on välja loginud, peaks taas automaatselt omanikuks saama root. Lugemisõigus tohiks olla ainult vastaval kasutajal. Kui kasutaja tahab vastu võtta teiste süsteemikasutajate teateid (nt talk abil), peab ta neile andma vastava seadmedraiveri jaoks kirjutusõiguse. Tuleb kontrollida, kas see on ikka ilmtingimata vajalik. PC-võrkudes saab piirata konto kasutamist mitmesse arvutisse korraga sisselogimiseks. Kaitseks ründajate märkamatu sissetungimise vastu tuleks kasutajate jaoks tõkestada võimalus, ennast samaaegselt mitmesse arvutisse sisse logida.

Kontrollküsimus:

- Kas kõikide kontode ja terminalide jaoks on määratletud ajapiirid, st ajutised juurdepääsupiirangud?

M 4.17 Tarbetute kontode ja terminalide blokeerimine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator

Kontod, mida pole tarvis pikema ja jooksul kasutada, tuleb sulgeda ja hiljem kustutada. Kui kontode kustutamisel jääb alles faile, millele ei vasta enam ükski olemasolev kasutaja, on oht, et need failid seotakse mõne hiljem registreeritud kasutajaga.

„Orvuks jäänud“ failide leidmine

Kasutajate eemaldamisel tuleb Unixis kustutada vastavad sissekanded /etc/passwd , /etc/group all ja kasutaja isiklikust kataloogist. Samuti tuleb jälgida, et kustutataks ka muud kasutajate sissekanded failides nagu /etc/hosts , shadow jms. Isikliku kataloogi failid tuleks eelnevalt varundada. Konto sulgemisel, kuid kindlasti enne konto kustutamist, tuleb selles teavitada vastavat kasutajat. Konto kustutamisel tuleb jälgida, et üles leitaks ka need kasutaja failid, mis ei asu tema isiklikus kataloogis. Seda saab nt teha programmiga find ja funktsiooniga - uid . Sellised failid tuleb kustutada või siduda teiste kasutajatega. Lisaks tuleb jälgida, et kustutataks töösolevad protsessid ja ootel ülesanded, nt Unixi all crontab .

Samuti tuleks terminalid, mida ei ole tarvis pikema ja jooksul kasutada, sulgeda ja hiljem eemaldada.

Unixi all tuleb süsteemi poolt määratud ebavajalikud Login ’id (nt sys , bin , adm , uucp , nuucp , daemon ja lp) sulgeda, tehes faili /etc/passwd vastavasse parooli-välja nt sissekande „LOCKED“. Kui loodav kasutaja vajab oma kontot ainult teatud piiratud aja jooksul, tuleks konto luua ainult selleks ajaks. Võib-olla on kasulik luua isegi kõik kontod ajapiiranguga ja neid regulaarselt (nt kord aastas) vastavalt vajadusele pikendada.

Kui on alust arvata, et kohtvõrgu kasutaja viibib pikemat aega eemal (puhkus, haigus, lähetus, . . .), tuleks tema konto selleks ajaks võrguserveris sulgeda, et tema kasutajatunnust ei saaks selle aja sees tööks kasutada. Iga kasutaja peab võrguadministraatorit teavitama oma pikemast eemalviibimisest.

Täiendavad kontrollküsimused:

- Kas kontrollitakse, milliseid kontosid pole juba pikemat aega kasutatud?
- Kas kontrollitakse, millised kontod on muutunud ebavajalikuks?
- Kas võrguadministraatorit informeeritakse olukordadest, kus võrgu kasutaja viibib pikemat aega eemal?
- Kas tagatakse, et kustutatud konto kõik failid seotakse kas teiste kasutajatega või kustutatakse?

M 4.18 Monitori- ja ainukasutajarežiimi pääsu reguleerimine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: administraator
Monitorirežiimi ja ainukasutajarežiimi buutimise takistamiseks tuleks võtta tarvitusele järgnevad meetmed:

- Kui võimalik (sõltuvalt Unixist ja kasutatavast riistvarast), tuleb Unix-serveri kaitseks kasutada BIOS-parooli.
- Ainukasutajarežiimis buutimisel tuleks küsida Super-User -parooli sisestamist, et volitamata isikutel oleks raskem Unix-serverile ligi pääseda.
- Kui klaviatuurilukud on olemas, tuleks neid süsteemikonsooli kaitsmiseks ka kasutada, et vältida juurdepääsu monitorirežiimile.

Käesolevat meedet täiendab meede M 4.21 Ülemaõiguste volitamatu võtu vältimine .

Kontrollküsimus:

- Kas juurdepääs konsoolile on kaitstud paroolide või muude meetmetega?

M 4.19 Unixi süsteemifailide ja -kataloogide atribuutide jaotuse piirangud

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: administraator

Kaudselt avatud programmide kontrollimine
Siin nimetatud meetmed kehtivad failide ja kataloogide puhul, mille eest vastutab administraator, st selliste puhul, mis on olulised kas kõikide kasutajate jaoks või mida kasutatakse administreerimise eesmärgil. Ainult ühe programmi volituste kontrollimisest ei piisa, kontrollida tuleb ka kõikide selle programmi kaudu avatavate programmide volitusi (eriti just Trooja hobuste vältimiseks). Kõikide süsteemifailide atribuudid peavad olema sisse seatud võimalikult selliselt, et neile pääseks ligi ainult süsteemiadministraator. Kataloogid tohivad kasutajatele anda ainult hädavajalikke privileege.

s-Bit'i vältimine
s-Bit'i tuleks kasutada ainult siis, kui see on ilmtingimata vajalik. Shell -skriptide puhul ei tohiks s-Bit olla määratletud. s-Bit'i tohivad määratleda ainult administraatorid, seejuures tuleb selle vajalikkust ka põhjendada ning vastav protseduur dokumenteerida. Kataloogides, milles peab kõigil kasutajatel olema kirjutusõigus (nt /tmp), tuleks määratleda t-Bit (Sticky-Bit).

Tervikluse kontroll
Unixi süsteemifailidele ja –kataloogidele määratud atribuutide terviklust tuleb regulaarselt kontrollida, nt Tripwire abil (vt lisaks M 4.26 Regulaarne turvakontroll Unix-süsteemis).

Kontrollküsimused:

- Kas atribuutide määramist Unixi süsteemfailidele kontrollitakse regulaarselt?
- Kas on olemas nimekirjad, mille alusel tehakse kontrolle?
- Kas s-Bit on määratletud ainult seal, kus seda ei õnnestu vältida?

M 4.20 Unixi kasutajafailide ja -kataloogide atribuutide jaotuse piirangud

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: administraator, kasutaja

Siin nimetatud meetmed kehtivad kasutaja failidele ja kataloogidele (kaasa arvatud meilifailidele).

Võõrjuurdepääsu takistamine
Kasutajad peavad oma failidele ja kataloogidele määrama sellised atribuudid, et teised kasutajad ei saaks nendele ligi pääseda. Kui aga ka teised kasutajad peavad ligi pääsema, tuleks sisse seada vastavad kasutajagrupid. Kasutajapõhiste konfiguratsioonifailide puhul nagu .profile, .exrc, .login, .cshrc peaks volitusi omama ainult vastav omanik. Unixi süsteemides on teatud programmidel kasutajapõhised konfiguratsioonifailid nagu .exrc, .emacs või .mailrc , mis töötatakse pärast programmi avamist automaatselt läbi, et määrata kasutajale sobivad parameetrid ja valikud. Et need ei saaks paigaldada Trooja hobuseid, peaks pääsuõiguseid olema ainult vastaval omanikul. Faili .exrc loetakse enne Editor 'ide ex või vi käivitamist. Kui samanimeline fail asub aktuaalses kataloogis, leiab teatud Unixi versioonides aset selle kontrollimine. Kõiki kasutatavaid Unixi versioone tuleb selles osas eelnevalt kontrollida, kuna iga kord, kui avatakse Editor, on võimalik käivitada ka operatsioonisüsteemi käskusid.

s-Bit'i vältimine
s-Bit'i tuleks kasutada ainult siis, kui see on ilmtingimata vajalik. Shell -skriptide puhul ei tohiks s-Bit olla määratletud. s-Bit'i tohiks määratleda ainult administraatori sekkumisel, selle vajadust tuleb põhjendada ja dokumenteerida.

umask
umask (user file creation mode mask) määrab iga kasutaja kohta kindlaks, millised pääsuõiguse reguleerimise atribuudid omistatakse tema poolt loodud uuele failile. Kasutajapõhistes konfiguratsioonifailides nagu /etc/profile või $HOME/.profile -failides peaks olema määratletud umask = 0027 (-rw-r——) või umask = 0077 (-rw———-), et uute failide failiatribuudid annaks õigused ainult selle loojale (vajadusel ka grupile).

Meilifailid
Meilifailide atribuute tuleks regulaarselt kontrollida, et juurdepääs nendele failidele oleks vaid nende omanikul. Unixi kasutajafailidele ja –kataloogidele määratud atribuutide terviklust tuleb regulaarselt kontrollida, nt Tripwire abil (vt M 4.26 Regulaarne turvakontroll Unix-süsteemis).

Kontrollküsimused:

- Kas kasutajad on informeeritud minimaalsete volituste määramise tähendusest?
- Kas administraator kontrollib määratud umask -väärtusi regulaarselt?
- Kas s-Bit on määratletud ainult seal, kus seda ei õnnestu vältida?

M 4.21 Ülemaõiguste volitamatu võtu vältimine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator

su-juurdepääsu piiramine

Käsuga su võib iga kasutaja saada Super-User -õigused, kui tal on olemas vastav parool. Kuna su puhul ei ole ebaõnnestunud katsete arv piiratud, kaasneb sellega suurem parooli leidmise oht, kui kasutatakse vastavate programmide kaasabi. Seetõttu peaks su 'le olema ligipääs ainult Super-User 'il. Alternatiivse lahendusena võib installeerida ka modifitseeritud su, mille puhul on ebaõnnestunud katsete arv piiratud, ooteaeg kuni järgmise su- avamisvõimaluseni suureneb pärast igat ebaõnnestunud sisselogimiskatset ja teatud arvu ebaõnnestunud katsete puhul suletakse avamisvõimalus ja/või terminal. Kõik su -käsu kasutamised tuleb logida. Kui süsteem võimaldab, võib Super-User' i sisselogimisnimeks määrata root 'i asemel midagi muud. Täiendavate Super-User-Login 'idena tuleks luua ainult administratiivseid Login 'e (vt M 2.33z Unixi ülemarollide jagamine).

Administreerimine ainult konsoolist

Administraator tohib töötada ainult läbi konsooli, et takistada liinide pealtkuulamise korral tema parooli teadasaamist. Solarise all saab seda saavutada näiteks faili /etc/default/login vastava konfigureerimisega. Selle asemel võib kasutada ka turvafunktsioone, mis takistavad administraatori paroolide spioneerimist. Sobivad mehhanismid on näiteks ühekordsed paroolid (vt meedet M 5.34z Ühekordsed paroolid ja Secure Shell M 5.64z Secure Shell (SSH)). BSD-Unixis saab root ennast sisse logida ainult terminalide kaudu, mis on tähistatud failis /etc/ttytab märkega secure. Kui see valik on kõikide terminalisissekannete juurest eemaldatud, saab administraator ennast terminalis root 'ina sisse logida ainult käsuga su. Tuleks kaaluda võimalust luua su käivitamiseks vastav kasutajagrupp, mis piiritleb selle kasutusvõimalusi.

Konsooli mitte tähistada märkega secure

Kui BSD-Unixis on konsool tähistatud failis /etc/ttytab märkega secure, ei küsita Single-User -režiimis käivitamisel parooli, mistõttu tuleb see sissekanne kindlasti eemaldada.

Ftp keelamine administratiivsete juurdepääsude jaoks

Fail /etc/ftpusers sisaldab Login -nimesid, mis ei tohi end ftp kaudu sisse logida. Ftp puhul edastatakse paroole kaitsmata tekstivormis. Seega tuleks siia sisse kanda administratiivsed juurdepääsud (root, bin, daemon, sys, adm, lp, smtp, uucp, nuucp, jne). Teatud tüüpinstallatsioonide puhul asub root mõnes muus failis.

s-Bit'i vältimine

Kui kasutaja või kasutaja programm käivitab mõne Super-User -faili (failid, mille omanikuks on root ja on määratletud s-Bit'iga), saab see kasutaja või programm käivitamisel Super-User -õigused. See on vajalik teatud rakenduste puhul, kuid seda saab ka kuritarvitada. Seega tuleb jälgida, et ainult hädavajalikud programmifailid oleks Super-User -failid ja et kolmandad isikud ei saaks lisada ühtki täiendavat Super-User -faili.

Vahetatavate andmekandjate seadmete automaatne ühendamine

Ühendatud kettal asuvate s-Bit programmidega saab kasutaja omandada Super-User- õigused. Automaatset ühendamist tuleks seega piirata. Teatud Unixi versioonid pakuvad koos mount -käsuga valikut, mille tagajärjel ignoreeritakse vastava failisüsteemi s-Bit'i. Vahetatavate andmekandjate puhul tasub kaaluda selle võimaluse kasutamist. Lubades ühiskasutusse katalooge, mida tohib teistest arvutitest ühendada, tuleb arvestada meetmes M 5.17 NFSi turvamehhanismid kirjeldatud piirangutega. Eeskätt ei tohiks lubada root -õigustega katalooge ja kirjutusõigustega katalooge võib lubada ainult vajadusel. Käesolevat meedet täiendab meede M 4.18 Monitori- ja ainukasutajarežiimi pääsu reguleerimine .

Kontrollküsimused:

- Kas käsku su saab käivitada ainult administraator?
- Kas käsu su kasutamine logitakse automaatselt?
- Kellele on antud konfiguratsioonifailide kirjutusõigusega juurdepääs?

M 4.22z Andmete konfidentsiaalsuse kao vältimine Unix-süsteemis

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: administraator

Käskudele juurdepääsu piiramine
Unixi käsud nagu *ps*, *finger*, *who, last* võimaldavad saada infot kasutaja kohta (nt töökäitumine). Paljudel Unixi derivaatidel on ka teisi käske, nt *listusers* Solarises. Tasub mõelda, kas nende käskude käivitamine peaks olema võimalik igal kasutajal (andmekaitse, *Login* -nimede spioneerimine jms). Kahtluse korral tuleks juurdepääsu nendele käskudele piirata.

Paroole ei tohi üle anda käsuparameetritena
Käskude kasutamisel ei tohi parameetritena sisestada konfidentsiaalset infot, nt paroole, kuna teised kasutajad saavad *ps* 'i abil seda infot näha.

Logifailid nagu *wtmp, utmp, wtmpx, utmpx,* jne peavad olema võimalusel sobivate pääsuõigustega volitamata avamise eest kaitstud, kuna nende kaudu võib saada kasutaja kohta palju infot.

M 4.23 Käitusfailide turvaline kutsumine

Algatamise eest vastutavad: IT-turvaosakond, administraator
Rakendamise eest vastutavad: administraator, kasutaja

Käitusfaile saab käivitada otse. Rakendusandmeid, nt tekstifaile, saab seevastu avada ainult vastava programmiga. Windowsi all tähistavad käitusfaile vastavad laiendid (nt .exe, .com, .vbs, .bat, .cmd) ja Unixi all failiõigused (x-Flag). Tuleb tagada, et avataks ainult kasutusse lubatud käitusfaile, aga mitte nt sissetoodud muudetud versioone (eriti Trooja hobuseid) (vt M 2.9 Aktsepteerimata riist- ja tarkvara kasutuse keeld). Ründaja võib käitusfaili selliselt muuta, et ta saab endale faili käivitava kasutaja privileegid. Selle takistamiseks tohivad käitusfailid olla ainult loetavad. Kirjutamisõigusega juurdepääs tohib olla ainult administraatoritel.

Käitusfaile, mille puhul on kirjutamisõigus vajalik, nt kuna neid veel arendatakse, tohib kasutada ainult eraldatud keskkonnas. Sama kehtib ka tarkvara puhul, st enne tootmissüsteemis kasutamise alustamist tuleb seda testida. Selleks võib kasutada eraldi testsüsteeme või eraldi kasutajakontosid, millel puuduvad muud õigused. Ainult nii saab vältida probleemide põhjustamist vastavate rakenduste poolt. Ka juba testitud tarkvara võib turvalisust mõjutada. Eriti kehtib see ülikeerukate rakenduste, nt veebiserveri puhul. Juba rakenduste käivitamisel peab olema tagatud, et iga protsess saaks ainult hädavajaliku hulga õigusi. Nii saab rünnaku puhul piirata kahjusid. Neid teenuseid ei tohi, kui võimalik, käivitada administraatori õigustega. Ka selleks võib kasutada piiratud volitustega kasutajakontosid. Tuleb mõelda õiguste selgele eraldamisele, Unixis või Linuxis näiteks *chroot* -keskkondade abil; mis aitaks piirata potentsiaalseid kahjusid. Lisaks tuleb tagada, et käivitada saaks ainult soovitud, kasutusse lubatud versiooni. Vastasel korral võib ründaja kopeerida sellesse kataloogi, mille jaoks tal on kirjutusõigus olemas, samanimelise modifitseeritud faili. Kui avamisel otsitakse kataloogidest faili, võidakse soovitud faili asemel käivitada modifitseeritud fail.

Paljudes operatsioonisüsteemides kantakse kataloogid, millest otsitakse käitusfaile, vastavas järjekorras *PATH* -muutuja alla. Kajastatud kataloogide arv peaks olema väike ja ülevaatlik. Suhtelised kataloogiandmed, mis sisaldavad hetkel aktuaalset töökataloogi, ei tohi asuda infona *PATH* -muutujas. Käitusfailid peavad olema salvestatud ainult selleks ettenähtud kataloogidesse. *PATH* -muutujas sisalduvate kataloogide kirjutusõigused tohib saada ainult vastav omanik. Seda tuleb regulaarselt kontrollida.

Täiendavad kontrollküsimused:

- Kas *PATH* -sissekandeid kontrollitakse regulaarselt?
- Kas käitusfailide asukohad on süsteemi peale laiali jaotatud?
- Kas käitusfailidele kehtestatud reeglid on kasutajatele teada?
- Kas käitusfailide terviklust kontrollitakse regulaarselt?

M 4.24 Järjekindla süsteemihalduse tagamine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond, administraator
Rakendamise eest vastutavad: administraator

Paljudes keerukates IT-süsteemides, nt Unixis või võrgus, on olemas administraatoriroll, millele ei kehti ükski piirang. Unixis on selleks *Super-User root,* Novell-võrgus *SUPERVISOR* või *admin*. Puuduvate piirangute tõttu on vigade või kuritarvitamise oht eriti suur.

Ärge töötage *Super-User-Login* 'i all
Vigade vältimiseks tuleb *Super-User-Login* 'i all töötada ainult siis, kui see on hädavajalik. Kõiki muid töid peab ka administraator tegema mõne muu kui administraatoritunnuse alt. Eriti oluline on hoiduda teiste kasutajate programmide käivitamisest administraatoritunnuse alt. Lisaks peaks rutiinne süsteemihaldus (nt varundamine, uue kasutaja loomine) toimuma ainult menüü alt juhtides.

Administraatoritevahelised kokkulepped
Ülesannete jaotamisega, reeglite püstitamisega ja kokkulepete saavutamisega tuleb tagada, et administraatorid ei teeks vastastikku segavaid või poolikuks jäävaid töid. Näiteks ei tohi mitu administraatorit samaaegselt töödelda ja muuta ühte ja sama faili, kuna kehtima jääb ainult viimati salvestatud versioon.

Secure Shell 'i kasutamine
Kui esineb terminali liinide pealtkuulamise oht, peaks administraator töötama ainult läbi konsooli, et vältida paroolide pealtkuulamist. Unix-süsteemide administreerimisel saab kasutada krüpteeritud sidet *Secure Shell* protokolliga. See võimaldab turvaliselt administreerida kaugemalasuvaid tööjaamu (vt M 5.64 Secure Shell (SSH)). Kõikide administraatorite jaoks tuleb lisaks määrata täiendavad kasutajatunnused, millele antakse ainult piiratud õigused ning neid peavad administraatorid kasutama administreerimisväliste ülesannete jaoks. Tööde jaoks, mis pole administreerimisega seotud, peavad administraatorid eranditult kasutama täiendavaid kasutajatunnuseid.

Muudatuste dokumenteerimine
Kõik tehtud muudatused tuleb dokumenteerida, et tagada nende kontrollitavus ja kergendada tööülesannete jaotamist (vt M 2.34 IT-süsteemi muutuste dokumenteerimine). Administreerimistegevuse hilisema kontrolli jaoks saab Unixi käsuga *script* luua sisestatud käskude logi. See käsk logib kogu terminaliistungi ASCII-faili. Sellise faili võib koostada näiteks juhul, kui on tarvis elektroonilist või väljaprinditud administreerimispäevikut.

Täiendavad kontrollküsimused:

- Kuidas tagatakse, et administraatori sekkumised ei tekita probleeme?

- Kas enne suuremaid muudatusi toimub varundamine?
- Kas administraatoritel on täiendavad kasutajatunnused, millel on piiratud õigused?
- Kas standardina kasutatakse täiendavaid kasutajatunnuseid?
- Kas peetakse administreerimispäevikut? Kas seal dokumenteeritakse kõik muudatused?

M 4.25 Logimine Unix-süsteemis

Algatamise eest vastutavad: IT-juht, IT turvaosakond

Rakendamise eest vastutavad: administraator

Unix-süsteemi logimisvõimalusi tuleb kasutada ning vajaduse korral täiendada ka veel programmide või kestaskriptidega.

Kasutusele tuleks võtta järgmised meetmed:

- Logifaile tuleb regulaarselt analüüsida. Analüüsimise ajad ei tohi olla korrapärased, kuna ründaja võib seda asjaolu ära kasutada. Näiteks kui administraator kontrollib süsteemis kajastunud sündmusi iga päev kell 17.00, saab ründaja alates kella 18.00-st märkamatult tegutseda.
- Olenevalt logitava sündmuse liigist võib olla vaja sellele võimalikult kiiresti reageerida. Et administraatorit sellistest sündmustest (nt liiga suur logifail, olulised katkenud serveriprotsessid, mitu root-sisselogimise katset ebatavalistel aegadel jne) automaatselt informeerida, tuleks kasutada alarmi jaoks poolautomaatseid logifaili parsereid (nt swatch, logsurfer või checksyslog).
- Logifailid tuleb vajaduse korral varundada enne, kui need muutuvad liiga suureks või enne, kui süsteem need kustutab. Tuleb kontrollida, milliste seaduses või lepingus ettenähtud säilitusaegadega tuleb arvestada.
- Failides wtmp, utmp, wtmpx, utmpx jne sisalduvasse infosse tuleks suhtuda eelarvamusega, kuna nende failidega on lihtne manipuleerida.
- Logifailide failiatribuudid peavad olema sellised, et volitamata isikud ei suudaks logifaile muuta ega analüüsida.
- Koostada ja kontrollida tuleb vähemalt järgmised logifailid: sisselogimised (ka ebaõnnestunud), su avamine, vealogide fail / oluliste sündmuste logimine (tõrkelogi), administraatori tegevused (eriti juurkasutaja antud käsud). Lisainfot leiate meetmest M 4.106 Süsteemi logimise aktiveerimine (Unix) .
- Käsk last näitab iga kasutaja sisse- ja väljalogimisinfot, nagu nt aega ja terminali. Administraator peaks selle käsuga regulaarselt kontrollima, kas kasutajad logivad ennast sisse läbi ebatavaliste kanalite, nt modemi või FTP kaudu.

Eriotstarbeline Loghost

Kui logifailid tekivad mitmes süsteemis, on soovitatav kasutada eriotstarbelist Loghost'i, mis on eriti tugevalt turvatud. Syslog-teadete edasisuunamine (forward) sellele Loghost'ile tuleb aktiveerida Syslog-konfiguratsioonifailis (vt M 4.106 Süsteemi logimise aktiveerimine (Unix)).

Tekkivaid logifaile tohib kasutada ainult IT-süsteemide nõuetekohase kasutamise kontrollimiseks, muu otstarve, nt kasutajate edukusprofiilide koostamine, on keelatud (vt M 2.110 Andmeprivaatsuse suunised logimisprotseduurides).

Kontrollküsimused:

- Kas logifaile analüüsitakse regulaarselt?
- Kas logimine on veel aktiivne ja kas mälumahtu on piisavalt?

- Kas logimise konfiguratsioonifailide terviklust kontrollitakse ja logitakse regulaarselt (nt Tripwire abil)?
- Kuidas arhiveeritakse logifaile ning kuidas kaitstakse neid manipuleerimise ja volitamata avamise eest?

M 4.26 Regulaarne turvakontroll Unix-süsteemis

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: administraator

Unix-operatsioonisüsteemid pakuvad standardlahendustes erinevaid turvafunktsioone. Abi on neist siiski ainult mõistliku kasutamise korral. Selleks vajalikke seadistusi tuleks abiprogrammidega automaatselt kontrollida, et:

- tuvastada ja kõrvaldada Unix-süsteemis esinevad ebakõlad ja
- anda süsteemihaldurile võimalus Unixi operatsioonisüsteemi hallata nii, olemasolevaid turvamehhanisme kasutatakse optimaalselt ära.

Vastavat kontrolli saab teostada Unix-süsteemides olemasolevate programmidega, isekirjutatud *Shell* -skriptidega või *Public-Domain* -programmidega. Teatud Unixi-variantide jaoks on olemas ka kommertsprogrammid.
Näited

- pwck - See käsk kuulub standardsete operatsioonisüsteemi käskude hulka. Selle käsuga saab kontrollida faili */etc/passwd* ühtsust. Kontrollitakse, kas kõik vajalikud sissekanded on tehtud, kas kasutaja jaoks on olemas *Login* -kataloog ning kas *Login* -programm on olemas. Sarnaseid funktsioone sisaldab Solarises käsk *logins*, millega saab leida ka paroolita kontosid.
- grpck - Selle käsuga kontrollitakse faili */etc/group* ühtsust. See kuulub samuti standardsete operatsioonisüsteemide käskude hulka. Kontrollitakse, kas kõik vajalikud sissekanded on tehtud, kas kõik grupi liikmed on ka kasutajaparoolide failis olemas ning kas grupinumber kattub seal märgituga.
- tripwire - Selle programmiga saab teha failide tervikluskontrolle. Selleks luuakse failide kontrollsummad ja salvestatakse need andmebaasi. *tripwire* on saadaval erinevates tasuta versioonides.
- cops - See *Public-Domain* -programm on mõeldud Unix-süsteemide turvalisuse kontrollimiseks, nt kontrollitakse erinevaid süsteemiseadistusi, pääsuõigusi, SUID-faile jms ning otsitakse potentsiaalseid turvalünki.
- tiger - Selle *Public-Domain* -programmiga saate Unix-süsteemides kontrollida sarnaselt *cops'* iga turvalünkade esinemist.
- SATAN - Selle *Public-Domain* -programmiga saab analüüsida võrgu turvalisust. See kontrollib võrkuühendatud Unix-süsteemi tuntud, kuid sageli kõrvaldamata puudujääkide osas.
- crack - Selle *Public-Domai*n -programmiga saab kontrollida, kas kasutatakse liiga lihtsaid ja kergesti äraarvatavaid paroole.

Täiendavad kontrollküsimused:

- Kas turvakontrolli teostamine ja tulemused dokumenteeritakse?
- Millised puudujääke kontrollivad kasutatavad programmid ja Shell -skriptid?

M 4.27 Sülearvuti paroolkaitse

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: kasutajad

Igal sülearvutil peab olema juurdepääsu piirang, mis ei lase arvutit volitamatult kasutada. Muude turvamehhanismide puudumisel peaks sülearvutite puhul minimaalse kaitse tagamiseks aktiveerima BIOS-buutimiskaitse, kui selle kasutamine on võimalik. Arvuti buudib alles pärast õige parooli sisestamist. Paroolide kasutamise reeglid leiate meetmest M 2.11 Paroolide kasutamise reeglid . Lisaks pakuvad peaaegu kõik operatsioonisüsteemid võimalust kasutada sisselogimisparoole ja määrata neile sobivaid piiranguid (nt minimaalne pikkus, kasutusiga jne). Kuna need vahendid pakuvad ainult piiratud turvalisust, tasub sülearvutites, millesse koguneb kiirelt suur hulk konfidentsiaalseid andmeid, kasutada täiendavat turvariistvara või -tarkvara. Selle alla kuuluvad nt kiipkaardid või *Token* 'id, mis turvavad autentimist.

Kui paroolivahendeid pole paigaldatud, tuleks, juhul kui andmeid ei krüpteerita, keelata kõvakettale konfidentsiaalse info salvestamine ja salvestada selle asemel mobiilsetele andmekandjatele, nt diskettidele või USB-mälupulkadele. Viimaseid tuleks hoida sülearvutitest eraldi, nt rahakotis. Lühikeste töökatkestuste puhul tuleb kindlasti aktiveerida juurdepääsu piirang, nt ekraanisäästur. Kui on tõenäoline, et töökatkestus on pikem, tuleb sülearvuti välja lülitada.

Täiendavad kontrollküsimused:

- Kas sülearvutite jaoks on olemas piisav juurdepääsu kaitse? Kas juurdepääsu kaitse õige kasutamise reeglitest peetakse kinni?
- Kas sülearvuti üleandmisel vahetatakse parooli?

M 4.28z Sülearvuti tarkvara reinstalleerimine kasutaja vahetumisel

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: administraator

Kui kasutaja vahetab sülearvutit, tuleb tagada, et selles ei leiduks ei konfidentsiaalseid andmeid ega arvutiviirusi. Andmete kustutamiseks võib kasutada täielikku ülekirjutamist või spetsiaalseid kustutusprogramme. Seejärel tuleb kasutada värskendatud viirusetõrjeprogrammi. Mõlemad protseduurid tuleb läbi teha kõikide kasutatud andmekandjate puhul nagu nt kõvakettad, disketid, CDd või USB-mälupulgad.

Sülearvuti kõvaketas on siiski soovitatav täielikult formaatida ja seejärel vajalik tarkvara ja andmed uuesti installeerida. Seejuures tuleb arvestada meetmega M 4.235 Andmete seisu võrdsustamine sülearvutis .

Täiendav kontrollküsimus:

- Kas enne formaatimist veendutakse, et eelmine kasutaja ei vaja enam vastavas sülearvutis leiduvaid andmeid?

M 4.29z Kaasaskantavatele IT-süsteemidele mõeldud krüpteerimistoote kasutamine

Algatamise eest vastutavad: IT-juht, IT turvaosakond

Rakendamise eest vastutavad: kasutajad

Takistamaks olukorda, kus hoolimata kõikidest ettevaatusabinõudest võidakse varastatud kaasaskantavast IT-süsteemist lugeda konfidentsiaalset infot, tuleks kasutada krüpteerimisprogrammi. Müügilolevate toodetega saab üksikuid faile, teatud alasid või kogu kõvaketast krüpteerida selliselt, et andmeid saavad lugeda ja kasutada ainult need, kellel on olemas vastav salajane võti.

Krüpteerimise turvalisus sõltub seejuures kolmest erinevast asjaolust:

- Kasutatav krüpteerimisalgoritm peab olema konstrueeritud selliselt, et kasutatud võtit omamata ei saaks krüpteeritud tekstist luua loetavat teksti. See tähendab, et algoritmi murdmise/dekrüpteerimise töövaev peab olema võrreldes saadava infoga liiga suur.
- Tuleb valida sobiv võti. Võimaluse korral tuleks genereerida juhuslik võti. Kui võtit saab valida sarnaselt parooli valimisele, tuleb järgida sellekohaseid reegleid, mis on toodud meetmes M 2.11 Paroolide kasutamise reeglid .
- Krüpteerimisalgoritmi (programmi), krüpteeritud teksti ja võtit ei tohi hoida koos ühel andmekandjal. Võtit tuleks hoida eraldi. Näiteks võib selle kirja panna pangakaardisuurusele pappkaardile ja hoida seda kaarti rahakotis.

Krüptograafilised võtmed tuleks salvestada vahetatavale andmekandjale, nt disketile, kiipkaardile või USB mälupulgale ning neid tuleks hoida kaasaskantavatest IT-süsteemidest eraldi (nt rahakotis).

Krüpteerimine võib toimuda sidus- või vallasrežiimis. Sidusrežiim tähendab, et krüpteeritakse kõik kõvaketta (või partitsiooni) andmed, ilma et kasutaja peaks seda ise aktiivselt korraldama. Vallasrežiimis krüpteerimise peab kasutaja käivitama iseseisvalt. Kasutaja peab siis ka otsustama, millised failid vajavad krüpteerimist.

Krüptograafiliste meetodite valimisel ja kasutamisel tuleb arvestada mooduliga B 1.7 Krüptokontseptsioon .

Kontrollküsimused:

- Kas kasutajaid õpetatakse krüpteerimisprogramme kasutama?
- Kas andmeid ja võtmeid hoitakse eraldi?

M 4.30 Rakendusprogrammide turvavahendite kasutamine

Algatamise eest vastutavad: IT-juht, IT turvaosakond
Rakendamise eest vastutavad: kasutajad

Mõningad PC-valdkonna standardsed tooted pakuvad mitmeid kasulikke IT turvafunktsioone, mille kvaliteet võib olla küll erinev, kuid need takistavad volitamata isikute juurdepääsu ja vähendavad võimalikke kahjusid.

Alljärgnevalt on lühidalt kirjeldatud viit sellist funktsiooni:

- Paroolkaitse programmi avamisel: programmi saab käivitada ainult siis, kui eelnevalt on sisestatud õige parool. See takistab programmi volitamata kasutamist.
- Üksikute failide juurdepääsukaitse: programm saab kaitstud faili avada ainult siis, kui sisestatakse selle failiga seotud parool. See ei lase programmil teatud failidele volituseta ligi pääseda.
- Vahetulemuste automaatne salvestamine: programm salvestab vahetulemusi automaatselt, seega mõjutab voolukatkestus ainult neid andmemuudatusi, mis leidsid aset pärast vastavat automaatset salvestamist.
- Eelmise failiversiooni automaatne varundamine: kui salvestatakse fail, mille puhul on samas asukohas sama nimega fail juba olemas, siis kõnealust eelmist faili ei kustutata, vaid sellele antakse teine tähis. Niimoodi takistatakse samanimelise faili juhuslikku kustutamist.
- Failide krüpteerimine: programm suudab faili salvestada krüpteeritult, mis takistab selle volitamata avamist. Faili sisule pääsevad ligi ainult need, kellel on vastavad salajased krüpteerimisvõtmed.
- Makrode automaatne kuvamine failides: selle funktsiooni eesmärk on takistada makrode automaatset käivitamist (makroviirustevastane kaitse).

Olenevalt selles, millist tarkvara ja sellega kaasaskäivaid täiendavaid turvafunktsioone rakendatakse, võib olla mõistlik neid funktsioone kasutada. Mobiilsete IT-süsteemide puhul tasub eriti kasutada paroolkaitset programmide avamisel ja automaatset salvestamist.

Kontrollküsimused:

- Milliseid turvafunktsioone pakuvad kasutatavad tarkvaratooted?
- Milliseid nendest funktsioonidest kasutatakse regulaarselt?
- Kas kasutajaid informeeritakse nende funktsioonide olemasolust?
- Kas käsiraamatutes või sertifitseerimisaruannetes käsitletud turvalisust puudutavaid juhiseid järgitakse?

M 4.31 Toite tagamine mobiilsel kasutamisel

Algatamise eest vastutavad: kasutajad
Rakendamise eest vastutavad: kasutajad

Kaasaskantavate PCde ja PDAde elektritoite tagamiseks kasutatakse reeglina akusid või patareisid. Sõltuvalt aku või patarei mahtuvusest ja mobiilse seadme ülesehitusest jätkub toidet vaid piiratud ajaks, nt mõneks tunniks. Et pinge katkemisega ei kaoks muutmälust vajalikke andmeid, tuleb järgida mõningaid raamtingimusi:

- Mobiilse lõppseadme hoiatavaid näite (kui on olemas), mis informeerivad aku tühjenemisest, ei tohi ignoreerida. Hoiatavad teated peavad olema seadistatud selliselt, et pärast esimest hoiatust jääks piisavalt aega andmete varundamiseks.
- Kui on tõenäoline, et mobiilne kasutamine toimub pikemat aega, tuleb laetavad patareid eelnevalt täis laadida ja vajadusel asenduspatareid kaasa võtta.
- Eriti just vanemate akude puhul on kasutusaeg lühem ja need võivad mahtuvuse lõpupoole väga kiiresti tühjeneda. Töötades tuleb seetõttu andmeid regulaarselt varundada, et vältida andmekadu. Kuna sellised akud võivad ka ooterežiimis kiiresti tühjeneda, tuleks laetust regulaarselt kontrollida ja sülearvuti või pihuarvuti konfiguratsioonist tehtud andmevarundusi hädajuhuks endaga kaasas kanda. Kui aku ilmutab vananemise märke, tasub see võimalikult ruttu uuema vastu välja vahetada.
- Laadimisel tuleks arvestada juhistega mobiilse IT-süsteemi kasutusjuhendis, et mitte lühendada asjatult aku eluiga.
- Enne reisile minekut või mobiilse IT-süsteemi üleandmist tuleb tagada, akud ja patareid oleksid piisavalt laetud. Akude laetust tuleks regulaarselt kontrollida, kuna akud tühjenevad aja jooksul ka siis, kui seadet ei kasutata.
- Toitejuhe võiks võimalusel alati kaasas olla.

Lisaks tasub mobiilse IT-süsteemi kasutamise ajal salvestada andmeid lühikeste ajavahemike tagant mõnele püsimäluga andmekandjale. Selleks võib kasutada ka standardprogrammide automaatset andmevarundust.

Kui juba ette on teada, et mobiilset IT-süsteemi on tarvis kasutada pikema aja jooksul, nt töölähetusel viibides, tuleks endaga kaasa võtta ka laetud varuaku. Varuakut tuleb hoida kaitsvas ümbrises, kuna aku kokkupuutel juhtivate materjalidega võivad tagajärjeks olla ülekuumenemisest ja süttimisest tekkivad kahjustused. Vastava õnnestuse võivad põhjustada ka täiesti igapäevased esemed nagu võtmed ja ketid.
Enne ükskõik millise IT-süsteemi aku vahetamist tuleks seade kindlasti välja lülitada, et mitte kahjustada selle mälu.

Teadmiseks

Halvim koht akude hoidmiseks (esmajoones just liitium-ioon-akude hoidmiseks) on kohapeal kasutatav sisselülitatud sülearvuti, seega sülearvuti, mis on niikuinii pidevalt vooluvõrku ühendatud. Dokkimisjaamas kasutamisel tuleks seega aku

kindlasti eelnevalt eemaldada.

Enne ükskõik millise IT-süsteemi aku vahetamist tuleks seade kindlasti välja lülitada, et mitte kahjustada selle mälu.

Kontrollküsimus:

- Kas kasutajatele on selgitatud aku optimaalse käsitsemise põhimõtteid?
- Kas kasutajaid on teavitatud, kuidas tagada kaasaskantavate seadmete optimaalne energiavarustus?
- Kas varuakusid hoitakse ja transporditakse vastavates kaitsepakendites?

M 4.32 Andmekandjate füüsiline kustutamine enne ja pärast nende kasutamist

Turvameetme kasutuselevõtmise eest vastutab: infoturbeosakond

Rakendamise eest vastutavad: erialavaldkondade eest vastutavad isikud

Peale meetmes M 2.167 Andmete kustutamiseks või hävitamiseks sobivate lahenduste valik antavate nõuannete andmekandjate kustutamiseks või hävitamiseks tuleb andmekandjate vahetamisel pidada silmas ka järgmisi aspekte. Magnetilised andmekandjad, mida vahetamisel kasutatakse, tuleks enne seda, kui neile kirjutatakse edastatav informatsioon, füüsiliselt kustutada. Nii tagatakse, et ei edastata jääkandmeid, mida ei ole nende saajal õigust saada.

Normaalse turvavajaduse jaoks piisav füüsiline kustutus toimub nii, et kogu andmekandja või vähemalt selle kasutatud piirkonnad kirjutatakse teatud kindla mustriga täielikult üle. Ka andmekandja formaatimine on võimalik, kui seda ei saa tühistada. Üksikute failide kustutamist tuleks vältida, sest sel juhul jääb jääkinformatsioon, mis võimaldab kustutatud faile rekonstrueerida, sageli alles.

Tavaliselt on ülekantud failid ka nende saaja jaoks kaitsmist väärt. Ka sel juhul on pärast andmete taassalvestamist andmekandja füüsiline kustutamine ette nähtud. Mittekustutatavate andmekandjate (nt WORMid) kasutamisest andmete vahetamise eesmärgil tuleb loobuda, kui nendele on salvestatud muu informatsioon, mis ei ole saajale mõeldud ja mida ei võimalik kustutada.

Kontrollküsimused:

- Kas andmekandjate vahetamise eest vastutav isik tunneb füüsilise kustutamise meetodeid?
- Kas füüsiliseks kustutamiseks kasutatavad programmid on nende töötajate käsutuses?
- Kas kaitsmist vajava informatsiooni saajaid on edastatavate andmete kaitsmise vajadusest informeeritud?

M 4.33 Viirustõrjeprogrammi kasutamine andmekandjate vahetamisel ja andmete edastamisel

Turvameetme kasutuselevõtmise eest vastutab: infoturbeosakond

Algatamise eest vastutavad: kasutajad

Lisaks punktis M 2.3 Andmekandjate haldus käsitletud kasutusjuhistele tuleks vahetult enne ja vahetult pärast andmete edastamist ning diskettide või muude andmekandjate vahetamist või edastamist kontrollida arvutit seoses viirustega (vt M 4.3 Viirusetõrjeprogrammide kasutamine). Seejuures tuleb silmas pidada, et kasutatav viirusetõrjeprogramm suudaks ka makroviirusi ära tunda.

Saatja kontrollimise protokoll tuleks edastatavale andmekandjale kaasa panna või lisada elektrooniliselt saadetavale failile manusena. Selle protokolli koopia on soovitatav alles hoida. Selle protokolli põhjal oleks saajal võimalik saada edastatud andmete terviklusest esmane ülevaade. See ei vabasta siiski vajadusest läbi viia uus viirusetõrje. Teiselt poolt võib saatja nende kaebuste korral, mis võidakse esitada andmete viirustega nakatatuse tõttu, välja selgitada, et andmete nakatumine tema arvutis oli ebatõenäoline.

Kontrollküsimused:

- Kas kasutatakse võimalikult uut viirusetõrjeprogrammi?
- Kas vahetamiseks mõeldud andmeid kontrollitakse enne nende vahetamist seoses viirustega?
- Kas selle kontrollimise protokoll edastatakse saatjale?
- Kas saadud faile ja andmekandjaid kontrollitakse enne nende arvutisse laadimist seoses viirustega nakatatuga?

M 4.34z Krüpteerimise, kontrollsummade ja digitaalallkirjade rakendamine

Turvameetme kasutuselevõtmise eest vastutab: infoturbeosakond

Turvameetme rakendamise eest vastutab: kasutaja

Kui edastatakse konfidentsiaalset informatsiooni või informatsiooni, mis peab säilitama oma tervikluse ja kui eksisteerib mingi võimalus, et need andmed satuvad volitamata isikute kätte ja need isikud võivad nende andmetega manipuleerida või saavad neid tehnilisi vigu ära kasutades muuta, tuleks andmete transportimisel või edastamisel rakendada nende kaitsmiseks krüptograafilisi protseduure.

Konfidentsiaalsuse kaitsmine krüpteerimise teel

Konfidentsiaalse informatsiooni edastamiseks on vaja need krüpteerida. Krüpteerimismeetodi olulised tunnused on algoritmi kvaliteet ja võtme valik. Tunnustatud algoritm, mis on normaalse turvavajaduse jaoks piisav, on 3DES, mis põhineb Data Encryption Standardil (DES). Seda on lihtne programmeerida eelkõige seetõttu, et programmi lähtetekst on paljudes erialastes raamatutes trükitud programmeerimiskeeles C. Edastatava informatsiooni konfidentsiaalsusele esitatavatele nõuetele vastamiseks peavad saatja ja saaja IT-süsteemid tagama krüpteerimisprogrammile piisava kaitse. Võimaluse korral tuleks see programm salvestada vahetatavale andmekandjale, mida hoitakse reeglina luku taga, ning mida installeeritakse ja kasutatakse ainult vajaduse korral.

Tervikluse kaitsmine kontrollsummade, krüpteerimise või digitaalse allkirja abil

Kui andmete vahetamisel tuleb tagada ainult edastatavate andmete terviklus, siis tuleb vahet teha sellel, kas andmeid tuleb kaitsta ainult juhuslike muudatuste, nt edastamisel tekkivate vigade või ka nendega manipuleerimise eest. Kui tuleb tuvastada ainult juhuslikke muudatusi, siis võib kasutada kontrollsumma meetodeid (nt tsükkelkoodkontrollid) või vigu korrigeerivaid koode. Lisaks pakuvad manipuleerimise vastu kaitset meetodid, mis loovad edastatava informatsiooni põhjal sümmeetrilist krüpteerimisalgoritmi (nt 3DES) kasutades sõnumiautentimiskoodi (message authentication code, MAC). Muud meetodid kasutavad asümmeetrilist krüpteerimisalgoritmi (nt RSA) koos räsifunktsiooniga ja loovad „digitaalse allkirja". Selliselt loodud „sõrmejäljed" (kontrollsumma, vigu korrigeerivad koodid, MAC, digitaalne allkiri) edastatakse saajale koos informatsiooniga, kes saab neid kontrollida.

Vajalike võtmete edastamiseks või vahetamiseks vajalik teave on ära toodud punktis M 2.46 Krüpteerimise õige korraldus . Krüptograafiliste meetodite ja toodete kasutamiseks vajalik muu informatsioon on esitatud moodulis B 1.7 Krüptokontseptsioon .

Kontrollküsimused:

- Kas konfidentsiaalsuse või tervikluse kaitsmiseks antakse töötajate käsutusse krüpteerimisprogrammid või kontrollsumma meetodid?
- Kas andmete edastamise eest vastutavaid töötajaid on võtmete nõuetekohasest kasutamisest informeeritud?
- Kas konfidentsiaalsuse/tervikluse kaitse tuleb tagada ainult andmete edastamisel/transportimisel või ka saaja või saatja süsteemis?

M 4.35z Saatmisele eelnev andmete kontroll

Turvameetme kasutuselevõtmise eest vastutab: Infoturbeosakond
Turvameetme rakendamise eest vastutab: Kasutajad

Enne andmekandja saatmist tuleb seda selles suhtes kontrollida, kas soovitud informatsioon – ja ainult see – on andmekandjalt rekonstrueeritav. Seda tuleb kontrollida nii kirjalike dokumentide kui ka elektrooniliste andmekandjate puhul. Ka kirjad ja muud analoogsed andmekandjad tuleks enne saatmist veelkord läbi vaadata, kas nad on täielikud ega sisalda lisainformatsiooni, mida ei pea edastama. See on oluline eelkõige siis, kui toimikute osi, milles nimetatakse nimesid, ei tohi konfidentsiaalsetel põhjustel kolmandatele isikutele edastada. Selleks saab need informatsiooniosad näit. mustaks värvides loetamatuks muuta. Et aga mustaksvärvitud informatsiooni on sageli võimalik suurema vaevata jälle loetavaks muuta, siis on siiski parem need edastamiseks toimikutest täiesti eemaldada, näit. enne väljaprintimist lähtefaili koopiast kustutada. Olenevalt informatsiooni kaitsmise vajadusest on selleks mitu võimalust.

Dokumendid tuleb struktureerida vastavalt nende konfidentsiaalsusele

- Dokumendid peaksid olema võimaluse korral struktureeritud nii, et mitteavalikku informatsiooni oleks lihtne eemaldada, näit. võiks see olla esitatud ainult lisas. Lisa peaks siis olema salvestatud ka elektrooniliselt eraldi failina, mis on klassifitseeritud konfidentsiaalsena.
- Kui dokumendid on juba olemas sellisel kujul, mis ei võimalda konfidentsiaalseid osi lihtsalt eemaldada, tuleb kaitsmist vajav informatsioon eemaldada enne dokumendi edastamist. Seejuures on põhiprobleemideks kõikide tundlikku informatsiooni sisaldavate tekstiosade identifitseerimine ja hoolikas eemaldamine. Et juba seda praktikas sageli ei tehta, siis tuleks selliste „kahjutuks tehtud“ dokumentide edastamisest võimalikult loobuda. Kui see aga on siiski vajalik, tuleb kogu kriitiline informatsioon eemaldada ja antud dokumentide turvatase uuesti kindlaks määrata. Igal juhul peavad dokumendid enne nende väljastamist läbima uue lubatavuskontrolli.

Paberdokumentides värvitakse tundlik informatsioon sageli ainult mustaks. Selleks tuleb läbi viia järgmised sammud:

- Kõigepealt tuleb paberdokumendis kõik kriitilist informatsiooni sisaldavad kohad hoolikalt ja piisavas ulatuses mustaks värvida.
- Seejärel tehakse nendest mustaksvärvitud lõike sisaldavatest dokumentidest koopiad.
- Seejärel kontrollitakse, kas mustaksvärvitud lõigud on koopial tõesti loetamatud.
- Kui see on kindel ja dokumendi väljaandmiseks luba antud, võib koopia väljastada. Mustaksvärvitud tekstiosadega originaali ei tohi mingil juhul väljastada, sest mustaksvärvitud lõike on sageli lihtne uuesti loetavaks muuta.
- Elektroonilistes dokumentides sisalduva konfidentsiaalse informatsiooni eemaldamiseks tuleb turvatavate lõikude tekst kõigepealt muude märkidega

asendada ja seejärel mustaks värvida. Selleks tuleks kasutada kindla pikkusega märgiridu, näiteks “XXXXXXXXXX”, et sõnade algset tähendust ei oleks võimalik enam isegi ära arvata. Enne failide edastamist tuleks kontrollida, et need ei sisaldaks jääkinformatsiooni, näit. varasematest töötlustest allesjäänud märke (vaata ka M 4.64 Ülekantavate andmete kontrollimine enne edastamist/peidetud info kõrvaldamine).

Elektroonilistelt andmekandjatelt tuleb nendele eelnevalt salvestatud informatsioon enne andmekandjate uuesti kasutamist füüsiliselt kustutada (vaata M 4.32 Andmekandjate füüsiline kustutamine enne ja pärast nende kasutamist). Elektrooniliste andmekandjate puhul on edastuse korrektsust võimalik kontrollida, kasutades selleks programmi, mis võrdleb algfaili edastatud failiga märkhaaval (mõnede operatsioonisüsteemide puhul kasutatakse näit. käsku comp). Enne ärasaatmist tuleks kõikidest andmekandjatele salvestatud failinimedest koostada nimestik, et selle abil kontrollida, et need andmekandjad sisaldavad ainult antud saajale mõeldud faile.

Täiendavad kontrollküsimused:

- Kas vahetatavaid andmekandjaid kontrollitakse enne andmete saatmist selles osas, kas soovitav informatsioon on andmekandjalt täielikult rekonstrueeritav?
- Kas elektroonilised andmekandjad kustutatakse enne järgmist kasutust füüsiliselt, kui eelnevalt olid sellele muud andmed salvestatud?

M 4.36z Faksi adressaatnumbrite blokeerimine

Algatamise eest vastutavad: ülemused, IT-turvaosakond
Rakendamise eest vastutavad: faksi kasutamise eest vastutav töötaja, faksi postikeskus

Vältimaks olukordi, kus faksi kaudu saadetakse infot või toimikuid kas juhuslikult või meelega mittesoovitud aadressidele, pakub tänapäeva tehnika selleks vähemalt kolme erinevat lahendust:

Faksiaparaadi või faksiserveri seadistamine
Teatud faksiaparaatide ja faksiserverite puhul saab takistada fakside saatmist kindlaksmääratud faksinumbritele (positiivne eraldamine) või tõkestada kõik muud numbrid peale üksikute väljavalitute (negatiivne eraldamine).

Kodukeskjaama seadistamine
Samasugust volituste kehtestamist saab saavutada ka moodsates kodukeskjaamades, mille puhul on eelduseks, et faksiseade peab olema telefonivõrku ühendatud ilmtingimata läbi sellise kodukeskjaama.

Lisaseadmete kasutamine
Olukorras, kus faksiseade või kodukeskjaam sellist võimalust ei paku, saab nt avaliku võrgu käitajalt üürida lisaseadme, mis takistab ühenduse loomist teatud numbritega (positiivne ja negatiivne eraldamine).

Täiendavad kontrollküsimused:

- Kas eksisteerib vajadus välistada teatud faksinumbrite kasutusvõimalus?
- Kas on ette tulnud olukordi, kus fakse on saadetud valedele adressaatidele?

M 4.37z Faksi saatjanumbrite blokeerimine

Algatamise eest vastutavad: IT-turvaosakond
Rakendamise eest vastutavad: faksi kasutamise eest vastutav töötaja, faksi postikeskus

Selleks, et teatud faksisaadetised oma enda faksiaparaati ei blokeeriks, nt faksirünnakute või reklaamsaadetiste tagajärjel tekkiva ülekoormuse tõttu, saab teatud faksinumbrid sulgeda.

Saatja numbri analüüsimine faksiaparaadi või faksiserveri poolt
Mõned moodsad faksiaparaadid (4. grupi aparaadid) suudavad saatjate numbreid analüüsida ja keelduda faksisaadetiste vastuvõtust teatud kindlaksmääratud numbrite puhul. See kehtib ka teatud faksiserverite puhul, kui need on ühendatud ISDN-võrguga. Lisaks sellele saab analüüsiks kasutada ka faksisaatja tuvastust (CSID'd - *Call Subscriber ID* 'd). Probleemiks on siiski tõsiasi, et faksi saatjal on võimalik oma numbri näitamist keelata, samuti on võimalik manipuleerida nii edastatava numbri kui ka saatja IDga.

Suletud kasutajagruppide loomine
Üks täiendav võimalus on luua telefoniteenuse pakkuja juures tasuline suletud kasutajagrupp, eeldusel, et vastuvõtjad ja saatjad on ühendatud digitaalsete keskustega. Osaliselt pakutakse vastavaid lahendusi ka moodsates kodukeskjaamades (vt B 3.401 Kodukeskjaam (PBX)).

Täiendavad kontrollküsimused:

- Kas on vaja blokeerida teatud saatjate faksinumbreid?
- Kas faksi kasutamise eest vastutav töötaja tunneb vajalikke vastumeetmeid?

M 4.40 Arvuti mikrofoni volitamata kasutamise vältimine

Algatamise eest vastutavad: IT-turvaosakond

Rakendamise eest vastutavad: kasutajad

Võrkuühendatud arvuti mikrofoni võib kasutada igaüks, kellel on juurdepääs vastavale seadmefailile (nt Unixis on selleks failiks /dev/audio). Windows NT all määravad pääsuõigused registrivõtmele (HKEY_LOCAL_MACHINE\HARDWARE\.) selle, kes kontrollib arvuti mikrofone. Seetõttu tuleb vastavate õiguste andmistel olla hoolikas. Juurdepääs seadmefailile peaks olema võimalik ainult seni, kuni keegi vastava IT-süsteemiga ka reaalselt töötab. Kui tekib vajadus olemasoleva mikrofoni kasutamine üleüldse ära keelata, tuleb see võimalusel kas välja lülitada või füüsiliselt seadmest eemaldada.

Pääsuõiguste määramine

Kui mikrofon on arvutisse integreeritud ja ainult tarkvaraliselt sisse ja välja lülitatav, peavad pääsuõigused olema välja jagatud selliselt, et volitamata kasutamine oleks võimatu. Selle ellurakendamiseks võib nt Unixis võtta kõikidelt kasutajatelt seadmefaili /dev/audio lugemisõiguse. See ei võimalda tavakasutajal kasutada mikrofoni, kuid helifailide kuulamine on siiski jätkuvalt võimalik.

Turvaline desaktiveerimine

Mikrofoniga varustatud IT-süsteemide puhul tuleb kontrollida, kas seadmefaili pöörduse korral muudetakse pääsuõigusi ja omanikke. Kui see on nii, või kui soovitakse, et iga kasutaja saaks mikrofoni kasutada, ilma et seda peaks iga kord süsteemiadministraatori käest eraldi küsima, peab administraator paigaldama käsu, **mille puhul kehtib järgnev**:

- aktiveeritav ainult siis, kui keegi on end IT-süsteemi sisse loginud,
- aktiveeritav ainult selle kasutaja poolt ja
- juurdepääsuõigus muutub pärast väljalogimist taas kehtetuks.

Füüsiline eraldamine

Kui juurdepääsu mikrofonile ei saa reguleerida turvalise käsuga, tuleb mikrofon füüsiliselt arvutist eraldada või arvuti võrgukeskkonnast lahti ühendada. Arvutid, millesse on sisse ehitatud mikrofon, tuleb konfidentsiaalse koosoleku ajaks ruumist kas eemaldada või vähemalt välja lülitada. Sülearvuti puhul tuleb lahutada kõik ebavajalikud ühendused sidevõrkudega, nt ISDNiga. Enamasti on lihtsaimaks võimaluseks vastava kaabli lahtiühendamine.

Kontrollküsimused:

- Kas arvuti mikrofoni saab välja lülitada või arvutist füüsiliselt eemaldada?
- Kellel on juurdepääs mikrofoni seadmefailile või registri sektsioonidele, mis võimaldavad manipuleerida riistvaraseadistustega?

M 4.41z Sobivate IT-süsteemide turvatoodete valimine

Algatamise eest vastutavad: IT-juht, IT turvaosakond, andmekaitsespetsialist, üksikute IT-rakenduste eest vastutavad töötajad

Rakendamise eest vastutavad: varumisosakond, administraator

Olenevalt IT-süsteemile esitatavatest turvanõuetest ei pruugi olemasolevad turvafunktsioonid olla piisavad, mistõttu võib olla vajalik kasutada täiendavaid turvatooteid. Tüüpilised näited on juurdepääsukontroll, juurdepääsuõiguste haldamine ja kontroll, logimine ja krüpteerimine.

IT-süsteemides tuleb nt tagada, et

- IT-süsteemi saaksid kasutada ainult volitatud isikud. Selleks tuleb välja valida sobivad autentimismehhanismid;
- kasutajad pääsevad andmetele ligi ainult sellisel määral, mis on vajalik tööülesannete täitmiseks. Siin on abiks kasutajate sobiv eraldamine ja õiguste määramine;
- ebakorrapärasused ja manipulatsioonikatsed oleksid nähtavad. Siin on abiks logimisfunktsioonid, krüpteerimine ja digitaalsed allkirjad;
- andmed oleksid juhusliku hävitamise või kaotamise eest kaitstud (käideldavuse kontrollimine). Siin on abiks nt varundusprogrammid.

Kui IT-süsteemi logimisvõimalustest ei piisa tõendite säilimise tagamiseks, tuleb neid täiendada. Seda nõuavad ka mitmed seadused. Näiteks tuleb sisestuskontrolli ajal tagada, et hiljem oleks võimalik kontrollida, kas andmetöötlussüsteemi lisati isikuid puudutavaid andmeid, kas neid andmeid muudeti või eemaldati, ning kes seda tegi. Kui IT-süsteem ei suuda takistada administraatori juurdepääsu teatud failidele ega isegi neid pöördusi logida ega ka kontrollida, võib nende andmete tekstikujul lugemise administraatori jaoks tõkestada krüpteerimisega eeldusel, et tal puudub vastav võti.

Soovitatavad miinimumfunktsioonid

IT-süsteemidel peaksid olema vähemalt järgmised turbefunktsioonid. Kui need standardses süsteemis puuduvad, tuleb süsteemi täiendada täiendavate turvatoodetega:

- Identifitseerimine ja autentimine: teatud arvu ebaõnnestunud autentimiskatsete järel peab süsteem lukustuma ning seda lukustust peab saama tühistada ainult administraator. Kui kasutatakse parooli, peab parool olema vähemalt kaheksakohaline ja seda ei tohi süsteemi salvestada krüpteerimata kujul.
- Õiguste haldamine ja kontroll: kõvaketaste ja failide jaoks peab olemas olema õiguste haldamine ja kontroll, seejuures tuleb eristada vähemalt lugemis- ja kirjutusõigusega juurdepääse. Kasutaja ei tohi operatsioonisüsteemile ligi pääseda.
- Administraatori ja kasutaja rollide lahutamine: administraatori ja kasutaja rollid peab saama selgelt lahutada, seejuures tohib õigusi lisada või ära võtta ainult administraator.
- Sisselogimise, väljalogimise ja õiguste rikkumise protseduure peab saama logida.

- Automaatne ekraanilukk: kui klaviatuuri või hiirt pole mõnda aega kasutatud, peab tööle lülituma ekraanilukk. Seda peab saama ka käsitsi sisse lülitada. Juurdepääs IT-süsteemile peab olema võimalik alles pärast edukalt toimunud identifitseerimist ja autentimist.
- Buutimiskaitse peab takistama arvuti volitamata buutimist mõne teise andmekandja pealt.

Kui operatsioonisüsteem ei toeta ühte või mitut nendest turvafunktsioonidest, tuleb kasutada vastavaid sobivaid turvatooteid.

Lisanõuded turvatoodetele:

- Kasutajasõbralik kasutajaliides vastuvõtlikkuse suurendamiseks.
- Arusaadav dokumentatsioon administraatorile ja kasutajale.
- Tuleb valida sellised tooted, mille dokumentatsioon sisaldab mh kasutatavate krüptograafiliste algoritmide loetelu.

Turvatoodete soovitatavad lisafunktsioonid:

- Administraatori, revidendi ja kasutaja rollide lahutamine; ainult administraator saab õigusi määrata või ära võtta ja ainult revidendil on juurdepääs logiandmetele.
- Administreerimistegevuste logimine.
- Logianalüüsi abistamine konfigureeritavate filtreerimisfunktsioonidega.
- Andmekogumite krüpteerimine sobiva krüpteerimisalgoritmiga sellisel viisil, et süsteemi tõrke (voolukatkestus, protseduuri katkemine) korral ei esineks andmekadusid.

Vastavate funktsioonide ellurakendamine võib toimuda nii riist- kui ka tarkvaraliselt. Toote soetamisel tuleb arvestada meetmega M 2.66z Sertifikaatidega arvestamine IT soetamisel .

Ajutine lahendus
Kui sobivat turvatoodet ei õnnestu kiiresti soetada, tuleb rakendada teisi sobivaid turvameetmeid. Need on tavaliselt organisatoorset laadi ning kasutajad peavad neid täpselt järgima. Näiteks kui IT-süsteemil puudub ekraanilukk, tuleb süsteem lühikesteks kasutusvaheaegadeks luku taha panna.

Kontrollküsimus:

- Kas enne IT-süsteemide soetamist kontrolliti, kas neil on olemas ka piisavad turvafunktsioonid?

M 4.42z Turvafunktsioonide rakendamine IT-rakenduses

Algatamise eest vastutavad: IT-juht, IT turvaosakond, andmekaitsespetsialist, üksikute IT-rakenduste eest vastutavad töötajad

Rakendamise eest vastutavad: rakenduste arendaja

Vajadus integreerida rakendusprogrammide alla veel täiendavaid turvafunktsioone, näiteks pääsukontrolle, pääsuõiguste haldamist ja kontrolle või logimist, võib tekkida mitmel erineval põhjusel:

- Kui IT-süsteemi logimisvõimalused kombinatsioonis kasutatud IT turvatootega ei piisa tõendite tagamiseks, tuleb need logimiselemendid ellu viia rakendusprogrammis endas.
- Kui IT-süsteemi pääsuõiguste täpsus koostöös kasutatud turvatoodetega pole nõuetekohase töö tagamiseks piisav, tuleb rakendusprogrammi integreerida täiendav pääsuõiguste haldamine ja kontroll. (Näide: andmebaas ühise andmekogumiga. Eelduseks on, et olenevalt kasutaja funktsioonist oleks tal võimalik ligi pääseda ainult teatud kindlatele aladele.)
- Kui administraatori juurdepääsu teatud failidele ei saa IT-süsteemi ja kasutatud IT-turvatoodete abil takistada või vähemalt seda juurdepääsu logida ja kontrollida, tuleb rakendusprogrammi integreerida täiendavad turvafunktsioonid. Näiteks võib andmete krüpteerimisega takistada administraatoril andmete tekstikujul lugemist, kui tal puudub sobiv võti. Nende IT-rakendustele esitatavate täiendavate nõuetega tuleb arvestada juba planeerimisel ja arendamisel, kuna nende hilisem realiseerimine on tavaliselt liiga suurte kulude tõttu võimatu.

Kontrollküsimus:

- Kas uute IT-rakenduste arendamisel tuvastatakse süstemaatiliselt, milliseid turvafunktsioone see rakendus sisaldama peab?

M 4.43z Automaatse ümbrikusüsteemiga faksiaparaat

Algatamise eest vastutavad: IT-turvaosakond

Rakendamise eest vastutavad: varuja

Automaatse ümbrikusüsteemiga faksiaparaadid takistavad saabunud fakside volitamata võtmist ja lugemist. Saabuvad faksid volditakse kokku selliselt, et nähtavale jääb ainult faksiplank ja keevitatakse siis läbipaistvasse kileümbrikusse. Seejärel kukub ümbrik faksiaparaadi lukustatavasse sahtlisse. Neile ümbrikele pääseb ligi ainult volitatud isik, kellel on olemas vastava sahtli võti. Faksi volitamata lugemine on seega võimalik ainult sahtli lahtimurdmise või kinnikeevitatud ümbriku avamise järel, mistõttu ei jää seega vähemalt märkamata.

Kontrollküsimus:

- Kas sellise seadme soetamine on vajalik?

M 4.47 Turvalüüsi operatsioonide logimine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator

Tuleb kindlaks määrata, mis liiki sündmuseid logida ning kes peavad vastavaid logiandmeid analüüsima. Logimine peab vastama kehtivatele seadustele. Logiandmete puhul tuleb arvestada eriti just nende kogumise eesmärgiga.

Turvalüüsi logimisel tuleks arvestada järgnevate punktidega:

- Logiandmeid (nt IP-aadresse) peab saama selgelt seostada konkreetsete arvutitega (või isikutega). Seejuures tuleb arvestada kohalduvate andmekaitseseadustega.
- Logiandmeid ei tule salvestada mitte ainult turvalüüsi üksikutesse komponentidesse, vaid ka tsentraalsesse logimisserverisse (Loghost 'i), et vähendada andmekao ohtu, mis võib olla põhjustatud kas häkkerirünnakust või süsteemi avariist.
- Logiinfo edastamine komponentidelt Loghost 'ile peab toimuma turvalise ühenduse kaudu, et logiinfot ei oleks võimalik enne lõplikku salvestamist muuta.
- Kui Loghost 'i ülekandmisel tuleb läbida ebausaldusväärseid võrke, tuleb andmed krüpteerida.
- Kasutatava andmekandja vaba salvestiruumi tuleb regulaarselt kontrollida.
- Logimise avarii korral (nt kui kõvakettale jääb alles liiga vähe salvestiruumi), tuleb kõik logiandmeid genereerivad funktsioonid sulgeda. Ideaaljuhul peab turvalüüs blokeerima igasuguse liikluse ja edastama administraatorile vastava teate.
- Logiandmed tuleb salvestada WORM-andmekandjale („ Write Once, Read Many “).
- Logimise liik ja maht peavad vastama töödeldavate andmete konfidentsiaalsusele ning kasutusotstarbele.
- Erilised seadistatavad sündmused, nt kasutajatunnuse korduvad valed paroolisisestused või keelatud ühenduskatsed, tuleb logimisel esile tõsta ja tulemüüri-administraatorit tuleb nendest kohe teavitada.
- Üksikud komponendid peaksid teostama aja sünkroniseerimise, et võimaldada andmetevaheliste seoste loomist. Vt lisaks M 4.227 Lokaalse NTP -serveri kasutamine aja sünkroniseerimiseks .

Väikestes võrkudes, millel kasutataks lihtsat turvalüüsi, võib vajadusel täiendavast Loghost 'ist loobuda.

Logimise maht paketifiltris

Keelatud pakettide logimine! Paketifiltrite logimine peaks hõlmama vähemalt neid pakette, millest keeldutakse paketifiltrite reeglite tõttu.

Sõltuvalt turvanõuetest võivad huvi pakkuda täiendavad pakettide klassid:

- „Ebatavalised“ paketid, nt vigase TCP-lippude kombinatsiooniga või vigase Header -infoga paketid. Sellistest pakettidest tuleks kindlasti vastava paketi-

filtri reegliga keelduda ning ka juba ainuüksi sel põhjusel logimisse kaasata, siiski on soovitatav logida selliseid pakette eraldi, kuna need võivad olla nn Stealth Scan 'ide tunnus. Lisaks võib vigaste pakettide kuhjumine olla märk võrgus esinevatest tehnilistest probleemidest.
- Ühendusele orienteeritud (nt TCP-põhisel) logimisel võib olla mõistlik logida ka vastuvõetud pakette, mis kuuluvad ühenduse loomise juurde (nt TCP-pakette, mis kuuluvad 3-suunalise- Handshake 'i juurde), samuti lisapakette, mis on osa olemasoleva ühenduse katkestamisest.
- Ühenduseta logimisel, mille käigus ei edastata suuri andmehulki (nt UDPpõhisel logimisel nagu DNSiga), võib olla mõistlikuks lahenduseks kõiki pakettide logimine.

See, milliseid täiendavaid paketitüüpe logitakse, sõltub esmajoones usaldusväärse võrgu kaitsevajadusest. Logimine ise ei taga turvalisust, infot tuleb lisaks ka vastavate kriteeriumite põhjal analüüsida.

Logimise alla kuuluvate pakettide kohta tuleks logida vähemalt järgnev info:

- Alg- ja siht-IP-aadress
- Alg- ja sihtport või ICMP-tüüp
- Kuupäev ja kellaaeg
- Paketifiltri vastav reegel

Kui kasutatakse lisaks ALGd, võib vastuvõetud pakettide logimisest loobuda, kuna proksi logib sel juhul ühendusinfot piisaval määral.

Logimise maht Application-Level - Gateway's

ALGs, mida kaitstakse välimise paketifiltriga suure hulga loata pakettide eest, tuleks iga ühenduse loomise (nii edukate kui ka katsetuste) puhul logida järgnevad andmed:

- Alg- ja siht-IP-aadress
- Alg- ja sihtport
- Teenus
- Kuupäev ja kellaaeg
- Ühenduse kestus
- Autentimisandmed või ebaõnnestunud autentimise asjaolu

Teatud kasutajate puhul peab saama logimise välja lülitada, et logiandmete liiga suure sissekannete arvu tõttu ei jääks oluline info märkamata. Selle valiku võib nt langetada üksikute kasutajate õigusteprofiili alusel.

Üksikute logide jaoks soovitatakse lisaks ka veel järgnevaid seadistusi:

DNS

- Päringutest keeldumine
- Päringute lubamine
- Teistest arvutitest algatatud („väljuvad“) tsooniülekanded

- ALG poolt algatatud („sisenevad“) tsooniülekanded

Reeglina takistab tsooniülekandeid juba ka DNS-serveri käitaja, mistõttu võib sellest kontrollist ka loobuda.

FTP

- Sihtaadress (URL)
- Tagasilükatud PORT-käsud
- Edastatud faili nimi
- Edastatud andmete hulk
- Olekuteade

HTTP

- Sihtaadress (URL)
- Edastatud andmete hulk
- Ühendusmeetod (nt GET, POST, CONNECT)
- Rakendatud filtrikriteeriumite info
- Olekuteade

NNTP

- Sihtaadress (URL)
- Edastatud andmete hulk
- Olekuteade

SMTP

- Saatja ja meili vastuvõtja meiliaadress
- Edastatud andmete hulk
- Rakendatud filtrikriteeriumite info
- Olekuteade edasisuunamise edu või ebaedu kohta

Järgnevate moodulite puhul ei ole eraldi logimine vajalik:

Moodul	Logimisest väljajätmise põhjus
HTTPS	„Jadamisi“ ühendatud juba logiva HTTP-proksiga
Hooldusmoodul	Olulisi logimisandmeid ei teki
IDS	Logiandmed tekivad IDSil eraldi. Neid ei tohi salvestada tsentraalselt, et vältida turvalüüsi moodulitest möödaminemist.

Tabel: moodulid, mis ei vaja eraldi logimist

Logimine muutub oluliselt lihtsamaks, kui tarkvara võimaldab „ logging facility “ vaba seadistamist (st üksikute logisissekannete tähistamist). See võimaldab määrata igale teenusele selge tunnuse, mille abil saab Loghost jaotada logiandmeid erinevatesse failidesse. Kui logiandmeid saadetakse võrgu kaudu tsentraalsele Loghost 'ile, tuleb jälgida, et erinevate arvutite ja teenuste logisissekanded märgistataks selliselt, et nende seosed oleksid üheselt mõistetavad. Lisaks on mõistlik lasta kõikidel teenustel oma logiandmed nummerdada. See võimaldab tuvastada logiandmete kadu või nendega manipuleerimist.

Logiandmete analüüsimine

Logiandmete analüüsis saab kasutada eritööriistu (logfile analyzer). Need näitavad logiandmeid erineval viisil, seejuures kasutab suurem osa tööriistadest logifailidest oluliste andmete kättesaamiseks tavalisi väljatrükiks koostatud dokumente. Kuigi regulaarsete väljatrükitavate dokumentide , mida saab kasutada ka logiandmete analüüsimisel, koostamiseks on olemas ka mõistlikke nimekirju, tuleb tavaliselt siiski ka kohandada.

Logifailide erinevate versioonide näideteks on:

- Kokkukuuluvate logiandmete grupeerimine ja märgistamine (nt LogSurfer).
- Oluliste logiandmete kuvamine, mille puhul saab ebaolulisi andmeid regulaarsete väljatrükidokumentidega kõrvale jätta. Sel moel saab näiteks kuvast välja jätta sellised logiandmed, mis dokumenteerivad edukat tööd (HTTP puhul nt GET) (nt checksyslog).
- Rünnete kuvamine. Logiandmete analüüs peab seejuures toimuma reaalajas.
- Logiandmete statistiline analüüs (nt kui sageli milline teade esines).

Lisaks on oluliste logiandmete kuvamisel on olemas tööriistad, mis võimaldavad silmatorkavate kõrvalekallete puhul käivitada ka teatud tegevusi (nt käskusid).

Tähelepanuäratavateks logisissekanneteks on nt:

- Kuhjuvad päringud portidele, millel ei käitata teenuseid,
- Ebaõnnestunud juurdepääsukatsed turvalüüside komponentidele,
- Ebausaldusväärsest võrgust saabuvad paketid, mis on varustatud usaldusväärse võrgu IP-aadressidega (märk IP-spoofing 'ust),
- Kahtlased, usaldusväärse võrgu serveritest väljuvad ühendused. Need võivad olla märgid sellest, et pärast edukat sissemurdmist kopeeris ründaja andmeid usaldusväärsest võrgust välja või laadis väljast andmeid, mida ta vajab oma edasise tegevuse jaoks.

Regulaarne analüüs

Logifaile tuleb regulaarselt analüüsida ning seetõttu tuleb kindlaks määrata, millised on minimaalsed vajalikud analüüsid. Lisaks tuleb määrata vähemalt umbkaudsed suunised, mis määravad, mida teha, kui analüüsimisel leitakse sissekandeid, milles esineb silmatorkavaid kõrvalekaldeid.

Kontrollküsimused:

- Milline info logitakse paketifiltrites?
- Kui kasutatakse ALGd: millist infot logib ALG erinevate teenuste kohta?
- Milliste ajavahemike tagant ja milliste kriteeriumite järgi analüüsitakse logisid?

M 4.56 Turvaline kustutus Windows operatsioonisüsteemides

Algatamise eest vastutavad: IT-turbespetsialist, administraator

Rakendamise eest vastutavad: kasutaja, administraator

Windows soovitatakse installeerida ainsa operatsioonisüsteemina, et takistada teiste operatsioonisüsteemide käivitumist (vt. M 4.339 Vahetavate andmekandjate volitamata kasutamise tõkestamine Windows 7-s). Kui on siiski vaja kasutada mõnda teist operatsioonisüsteemi (multiboot- süsteem), siis on soovituslik tarvitada kõvaketta krüpteerimiseks tarkvara, mis takistab mõne teise operatsioonisüsteemi juurdepääsu konfidentsiaalsetele andmetele. Windows 7 ja Windows Server 2008 kasutuses olev kõvaketta krüpteerimistarkvara BitLocker on multiboot -süsteemide jaoks sobimatu. Tuleb kasutada multiboot -süsteemi jaoks sobivat rakendust, mis on loodud mõne teise firma poolt. Alternatiivina saab kõvaketta krüpteerimiseks kasutada ka Encrypting File System'it (EFS). EFS toetab üksikute failide krüpteerimist (vt. M 4.147z EFS-i turvaline kasutamine Windows 'i keskkonnas).

Windowsi prügikast

Windowsi operatsioonisüsteemis paigutatakse kustutatud failid vastavasse kausta nimetusega „Prügikast", kui kasutaja ei nõua kohest kustutamist. Sellest kaustast kustutatakse failid alles siis, kui failide maht ületab eelnevalt määratud normi, või kui kasutaja ise kustutamiseks käsu annab. Seetõttu peab prügikasti regulaarselt tühjendama, et kõvaketas ei saaks liiga täis ja kasutaja ei kaotaks ülevaadet. Maksimaalset kõvaketta ruumi, mida prügikast kasutada tohib, saab ka muuta. Selleks tuleb ikooni „Prügikast" alamenüüst „Atribuut" valida sobiv maht, näiteks 2MB. Konfidentsiaalse sisuga faile ei tohi prügikasti asetada, vaid need tuleb kohe kustutada. Seda saate teha, hoides all nuppu Shift. Windowsis on võimalik prügikastist kustutatud faile vastava tarkvara abil taastada. Failid, mis on eriti konfidentsiaalse sisuga, tuleb seetõttu üle kirjutada, mitte prügikasti asetada (vt B 1.15 Andmete kustutamine ja hävitamine , M 2.3 Andmekandjate haldus ja M 4.56 Turvaline kustutus Windows operatsioonisüsteemides). Windows 7 ja serveri versioonide korral saab failid kohe kustutada, ilma et seda peaks prügikasti kaudu tegema. Kasutajate tähelepanu peab juhtima sellele, et failide kohest kustutamist saab määrata prügikasti atribuutidest (Ära teisalda faili prügikasti. Eemalda fail kohe kustutamisel).

Windows 7 ja serveri versioonide korral on

võimalik vastaval andmekandjal või alajaotuses olevat vaba ruumi üle kirjutada, kasutades selleks käsklust cipher.exe/w. Programm cipher.exe teeb kokku kolm ülekirjutamist. Esimesel korral kirjutatakse vabastatud ruum üle 0x0, teine kord 0xF ja kolmas kord suvaliste pseudofailidega. Selle käskluse andmise juures tuleb aga arvestada, et väiksemaid kustutatud faile (alla 4KB) ei pruugita üle kirjutada, kui nad asetsesid otse MFT-l ja mitte eraldi andmekandja klastris. Protsess sobib ka krüpteeritud failide puhastamiseks veel vahemälus paiknevatest krüpteerimata failiosadest. Selleks, et konfidentsiaalsed failid saaksid taastamatult kustutatud, tuleb kasutada spetsiaalset kustutustarkvara, millega on võimalik kõik seda faili puudutavad andmed andmekandjal üle kirjutada.

Varikoopiad (Shadow Copies)

Windowsi klientides on võimalik kõvakettale salvesta nn varikoopiaid (nimeta-

takse ka eelkäijaversioonideks), mis sisaldavad failide ja kaustade varasemaid versioone. Varikoopiate funktsiooni saab kõikide failisüsteemide jaoks sisse lülitada dialoogiaknas „Properties”. Varikoopiate funktsiooni aktiveerimisel on võimalik kustutatud faile ja failide varasemaid versioone asjaomases failisüsteemis teatud ajaks taastada ning seda ka siis, kui originaalfail on mõne programmiga juba turvaliselt kustutatud. Seetõttu tuleks varikoopiate funktsiooni kasutamist kindlasti vältida neis arvutites, kus andmeid on tarvis turvaliselt kustutada. Ka siin võib lisaturvet pakkuda failisüsteemi krüpteerimine, sest nii krüpteeritakse ka varikoopiad.

Kontrollküsimused:

- Kas on kindlustatud, et kõvakettal ei ole ühtegi muud operatsioonisüsteemi peale Windowsi ja kui on, kas kasutatakse kõvaketta krüpteerimistarkvara?
- Kas prügikasti andmemahu suurus on mõistlik?
- Kas kõik kasutajad on teadlikud, et prügikasti kaudu failide kustutamine ei ole usaldusväärne?
- Kas lisaks kõigele kasutatakse spetsiaalset kustutustarkvara, mis konfidentsiaalsed failid taastamatult kustutab?

M 4.57 CD-ROMi automaattuvastuse blokeerimine

Algatamise eest vastutavad: IT-turvaosakond

Rakendamise eest vastutavad: administraator, kasutaja

Windowsi all saab CD-ROMe automaatselt tuvastada ja töödelda. Seeläbi saab CD-ROMil salvestatud andmeid arvutis ka automaatselt käivitada. Sel põhjusel tuleks automaatne CD-ROMi tuvastamine permanentselt keelata. Automaatse CD-ROMi tuvastuse desaktiveerimine võib toimuda ka kasutajapõhiselt (poliitika User configuration | Administrative templates | System | Deactivate Autplay). Poliitikaid võib defineerida nii lokaalsete kui ka Active-Directory -põhiste grupipoliitikatena.

Kui automaatset CD-ROMi tuvastust ei saa täielikult desaktiveerida, tuleb see dokumenteerida. Ükshaaval saab automaatse CD-ROMi tuvastuse tühistada iga CD-ROMi jaoks eraldi, vajutades plaadi sissepanemisel SHIFT-klahvile. Kogemused näitavad, et praktikas kasutatakse seda võimalust harva.

Kontrollküsimused:

- Kas automaatne CD-ROMi tuvastus on välja lülitatud?
- Kas kasutajaid informeeritakse sellest, kuidas nad saavad automaatset CDROMi tuvastust ajutiselt takistada?

M 4.63 Kaugtöökohaarvutite turvanõuded

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT-turvaspetsialist

Rakendamise eest vastutavad: IT-juht, administraator

Kaugtöökohaarvutite turvatehnilised nõuded tulenevad kaugtöökohal töödeldavate andmete kaitsevajadusest ja nende andmete kaitsevajadusest, millele kaugtöötajad asutuse sidearvuti kaudu ligi pääsevad. Mis kõrgem kaitsevajadus, seda rohkem meetmeid läheb tarvis, et seda kaitset tagada.

Kaugtöökohaarvutite üldised turvanõuded on:

- Kaugtöökoha arvuteid tohivad kasutada ainult volitatud isikud. See tagab, et ainult volitatud isikud saavad kasutada andmeid ja programme, mis on salvestatud kaugtöökohaarvutitele või millele pääseb ligi sidearvuti kaudu. Volitatud isikud on kaugtöökohaarvuti administraator ja kaugtöötaja ise koos oma asendajaga.
- Kaugtöökohaarvuteid tohib kasutada ainult kindlatel eesmärkidel. See aitab takistada olukorda, kus kaugtöötajad arvutit volitamata viisil kasutavad või muudavad. Näiteks on keelatud installeerida kasutusloata programme. See aitab vältida väärast kasutamisest ja kuritarvitamisest tulenevaid kahjustusi.
- Kaugtöökohaarvuti vargusest või defektist tulenevad kahjustused ei tohi olla liiga suured. Kaugtöökohaarvuteid kasutatakse tavaliselt vähese turvalisusega keskkondades, seega on varguse või rikke oht suurem kui asutuse kaitstud töökeskkonnas. Selle tõttu võib kannatada nii käideldavus kui ka salvestatud andmete konfidentsiaalsus. Vargustest tulenevate kahjude minimeerimiseks tuleks andmeid salvestada näiteks ainult krüpteeritult. Defektidest tulenevate kahjustuste piiramiseks tuleb andmeid regulaarselt varundada.
- Kaugtöökohaarvutite manipulatsioonikatsed ning edukad manipulatsioonid peavad olema kaugtöötaja jaoks tuvastatavad. See tagab kaugtöökohaarvutite tervikliku seisundi, olgugi et manipulatsioonikatseid ei saa välistada. Kaugtöökohaarvutis töödeldavate andmete kaitsevajadus määrab turvaeesmärgid ja seega ka kaugtöökohaarvutile esitatavad tehnilised nõuded. Tuleb dokumenteerida, millised järgnevalt kirjeldatud turvalisust puudutavad funktsioonid peavad kaugtöökohaarvutil olema ja kuidas neid rakendada. Kaugtöökohaarvutis on mõistlik kasutada järgnevaid funktsioone. Kaugtöökohaarvutil peavad olema identifitseerimis- ja autentimis- mehhanismid.

Eriti olulised on järgnevad punktid:

- Turvalisuse seisukohast kriitilisi parameetreid nagu paroole, kasutajatunnuseid jms tuleb hallata turvaliselt. Paroole ei tohi kaugtöökohaarvutisse mingil juhul salvestada krüpteerimata kujul.
- Juurdepääsu protsess peab reageerima sisestustel tehtud vigadele nii, nagu see on eelnevalt defineeritud. Kui näiteks kolm korda järjest on autentimine ebaõnnestunud, tuleb juurdepääs kaugtöökohaarvutile kas tõkestada või ajavahemikke, mille möödumisel on võimalik uuesti proovida, järkjärgult suurendada.
- Turvaparameetritele peab olema võimalik määrata teatud miinimumnõudeid. Näiteks peab parooli miinimumpikkus olema kaheksa tähemärki.

- Pärast seda, kui klaviatuuri või hiirt pole teatud aja jooksul kasutatud, peab automaatselt tööle lülituma ekraanilukk, mida peab saama desaktiveerida ainult pärast kasutaja identifitseerimist ja autentimist.
- Kaugtöökohaarvutil peab olema juurdepääsukontroll. Eriti tuleb tagada järgmiste nõuete rakendamine:
- Kaugtöökohaarvuti peab suutma erinevaid kasutajaid teineteisest eristada. Kaugtöökohaarvutil peab saama määrata vähemalt kaks lahutatud rolli, nimelt administraator ja kaugtöötaja.
- Diferentseeritud õiguste struktuuri (lugemine, kirjutamine, käivitamine,. . .) abil peab saama reguleerida juurdepääsu failidele ja programmidele.
- Kaugtöökohaarvutites peab olema logimisvõimalus. Mõistlik oleks rakendada järgmisi nõudeid:

Miinimummaht, mida kaugtöökohaarvuti logima peab, peab olema seadistatav.

Näiteks peavad olema logitavad järgnevad tegevused ning alltoodud vead:

- Autentimisel: kasutajatunnus, kuupäev ja kellaaeg, sisselogimiskatse tulemus jne.
- Juurdepääsu kontroll: kasutajatunnus, kuupäev ja kellaaeg, juurdepääsukatse tulemus, juurdepääsu liik, mida ja kuidas muudeti, loeti, kirjutati jne.
- Administraatori tegevuste läbiviimine,
- Funktsionaalsete vigade esinemine.
- Volitamata isikutel ei tohi olla võimalik logifunktsiooni välja lülitada. Volitamata isikute jaoks ei tohi logiandmed olla ei loetavad ega muudetavad.
- Logimine peab olema ülevaatlik, terviklik ja korrektne.

Kui kaugtöökohaarvutis peab olema logiandmete kontrollimise mehhanism, võiks sellele kehtestada nt allolevad nõudmised:

- Logiandmete kontrollimise funktsioon peab suutma logimisel kasutatavaid andmeid liigiti eristada (nt filtreerida, et leida kõik volitamata juurdepääsud kõikide ressursside puhul ühes kindlas etteantud ajavahemikus).
- Kontrollifunktsioon peab suutma väljastada kontrollitavaid („loetavaid“) kontrollaruandeid, et ükski turvalisust mõjutanud sündmus ei jääks märkamata. Kaugtöökohaarvutites peavad olema andmevarunduse funktsioonid. Need peavad muuhulgas täitma järgnevaid nõudeid:
- Andmevarundusprogramm peab olema kasutajasõbralik ja töötama kiirelt. See peab võimaldama automaatset tööd.
- Konfiguratsiooniga peab saama määrata, milliseid andmeid millal varundatakse.
- Peab olema võimalus igasuguste varundatud andmete importimiseks. Funktsioon peaks suutma varundada mitut generatsiooni.
- Varundada peab saama ka töös olevate protsesside vahepealseid tulemusi.
- Kaugtöökohaarvutites peab olema krüpteerimiskomponent. Siinkohal tuleb esmalt mõelda, millist funktsiooni vajatakse: valitud andmete krüpteerimine (offline) või kogu kõvaketta automaatne krüpteerimine (online). Üldjoontes tuleks eelistada kõikide andmekandjate automaatset krüpteerimist, kuna see on kasutajasõbralikum ja tõhusam. See eeldab sobiva krüpteerimistoote

kasutamist ja seda, et süsteemi avarii (voolukatkestuse, protseduuri katkemise) korral ei esine andmekadusid.

Lisaks oleks mõistlik kehtestada järgmised nõuded:

- Kasutatav krüpteerimisalgoritm peab vastama nõuetele meetmes M 2.164 Sobiva krüptoprotseduuri valimine .
- Võtmete haldamine peab olema kooskõlas kaugtöökohaarvuti funktsioonidega.

Siinjuures on oluline teha vahet algoritmide põhiliste erinevuste vahel: sümmeetrilised protseduurid kasutavad krüpteerimiseks ja dekrüpteerimiseks salajast võtit, asümmeetrilised protseduurid kasutavad krüpteerimiseks avalikku võtit ja dekrüpteerimiseks privaatset (saladuses hoitavat) võtit.

- Kaugtöökohaarvuti peab suutma turvaliselt hallata turbe seisukohast olulisi parameetreid, nt võtmeid. Näiteks ei tohi kaugtöökohaarvutis hoida võtmeid (ka neid, mida parasjagu ei kasutata) mitte kunagi kaitsmata kujul, st loetavalt.

Kui kaugtöökohaarvutil peaksid olema tervikluse kontrolli mehhanismid, oleks mõttekas kehtestada tootele järgnevad nõuded:

- Tervikluse kontrollimisel tuleb rakendada meetodeid, mis suudavad usaldusväärselt tuvastada kaugtöökohaarvutite või neisse salvestatud andmete tahtlikke manipulatsioone, samuti programmide loata paigaldamist.
- Andmeedastuse tarbeks peavad tootel olema mehhanismid, mille abil oleks võimalik tuvastada tahtlikku aadressiväljade ja kasutajaandmetega manipuleerimist.

Sellele lisaks tohi eelnimetatud andmetega olla võimalik märkamatult manipuleerida ainult seeläbi, et tuntakse kasutatud algoritme, st kasutus peab olema seotud spetsiaalsete lisateadmistega.

- Kaugtöökohaarvutil peab olema buutimiskaitse, takistamaks olukorda, kus buuditakse volitamata vahetatavate andmekandjatega, nt DVDlt või USB-mälupulgalt (vt M 4.4 Eemaldatavate andmekandjate draivipilude ja väliste andmekandjate nõuetele vastav kasutamine).
- Kaugtöökohaarvuti kasutajakeskkonda peab saama piirata. Administraator peab saama määrata, milliseid programme tohib kaugtöötaja käivitada, millised lisaseadmed saab ta kasutada ning milliseid muudatusi tohib kaugtöötaja süsteemis teha. Lisaks ei tohi kaugtöötajal olla võimalust muuta volitamata turvalist tööd tagavaid olulisi seadistusi või paigaldada keelatud võõrtarkvara.
- Kaugtöökohaarvutisse peab olema paigaldatud residente arvutiviiruse programm, et arvutit pidevalt arvutiviiruste suhtes kontrollida (vt M 4.3 Viirusetõrjeprogrammide kasutamine). Enne kui hakatakse sisse lugema andmeid vahetatavatelt andmekandjatelt, enne andmekandjate üleandmist või saatmist ning enne andmete vastuvõtmist tuleb andmeid kontrollida viiruste suhtes (vt M 4.33 Viirustõrjeprogrammi kasutamine andmekandjate vahetamisel ja andmete edastamisel).

- Kui kaugtöökohaarvutit administreeritakse kaughoolduse kaudu, tuleb tagada, et kaugadministreerimist saaks teha ainult volitatult. Kaughooldusel tuleb tagada kaughoolduspersonali autentimine, ülekantavate andmete krüpteerimine ja administreerimisprotseduuride logimine.
- Kaugtöökohaarvuti tarkvara peab olema kasutajasõbralik. See peab olema kergesti kasutatav, arusaadav ja lihtsasti õpitav, kuna kaugtöötaja peab töötama iseseisvamalt kui teised töötajad. Eriti peab kaugtöötajal olema juurdepääs põhjalikule ja selgele dokumentatsioonile, mis puudutab operatsioonisüsteemi ja paigaldatud programme.

Mainitud funktsioonidest tuleb valida need, mida läheb tarvis lähtuvalt kaugtöökohaarvuti turvalisuse nõuetest. Nende funktsioonide alusel tuleb valida sobiv operatsioonisüsteem. Kui see ei toeta kõiki vajalikke funktsioone, tuleb kasutada lisatooteid. Seejuures peaksid ühe asutuse kõik kaugtöökohaarvutid olema võimalikult ühesugused, et kergendada nõustamist ja hooldamist. Turvatehnilise sobivuskontrolli juures tuleb arvestada mooduliga B 1.10 Tüüptarkvara .

Administraatorid peavad terviksüsteemi konfigureerima selliselt, et oleks võimalik saavutada maksimaalne turvalisus.

Kontrollküsimused:

- Kas on dokumenteeritud, millised turvalisuse seisukohast olulised funktsioonid peavad olema kaugtöökohaarvutis ja kuidas neid rakendada?
- Kas kaugtöökohaarvutid pakuvad kõiki hädavajalikke funktsioone?
- Kas on tagatud, et kaugtöökohaarvutile ja sidearvutile pääsevad ligi ainult volitatud isikud?
- Kas on tagatud, et andmete, kaugtöökohaarvutite ja sidearvutite manipulatsioonid on tuvastatavad?

M 4.64 Ülekantavate andmete kontrollimine enne edastamist/peidetud info kõrvaldamine

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: administraator, kasutajad

Enne faili meili teel saatmist või andmekandja vahetamist või enne faili avaldamist veebiserveris tuleks kontrollida, ega see ei sisalda jääkinformatsiooni, mis ei ole avaldamiseks ette nähtud. Selline jääkinformatsioon võib pärineda mitmest lähteallikast ja seega võivad olla erinevad ka tegevused, mis selle vastu tuleb ette võtta. Alljärgnevalt kirjeldatakse sellise jääkinformatsiooni säilimise kõige sagedamini esinevaid põhjusi. Üldiselt tuleks nt tekstitöötluseks või tabelarvutuseks kasutatava standardtarkvara puhul kontrollida, millist lisainformatsiooni nendega koostatud failides salvestatakse. Seejuures salvestatakse osa sellest informatsioonist kasutaja teadmisel ja osa nii, et kasutaja seda ei tea. Enne failide edastamist tuleks vähemalt pisteliselt kontrollida, et need ei sisaldaks soovimatut informatsiooni. Selleks tuleks kasutada teist redaktorit kui seda, mida kasutati faili loomisel. Seejuures tuleb silmas pidada, et mitte igat jääkinformatsiooni ei saa lihtsalt ilma failiformaati kustutamata kustutada. Kui nt tekstitöötlusfailist kustutatakse mõned baidid, siis ei tunne tekstitöötlusprogramm seda failiformaati teatud tingimustel enam ära.

Jääkinformatsiooni kõrvaldamiseks:

- võib faili salvestada mõnes muus failiformaadis, nt formaadis „ainult tekst” või HTMLis,
- võib kasutusandmed sama standardtarkvara mõnda teise instantsi kopeerida, kusjuures IT-süsteemis ei pea muu rakendus töötama. Seda soovitatakse eelkõige suurema muutmisajalooga failide puhul.

Selleks, et ennetada informatsiooni edastamist, mis algselt on salvestatud selle koostajate teadmisel, nagu näiteks „peidetult” vormindatud teksti edastamist, mille olemasolu aga unustati, võib osutuda otstarbekaks fail välja printida. Seejuures tuleks aktiveerida kõik valikud, mis prindivad välja ka peidetud informatsiooni.

Jääkinformatsioon (slack bytes)

Andmekandjate vahetamisel võib probleeme tekkida kettatühemikega (slack space). Igal operatsioonisüsteemil on väikseim fikseeritud suurusega füüsiline salvestusüksus. DOS-is on selleks üks sektor, mis hõlmab 512 baiti. Unix-süsteemide puhul on selleks plokk, kusjuures ploki suurus oleneb kasutatud Unixi variandist. DOS-is ühendatakse partitsiooni üksikud sektorid loogiliselt klastriteks (cluster). See, kui mitu sektorit ühe klastri moodustavad, oleneb partitsiooni suurusest. Kui fail avatakse, paigutatakse selle juurde üks või mitu klastrit. Viimast klastrit ei kasutata seejuures täielikult ära, kui salvestatava faili suurus ei juhtu olema klastrisuuruse kordne. See vajab salvestusruumi. Keskmine salvestusruumi tarbimus suureneb seega koos klastri suurusega. Et see omakorda suureneb koos partitsiooni suurusega, ei tohiks partitsioonid olla liiga suured. Toome ühe näite: kui partitsiooni suurus jääb 1024 ja 2047 MB vahele, siis on üksiku klastri suurus 32 KB. Seega läheb iga faili puhul keskmiselt 16 KB salvestusruumi kaduma. Teine probleem on siin see, et (DOS-il põhinevate operatsioonisüsteemide puhul) viimase klastri või ploki ülejäänud baite täiendatakse põhimälus juhuslikult olevate

baitide, niinimetatud slack byte'idega. Need võivad sisaldada mõttetuid sisestusi, failistruktuuri käsitlevat informatsiooni, aga ka paroole. Ka ühelt andmekandjalt teisele kopeerimisel võidakse fail olenevalt klastri suurusest slack byte'idega täita. Enne failide edastamist tuleks kindlaks teha, et need ei sisalda enam slack byte'e. Seda saab kontrollida vastava redaktori (nt HexEditor) abil. Lisaks sellele on paljudel Windowsi rakendusprogrammidel see probleem, et programm, millega faili töödeldakse, ei kirjuta hõivatavat salvestusruumi rakendusandmetega tervenisti üle, vaid võivad tekkida lüngad, mis sisaldavad ka IT-süsteemi vanu andmevaramuid.

Peidetud tekst / kommentaarid

Fail võib sisaldada tekstiosi, mis on formaaditud „peidetuna" või „varjatuna". Mõned programmid võimaldavad ka lisada kommentaare, mis on väljatrükil ja sageli ka ekraanil näha. Sellised tekstilõigud võivad sisaldada märkusi, mis ei ole mõeldud faili saajale. Seetõttu tuleb failidest enne nende asutusevälistele isikutele edastamist selline lisainformatsioon kustutada.

Muudatuste markeeringud

Failide töötlemisel võib olla mõttekas kasutada tehtavate muudatuste markeeringuid. Et neid saab väljatrükil ja ekraanil näha, siis tuleks enne failide edastamist kontrollida, ega need ei sisalda muudatuste markeeringuid.

Versioonid

Praktiliselt kõikides kaasaegsetes kontoritarkvara komplektides (kontoripaketid) on olemas võimalus salvestada ühe dokumendi erinevaid versioone ühte faili. See on vajalik selleks, et vajaduse korral saaks varasemate tööetappide juurde tagasi pöörduda. See võib aga väga kiiresti viia väga suurte failide tekkimiseni, nt kui salvestatakse graafikafaile. Mingil juhul ei tohiks valida võimalust „Versiooni automaatne salvestamine faili sulgemisel", sest siis salvestatakse iga kord, kui fail suletakse, lisaks kogu eelnev versioon.

Faili omadused

Faili omaduste ehk failiinfona salvestatakse failis informatsioon, mis peab hilisemal otsimisel aitama faili uuesti üles leida. Olenevalt rakendusest võib see informatsioon sisaldada nimetust, kaustastruktuure, teavet versiooni kohta, töötlejaid (mitte ainult allakirjutanut), kommentaare, töötlemisaega, viimase printimise kuupäeva, dokumendinime ja -kirjeldusi. Mõned neist andmetest salvestavad programmid ise ja töötleja ei saa neid muuta, muu informatsioon tuleb sisestada käsitsi. Enne faili edastamist asutusevälistele isikutele tuleb kontrollida, millist liiki lisainformatsiooni fail sisaldab.

Kiirsalvestus

Tekstitöötlusprogrammid pakuvad kiirsalvestust, et saaks salvestada ainult alates viimasest salvestusest tehtud muudatusi ning ei peaks kogu dokumenti salvestama. See protseduur võtab seega vähem aega kui täielik salvestusprotseduur. Täielik salvestusprotseduur nõuab aga vähem kõvakettamälu kui kiirsalvestus. Olulisim puudus on siiski see, et teatud tingimustel võib fail sisaldada tekstifragmente, mis oleks tulnud veelkordsel läbitöötamisel kõrvaldada.

Seepärast tuleks kiirsalvestusvalikud välja lülitada. Kui kasutaja otsustab sellest hoolimata kiirsalvestuse kasuks, siis tuleks tal järgmiste situatsioonide korral viia alati läbi täielik salvestusprotseduur:

- kui dokumendi töötlemine on lõpetatud,
- enne kui kasutatakse järgmist rakendust, mis nõuab palju salvestusruumi,
- enne kui dokumendi tekst viiakse mõnda teise rakendusse üle,
- enne kui dokument konverditakse mõnda teise failiformaati ja
- enne kui dokument saadetakse e-posti teel või väljastatakse andmekandjate vahetamise käigus.

Kontrollküsimused:

- Kas arvutikasutajaid on informeeritud failides sisalduvast jääkinformatsioonist tuleneda võivatest ohtudest?
- Kas arvutikasutajatele on selgitatud kiirsalvestusvalikute kasutamisest tuleneda võivaid ohte?

M 4.65 Uue riist- ja tarkvara testimine

Algatamise eest vastutavad: IT-juht, IT turbespetsialist

Rakendamise eest vastutavad: IT-juht, IT turbespetsialist

Enne uue riistvara või tarkvara kasutuselevõttu toomiskeskkonnas tuleb neid testsüsteemidel kontrollida. Lisaks toote töökõlblikkusele tuleb kontrollida, et uute komponentide kasutamine ei mõjuks juba kasutatavatele IT-süsteemidele negatiivselt. Kuna kahjulikke funktsioone ei saa enne teste välistada ja testimisel kutsutakse esile vigu, tuleb alati kasutada tootmisest isoleeritud testsüsteeme. Isoleeritud testsüsteemide kasutamine on vajalik ka siis, kui tuleb nt kontrollida e-posti teel saadud, ise ennast lahti pakkivaid faile, veendumaks, et neis ei esine kahjulikke funktsioone.

Üldiseid tarkvara vastuvõtu ja kasutamisse lubamise ning testimise protseduure on kirjeldatud moodulis B 1.10 Tüüptarkvara . Alles pärast testi läbimist tohib lubada uute komponentide installeerimist tootmissüsteemidesse.

Kontrollküsimused:

- Kas kõiki uusi IT-komponente testitakse enne kasutamist?
- Kas teste viiakse eranditult läbi isoleeritud testsüsteemides?

M 4.67 Tarbetute andmebaasikontode sulgemine ja kustutamine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: administraator

Kui uus kasutaja vajab oma andmebaasikontot ainult mõneks ajaks, tuleks juhul, kui andmebaas sellist võimalust pakub, vastavale kontole kehtestada kehtivuspiirang. Võib-olla on kasulik luua isegi kõik kontod ajapiiranguga ja neid regulaarselt (nt kord aastas) vastavalt vajadusele pikendada. Lisaks tuleb andmebaasi haldajaid teavitada võimalikult ruttu kasutaja töösuhete lõppemisest. Konto tuleb sulgeda hiljemalt kasutaja viimasel tööpäeval. Ka siis, kui kasutaja hakkab täitma teisi tööülesandeid, asub mõnele muule vastutusalale või liitub mõne muu projektiga, tuleb ebavajalikud andmebaasikontod sulgeda või kohandada pääsuõigused olukorraga sobivaks.

Lisaks tuleb regulaarselt kontrollida, kas olemasolevaid andmebaasikontosid ka tõepoolest reaalselt vajatakse. Eriti just tuleks sulgeda ka kõik mittevajalikud standardkontod.

Täiendavad kontrollküsimused:

- Kas on olemas organisatsioonilised ettekirjutused ajapiiranguga andmebaasikontode loomiseks, eriti siis, kui andmebaasisüsteem selliste kontode sisseseadmist ei toeta?
- Kas regulaarselt kontrollitakse, milliseid andmebaasikontosid enam ei vajata?
- Kas andmebaasi haldajatele teatatakse, kui andmebaasi kasutaja oma kontot enam ei vaja?

M 4.68 Järjekindla andmebaasi halduse tagamine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond, administraator
Rakendamise eest vastutavad: administraator

Andmebaasi haldamine on andmebaasi süsteemi (DBSi) käitamise kontseptsiooni keskpunktis, mille põhjal tagatakse muuhulgas ka andmebaasi läbivalt ühtlane haldamine. Töö kontseptsioonis peavad olema defineeritud kõik DBS'i jaoks olulised protsessid koos täpselt kindlaksmääratud lähtepunktidega, teostamisjärjestustega ja eesmärkidega ning protsesside läbiviimiseks volitatud rollidega koos nende õiguste ja kohustustega. Edasise projekti käigus tuleb defineeritud rollidele määrata reaalsed isikud. Rollide kirjelduses kirjeldatakse teatud funktsioonide teostamiseks vajalike rollide ülesandeid, pääsuõigusi ja volitusi (vt lisaks M 2.132 Andmebaasi kasutajate ja kasutajagruppide konfigureerimise reeglid). Andmebaasi haldamissüsteemis (DBMSis) tuleb defineeritud rollid sisse seada kasutajarühmadena, millel on rollidest sõltuvad õigused. Vastutavad kasutajad määratakse kasutajatunnuste kaudu kasutajarühmadesse, lähtuvalt rolliprofiilist. Eriti tuleb arvestada järgneva infoga:

- Süsteemiadministraator on andmebaasisüsteemi õiguste haldamisel eriline kasutaja, kes on olemas juba pärast DBMSi installeerimist. Sellel kasutaja pole mingeid andmebaasisüsteemi kasutuspiiranguid, mistõttu on olemas vigade tekke ning süsteemi kuritarvitamise risk. Seda tunnust tohivad kasutada ainult vähesed süsteemiadministraatorid konkreetsete administreerimisülesannete jaoks, nt andmebaasiadministraatorite määramiseks erinevatele andmebaasidele.
- Üksikute andmebaaside andmebaasiadministraatorite kasutajarühmad ja rühmadesse kuuluvad kasutajad ei ole oma vastutusala andmebaaside kasutamisel ja nendega manipuleerimisel mingil moel piiratud , mistõttu on olemas üldine potentsiaalne oht. Nende ülesannete jaoks vajalikud õigused tuleb selgelt defineerida ja dokumenteerida ning sama kehtib neid õiguseid omavate isikute kohta.
- Sageli töötavad administraatorid andmebaasiga ka tavakasutaja rollis, kuna lisaks administreerimisülesannetele on neil ka tavakasutaja ülesandeid või siis kasutavad nad andmebaasi administreerimiskeskkonda dokumentide salvestamiseks ja haldamiseks. Sel puhul tuleb neile lisaks administraatoritunnusele luua ka tavaline kasutajatunnus, mida kasutatakse vastavate andmebaasitööde jaoks. Administraatoritunnust tohib kasutada ainult administreerimistegevuste jaoks.
- Kasutaja liigitamist korraga mitmesse kasutajarühma tuleb täpselt planeerida, kuna kasutaja saab kõik volitused kõikidest kasutajarühmadest, mille alla ta liigitati.

Lisaks tuleb ülesannete selge jaotamisega, kohustuslike reeglite kehtestamisega ning administraatoritevaheliste kokkulepetega tagada, et administraatorid ei teeks vastastikku segavaid või poolikuks jäävaid töid. Seejuures peavad olema täidetud järgnevad tingimused:

- Tuleb määrata muudatuste liik ja teostamisviis, samuti dokumenteerimise kord.
- Kirjeldada tuleb muudatuste liiki, mahtu ja põhjust.
- Andmebaasiobjektide või andmete muutmine eeldab üldjuhul IT-rakenduse eest vastutava isiku luba. Kui tegu on tsentraalse andmebaasiobjektiga, vajab muudatus kõikide IT-rakenduste eest vastutavate isikute luba.
- Tuleb määrata planeeritud muudatuste elluviimise hetk ja see teatavaks teha.
- Enne muudatusi tuleb andmebaas täielikult varundada.
- Toimuva töö jaoks tuleb määrata kontrollintervall, mille ajal kontrollitakse dokumentide/logide aktuaalsust ja õigsust (vt lisaks M 4.69 Andmebaasi regulaarne turvakontroll).

Vältimaks andmebaasi tervikluse ohustamist ja üksikute andmehulkade ebakõlasid, tuleb kõik rakenduse andmebaasiobjektid luua ekstra vastava rakenduse jaoks sisseseatud kasutajagrupi alla, et neid seal hallata. Sellesse kasutajagruppi tohib määrata ainult neid kasutajaid, kes vajavad oma ülesannete täitmiseks otsest juurdepääsuõigust vastava rakenduse andmebaasiobjektidele. Lisaks peab vastava rakenduse eest vastutav andmebaasiadministraator olema selle kasutajagrupi liige.

Täiendavad kontrollküsimused:

- Millised meetmed võetakse tarvitusele, et vältida andmebaasiadministraatori töösamme, mis võivad viia ebakõladeni?
- Kas kõikidel andmebaasiadministraatoritel on täiendav, piiratud õigustega kasutajatunnus?
- Kas ühe rakenduse andmebaasiobjektidele luuakse eraldi kasutajagrupid?
- Kas andmebaasi haldamise ja kasutamise nõuded on käitamise kontseptsioonis kindlaks määratud?

M 4.69 Andmebaasi regulaarne turvakontroll

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: administraator

Andmebaasiadministraator peab regulaarselt, kuid vähemalt kord kuus läbi viima andmebaasisüsteemi (DBSi) turvakontrolli, mis peab olema reguleeritud käitamise kontseptsioonis. Sõltuvalt kontrolli tulemustest tuleb tarvitusele võtta vastavad meetmed, et likvideerida võimalikud kõrvalekalded käitamiskontseptsioonis loetletud nõuetest. Need meetmed ja vastutusalad peavad olema samuti reguleeritud käitamiskontseptsiooniga. Turvakontrolli raames tuleb kontrollida vähemalt järgnevaid aspekte, kusjuures (*)-märgistusega punkte saab vastavate skriptidega automatiseerida:

- Kas käitamiskontseptsiooniga ette kirjutatud tõendite loomine (nt muudatuste dokumenteerimine) toimub korrektselt?
- Kas vajalikud ja planeeritud varundamis- ja turvamehhanismid on aktiivsed ja tõhusad?
- Kas andmebaasi kasutajate hulgas leidub selliseid, kelle paroolid on kergesti äraarvatavad või puuduvad hoopis?
- Kas on kasutajaid, kes ei vaja enam oma ülesannete täitmiseks neile antud volitusi?
- Kes peale andmebaasiadministraatori tohib või saab ligi pääseda andmebaasitarkvara failidele või andmebaasi failidele operatsioonisüsteemi tasandil?
- Kellel peale andmebaasiadministraatori on juurdepääs andmebaaside süsteemitabelitele?
- Kes tohib andmebaasidele ligi pääseda interaktiivse *SQL-Editor*'iga?
- Millistel kasutajatunnustel on modifitseerimisvolitustega juurdepääsuõigus rakenduste andmebaasiobjektidele?
- Millistel kasutajatunnustel on lugev ja/või modifitseeriv juurdepääsuõigus rakenduste andmetele?
- Millistel kasutajatel on samad õigused nagu andmebaasiadministraatoril?
- Kas andmebaasisüsteemil on piisavalt vabu ressursse?

Täiendavad kontrollküsimused:

- Millal toimus viimane turvakontroll?
- Kas turvakontrolli teostamine ja tulemused dokumenteeritakse?
- Kas pärast turvalünkade avastamist võetakse tarvitusele meetmed nende kõrvaldamiseks?

M 4.70 Andmebaasiseire teostamine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: administraator

Tagamaks andmete käideldavust, andmebaasi terviklust ja andmete konfidentsiaalsust, läheb tarvis regulaarselt ja sobivate ajavahemike tagant toimuvat andmebaasiseiret. Järgnevalt selgitatakse mõningaid aspekte, millega tuleb seejuures arvestada, nt andmete fragmenteerumist andmebaasis, tegelikku andmemahtu ja selle muutumist seoses kasutusesolevate ressurssidega (täituvust) ning andmebaasi koormust.

Andmebaasi fragmenteerumine
Andmebaasi tuleb regulaarselt võimaliku fragmenteerumise suhtes kontrollida, et vajadusel planeerida ja ellu viia vastumeetmeid, nt andmebaasi reorganiseerimist. Andmebaasi haldussüsteei (DBMSi) salvestiruumi hallatakse tavaliselt kindlas suuruses plokkidena, st salvestiruumi muutmine (tavaliselt suurendamine) toimub ainult plokkhaaval. Andmehulkade salvestamisel jaotatakse need minimaalse plokkide hulga peale. Üldjuhul lisatakse andmeid, kasutades esmalt vabu plokke ja seejärel luuakse vastavalt vajadusele uusi. Kustutamisel vastavad plokid vabastatakse ja neid saab kasutada uute andmete jaoks. Aja jooksul tekib andmete muutmise tõttu salvestusalas segu kasutatud ja kasutamata plokkidest, samuti üha suurem arv poolikult hõivatud plokke. Lisaks sellele jaotuvad andmehulad andmekandjale laiali ka füüsiliselt. Selline fragmenteeritus kulutab asjatult salvestiruumi ja aeglustab andmebaasi kasutamist, kuna andmehulki ja vaba salvestiruumi tuleb otsida suuremalt alalt. Kui andmebaasi fragmenteeritus ületab ülanimetatud põhjustel kindlaksmääratud piiri, tuleb andmebaasi reorganiseerida. Andmebaasi tootjad ja teised tootjad pakuvad selle ülesande jaoks administreerimis- ja abiprogramme.

Andmemaht ja täituvus
Vältimaks liiga tugevat/kiiret fragmenteerumist, võimaldavad osad andmebaasi haldamissüsteemid teatud parameetrite defineerimisega reserveerida juba tabelite loomisel teatud hulga kokkukuuluvad plokke. Sellega suureneb sama andmehulga juures täituvus.
Andmebaasi faile tuleb regulaarselt andmemahu ja täituvuse osas kontrollida. Seejuures kontrollitakse regulaarselt, kas andmemaht muutub koos täituvusega vastavalt määratud tingimustele. Kui kasv on oodatust suurem, võib salvestuseks kasutada olev salvestiruum olla ebapiisav. Kontrollist tuleb tuletada vastavad meetmed, nt salvestusmahu suurendamine.

Näide

Oracle-andmebaasis määratakse igale tabelile kindel arv *Extent* 'e (Oracle keelekasutuses: loogiline suurusühik). Tabeli andmed salvestatakse vähemalt ühte *Extent*'i. Kui ühe *Extent* 'i maht on hõivatud, loob DBMS automaatselt järgmise *Extent* 'i. Tabeli loomisel saab määrata järgnevad väärtused:

- Esimese ja järgneva *Extent* 'i suurus baitides
- Kõikide edasiste *Extent* 'ide kasv protsentides, seejuures on see arv seotud teise *Extent* 'i suurusega
- Maksimaalne tabeli jaoks loodavate *Extent* 'ide arv
- Reserveeritud plokid hilisemate muudatuste jaoks protsentides

Kui uute *Extent* 'ide loomise tõttu muutub vaba salvestusmaht *Tablespace* 'i piires liiga väikeseks (vt G 2.39 Andmebaasi haldussüsteemi keerukus), tuleb lisada uus *Tablespace*. *Tablespace* 'ide arvu vähendamine on võimalik ainult läbi täieliku reorganiseerimise.

Koormus
Lisaks tuleb regulaarselt kontrollida andmebaasi töökoormust, eriti selle suhet kehtestatud ülempiiriga (vt M 4.73 Valitavate andmehulkade ülempiiride määramine). See, milline info on oluline konkreetse andmebaasiseire jaoks, sõltub nende konkreetsest tööviisist, seega kasutatava andmebaasi standardsest tarkvarast. Vastavalt sellele tuleb rakendada individuaalseid meetmeid, mis modifitseerivad andmebaasi konfiguratsiooni selliselt, et see vastaks nõuetele, mis puudutavad juurdepääsu kiirust, sooritatavaid tehinguid jne.

Andmebaasi seiret saab sageli skriptide abil ka automatiseerida. Selle eelduseks on siiski, et kasutatav andmebaasitarkvara võimaldab infot kasutada analüüsitaval kujul.

Täiendavad kontrollküsimused:

- Kas andmebaasifaile, olulisi tabeleid ja andmebaasi koormust kontrollitakse regulaarselt?
- Kas seire ajavahemikud on piisavad?

M 4.71 Andmebaasi linkide kasutamise kitsendamine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: administraator

Andmebaasilinkide (*DB-Link* 'ide) kaudu saab DBMSi piires ühest andmebaasist ligi pääseda teise andmebaasi andmetele, sõltuvalt olukorrast võivad andmed asuda isegi mõnes teises DBMSis. Tagamaks andmetele sobivat kaitset, tuleks seda tehnikat kasutada ainult vastava volituste kontseptsiooni raames. Selles kontseptsioonis tuleb esmajoones reguleerida kasutaja õiguste kontrolli DB-linkide kasutamisel. Nii saab määrata, et kasutaja saab ligipääsuvõimaluse võõrale andmebaasile, kui seal on olemas sama kasutajatunnus, millega kasutaja logib ennast sisse lokaalsesse andmebaasi. Parema kaitse tagamiseks saab ära kasutada võimalust luua eraldi DB-link ning siduda see konkreetse kasutajatunnusega ja parooliinfoga. Volituste kontseptsioonis tuleb DB-linke silmas pidades reguleerida järgnevaid aspekte:

- Üldiselt peaks CREATE-käsu abil DB-linkide loomise õigus olema ainult administraatoril. Eriti kehtib see DB-linkide kohta, mida tohivad kasutada kõik andmebaasi kasutajad (nn PUBLIC DB-lingid). Seega ei tohiks tavalistele kasutajatunnustele anda volitusi DB-linkide loomiseks.
- Ühe kasutaja paralleelselt kasutatavate DB-linkide hulka tuleb piirata, et hoida andmebaasiserveri koormust kontrolli all (vt M 4.73 Valitavate andmehulkade ülempiiride määramine). Vastasel korral võib ründaja seda ära kasutada, et vähendada andmebaasiserveri läbilaskevõimet või serverit täielikult üle koormata.
- Administraatorite loodud DB-linkide dokumenteerimine on ülimalt oluline. Dokumentatsioon peaks lisaks ühendusliigile (konkreetse kasutajatunnuse kaudu või eeldusel, et vastav kehtiv andmebaasitunnus on samuti loodud ühendatud andmebaasi jaoks) sisaldama ka seda infot, millised kasutajad suudavad vastavat DB-linki kasutada.

Täiendavad kontrollküsimused:

- Kas PUBLIC DB-linkide kasutamisest on loobutud?
- Kas andmebaasi kontseptsioon sisaldab ettekirjutusi DB-linkide kasutamise kohta?
- Millistel kasutajatunnustel on õigus luua DB-linke?

M 4.72z Andmebaasi krüpteerimine

Algatamise eest vastutavad: IT-juht, IT turvaosakond

Rakendamise eest vastutavad: rakenduste arendaja

Olenevalt andmebaasi salvestatud infost ja sellele kehtivatest konfidentsiaalsus- ja terviklusnõuetest võib olla vajalik neid andmeid krüpteerida. Seejuures eristatakse sidus- ja vallasrežiimis krüpteerimist:

- Sidusrežiimis krüpteerimisel krüpteeritakse ja dekrüpteeritakse andmed töö käigus, ilma et kasutajad seda märkaksid. Selleks võib kasutada vahendeid, millega krüpteeritakse kas operatsioonisüsteemi tasandil kogu kõvaketas või selliseid, millega krüpteeritakse ainult andmebaasi rakendusandmed.
- Vallasrežiimis krüpteerimisel krüpteeritakse andmed alles pärast töötlemist ja dekrüpteeritakse enne edasitöötlemist. Tavaliselt tehakse seda vahenditega, mis pole andmebaasisüsteemi integreeritud, ning see võib olla eriti mõistlik just andmebaasi varunduste või andmeedastuste jaoks. Seejuures tuleb jälgida, et kõvakettal oleks piisavalt ruumi, kuna krüpteerimine/dekrüpteerimine saab ainult siis edukalt toimuda, kui kõvakettal on piisavalt ruumi nii andmebaasi originaali kui ka krüpteeritud versiooni jaoks.

Lisaks on võimalik salvestada andmeid jätkuvalt ka loetavas tekstivormis, kuid rakendada võrgujuurdepääsu jaoks krüpteeritud andmeedastust. Seda saab teha nt Oracle SQL*Net tootepere Secure Network Services abil. See, milliseid andmeid milliste meetoditega krüpteerida, tuleb määrata juba andmebaasi tüüptarkvara valimisel (vt M 2.124 Sobiva andmebaasitarkvara valimine). Seejuures tuleks andmehulkade krüpteerimise nõudeid võrrelda vastavate andmebaasitarkvara funktsioonidega. Miinimumnõudena peab igal juhul olema tagatud, et andmebaasi kasutajatunnuste paroolid deponeeritaks krüpteeritult.

Kui ükski turustatav andmebaasi tüüptarkvara ei vasta vajalikele nõuetele, tuleb uurida lisatoodete kasutamise võimalust, et sulgeda vastavad turvalüngad. Kui lisatooteid pole saada, tuleb ettevõttes või ametiasutuses koostada krüpteerimisstrateegia elluviimise kontseptsioon.

Kontrollküsimused:

- Kas andmebaas või lisatooted pakuvad sobivaid krüpteerimistehnoloogiaid?
- Kas vastutavaid isikuid on teavitatud nõuetekohasest võtmehaldusest?

M 4.73 Valitavate andmehulkade ülempiiride määramine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: administraator, rakenduste arendaja

Andmebaasisüsteemides juurdepääsude paremaks kontrollimiseks ja selle jõudluse parandamiseks, tuleb kindlaks määrata andmebaasisüsteemide teatud parameetrite ülempiirid. Lisaks saab selle meetmega vähendada teatud tüüpi *Denial-of-Service* -rünnete (vt G 5.65 Teenusetõkestus andmebaasisüsteemis) tõenäosust.

Näited

- Ülempiiride kehtestamine andmehulkadele, mida võidakse valida ühe andmepöörduse raames
- Maksimaalne arv sisselogimisi ühe kasutajatunnuse kohta
- Maksimaalne CPU-aja kasutamine ühe sisselogimise kohta
- Andmebaasiühenduse kogukestvus
- Maksimaalne lubatud mitteaktiivne aeg sisselogimise ajal

Siinkohal tuleks esmajoones arvestada järgmiste alltoodud soovitustega.

Valitavate andmehulkade ülempiiride määramine

Maksimaalne arv andmehulki, mida saab valida ühe andmepöörduse raames, tuleb defineerida eriti just siis, kui andmebaasi on salvestatud suur kogus andmeid. Kui sellised piirid puuduvad, saab kasutaja valida sihilikult või kogemata suvaliselt suure hulga andmeid. See takistab nii üksiku kasutaja tööd kui põhjustab ka kõikide teiste andmebaasi kasutajate jaoks liiga pikki ooteaegu. Kui seejuures valitakse välja andmehulgad eesmärgiga neid modifitseerida, ei saa teised kasutajad neid kasutada enne, kui tehing on lõpetatud. Ülempiirid tuleb defineerida andmebaasile ligipääsevate rakenduste raames. Seejuures tuleb rakendada sobivaid kontrolle/lukke, mis kontrollivad piiridest kinnipidamist. Kui rakendus pakub otsingufunktsioone, tuleks keelata piiramatult laia otsingu kasutamine ja nõuda otsingukriteeriumite sisestamist. Kui rakendusprogrammi ja andmebaasi vaheline kaugus on suur (nt ühendusel läbi interneti), tuleb tulemusi vahetada plokkides, mille jaoks tuleb vajadusel samuti määrata ülempiirid.

Näide

Rakendusprogramm võtab internetiühenduse kaudu ühendust andmebaasiga. Rakendusprogrammi poolt andmebaasile edastatud päringud võivad vastuseks saada väga suuri andmehulki. Et liiga suured tulemusteplokid andmete edastamist rakendusele liigselt ei aeglustaks, kapseldatakse andmebaasil päring eraldi protseduuri. See protseduur edastab igal päringul kindla hulga andmeid (nt 5 andmehulka), kuni kõik tulemused on täielikult edastatud. Rakendus saadab terve rea päringuid DBMSile ja seab saadud osatulemused taas kokku või kuvab võimalusel ka juba osalisi tulemusi.

Ressursipiirangute kehtestamine

Mõned tootjad pakuvad ka võimalust määrata andmebaasi kasutamisele ressursipiiranguid.

Näited

Järgneva käsuga saab Oracle-andmebaasis andmebaasitunnuse “Meier” jaoks piirata ajutise *Tablespace* 'i „Temp"kasutuse 100 MB peale:

ALTER USER Meier TEMPORARY TABLESPACE Temp QUOTA 100M ON Temp;

Järgneva käsuga luuakse profiil „Testija", mis piirab sessioonide arvu, maksimaalset CPU-aega sessiooni kohta, andmebaasiühenduse maksimaalset aega ja maksimaalset ooteaega (IDLE). Vastava profiili võib siis siduda üksikute kasutajatega.

CREATE PROFILE Tester LIMIT
SESSIONS PER USER 2,
CPU _PER_SESSION 6000,
IDLE_TIME 30,
CONNECT_TIME 500;

Ingres-andmebaas võimaldab nt kasutajatele ja gruppidele määrata piire päringu maksimaalse sisendi ja väljundi jaoks või päringu kohta kehtivatele lausetele. Lisaks saab piirata kasutajate arvu, kes tohivad samaaegselt andmebaasi kasutada. Sõltuvalt litsentsimudelist saab nende piiramisega DBMSi parameetriseadistuste abil tagada ka seda, et andmebaasi tarkvara puhul ei ületataks maksimaalselt saadaolevate litsentside arvu. Lisaks põhjustavad liiga paljud paralleelsed kasutajad liiga suurt töökoormust, millega andmebaasi server ei pruugi toime tulla. Seeläbi pikeneb ülekande keskmine kestus. Kui sel juhul ei saa andmebaasi ressursse enam laiendada, on ka siin abiks maksimaalselt võimalike paralleelsete juurdepääsude piiramine.

Teisest küljest võib võimalike paralleelsete kasutajajuurdepääsude piiramine kasutaja jõudlust oluliselt piirata. Seega tuleks seda funktsiooni kasutada ainult pärast hoolikat kontrollimist või ajutiselt, näiteks erandkorras esineva tippkoormuse puhul. Kui andmebaasi kasutajate arv väheneb ja on tõenäoline, et praegused ressursid tulevastele jõudlusnõuetele ei vasta, või et läheb tarvis rohkem litsentse, tuleb planeerida vastav laiendamine. Eeldatavate vajaduste osas tuleks selgusele jõuda juba andmebaasitarkvara valimisel, et luua vajadusel kontseptsioon ressursipiirangute rakendamiseks (vt M 2.124 Sobiva andmebaasitarkvara valimine).

Täiendavad kontrollküsimused:

- Kas rakendustes kontrollitakse ja järgitakse ülempiiridest kinnipidamist?
- Kas rakendustes takistatakse piiramatult laia otsingu kasutamisvõimalust?
- Kas andmebaasi ressursipiirangu nõuded on sõnastatud ja dokumenteeritud?

M 4.78 Konfiguratsioonimuudatuste hoolikas teostamine

Algatamise eest vastutavad: IT turvaspetsialist, IT-juht

Rakendamise eest vastutavad: administraator

IT-süsteemi tavatöö režiimis on muudatuste tegemine alati seotud teatud ohuga, mistõttu tuleb seejuures olla eriti hoolikas. Enne süsteemi muutma asumist tuleb esmalt varundada vana konfiguratsioon, et tagada selle kiire kasutuselevõtt, kui uue konfiguratsiooniga peaks esinema probleeme.

Võrku ühendatud IT-süsteemide puhul tuleb kasutajaid teavitada õigel ajal hooldustöödest, nt sissekandega sisevõrgus või e-posti teel, et nad jõuaksid aegsasti süsteemi välja lülitada ning oskaksid õigesti tuvastada probleeme, mis võivad tekkida pärast muudatust. Konfiguratsiooni muudatusi tuleb teha alati sammhaaval. Vahepeal tuleb alati kontrollida, kas muudatus tehti õigesti ja kas IT-süsteem ning puudutatud rakendused on jätkuvalt töökõlbulikud. Süsteemifailide muudatuste järel tuleb teha taaskäivitus, et kontrollida, kas IT-süsteemi käivitamine toimib korrektselt. Võimalike probleemide kõrvaldamiseks tuleks hoida käepärast taaskäivitamise jaoks vajalikud andmekandjad, nt buutimisdisketid ja käivitus-CD-ROM-id.

Enne konfiguratsiooni muutmist tuleb asjassepuutuvad failid ja kataloogid varundada. Keerukaid konfiguratsioonimuudatusi tuleks võimaluse korral teha koopiates, mitte originaalfailides. Enne muudatuste kasutuselevõtmist tavatöö režiimis, tuleb lasta kõik tehtud muudatused mõnel kolleegil üle kontrollida.

Kõrgete käideldavusnõuetega IT-süsteemide puhul tuleb kasutada varusüsteeme või tagada vähemalt piiratud IT-töö. Ideaaljuhul peaks protseduur vastama avariikäsiraamatu ettekirjutustele. Tehtud konfiguratsioonimuudatused tuleb sammsammult kirja panna, et probleemide korral saaks muudatusi sammhaaval tühistada ja nii IT-süsteemi taas töökorda seada (vt lisaks M 2.34 IT-süsteemi muutuste dokumenteerimine).

Kontrollküsimused:

- Kas kasutajaid teavitatakse hooldustöödest sobival moel?
- Kas süsteemi muutmist tehakse ja dokumenteeritakse sammhaaval?
- Kas kõikidest failidest, mida tuleb muuta, on olemas varukoopiad?
- Kas muudatusi saab hiljem tühistada?

M 4.79 Kohapealse võrguhalduse turvalised pääsumehhanismid

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: administraator

Teatud aktiivsete komponentide puhul saab komponente hallata ka kohaliku juurdepääsu kaudu. Selline lokaalne juurdepääs on leiab tavaliselt aset läbi jadaühenduse (tavaliselt liides V.24 või EIA-232-E). Turvalise kohaliku juurdepääsu tagamisel tuleb arvestada järgnevate meetmetega:

- Aktiivsed võrgukomponendid ja nende lisaseadmed, nt ühendatud terminalid, tuleb turvaliselt üles seada (vt M 1.29 IT-süsteemi õige paigutus)
- Kohalik juurdepääs kohalike komponentide administreerimisele peab olema tarkvaraliselt ja/või mehaaniliselt tõkestatud
- Kui kohalik juurdepääs on varustatud parooliga, tuleb selle standardparool ära muuta kohe pärast selle kasutuselevõttu (infot uue parooli valimise leiate meetmest M 2.11 Paroolide kasutamise reeglid)
- Tuleb aktiveerida pidevalt ühendatud terminalide või arvutite turbefunktsioonid, nt automaatne ekraanilukk või automaatne väljalogimine.

Kohalik administreerimine pakub järgnevaid eeliseid:

- Väheneb paroolide pealtkuulamise oht.
- Ka siis, kui mõnes võrgusegmendis, milles asub aktiivne komponent, esineb avarii või kui kogu võrk peaks rivist välja langema, saab administreerimisülesandeid siiski jätkuvalt täita.

Kohalikul administreerimisel on ka puudusi:

- Aktiivseid võrgukomponente saab üldjuhul konfigureerida selliselt, et aktiivseid võrgukomponentidele administreeritaks kas kohalikult või tsentraalselt. Konfiguratsioonimeetodite valimise jaoks ei saa siinkohal anda üldkehtivat soovitust. Siiski tuleb arvestada, et kui konfiguratsiooni loomisel lähtutakse eranditult kohalikust administreerimisvõimalusest, ei ole aktiivsete võrgukomponentide tsentraalne administreerimine enam võimalik. Seda tööd tuleb siis ka alati kohapeal vastavate komponentide juures teha. Sel juhul suureneb tõrke korral reageerimisaeg, kuna tee komponentide asukohani võib olla pikk.
- Kohalik juurdepääs V.24 või EIA-232-E liidese kaudu on üldjuhul aeglasem kui kaugjuurdepääs võrgu kaudu.

Täiendav kontrollküsimus:

- Kas kohaliku juurdepääsu standardparoolid on vahetatud turvaliste vastu?

M 4.80 Kaug-võrguhalduse turvalised pääsumehhanismid

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator

Teatud aktiivseid võrgukomponente saab administreerida ning kontrollida kaug-juurdepääsu kaudu. Juurdepääs toimub kas ühendusele orienteeritud või ühenduseta protokollide abil.

Siia alla kuuluvad:

- Puhtad andmeedastusprotokollid, nt et edastada uusi püsivara versioone või konfiguratsioonifaile, nt FTP, TFTP (viimase kasutamisest tasub kindlasti hoiduda) või RCP (vt M 6.52 Võrgu aktiivkomponentide konfiguratsiooni-andmete regulaarne varundamine)
- Interaktiivse kommunikatsiooni protokollid, nt SSH,
- Võrguhalduse protokollid, nt SNMP.

Kõikide juurdepääsuliikide puhul tuleb tagada, et volitamata juurdepääs oleks välistatud.

Võrgukomponentide turvalise kaugvõrguhalduse korral tuleb tähelepanu pöörata alljärgnevale:

- Interaktiivseks suhtluseks tohib kasutada üksnes turvalisi protokolle, nagu näiteks SSH-d või HTTP-d. Ebaturvalisi protokolle, nagu Telnet või HTTP, ei tohi kasutada või tohib seda teha üksnes selleks ettenähtud administraatorivõrgus (Out-of-Band-Management).
- Interaktiivsete suhtlusprotokollide jaoks tuleks aktiveerida võrgukomponentide Auto-Logout-valik, et lukustada või lõpetada ühendused määratud ajavahemiku järel ilma kasutajate tegevuseta.
- Ka andmete edastamiseks (püsivaraversioonide või konfiguratsioonifailide varundamine) tohib kasutada üksnes turvalisi protokolle, nagu näiteks SCP.
- Ebaturvalisi protokolle, nagu näiteks TFTP, FTP või RCP, tohib kasutada üksnes isoleeritud administraatorivõrgus.
- SNMP-d tohiks kasutada üksnes alates versioonist 3 (SNMPv3), sest alles sellest versioonist alates toetatakse tugevamat autentimist ja krüpteerimist.
- Kui SNMP-d kasutatakse ebaturvalises versioonis (SNMPv1 või SNMPv2), siis üksnes koos Out-of-Band-Management'iga. SNMPv1 ja SNMPv2 ei tohi mingil juhul kasutada väljaspool isoleeritud administraatorivõrke, sest need ei paku suhtluse kaitsmiseks piisavalt võimalusi.
- Kõik standardsed paroolid või võrgukomponentide community-nimed tuleb välja vahetada turvaliste paroolide või community-nimede vastu (vt M 4.82 Võrgu aktiivkomponentide turvaline konfigureerimine). Community-nimede ja paroolide ühendamine puudutab paljude aktiivsete võrgukomponentide puhul protokolle FTP, Telnet ja SNMP.
- Paljud komponendid pakuvad ka võimalust piirata juurdepääsu administreerimispääsudele (Management-Interface) MAC- või IP-aadresside baasil.
- Võimaluse korral tuleks seda valikut kasutada, et võimaldada juurdepääs ainult eriotstarbelistest haldusjaamadest.

- Enamike mainitud protokollide puhul tuleb arvestada, et paroolide ja Community nimede edastamine toimub loetava teksti kujul, seega on need üldiselt pealtkuulatavad (vt M 5.61 Sobiv füüsiline segmenteerimine ja M 5.62z Sobiv loogiline segmenteerimine).
- Selleks tuleb vahetada võrgukomponentide standardparoolid või Community nimed turvaliste paroolide või Community nimede vastu (vt M 4.82 Võrgu aktiivkomponentide turvaline konfigureerimine). Community nimede ja paroolide ühendamine puudutab paljude aktiivsete võrgukomponentide puhul protokolle FTP, Telnet, SNMP ja CMIP. Teatud komponendid võimaldavad juurdepääsu piirata MAC- või IP-aadresside põhjal. Võimalusel tuleks seda valikut kasutada, et võimaldada juurdepääs ainult eriotstarbelistest haldusjaamadest.

Andmeedastuse protokolle (TFTPd, FTPd, RCPd) tohivad käivitada ainult võrukomponendid ise. Eriti oluline on see autentimiseta protokollide puhul, nt TFTP. Interaktiivsete kommunikatsiooniprotokollide (Telnet'i) jaoks tuleb aktiveerida võrgukomponentide automaatne väljalogimine.

Näide:
SNMP puhul standardina määratud Community nimed „public"ja „private"tuleb vahetada teiste nimede vastu.

Kontrollküsimused:

- Kas kõik standardparoolid ja Community nimed on vahetatud turvaliste isevalitute vastu?
- Kas andmeedastusi on võimalik algatada ainult võrgukomponentidel?
- Kas interaktiivseks suhtluseks ja andmete edastamiseks kasutatakse üksnes turvalisi protokolle?
- Kas interaktiivsete suhtlusprotokollide jaoks on aktiveeritud võrgukomponentide Auto-Logout-valik?
- SNMP rakendamisel: Kas kasutatakse vähemalt SNMPv3?
- Ebaturvaliste protokollide kasutamisel: Kas neid kasutatakse peamiselt selleks ettenähtud administraatorivõrgus (Out-Of-Band-Management)?
- Kas standardseid paroole ja community-nimesid muudetakse enne aktiivsete võrgukomponentide kasutuselevõttu?
- Komponentide kasutamise korral, mille puhul saab piirata juurdepääsu MAC-i või IP-aadressidele Kas lubatud on ainult juurdepääs eriotstarbelistest haldusjaamadest?
- Kas interaktiivseks suhtluseks ja andmete edastamiseks kasutatakse üksnes turvalisi protokolle?
- Kas interaktiivsete suhtlusprotokollide jaoks on aktiveeritud võrgukomponentide Auto-Logout-valik?
- SNMP rakendamisel Kas kasutatakse vähemalt SNMPv3?
- Ebaturvaliste protokollide kasutamisel Kas neid kasutatakse peamiselt selleks ettenähtud administraatorivõrgus (Out-Of-Band-Management)?
- Kas standardseid paroole ja community-nimesid muudetakse enne aktiivsete võrgukomponentide kasutuselevõttu?

- Komponentide kasutamise korral, mille puhul saab piirata juurdepääsu MAC-i või IP-aadressidele Kas lubatud on ainult juurdepääs eriotstarbelistest haldusjaamadest?

M 4.81 Võrgutoimingute audit ja logimine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator, revident

Ajakohane logimine, auditeerimine ja revisjon on võrgu turvalisuse seisukohalt olulised faktorid.

Logimine võrguhaldussüsteemi piires või teatud aktiivsete võrgukomponentide juures võimaldab salvestada teatud (ülddefineeritavaid) seisundeid hilisema analüüsi jaoks. Tüüpilised logitavad juhtumid on nt vigaste pakettide edastamine võrgukomponendile või võrgu jõudlus teatud ajahetkedel. Selliste logide analüüs sobivate abivahendite abil võimaldab nt teha järeldusi selle kohta, kas võrgu ribalaius vastab hetkenõuetele ning aitab tuvastada võrgust tulevaid süstemaatilisi ründeid.

Auditi all mõistetakse teenuse kasutamist, mis jälgib eriti just turvalisuse seisukohast kriitilisi sündmuseid. See võib toimuda nii online kui offline. Online-auditi korral toimub sündmuste jälgimine ja analüüsimine reaalajas, milleks kasutatakse sobivat tarkvaratööriista (nt võrguhaldussüsteemi). Offline -auditi korral andmed logitakse või võetakse olemasolevast logifailist. Offline -auditi abil kontrollitavate faktorite alla kuuluvad sageli ka kasutusaja ja tekkivate kulude andmed.

Revisjoni käigus kontrollib (Offline -) auditi käigus kogutud andmeid üks või mitu sõltumatut töötajat (nelja silma printsiipi järgides), et avastada ebakorrapärasusi IT-süsteemide töös ja kontrollida administraatorite tööd.

Võrguhaldussüsteemiga võimalikud logimis- ja auditeerimisfunktsioonid tuleb aktiveerida mõistlikul hulgal. Lisaks jõudluse mõõtmisele võrgukoormuse seireks tuleb eriti just analüüsida sündmusi (Events), mille loob võrguhaldussüsteem, või kasutada spetsiifilisi andmekogujaid (nt RMON-sonde), millega saab kontrollida ja analüüsida turvalisuse seisukohast kriitilisi sündmusi.

Logimisel tekib tavaliselt nii palju sissekandeid, et nende tulemuslik analüüsimine on võimalik ainult tarkvaratööriista abil. Auditi puhul keskendutakse turvalisuse seisukohast kriitiliste sündmuste kontrollimisele. Lisaks kontrollitakse auditi käigus sageli ka andmeid kasutusaegade ja tekkivate kulude kohta.

Auditi jaoks on seejuures eriti olulised järgnevad sündmused:

- Andmed IT-süsteemide tööaja kohta (millal lülitati milline IT-süsteem sisse/välja?)
- Pöördused aktiivsetesse võrgukomponentidesse (kes logis millal sisse?)

- Turvalisuse seisukohast kriitilised edukad ja ebaõnnestunud juurdepääsud võrgukomponentidele ja võrguhalduskomponentidele
- Võrgukoormuse jaotus ühe päeva või ühe kuu tööaja peale ja võrgu üldine jõudlus

Lisaks tuleb logida järgnevad sündmused:

- IT-süsteemi tõrkeid põhjustada võivad riistvaravead
- IT-süsteemi IP-aadressi loata muutmine (TCP/IP-keskkonnas)

Audit võib toimuda nii online kui ka offline. Online -auditi käigus edastatakse vastavalt kategooriatesse jaotatud sündmused otse audiitorile, kes saab vajadusel võtta tarvitusele sobivad vastumeetmed. Selleks tuleb sündmused jaotada sobivatesse kategooriatesse, et vastutav administraator või audiitor saaks kohe olulistele sündmuste esinemisel reageerida ja ei kaotaks infotulvas ülevaadet. Kas rollijaotus on vajalik? Offline -auditi korral töödeldakse logifailide või eriotstarbeliste auditeerimisfailide andmeid auditeerimistööriista abil ning neid kontrollib audiitor. Viimasel juhul saab turvalisuse säilitamise ja taastamise meetmeid võtta tarvitusele ainult viivitusega. Üldiselt on soovitatav Online - ja Offline -auditit omavahel kombineerida. Seejuures filtreeritakse Online -auditi jaoks turvalisuse seisukohast kriitilisi sündmusi ja edastatakse kohe audiitorile.

Lisaks analüüsitakse vähem kriitilisi sündmuseid offline. Logimise ja auditi jaoks saab kasutada standardseid haldusprotokolle nagu nt SNMPd ja sellele toetuvat RMONi, kuid ka kasutatava võrguhaldustoote eriotstarbelisi logisid. Mitte mingil juhul ei tohi auditi või logimise raames koguda kasutajate paroole! See tekitab suure turvariski, juhul kui keegi sellele infole volitamata ligi pääseb. Ka valesti sisestatud paroole ei tohi logida, kuna need erinevad kehtivatest paroolidest tavaliselt ainult ühe märgi võrra või siis on kaks märki vahetusse läinud.

Lisaks tuleb määrata, kes peab logide ja auditite andmeid analüüsima. Siinkohal tuleb tagada, sündmuse põhjustaja ja analüüsija (nt administraator ja audiitor) ei oleks üks ja sama isik. Lisaks tuleb jälgida, et järgitaks kõiki andmekaitsest tulenevaid ettekirjutusi. Kõikide kogutud andmete puhul tuleb arvestada eesmärgiga. Logi- või auditifaile tuleb regulaarselt analüüsida. Nende maht võib kiiresti väga suureks paisuda. Selleks, et piirata logi või auditi faile suurusele, mis võimaldaks neid tegelikult analüüsida, tuleks valida sobivad analüüsiintervallid, kuid igal juhul piisavalt lühikesed, mis tagaks tõhusa analüüsi.

Kontrollküsimused:

- Kas salvestatud logi- ja auditifaile kontrollitakse regulaarselt?
- Kas turvalisuse seisukohast kriitiliste sündmuste võimalikke tagajärgi analüüsitakse?
- Kas kasutajate paroolide kogumine on logimise raames välistatud?

M 4.82 Võrgu aktiivkomponentide turvaline konfigureerimine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: administraator
Serverisüsteemide ja lõppseadmete turvalisuse kõrval jäetakse tegelik võrguinfrastruktuur koos aktiivsete võrgukomponentidega sageli unarusse. Siiski tuleb eriti just tsentraalseid aktiivseid võrgukomponente hoolikalt konfigureerida. Kui serverisüsteemi vale konfiguratsioon mõjutab ainult vastavaid kasutajaid, kes selles süsteemi teenuseid kasutavad, võib marsruuteri vale konfiguratsiooni tagajärjeks olla suurema alamvõrgu või lausa terve võrgu avarii või andmete märkamatu kompromiteerimine. Võrgukontseptsiooni raames (vt M 2.141 Võrgukontseptsiooni väljatöötamine) tuleb määrata ka aktiivsete võrgukomponentide turvaline konfigureerimine. Arvestada tuleks ennekõike järgnevate aspektidega:

- Marsruuteri ja 3. kihi kommuteerimise jaoks tuleb valida, milliseid protokolle edastatakse ja milliseid läbi ei lasta. See võib toimuda sobivate filtreerimisreeglite juurutamise abil.
- Tuleb määrata, millised IT-süsteemid millises suunas marsruuteri kaudu suhtlevad. Ka seda saab realiseerida filtreerimisreeglite abil.
- Kui aktiivsed võrgukomponendid seda toetavad, tuleks kindlaks määrata, millistel IT-süsteemidel on juurdepääs kohtvõrgu kommutaatorite ning jaoturite portidele. Selleks analüüsitakse päringut esitava IT-süsteemi MAC-aadressi ja kontrollitakse selle volitusi.

Marsruutimisfunktsioonidega aktiivsete võrgukomponentide jaoks läheb tarvis marsruutimise Update -funktsiooni sobivat kaitset. Seda läheb tarvis marsruutimistabelite värskendamiseks, et tagada dünaamiline kohandamine vastavalt kohtvõrgu tegelikele oludele. Siinkohal saab eristada kahte erinevat turvamehhanismi:

- Paroolid - Paroolide kasutamine kaitseb selliselt konfigureeritud marsruutereid marsruutimis-värskenduste vastuvõtmise eest läbi marsruuterite, millel puudub vastav parool. Seeläbi saab marsruutereid kaitsta valede või kehtetute marsruutimisvärskenduste vastuvõtmise eest. Paroolide eelis teiste kaitsemehhanismide ees on nende vähene andmekulu, mis tarbib väga vähe ribalaiust ja arvutusaega.
- Krüptograafilised kontrollsummad - Kontrollsummad kaitsevad kehtivaid marsruutimisvärskendusi märkamatute muudatuste eest, kui need läbi võrgu liiguvad. Koos järjenumbriga või ainuomase nimetajaga võib kontrollsumma kaitsta ka vanade marsruutimisvärskenduste taaspaigaldamise eest.

Marsruutimisvärskenduse sobiva kaitse eelduseks on sobiva marsruutimisprotokolli valik. RIP-2 (Routing Information Protocol Version 2, RFC 1723) ja OSPF (pen Shortest Path First, RFC 1583) toetavad paroole oma põhispetsifikatsioonis ja suudavad laiendite abil kasutada MD5 (Message Digest 5) meetodi krüptograafilisi kontrollsummasid.

Kontrollküsimused:

- Kas võrgukontseptsiooni loomisel arvestati aktiivsete võrgukomponentide turvalise konfiguratsiooniga?

- Kas kasutatakse sobivat marsruutimisprotokolli?
- Kuidas kaitstakse marsruutimisvärskendusi?
- Kas kasutatava marsruutimisprotokolli kaitsemehhanismid (nt marsruutimisvärskenduste raames) vastavad tehnika tasemele?

M 4.83 Võrgukomponentide riistvara ja tarkvara värskendamine ja täiendamine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: administraator

Tarkvara värskendamise (*update*) abil saab kõrvaldada selle kitsaskohti ja täiendada funktsioone. See puudutab näiteks aktiivsete võrgukomponentide nagu kommutaatorite ja marsruuterite käitustarkvara, kuid ka võrguhaldustarkvara. Värskendused on eriti vajalikud siis, kui leitakse mõni puudujääk, mis mõjutab võrgu turvalist kasutamist, kui rikked esinevad korduvalt või funktsiooni täiendamine on vajalik turvatehniliste nõuete või erialaste nõudmiste tõttu. Ka riistvara uuendamine võib olla teatud juhtudel kasulik, nt kui kommutaatori uuem versioon pakub kõrgemat edastus- ja filtreerimisjõudlust. Nende meetmetega on võimalik suurendada käideldavust, terviklust ja konfidentsiaalsust.

Enne uuendamist või värskendamist tuleb hoolikalt kontrollida uute komponentide funktsioone, ühilduvust ja usaldusväärust. Seda on kõige mõistlikum teha füüsiliselt eraldatud testvõrgus, enne kui värskenduse või uuenduse kasutuselevõttu tootmisvõrgus (vt M 4.78 Konfiguratsioonimuudatuste hoolikas teostamine *)*.

Täiendav kontrollküsimus:

- Kas värskendusi/täiendeid kontrollitakse enne tootmises kasutuselevõtmist, kas need ühilduvad juba olemasolevate komponentidega?

M 4.84 BIOSi turvamehhanismide kasutamine

Algatamise eest vastutavad: IT-juht, IT turvaosakond

Rakendamise eest vastutavad: administraator, kasutaja

Moodsad BIOSi variandid pakuvad mitmeid turvamehhanisme, mida kasutajad ja süsteemiadministraatorid peavad tundma. BIOSi sissekandeid ei tohi mitte mingil juhul muuta koolitamata kasutaja, kuna selle tagajärjel võivad tekkida tõsised rikked.

- Paroolkaitse: enamike BIOSi variantide puhul saab aktiveerida paroolkaitse. Sellest on küll suhteliselt lihtne mööda pääseda, kuid kui muud kaitsemehhanismid puuduvad, tuleks seda siiski kasutada. Tavaliselt saab valida, kas parooli kontrollitakse enne igat arvuti käivitamist või ainult BIOSi seadistustele ligi pääsemiseks. Osaliselt saab nende kontrollide jaoks määrata isegi erinevaid paroole. Et volitusteta isikud ei saaks BIOSi seadistusi muuta, peab häälestamise või administraatoriparool olema alati aktiveeritud. Teatud (kahjuks väheste) BIOSi variantide puhul saab parooliga takistada juurdepääsu disketiseadmetele. Seda võimalust tuleks kasutada, et vältida tarkvara volitamata paigaldamist või andmete märkamatut kopeerimist.
- Buutimisjärjekord: buutimisjärjekord peab olema selline, et esimesena buuditakse alati kõvakettalt. Näiteks peab seadistus olema „C, A”. See kaitseb buutimisviirustega nakatamise eest juhul, kui diskett jäeti kogemata kettaseadmesse, samuti hoiab see aega kokku ja säästab disketiseadet. Buutimisjärjekorra muutmine aitab takistada olukorda, kus buuditakse väliselt andmekandjalt. See tagab, et buutimise ajal ei loeta disketiseadmesse asetatud disketti, mis võib nakatada PC buutimisviirusega (vt G 5.23 Pahavara).

Olenevalt kasutatavast BIOSist ja operatsioonisüsteemist tuleb takistada ka muudelt vahetatavatelt andmekandjatelt, nt CD-ROMidelt buutimist. Buutimisjärjekorra muutmata jätmise korral on võimalik mööda pääseda ka muudest turvamehhanismidest, nt pääsuõiguste kontrollimise mehhanismidest (vt M 4.1 IT-süsteemide paroolkaitse). Selle näitena võib välja tuua mõne muu operatsioonisüsteemi käivitamise nii, et määratud turvaatribuute ignoreeritakse. Üldjuhul tuleb buutimisjärjekorda kontrollida buutimiskatses, kuna teatud kontrollerid tühistavad sisemise järjestuse ja vajavad eraldi seadistamist.

- Viirusetõrje, viirusehoiatus: selle funktsiooni aktiveerimisel nõuab arvuti enne buutimissektori või MBRi (Master Boot Record) muutmist kinnitust, kas muudatus on lubatud.

Kontrollküsimus:

- Millised BIOSi turvamehhanismid on aktiveeritud?

M 4.85z Sobiv krüptomoodulite liideste disain

Algatamise eest vastutavad: IT turvaosakond

Rakendamise eest vastutavad: IT turvaosakond

Krüptomoodul peab olema sellise disaini ja konfigureerimisvõimalustega, et kogu infovoogu moodulist ja moodulisse või lausa vahetut füüsilist juurdepääsu mooduli andmekogumile saaks kontrollida, st piirata. Olenevalt kasutamise viisist või kaitsevajadusest tasub kasutada füüsiliselt lahutatud sisend- ja väljundporte. Igal juhul peaksid moodulliidesed olema sellise ehitusega, et üksikud andmekanalid oleksid üksteisest loogiliselt eraldatud, kuigi need võivad jagada ühist sisend- või väljundporti. Krüptomooduli võtmehalduse kontekstis tuleb tagada, et väljundkanalid oleksid sisemisest võtmegenereerimisest või manuaalse võtmesisestuse sisestuspordist vähemalt loogiliselt eraldatud. Sageli on välise toitepinge või toiteallika ühendamiseks ja eranditult parandus- või hooldustööde tegemiseks olemas eraldi liidesed.

Krüptomooduli seisukohast on seega otstarbekohane rakendada järgnevat jaotust ja kasutuskorda:

- Andmete sisestamise liides, mis vahendab kõiki krüptomooduli sisestusandmeid, mida moodulis töödeldakse (nt krüptograafilisi võtmeid, autentimisinfot, teiste krüptomoodulite seisundiinfot, loetava teksti kujul andmeid jne).
- Andmete väljastamise liides, mis vahendab kõiki krüptomooduli andmeid, mis moodulist edastatakse (nt krüpteeritud andmeid, autentimisinfot, teiste krüptomoodulite juhtimisinfot jne).
- Juhtandmete sisestamise liides, mis edastab kõiki juhtkäsklusi, -signaale ja -andmeid, mis on vajalikud mooduli töö juhtimiseks ja töörežiimi seadistamiseks.
- Juhtandmete väljastamise liides, mis edastab kõiki signaale, näite ja andmeid, mida väljastatakse ümbritsevasse keskkonda, et kuvada krüptomooduli sisemine turvaseisund.
- Hooldusliides, mida kasutatakse eranditult hoolduse ja parandamise otstarbel.

Krüptokomponendi dokumentatsioon peab sisaldama kõikide komponentide kirjeldust (riistvara, püsivara ja/või tarkvara). Lisaks peab dokumentatsioon sisaldama moodulliideste täielikku spetsifikatsiooni koos füüsiliste või loogiliste portide, manuaalsete või loogiliste juhtüksuste, füüsiliste või loogiliste näidikelementide ja nende füüsiliste, loogiliste või elektriliste omadustega. Kui krüptokomponent sisaldab hooldusliidest, peab dokumentatsioon sisaldama ka tehtavate hooldustööde täielikku spetsifikatsiooni. Kõik moodulisisesed füüsilised ja loogilised sisend- ja väljundkanalid peavad olema selgelt välja toodud.

Lisaks krüptokomponentide konkreetsele integreerimisele ettenähtud kasutuskeskkonda tuleb kirjeldada ka nende kasutamist. Lisaks peab dokumentatsioon sisaldama turvafunktsioonide kogumit ja näitama võimaluse korral ka sõltuvust riist-, püsi- või tarkvarast, mis ei kuulu krüptokomponendi kontseptsiooni kohaselt selle vahetusse tarnepaketti.

Moodulliideste dokumentatsiooni peab saama mooduli tootja käest. Dokumentatsioon on vajalik näiteks administraatorile, kes tahab krüptomoodulit integreerida oma süsteemikeskkonda, või hindajale, kes tahab hinnata krüptomooduli turvalisust.

Kontrollküsimused:

- Milline info on krüptomooduli liideste kohta olemas?
- Kas infot on piisavalt?

M 4.86 Krüptomoodulite kindel rollijaotus ja konfigureerimine

Algatamise eest vastutavad: IT turvaosakond

Rakendamise eest vastutavad: IT turvaosakond

Paljud krüptograafilised turvakomponendid pakuvad võimalust eristada mitut kasutajarolli ning volitatud personali vastavaid täidetavaid ülesandeid. Olenevalt kaitsevajadusest läheb selleks tarvis juurdepääsukontrolli- ja autentimismehhanisme, et kontrollida, kas kasutajal on ka tegelikult õigus soovitud teenust käivitada.

Lähtuvalt erinevatest rollidest on võimalik kasutada alljärgnevat jaotust:

- kasutajaroll, kes turvakomponente kasutab (nt lõpposaleja, kasutaja);
- operaatoriroll, kes on vastutav installeerimise ja krüptograafilise haldamise eest (nt turvaadministraator);
- hooldusroll, kes on vastutav hooldus- ja parandustööde eest (nt hooldustehnik, revident).

Krüptokomponentide puhul, mis võimaldavad kasutaja- ja administraatorirolle lahutada, tuleb seda võimalust ka kasutada ning selleks peab administraator tegema põhiseadistused, nt määrama parooli või võtme pikkuse, et kasutaja ei saaks mugavusest või teadmatusest valida endale ebaturvalisi seadistusi. Erinevate rollide kõrval tuleb eristada ka erinevaid tegevusi ehk turvakomponentide pakutavaid teenuseid.

Krüptomoodul peab pakkuma vähemalt järgmisi teenuseid:

- seisundinäit krüptokomponendi hetkeseisundi kuvamiseks;
- enesetest iseseisvate enesetestide algatamiseks ja läbiviimiseks;
- möödaviik (bypass), et aktiveerida ja desaktiveerida möödaviiku, mille abil saab läbi krüptomooduli transportida loetaval tekstikujul olevat infot või kaitsmata andmeid.

Personali autentimiseks turvakomponendi suhtes saab kasutada erinevaid meetodeid: parool, PIN, krüptograafiline võti, biomeetrilised andmed jne. Krüptokomponent peab olema konfigureeritud selliselt, et igal rollivahetusel või teatud aja möödudes, mil seda aktiivselt ei kasutata, tuleb autentimisinfo uuesti sisestada. Lisaks on soovitatav piirata autentimiskatseid (nt määrata vigaste autentimiste piirarvuks 3).

Kontrollküsimus:

- Kas krüptomoodulite konfiguratsioon on turvaline?

M 4.87z Krüptomoodulite füüsiline turve

Algatamise eest vastutavad: IT turvaosakond
Rakendamise eest vastutavad: IT turvaosakond

Nagu meetmes M 2.165 Sobiva krüptotoote valimine kirjeldatud, võivad krüptomoodulid olla tarkvaralised, püsivaralised või riistvaralised. Püsivaral või riistvaral põhinevad tooted valitakse eriti just neil juhtudel, kui krüptomoodul peab olema manipulatsioonide eest tugevalt kaitstud. Seega peab krüptomoodul olema füüsiliste turvameetmete kasutamise või vastavate materjaliomaduste abil konstrueeritud selliselt, et volitamata füüsiline juurdepääs mooduli sisule oleks edukalt takistatud. See peab ära hoidma võimalikke tehnilisi manipulatsioone või muid mõjutusi töös. Olenevalt krüptomooduli turvalisuse astmest tuleb kasutada nt passiveerimismaterjale, sobivaid manipuleerimisevastaseid meetmeid või mehaanilisi lukke. Sellesse meetmete kategooriasse kuulub ka automaatne avariikustutus, mis kustutab või hävitab ründekatse tuvastamise korral kõik loetava teksti kujul olevad konfidentsiaalsed võtmeanded ja võtmeparameetrid.

Erinevate andurite ja seireseadmete abil saab tagada, et krüptomooduli töötingimused, nt toide, taktsagedus, temperatuur, mehaaniline koormus, elektromagnetiline mõju jne vastaksid etteantud nõuetele.

Ettenähtud funktsioonide säilitamiseks peab krüptomoodul suutma ise käivitada ja läbi viia teste. Need testid võivad puudutada järgmisi valdkondi: algoritmide testid, tarkvara ja püsivara testid, funktsioonitestid, statistilised juhutestid, vastavustestid, tingimuste testid, võtmete genereerimise ja laadimise testid. Negatiivse testitulemuse tagajärjel peab krüptomoodul kasutajat tekkinud olukorrast teavitama, edastades talle sellekohase veateate ja lülituma ümber vastavale vearežiimile. Nimetatud vearežiimist tohib seade väljuda alles pärast vea või vigade kõrvaldamist.

Tarkvaratoodete kasutamisel peab krüptomooduli füüsiline turvalisus olema tagatud vastava IT-süsteemi või selle kasutuskeskkonnaga. Selliste IT-süsteemide turvatehnilised nõuded leiate süsteemipõhistest moodulitest.

Tarkvaraline lahendus peab oskama sooritada eneseteste, et tuvastada Trooja hobuste või arvutiviiruste põhjustatud modifikatsioone.

M 4.88 Nõuded operatsioonisüsteemide turvalisusele krüptomoodulite kasutamise korral

Algatamise eest vastutavad: IT turvaosakond

Rakendamise eest vastutavad: IT turvaosakond

Krüptomoodulite kasutamise puhul on oluline nende sidumine host-süsteemi vastava operatsioonisüsteemiga ehk mooduli sõltuvus vastavast operatsioonisüsteemist.

Operatsioonisüsteemi ja krüptomooduli koosmõju peab tagama järgmise seisundi:

- krüptomooduli väljalülitamine või eiramine (nt manipuleerimise või draiverite vahetamisega) peab olema välistatud;
- kasutatavaid ega salvestatud võtmeid ei tohi olla võimalik kompromiteerida (nt RAM-alade lugemisega);
- kaitstavaid andmeid tohib olla võimalik salvestada andmekandjale krüpteerimata kujul või infotöötlussüsteemist välja saata (nt võrguühenduse korral) ainult siis, kui kasutaja on sellest teadlik ja seda protseduuri ise kontrollib;
- krüptomooduli manipulatsioonikatsed peavad olema tuvastatavad.

Operatsioonisüsteemi turvalisusele tulenevad olenevad krüptomooduli liigist (riistavaraline või tarkvaraline versioon, IT-komponentidesse integreerimise viis jne), kasutustingimustest ja kaitstavate andmete turbevajadusest erineva tugevusega nõuded. Tarkvaraliste krüptomoodulite korral on turvalise operatsioonisüsteemi kasutamine eriti oluline. Kaubanduslikult kättesaadavad operatsioonisüsteemid on tavaliselt sedavõrd keerukad ja lühikeste uuendustsüklitega, et andmete või süsteemi turvalisus on vaevu kontrollitav ja tõendatav. Erandiks võivad olla spetsiaalsele tootjale kuuluvad või erikasutuse jaoks optimeeritud operatsioonisüsteemid (nt erilised operatsioonisüsteemid krüptoseadmetes).

Seega kui krüptograafilisi tooteid kasutatakse standard-operatsioonisüsteemides nt andmete krüpteerimiseks või meilide kaitsmiseks, on oluline, et selles operatsioonisüsteemis oleks kasutusele võetud kõik standardsed turvameetmed.

Vastavate IT-süsteemide turvatehnilised nõuded leiate süsteeme käsitlevatest moodulitest, nt 3. kihi klientide või serverite alt.

Riistvaraliselt lahendatud krüptomoodulid võivad olla sellise konstruktsiooniga, et need kompenseerivad operatsioonisüsteemi turvalisuse puudujääke või siis kõrvaldavad need täielikult. Sellisel juhul vastutab ülalmainitud nõuete täitmise eest täielikult krüptomoodul. See peab näiteks suutma tuvastada, kas krüpteerimata

andmeid kirjutatakse andmekandjale või muudele seadmeliidestele moodulit eirates ja kas selleks on volitused olemas või mitte. Kasutaja peab oma keskkonna jaoks loodud turvapoliitika kohaselt otsustama, milline operatsioonisüsteemi ja krüptomooduli kombinatsioon on vajalik.

M 4.90w Krüptoprotseduuride kasutamine ISO/OSI etalonmudeli eri kihtides

Algatamise eest vastutavad: IT turvaosakond

Rakendamise eest vastutavad: IT turvaosakond

ISO normile vastav OSI etalonmudel

Krüptograafilisi meetodeid saab rakendada ISO/OSI etalonmudeli erinevates kihtides. See mudel, mida selgitatakse lühidalt selle käsiraamatu meetmes M 5.13 Võrgu ühendusaparatuuri õige kasutamine , määratleb neli transpordile ja kolm rakendustele orienteeritud kihti. Erinevate süsteemide ühe kihi instantsid suhtlevad üksteisega protokollide abil. Iga kiht pakub oma teenuseid järgmisele kõrgemale kihile. Lisaks tavalistele kommunikatsiooniteenustele võib tegu olla ka turvateenusega. Seda, milline turvateenus tuleks paigaldada millisesse kihimudeli kihti ja milliseid mehhanisme selleks kasutada, kirjeldatakse standardi ISO 7498 teises osas (turvaarhitektuur). Ka neil juhtudel, kui konkreetsed kommunikatsioonisüsteemid, etalonmudelid või protokollid ei käitu alati ISO etalonmudeli kohaselt, aitab ISO etalonmudeli tundmine kaasa toodete turvafunktsioonide hindamisele ja kergendab sellega ka „turvaliste“ terviksüsteemide süstemaatilist koostamist.

Joonis: toodete turvafunktsioonide hindamine ISO etalonmudelil põhinevatest teadmistest lähtuvalt

Järgnevalt püüame selgitada, millised eelised ja puudused on seotud krüptograafiliste meetodite kasutamisega vastavates kihtides. Krüptograafilisi meetodeid rakendatakse sideprotsessis tekkiva erineva info kaitsmiseks, seega info krüpteerimiseks, krüptograafiliste kontrollsummadega varustamiseks või allkirjastamiseks. Esiteks saab kaitsta kasutaja edastatavaid andmeid, teiseks aga eranditult infovahetuse käigus tekkivat infot (nt liiklusvoo infot). OSI erinevates kihtides võivad erinevate turvateenuste jaoks eksisteerida samaaegsed turvaseosed. Turvateenuse rakendamise kihist kõrgemas kihis asub info (mis kirjeldab seda teenust) kaitsmata kujul. Krüptograafilised mehhanismid (krüpteerimine, digiallkiri, krüptograafilised kontrollsummad) toetavad olulisi turvateenuseid (tagavad autentimist, konfidentsiaalsust, terviklust, kommunikatsiooni ja andmete päritolu tõendamist). Selleks esmalt väike ülevaade aspektidest, mis räägivad OSI erinevates kihtides krüptograafiliste meetodite kasutamise poolt või vastu:

Krüptograafiliste protseduuride kasutamine

ülemistel kihtidel:

alumistel kihtidel:

+:

mõistlik, kui rakenduse andmeid tuleb kaitsta rakenduse lähedal või kui „ebaturvalist kanalit“ tuleb hoida võimalikult lühikesena

+:

mõistlik, kui on tarvis ühendada kahte võrku, mis on turvalised, kasutades ebaturvalist ühendust, nt kahe institutsiooni ühendamiseks avalike võrkude kaudu

+:

igal juhul alati siis, kui andmeid ei kaitsta madalamates kihtides

+:
võrgu kaitsmiseks volitamata juurdepääsude eest
+:
mõistlik, kui on palju vahetuvaid kommunikatsioonipartnereid erinevates asukohtades
+:
alati siis, kui tuleb kaitsta liiklusvoo infot, nt aadressiinfot
+:
kasutajad võivad seda rakendada vastavalt oma vajadustele
+:
kogu kõrgemalasuv päise- ja kasutajainfo on krüpteeritud
+:
kaitse kasutajale lähemal ja äratuntavam
+:
kasutaja jaoks läbipaistev lahendus, väiksem väärkasutuse risk
-:
õõnestavad tulemüüride poolt pakutavat kaitset
+:
lihtsam võtmehaldus
-:
sagedane väärkasutus
-:
kaitseb ainult kuni kihini, milles asuvad turvaprotokollid
-:
põhineb sageli tarkvaral, krüptograafilised võtmed ja algoritmid on lihtsamini manipuleeritavad
-:
sageli riistvara, seega kallim ja vähem paindlik
-:
suurem sõltuvus operatsioonisüsteemist või riistvarast, mille peal see töötab
-:
ei paku sageli end-to-end turvalisust

Tabel: krüptograafiliste protseduuride kasutamine OSI kihtides

Lihtne võtmehaldus tekib tavaliselt siis, kui saab kasutada grupeerimisvõtmeid, nt nii, et ehitatakse turvalised alamvõrgud (VPN), mille puhul saab juurdepääsud varustada krüptoseadmetega. Alumiste kihtide krüptograafilised tooted on soetamishinna poolest ülemiste kihtide omadest tavaliselt oluliselt kallimad, kuid seevastu läheb neid tarvis ka vähemal hulgal. Lisaks on administreerimise ja juurutamisega seotud vaev tavaliselt väiksem, kuna turvateenuseid ei pea juurutama erinevate rakenduste alla. Ka „eksootilised" rakendused, st rakendused, millel puuduvad oma turvafunktsioonid, saavad seeläbi turvaliselt andmeid vahetada. Sageli saab kasutada krüptograafiliste teenuste kombinatsiooni erinevates kihtides. See sõltub vastavatest turvanõuetest ja kasutustingimustest, nt kuludest, jõudlusest ja vastavate komponentide saadavusest. Otsustavad faktorid on ka eeldatavad ohud, mille vastu turvateenused peavad kaitset pakkuma, samuti aluseks olev süsteemiarhitektuur.

Turvalisuse lõppseadmed ja turvalisuse ühendamiselemendid

Turvasüsteemid võivad olla lahendatud lõppseadmena või selle osana või ka ühenduselemendina või selle osana. Ühenduselemendid on nt aktiivsed võrgukomponendid, nagu marsruuterid või lüüsid. Erinevalt lõppseadmetest on turvalisust tagavatel ühenduselementidel tavaliselt kaks võrguliidest, mis on ühendatud selle süsteemi jaoks tüüpilises kihis vastava krüptomooduliga (riist- või tarkvaraga). Üks liides on ühendatud „turvalise" võrguga (nt majasisese võrguga), teine liides „ebaturvaliseks" hinnatud võrguga (nt avaliku võrguga). Turvalisust tagavate lõppseadmete eeliseks on asjaolu, et turvamehhanisme saab hästi kohandada rakenduse nõuetele. Tüüpilised turvalisust tagavad lõppseadmed on krüptotelefonid, krüptofaksiaparaadid või PCde jaoks mõeldud riist- või tarkvaralised turvalahendused. Turvalisust tagavad lõppseadmed pakuvad tavaliselt lahendusi üksikutele töökohtadele. Kohati toetavad need lahendused vaid ühte teenust. Piirid on siiski voolavad (helistamine läbi interneti-PC, andmesisendiga krüptotelefon). Lõppseadmetes ei ole erinevalt ühenduselementidest turvakihi valik piiratud, kuna lõppseadmed on põhimõtteliselt täielikud, st varustatud seitsme kihiga.

Turvalisust tagavad ühenduselemendid on sageli konstrueeritud sellise võimsusega, et need suudavad kaitsta suuremaid tööüksusi kuni tervete institutsioonideni välja. Seejuures püüavad selliste süsteemide tootjad toetada võimalikult palju teenuseid või kõrgema kihi protokolle, et võimaldada universaalset kasutamist.

Ka lõppseadmete operatsioonisüsteemide sõltumatus annab oma panuse ühenduselementide universaalsesse kasutatavusse. Muidugi saab ka üksikuid lõppseadmeid kaitsta turvalisust tagavate ühenduselementidega. Siiski kaasneb seadmete suurema jõudlusega sageli ka kulude suurenemine. Ühenduselementide puhul on määratluse kohaselt tegu ebatäielike OSI-süsteemidega. Seega piirdub ka turvateenuste juurutamisvõimalus nende kihtidega, mis on ühenduselemendil olemas. Kasutatakse ka kombineeritud variante. See eeldab, et turvalisust tagavad lõppseadmed ja turvalisust tagavad ühenduselemendid on häälestatud koostööks, eriti just seoses kasutatavate turvamehhanismide ja turvaparameetritega (nt krüptograafilised võtmed).

Kasutaja-, juhtimis- ja haldusinfo

Kasutaja huvitub peamiselt kasutajainfo edastamisest kaugemalasuvatele kasutajatele. Olenevalt konkreetsest etalonmudelist (nt ISDN), edastatakse süsteemide (lõppseadmete, ühenduselementide) vahel lisaks ka veel juhtimis-, signaliseerimis- ja haldusinfot eesmärgiga luua/katkestada ühendusi, saada endale teenusekvaliteedi parameetrid, konfigureerida võrku, võrguoperaatori võrgu seireks jne. Vastaval võrgul on seejuures ülesanne edastada kasutajainfot muutmata ja analüüsimata kujul, st kasutajainfot peavad tõlgendama ainult lõppseadmed. Sellega saab infot koguda ülejäänud võrgu infrastruktuurist sõltumatult, vajaduse korral isegi tootjapoolseid turvafunktsioone (suletud kasutajagruppe) kasutades. Transpordikihtide juhtimis-, signaali- ja haldusinfo peab olema võrguoperaatori võrguelementidele analüüsitav, muudetav ja genereeritav. Sellega ei kuulu see info üldjuhul võrguoperaatorist sõltumatu kaitse (nt krüpteerimise) alla. Selle info kaitsmine vajab lisaks vastavatele standarditele usaldusväärset koostööd võrguoperaatoriga. Ohud võivad tuleneda sellest, et toodete turvafunktsioone hinnatakse valesti. Krüptoseadmete valimisel tuleb täpselt kontrollida, milliseid infoosakesi see kaitseb ja filtreerib. Samuti tuleb vastupidiselt kontrollida, milline info jääb

hoolimata krüptoseadmete kasutamisest kaitsmata ja kui suurel määral on see konkreetses kasutusvaldkonnas vastuvõetav.

Näide:
ISDNi puhul toimub kasutajainfo edastamine tavaliselt läbi B-kanalite. Pakettandmete edastamiseks saab aga kasutada ka D-kanalit, mida kasutatakse peamiselt signaliseerimiseks. Kui eesmärk on kõikide kasutajaandmete kaitsmine, ei ole paketiandmete edastamisel D-kanali kaudu B-kanali kaitsmine tavaliselt piisav.

Turvalisus ühendust edastavates võrkudes
Ühendust edastavates võrkudes seatakse ühenduse loomise käigus sisse teatud ribalaiusega kanalid, mida kommunikatsioonipartner saab hakata eksklusiivselt kasutama. Pärast ühenduse sisseseadmist toimub kasutajaandmete edastamine, millele järgneb ühenduse loomine. Võrguoperaator saab luua püsiühendused, mille puhul jäävad ära osaleja jaoks tavaliselt vajalikud ühenduse loomised ja katkestamised. Ühendust edastava võrgu näide on ISDN. Ühenduse loomisega seatakse kommunikatsioonipartnerite vahel sisse kasutusandmete kanalid OSI 1. kihis, mida nimetatakse ISDNi puhul B-kanaliteks. Edastatavate andmete konfidentsiaalsuse tagamiseks saab selle kanali krüpteerida. Kui lisaks sellele tuleb kaitsta ka signaliseerimiskanalit, seega N-ISDNi puhul D-kanalit (1.–3. kiht), tuleb arvestada sellega, et lõppseadme vastaspooleks võivad olla nii kommunikatsioonipartneri lõppseade kui ka võrguoperaatori keskused. D-kanalit tavaliselt ei krüpteerita, kuna selleks tuleks kehtestada erinõuded võrguoperaatorile. Sel juhul tuleb tagada D-kanali seire ja filtreerimine.

Ühenduse krüpteerija
Erijuhul tuleb tagada sünkroonsete täis-dupleks-püsiühenduste krüpteerimine, kuna neil juhtudel saab tagada ka võrguliikluse konfidentsiaalsuse. Kui andmeid ei edastata, krüpteeritakse täiteandmeid nii, et ühenduses on pidevalt näha ühtlane „müra". Ühenduse krüpteerijad kujutavad endast alternatiivi kaitstud ühenduste paigaldamisele.

Turvalisus pakette saatvates võrkudes
Pakette saatvate võrkude puhul tuleb vahet teha ühendusele orienteeritud ja ühendustest vabade pakettide saatmise vahel. Ühendusele orienteeritud pakettide saatmise puhul luuakse ühenduse loomise faasis virtuaalühendus, mis määrab seejärel kindlaks andmetee läbi pakettvõrgu. Andmepakette marsruuditakse pärast ühenduse loomist läbi võrgu lähtuvalt määratud virtuaalsest kanalinumbrist samal andmeteel. Saatja ja/või vastuvõtja aadressid pole selleks vajalikud.

Üks näide sellest on X.25-võrk. Ühenduseta pakettide saatmise puhul ei eksisteeri ühenduse loomise ja katkestamise faase. Andmepakette saadetakse ükshaaval – muu hulgas on need varustatud lähte- ja sihtaadressiga. See on tüüpiline kohtvõrgu andmesides. Kihi valimine, milles turvamehhanismid mõjuvad, määrab kindlaks, milliseid infohulki kaitstakse. Mida madalam on valitud turvakiht, seda mahukam on info kaitsmine. Kui kasutajaandmed läbivad kihtide 7 kuni 1 (saatja) instantse, lisatakse andmetele täiendavat juhtimisinfot. Kui küsimus pole seega mitte ainult kasutajaandmete kaitsmises, vaid ka andmevoo

kaitsmises, saab kasutada OSI madalamat kihti. Teisest küljest kehtib jällegi tõsiasi: mida madalam on OSI valitud kiht, seda vähem ühenduselemente (järgureid, sildasid, kommutaatoreid, marsruutereid, lüüse) saab läbipaistvalt ületada.

Ühenduselement	Ühenduselemendi kõrgeim kiht
Järgur	1
Sild, 2. kihi kommutaator	2
Marsruuter, 3. kihi kommutaator, X.25 Packet Handler	3
Lüüs	7

Tabel: vastandamine: ühenduselement – ISO kiht

Kui turvateenused peavad mõjuma ühenduselementide kaudu, tuleb need realiseerida kihis, mis asub kõrgemal ühenduselemendi kõrgeimast (alam-) kihist. See tagab, et edastamisseadmed suudavad kaitstud infot edasi suunata töötlemata/tõlgendamata kujul.

Vale võrgukonfiguratsiooni näited ja tagajärjed:

- Kõik marsruuteri ja avalike ühendusvõrkude kaudu ühendatud kahe kohtvõrgu lõppseadmed peavad konfidentsiaalsuse tagamiseks – eriti avalike sidevõrkude piires – olema varustatud 2. kihi krüpteerimiskomponentidega. Marsruuter peab kohtvõrgu andmepakettide edasijuhtimiseks avalike võrkude kaudu analüüsima 3. kihi aadresse. Kuna kõik 3. kihi andmed on varjatud 2. kihi krüpteeringuga, ei saa 3. kihi aadresse edukalt analüüsida. See takistab andmeedastust. Abinõuna tuleb kasutada 3. (ülemise alamkihi) või kõrgema kihi krüpteerimiskomponente.
- Suurem osa asutuse kirjavahetusest peab edaspidi toimuma elektrooniliselt X.400 (7. kihi) kaudu. Andmete tervikluse kaitsmiseks planeerib asutus 4. kihi krüptokomponentide kasutamist lõppseadmetes (kõnealusel juhul PC-des). Kaitsmise eesmärgil varustatakse andmepaketid saatja juures 4. kihi krüptograafiliste kontrollsummadega, mida kontrollib vastuvõtja vastav 4. kihi krüptokomponent. Kohale tohib toimetada ainult õigete kontrollsummadega andmepakette. Kui aga osadel MTAdel (message transfer agent ehk siis 7. kihi elektrooniliste teadete edastaja) puuduvad sobivad krüptokomponendid, ei saa krüptokomponentideta MTAd luua kehtivaid kontrollsummasid, nii et järgnevad krüptokomponentidega MTAd või lõppseadmed peavad andmetest nõuetekohaselt loobuma. Aga isegi siis, kui kõik kasutatava MTAd on sarnaselt lõppseadmetega varustatud ühilduvate krüptokomponentidega, ei ole andmete terviklus ikkagi veel tagatud. Tagatud võib olla küll andmete lõikhaaval kaitsmine, kuid MTAde piires on andmeid siiski jätkuvalt võimalik märkamatult võltsida. Lisaks võivad (olenevalt protokollist) üksikud 4. kihi andmepaketid kaduma minna, mis põhjustab lünkasid tervikteates, mille puutumatust tegelikult tagada soovitakse. Üks võimalikke abinõusid on andmete tervikluse kaitsmine 7. kihis. Nagu näidetest selgub, tuleb täpselt kontrollida, milline on võrgu topoloogia ja milliseid võrgualasid tuleb kaitsta, et leida kohandatud lahendus koos soovitud (turva-) omadustega.

Lõikhaaval turvalisus ja läbiv turve

Sidesüsteemide kasutajad ootavad sageli, et turvateenused oleksid läbivad ehk alates info sisestamisest (andmed, kõne, pildid, tekst) lõppseadmes A kuni info väljastamiseni kaugemalasuvas lõppseadmes B. Kui läbiv turvateenus pole tagatud, eksisteerib vastav info – lisaks olemasolevatele lõppseadmetele – kaitsmata kujul veel ka teistes süsteemides. Näiteks, kui kahe osaleja vahelise kommunikatsioonisuhte konfidentsiaalsus ei ole kaitstud otspunktkrüpteeringuga, eksisteerivad need andmed vähemalt ühes võrguelemendis ka krüpteerimata kujul. Sellised võrguelemendid tuleb tuvastada ja muuta sobivate meetmetega turvaliseks. Töötajad, kellel on juurdepääs just sellistele kaitsmata võrguelementidele (nt administraatorid), peavad olema piisavalt usaldusväärsed. Turvateenuseid ei pakuta sel juhul läbivalt, vaid lõikhaaval. Tuleb jälgida, et kõik olulised lõigud saaksid sobivalt kaitstud.

Mitmekordne kaitsmine OSI erinevates kihtides

Edastatava info mitmekordne kaitsmine OSI erinevates kihtides ei ole halb, kui järgitakse teatud reegleid, mis on tagatud standarditele vastavate toodete puhul. Eriti just krüpteerimisel tuleb kasutada juba koolist tuntud sulureegleid. Nii vastab krüpteerimine sulu avamisele, dekrüpteerimine aga sulu sulgemisele. Sulgude sees saab omakorda kasutada täiendavaid turvamehhanisme. Mitmekordse kaitse puuduseks võib olla asjaolu, et täiendavate operatsioonide tõttu väheneb andmete läbilaskevõime, või et edastatavate andmete kogus väheneb seeläbi, et liiasuse suurendamiseks tuleb edastada täiendavaid andmeid (nt krüptograafilisi kontrollsummasid). Mitmekordne kaitse tekib ka andmete läbi, mida kaitstakse enne edastamist krüptosüsteemide abil, nt digitaalse allkirjaga varustatud dokumendid. Seeläbi suureneb andmete edastamise ohutus olenevalt kasutatavatest turvateenustest. Sageli saab terviksüsteemi turvalisust saavutada alles mitut turvaprotokolli või turvatoodet omavahel kombineerides. Kui kasutada saab nt rakenduslähedasi turvalahendusi, mille rakendamise usaldusväärsust pole siiski kontrollitud (puudub sõltumatute osapoolte, nt ITSECi, CC hinnang) ja on olemas usaldusväärsed transpordile orienteeritud turvatooted kaitsmaks ebaturvalisi võrgulõike kaugemalasuvate institutsioonide vahel, võib meetmete kombineerimise abil saavutada piisavalt tervikliku turvalahenduse. Puuduseks on tavaliselt suurem administreerimise töövaev ja/või suurem soetamiskulu.

M 4.91 Süsteemihaldussüsteemi turvaline installeerimine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator

Süsteemihaldussüsteemi installeerimine nõuab ulatuslikku ja hoolikat planeerimist.

Pärast süsteemi analüüsimist (vt M 2.168 IT-süsteemi analüüs enne süsteemihaldussüsteemi evitust , haldusstrateegia kindlaksmääramist (vt M 2.169 Süsteemihalduse strateegia väljatöötamine) ja sobiva haldussüsteemi valimist (vt M 2.171 Sobiva süsteemihaldustoote valimine) tuleb hakata hoolikalt planeerima toote installeerimist ning see vastavalt plaanile ka teoks teha.

Sõltuvalt haldustoote baasiks olevast arhitektuurist, tuleb kohtvõrgu jaoks luua selge haldussüsteemi konfiguratsioon, mis arvestaks eriti just sõnastatud haldusstrateegiaga.

Enamasti tuleb haldussüsteemide installeerimiseks paigaldada vastavatele arvutitele haldustarkvara, mis hoolitseb halduskonsooli või -serverite ja lokaalsete arvutite vahelise kommunikatsiooni eest. Sageli tuleb kesksetesse arvutitesse (serveritesse või lüüsidesse) installeerida ka andmebaasisüsteemid, millesse haldustarkvara salvestab pidevalt haldusinfot. Sõltuvalt tootest võib olla võimalik seda ühendada ka juba olemasoleva andmebaasisüsteemiga. Üldiselt esitab täiendavalt installeeritav tarkvara oma nõuded arvuti kohapealsetele ressurssidele. Seega tuleb planeerimisel arvestada kohalike olemasolevate süsteemiressurssidega. Vajadusel tuleb teatud süsteeme täiendada. Nende kuludega tuleb haldustoote valimisel arvestada.

Lisaks nimetatud kriteeriumitele, mis peavad üldjuhul tagama süsteemi reguleeritud tehnilise toimimise, tuleb turbe seisukohast kaasata turbeastme määramisse vastavalt IT etalonturbele (vt BSI standardit 100-2 IT etalonturbe meetod) ka haldussüsteemi juurde kuuluv tarkvara ja vastavad andmed ning kehtestada nende turbeastmeks kõrge. Haldussüsteemi kompromiteerimise tagajärjeks ei pruugi olla mitte ainult kogu võrgu avarii; süsteemis märkamatuks jäävad muudatused võivad põhjustada palju suuremaid kahjustusi, mis võivad väga lühikese ajaga ohtu seada isegi terve asutuse eksistentsi.

Installeerimisel tuleb arvestada eriti just järgnevate punktidega:

- Kõiki arvuteid, milles hoitakse haldusinfot, tuleb kaitsta eriti hoolikat.
- Tuleb rakendada meetmeid 3. komplekti moodulitest, lähtuvalt kasutatavast süsteemist.
- Eriti tuleb operatsioonisüsteemi mehhanismid konfigureerida selliselt, et kohalikult salvestatud haldusinfole ei saaks volitamata ligi pääseda.

- Haldustarkvarale tohivad ligi pääseda ainult volitustega administraatorid ja revidendid.
- Juurdepääs arvutitele peab olema piiratud.
- Kommunikatsioon halduskomponentide vahel peab toimuma krüpteeritult – kui toode seda toetab – et takistada haldusinfo pealtkuulamist ja kogumist.

Kui tootel puudub krüpteerimise tugi, tuleb kommunikatsiooni turvamiseks võtta tarvitusele erimeetmed (vt M 5.68z Krüpteerimisprotseduuride kasutamine võrgusuhtluses).

Kontrollküsimus:

- Kas süsteemihaldussüsteemid on installeeritud turvaliselt?

M 4.92 Süsteemihaldussüsteemi turvalise töö tagamine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: administraator

Süsteemihaldussüsteem võib teadupärast koosneda erinevatest haldustööriistadest (vt M 2.171 Sobiva süsteemihaldustoote valimine) ning selle turvalise kasutamise võimaldamiseks tuleb tagada ja kontrollida, kas kõikide asjassepuutuvate komponentide konfiguratsioon on turvaline (vt lisaks M 4.91 Süsteemihaldussüsteemi turvaline installeerimine). Selleks tuleb sobival moel kaitsta süsteemihaldussüsteemi poolt hallatavate ja seega süsteemi osasid tarkvara ja/või andmete kujul sisaldavate komponentide operatsioonisüsteeme. Kaitsmise alla kuulub ka haldussüsteemi tsentraalseid ülesandeid täitvate arvutite (haldusserveri, haldusandmebaasidega arvutite) turvaline paigutus. Lisaks tuleb hoolitseda turvalise andmeedastuse eest (vt M 5.68 Krüpteerimisprotseduuride kasutamine võrgusuhtluses). Järgnevate punktide täitmist tuleb jälgida eriti just haldussüsteemi käitamise ajal:

- Süsteemidokumentatsiooni täiendamise raames tuleb dokumenteerida haldussüsteemi kaasamisega lisandunud riist- ja tarkvarakomponendid.
- Ka haldussüsteemi enda muudatused tuleb dokumenteerida ja/või logida.
- Vastavad täiendused tuleb sisse viia ka avariikäsiraamatusse. Eriti just tuleb uuesti läbi töötada käivitus- ja taasteplaanid, kuna paljud hallatavate operatsioonisüsteemide standardfunktsioonid saavad pärast haldussüsteemi kasutuselevõtmist toimida ainult haldussüsteemi funktsioonide kaasabil. Teisest küljest peab avariikäsiraamat sisaldama juhiseid ka selle kohta, kuidas teha süsteemi haldussüsteemi puudumisel (nt tsentraalse komponendi täieliku avarii korral) lühikese aja jooksul piisaval määral töökõlblikuks (avariirežiimi reeglid), (vt lisaks moodulit B 1.3 Hädaolukorraks valmisoleku kontseptsioon).
- Juurdepääs haldussüsteemi komponentidele või andmetele toimub tavapärasest eranditult haldussüsteemi enda või muude volitatud süsteemimehhanismide (nt andmevarundussüsteemi) kaudu. Seega tuleb tavakasutajatele seda juurdepääsu piirata. Sama kehtib tavajuhul ka üksiku arvuti kohaliku administraatorirolli kohta. Kui erandjuhul tuleb tõepoolest arvuti abil ligi pääseda haldussüsteemi kohalikele komponentidele (nt *Crashrecovery* või komponentide uuesti installeerimise korral, juhul, kui haldussüsteem seda haldamise raames ei toeta), tuleks vastavad volitused anda selgelt eraldi ja ainult selle ülesande täitmiseks.
- Turvapoliitikast lähtuvalt tuleb määrata volitused. Ka halduse puhul tuleb administraatori ja revidendi töörollid teineteisest eraldada – sõltuvalt tootest tuleb veel määrata ka erinevate õigustega administraatorid (nt töögruppide administraator, valdkondade administraator). Soovitatav on määratleda kindlad rollid ja anda seejärel kasutajatele vastavad volitused, lähtudes neile usaldatud rollidest. Seeläbi antakse töötajatele juurdepääsuks vajalikud volitused ainult haldussüsteemi nendele komponentidele või andmetele, mi-

da on antud hetkel tarvis tööülesannete täitmiseks. Sõltuvalt haldussüsteemist seatakse kasutajad sisse kas haldussüsteemis või arvutite kasutajahalduses. Kuna olemasolevates süsteemides pole ette nähtud otsest erinevate rollide (nt administraatori ja revidendi) määratlemist, tuleb rollisüsteem koos vastavate volitustega luua erinevate kasutajakontode abil (nt Administraator, Revident, ArvutiAdmin, Andmekaitsespetsialist). Sõltuvalt süsteemist ei ole selline meetod täiuslik ja võib olla küllaltki töömahukas, nt seepärast, et igale süsteemikomponendile (failile, programmile) tuleb eraldi määrata üksikute rollide volitused ja seejärel tuleb neid ka eraldi veel hooldada.

- Juurdepääs haldustarkvarale peab olema kaitstud turvaliste paroolidega. Paroole tuleb vastavalt turvapoliitikale regulaarselt muuta.
- Haldusstrateegia kohaselt tuleb haldustarkvara ebavajalikud funktsioonid võimalusel sulgeda.
- Logifaile tuleb regulaarselt kontrollida, et neis ei esineks anomaaliad (nt funktsioonide teostamist, mida ei ole tegelikult üldse ette nähtud). Selleks tasub kasutada logianalüüsijaid, mis on kas integreeritud haldustootesse või siis saadaval lisatarkvarana ja suudavad (enamasti) vajadusel genereerida alarmteateid (meilid, piiparid).
- Volitamata muudatuste võimalikult kiireks avastamiseks tuleks regulaarselt kontrollida haldussüsteemi terviklust. Eriti kehtib see haldussüsteemi kõikide konfiguratsiooniandmete kohta.
- Kui süsteemihaldussüsteemi kaudu toimub ka tarkvara jaotamine, tuleb regulaarselt muudatuste osas kontrollida ka jaotatavaid programmiandmeid, et takistada modifitseeritud tarkvara jaotamist üle kogu võrgu.
- Testimisega tuleb välja selgitada, kuidas käitub haldussüsteem süsteemi avarii korral. Sõltuvalt haldusstrateegiast ja turvapoliitikast tuleb tagada haldussüsteemi või süsteemi kohalike osakomponentide automaatne taaskäivitumine. Sellega välditakse olukorda, kus haldussüsteemiga ühendatud arvutid on halduse jaoks pikemat aega ligipääsmatud (vt ka M 6.57 Avariiplaani koostamine haldussüsteemi avarii puhuks).
- Süsteemi avarii korral ei tohi halduseandmebaasid hävineda ega muutuda üksteisele vastukäivaks. Sellega välditakse ründeid, mis näevad ette vasturääkivuste tahtlikku esilekutsumist. Selleks peab haldussüsteem suutma ära kasutada kas andmebaasisüsteemi, mis toetab vastavaid *Recovery* - mehhanisme, või siis peab haldussüsteem olema ise varustatud vastavate mehhanismidega (vt M 2.170 Nõuded süsteemihaldussüsteemile). Kui valitud süsteem vastavaid mehhanisme (nt mitme haldustööriista kasutamist) ei toeta, peavad haldusinfot salvestavad arvutid olema maksimaalselt kaitstud (ka füüsiliselt) (vt 3. komplekti mooduleid).
- Haldussüsteem peab sisaldama sobivat varundamismehhanismi haldusandmete varundamiseks või siis tegema koostööd varundamissüsteemiga. Varundusest pärit vanemate andmekogude sisselugemisel tuleb reeglina arvestada, et neid on tarvis täiendavalt käsitsi töödelda, et viia need kooskõlla süsteemi hetkekonfiguratsiooniga.
- Ka varundusmeetodi abil varundatud haldusandmete kogumeid tuleb hoida selliselt, et volitamata kolmas osapool ei pääseks nendele ligi. Tavaliselt pole andmed varunduse andmekandjale salvestatud turvaliselt, seega saab neid vaadata igaüks, kellel on olemas varundusprogramm ja sobiv kettaseade.
- Jaotamist haldusdomeenidesse ja nende vastutusaladesse tuleb regulaar-

selt kontrollida, kas need on jätkuvalt kehtivad. Eriti tuleks sellega arvestada siseste ümberstruktureerimiste puhul.

M 4.93z Regulaarne tervikluse kontroll

Algatamise eest vastutavad: IT-juht, IT-turbespetsialist
Rakendamise eest vastutavad: administraator

Failisüsteemi, failiatribuutide ja protsessiinfo ning muude süsteemikonfiguratsiooni oluliste elementide (nt Windowsi registri) regulaarne kontrollimine võimalike ootamatute muudatuste suhtes aitab tuvastada ebakõlasid. Selliste ebakõlade tuvastamist saab kasutada süsteemi töökindluse tagamiseks. Muuhulgas võimaldab see varakult tuvastada ka ründeid. Kui tegu on tõesti ründega, on oluline tuvastada ründaja valitud tegutsemisviis. Esmalt võimaldab see tuvastada võimalikke andmemanipulatsioone, teisalt aitab aga leida ka varjatud tagauksi, mille võis paigaldada ründaja eesmärgiga kunagi hiljem arvutile ligi pääseda. Manipulatsioonide tuvastamiseks saab kasutada programme, mis arvutavad suure hulga süsteemi failide jaoks või muude ressursside kohta välja krüptograafilised kontrollsummad. Seejuures tuleb eristada tervikluse kontrollimise programme, mis töötavad ainult faili tasandil, ja selliseid, mis suudavad kontrollida ka protsesse ja spetsiaalseid konfiguratsiooniandmeid, nt Windowsi registrit või kernel 'i andmestruktuure. On soovitatav, et neid tööriistu peaks saama ka tsentraalselt hallata ja seirata. Lisaks peavad programmi poolt kasutatavad krüptograafilised mehhanismid vastama kaasaegsetele tehnilistele nõuetele.

Mõned programmid suudavad vaid kindlaks teha, kas failisüsteemi on muudetud või mitte. Selleks kontrollitakse, kas pääsuõiguseid, viimase sisseviidud muudatuse kuupäeva või vastava faili sisu on muudetud. Modifikatsioonide tuvastamiseks võrreldakse eelnevalt loodud krüptograafilisi kontrollsummasid värskelt väljaarvutatud kontrollsummadega. Eriseadistusega saab sageli tuvastada ka ainult lugemisega piirdunud juurdepääsu. Takistamaks tervikluse kontrollimise programmi enda või süsteemi kontrollsummasid sisaldava faili võltsimist ründaja poolt, peavad need asuma kirjutuskaitsega andmekandjal. Failisüsteemi lubatud muudatuste puhul peab siiski muutuma ka kontrollsumma fail, seega tuleks selleks otstarbeks kasutada CD-, DVD- või muid vahetatavaid plaate. Alternatiiviks on teha kontrollsumma faili kättesaadavaks läbi võrgu, rakendades sellele kirjutuskaitset. Kui tervikluse kontrollprogrammi hallatakse võrgu kaudu, tulekski eelistada just seda meetodit.

Tervikluse kontrolli tuleks teha regulaarselt, nt igal öösel. Sobiva kontrollintervalli valik sõltub olulisel määral vastava IT-süsteemi kasutusotstarbest ja kasutuskeskkonnast. Tervikluse kontrolli läbiviimisel tuleb arvestada ka kontrollsummade kontrollile kuluva mäluruumi ja arvutusajaga. Tervikluse kontrollprogrammi kasutamine ei tohi takistada igapäevaste tööprotsesside toimimist. Iga suurema IT-süsteemi käitamise raames toimub süsteemifailides pidevalt suuremaid ja väiksemaid muudatusi. Seega on soovitatav seadistada tervikluse kontrollprogrammi selliselt, et muudatusi tuvastatakse ainult olulistes failides. Vastasel korral esineb oht tekitada suurel hulgal muudatusi kajastavaid teateid, mille põhjuseks on tegelikult tavaline tööprotsess ning mis pole seotud rünnakutega (false positives). Selle tulemusel võib juhtuda, et logifaile ei jõuta enam piisavalt kiiresti analüüsida. Süsteem peaks

administraatorile tulemustest teada andma ka siis, kui muudatusi ei tuvastatud, nt automaatselt meili teel või mõnel muul sobival meetodil. Juba eelnevalt tuleb kindlaks määrata, millised meetmed tuleb tarvitusele võtta siis, kui tuvastatakse reaalne tervikluse kadu. Näiteks on oluline teada, kas tarvituselevõetavad töösammud tuleb läbi teha käsitsi või need toimuvad automaatselt.

Täiendavad kontrollküsimused:

- Kas terviklust kontrollitakse regulaarselt?
- Kas kontrollsumma fail ja kontrollprogramm ise on piisaval määral manipulatsioonide eest kaitstud?
- Kas on tagatud, et oluline info tervikluse kao kohta ei mattu ebaoluliste, muudatusi kajastavate teadete (false positives) alla?
- Kas on määratletud, milliseid meetmeid tuleb rakendada tervikluse kao korral? Kas on kehtestatud kohustuslikud operatsioonid, mis toimivad kas automaatselt, või mis tuleb läbi teha käsitsi?
- Kas tervikluse kontrollprogramm kasutab kaasaegsetele tehnilistele nõuetele vastavaid krüptograafilisi mehhanisme?

M 4.94 Veebiserveri failide turve

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: administraator

Veebiserveril olevad failid ja kataloogid peavad olema kaitstud volitamata muutmise eest, kuid lisaks ka veel, sõltuvalt turvanõuetest, volitamata lugemise eest. See kehtib eriti selliste programmide (skriptide või serveritäienduste) puhul, mida kasutatakse veebiserveri dünaamilise sisu genereerimiseks.

Üldised aspektid

Üldiselt tuleb eristada kahte erinevat aspekti, nimelt kaitse kohalike kasutajate volitamata juurdepääsu eest ja kaitse väljast WWWkaudu tulevate juurdepääsude eest.

Kaitse volitamata muudatuste eest

Paljudel veebiserveritel muutuvad pidevalt ainult logifailid, ülejäänud failid on staatilised. Eriti kehtib see süsteemiprogrammide ja WWW-lehekülgede kohta.

WWW-lehekülgi uuendatakse küll regulaarselt, kuid neid ei tohiks töödelda veebiserveril endal. Lokaalsete WWW-failide kirjutamis- ja lugemisõigused peaks võimaldama juurdepääsu ainult volitatud kasutajatele. Seega tuleks juba veebilehe planeerimisel luua vastav kasutaja- ja rollikontseptsioon (vt ka M 2.173 Veebiserveri turbestrateegia väljatöötamine). Vältimaks failide märkamatut muutmist veebiserveril, saab kõikide staatiliste failide ja kataloogide jaoks luua kontrollsummad, nt mõne programmiga nagu tripwire (vt M 4.93z Regulaarne tervikluse kontroll). Neid tuleb regulaarselt kontrollida. WWW-failide volitamata muutmise täielikuks välistamiseks võib staatilised andmed salvestada mõnele kirjutuskaitsega andmekandjale (nt CD-ROMile või kirjutuskaitsega kõvakettale).

Enda serveripoolsete programmide turvaline programmeerimine

Kui veebileht ei koosne ainult staatilistest HTML-failidest, vaid sisaldab ka dünaamiliselt genereeritavat sisu, tuleb selleks kasutatavaid programme (nt CGI-skripte, Java Server Pages) programmeerida eriti hoolikalt, et läbi vastava sisu ei saaks serverile volitamata ligi pääseda või serverit ennast kompromiteerida.

CGI-skriptide, programmide ja konfiguratsioonifailide kaitse Serveril tuleb selliseid programme kaitsta volitamata juurdepääsu eest. Kirjutusõigust tohivad omada ainult need kasutajad või kasutajategrupid, kes vastavat juurdepääsu nendele programmidele või skriptidele ka ilmtingimata vajavad (nt arendajad või administraatorid). Tavaliselt ei kasutajal, kelle tunnuse all veebiserveri protseduur toimub, olla volitusi programme kirjutada. Eriti just skriptid peaksid olema tavakasutajate jaoks loetamatud, kuna need võivad sisaldada konfidentsiaalset infot, nt andmebaasidele juurdepääsemiseks vajalikke autentimisandmeid.

Sama kehtib võimalike olemasolevate konfiguratsioonifailide kohta.

Kaitse interneti kaudu tuleva volitamata juurdepääsu eest

WWW kaudu toimuvat juurdepääsu veebiserveri failidele või kataloogidele saab juhtida mitmel erineval viisil.

Milliseid juurdepääsu juhtimise viise toetatakse ja kuidas neid rakendada, sõltub kasutatavast serveritootest. Järgnevalt on toodud levinumad võimalused, mida toetab suurem osa veebiserveritest ja klientidest.

Klientide autentimine IP-aadresside kaudu

WWW-failide juurdepääsupiirangu kehtestamisel saab paljudes serverites aluseks võtta vabalt valitavad IP-aadressid, alamvõrgud ning domeenid. Autentimine numbriliste IP-aadresside kaudu ei paku samaväärset kaitset krüptograafiliste meetoditega, kuna IP-Spoofing'ul põhineva ründega saab sellest mööda pääseda.

IP-Spoofing 'u puhul võltsib ründaja IP-pakette, et teeselda pärinemist usaldusväärsest IT-süsteemist (vt G 5.48 IP-aadressi võltsimine). Tulemüüri abil saab siiski olukorda, kus välised end edukalt sisesteks maskeerivad, vältida.

Kui juurdepääsu ei piirata numbriliste IP-aadresside või alamvõrkude peale, vai kindlate arvutinimede või domeeninimede peale, tuleb lisaks arvestada DNS-Spoofing'u ohuga (vt G 5.78 DNS-i võltsimine).

Probleem proksiserveritega

Kui WWW-brauser võtab veebiserveriga ühendust proksiserveri kaudu, tuleb arvestada, et veebiserver saab teada ainult proksi IP-aadressi. Proksi saab olla usaldusväärne ainult siis, kui kõik selle taga olevad IT-süsteemid ja kasutajad on samuti usaldusväärsed.

Kui juurdepääs WWW-failidele on piiratud etteantud IP-aadresside, alamvõrkude või domeenidega, võib olla mõistlik neid täiendavalt parooliga kaitsta.

Paroolkaitse

Praktiliselt kõikidesse veebiserveritesse on täiendava juurdepääsujuhtimise võimalusena integreeritud kaitse, mis toimib läbi kasutajanimede ja paroolide.

Esmakordsel juurdepääsul sel moel kaitstud kataloogile sisestab kasutaja oma brauserisse enda kasutajanime ja parooli, mis peab andma volituse juurdepääsuks vastavale ressursile. HTTP-protokolli kaudu saab paroolkaitset (kasutaja autentimist) rakendada mitmel erineval viisil, mis erinevad rakendamiseks vajaliku töömahu ja lahenduse turvalisuse poolest. Kasutajate autentimiseks tuleb valida sobiv meetod, mis vastab kehtestatud turvanõuetele. Kõrgema turbevajaduse puhul tuleks kasutada andmeedastuse krüpteerimiseks SSLi ning vajadusel ka kasutajate autentimist klient-sertifikaatide abil. Täpsemat infot leiate meetmest M 4.176 Autentimismeetodite valimine veebilehtede jaoks , infot SSLi kohta leiate meetmest M 5.66z SSL-i/TLS-i kasutamine kliendis .

Andmete krüpteerimine

Lisavõimalus WWW-failide kaitsmiseks on hoida andmeid veebiserveril krüpteeritult, nii, et andmeid saavad lugeda ainult need, kellel on olemas õige krüptograafiline võti. Lisaks pakub see meetod kaitset volitamata kohaliku juurdepääsu eest, kuid nõuab vastavat võtmehaldust, mis võib olla töömahukas.

Kontrollküsimused:

- Kuidas kaitstakse WWW-faile volitamata kohaliku juurdepääsu eest?
- Kas CGI-skriptid ja konfiguratsioonifailid on piisavalt kaitstud?

M 4.95 Minimaalne operatsioonisüsteem

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator

Turvalisuse seisukohast problemaatilises keskkonnas asuvad arvutid peavad olema sellise kontseptsiooniga, et need pakuks võimalikult vähe võimalusi enese ründamiseks. Kuna tänapäevased operatsioonisüsteemid pakuvad standardina võimalikult palju võrguteenuseid, ei piisa serveri turvaliseks käitamiseks ainult hea kontseptsiooniga serveriteenusest (nt SSLil baseeruvast veebiserverist). Ka operatsioonisüsteem peab olema kaitstud, kuna vastasel korral saab operatsioonisüsteemis oleva nõrga koha abil serveriteenuse turvafunktsioonidest mööda minna. Nn minimaalset operatsioonisüsteemi iseloomustavaks omaduseks on tõsiasi, et ideaaljuhul ei paku see ühtki võrguteenust. Seega ei saa potentsiaalne ründaja ära kasutada nõrka kohta selle operatsioonisüsteemi võrguteenuses. Ja kui ründaja peaks siiski mõne nõrga koha kaudu arvutile ligi pääsema, on minimaalne süsteem talle jätkuvalt takistuseks. Mida vähem programme ründaja sihtarvutist leiab, seda raskem on tal edasisi nõrku kohti leida ja neid ära kasutada. Lisaks kergendab see olulisel määral serveri hooldust, kuna puuduvatele teenuseprogrammidele ei ole ka tarvis installeerida paikasid või remondipakette.

Järgnevalt kirjeldatakse operatsioonisüsteemi konfigureerimist internetiserveri näitel, kuna siin esitatakse operatsioonisüsteemile tavaliselt väga kõrged turvanõuded. Internetiserveril on tavaliselt ainult üks ülesanne: pakkuda teistele arvutitele pidevalt teatud hulgal teenuseid (nt valmidust meile vastu võtta). Selle aluseks olev operatsioonisüsteem ei tohiks pakkuda ühtki täiendavat teenust.

Seetõttu tuleb internetiserveri installeerimisel pidada kinni järgnevast protseduurist:

- Operatsioonisüsteemi alusinstallatsioon - Kui installeerimisel saab mõjutada installeeritavate pakettide mahtu, tuleks paigaldada ainult sellised paketid, mis on hädavajalikud. Teatud pakettide vajalikkus pole alati selge, seega tuleks hoiduda ainult ilmselgelt ebavajalike pakettide installeerimisest.
- Ebavajalike programmide väljalülitamine - Arvuti käivitamisel käivitatakse mitmed programmid automaatselt. Osad nendest programmidest on internetiserveri jaoks täiesti kasutud ja tuleks seetõttu desaktiveerida. Desaktiveerimine võib toimuda automaatkäivituse keelamisega (käivitusskriptidega Unixis) ning vastavate programmide kustutamisega. Turvalisuse põhjustel tasuks eelistada kustutamist, kuna sel juhul ei saa ründaja enam teenust uuesti aktiveerida. Siiski on mõnikord väga raske kõiki teatud teenuse juurde kuuluvaid faile üles leida ja kustutada, mistõttu tuleks kahtluse korral kustutamisest siiski hoiduda.
- Võrguparameetrite konfigureerimine - Kui seda pole tehtud juba installeerimisel, tuleb nüüd seadistada internetiserveri võrguparameetreid. Internetiserveri ohutuse jaoks on oluline valida Default Gateway ja Domain Name Server. Kui aga internetiserveri ja interneti vahel toimuv side kasutab proksit (vt M 2.73 Sobiva turvalüüsi (tulemüüri) põhistruktuuri väljavalimine), on Default Gateway üleliigne. Ilma Default Gateway 'ta ei saa internetiserver edastada oma vastuseid otse internetti, seega, proksist mööda minnes ei saa kommunikatsioon toimida, st see välistab ka ründed. Ka DNS on internetiserveri jaoks sageli üleliigne ja seda tuleks võimalusel vältida, kuna see

pakub otsest sidekanalit operatsioonisüsteemiga (vt M 4.96z DNSi desaktiveerimine). Lisaks on veel mitmeid parameetreid, mis mõjutavad otseselt nn TCP/IP pinu, nt IP-pakettide maksimaalne suurus. Need parameetrid sõltuvad olulisel määral vastavast operatsioonisüsteemist, mistõttu võib siinkohal soovitada ainult IP-edasisuunamise (forward 'i) väljalülitamist. Täiendavad muudatused võivad suurendada nt stabiilsust vigaste IP-pakettide suhtes või suurendada ka võrgu läbilaset.

- Tarbetute võrguteenuste väljalülitamine - Mõned vajalikud teenuseprogrammid pakuvad ka mitmeid täiendavaid teenuseid (eriti on siinkohal silmas peetud Unixi inetd 'i). Vastavaid konfiguratsioonifaile tuleb piirata vajalike võrguteenuste peale (vt lisaks M 5.16 Võrguteenuste inventuur).
- Turvaprogrammide installeerimine - Juhul, kui need puuduvad, tuleks operatsioonisüsteemi täiendada täiendavate turvaprogrammidega. Eriti mõistlik oleks paigaldada tervikluse kontrollimise programm (vt M 4.96z DNSi desaktiveerimine) ja tarkvarapakettide filter.

Soovitav on installeerida ka viirusetõrjet ja logianalüüsi võimaldavad programmid.

Kui tekib vajadus internetiserveri kaugadministreerimise järele, tuleb installeerida vastav turvatoode, nt Secure Shell Daemon (vt M 5.64z Secure Shell (SSH)) ja kontrollida regulaarselt süsteemi turvalisust (vt lisaks M 4.26 Regulaarne turvakontroll Unix-süsteemis).

- Võrguteenuste konfigureerimine ja kontroll - Ideaaljuhul ei paku minimaalne operatsioonisüsteem ühtki võrguteenust ja seega on väljast tulevate rünnete oht välistatud. Eriti just suuremates võrkudes ei ole see protseduur oma haldamise tõttu praktiline, mistõttu on kaugjuurdepääs vajalik. Seda, kas internetiserver võimaldab kasutada teenuseid või mitte, saab Unixi all kontrollida käsuga netstat-a. Iga loetletud teenust tuleb konfiguratsiooni abil piirata nõnda, et sellele pääseksid ligi ainult volitatud arvutid (nt tuleb kaugpöördust internetiserverile lubada ainult võrguhalduse arvutitele).
- Ebavajalike programmide kustutamine - Niipea, kui minimaalse operatsioonisüsteemi installeerimine on lõpetatud, tuleks kõik programmid, mis võivad potentsiaalset ründajat abistada, kohe kustutada. Eriti tuleb eemaldada olemasolevad kompilaatorid, kuna ründajal võib neist palju kasu olla. Lisaks ei ole internetiserveril asuvad kompilaatorid ka veel seepärast mõttekad, et need arvutid on tootmismasinad ja programmide arendamine ning testimine peab jääma muude arvutite ülesandeks. Mõeldav on ka kõikide editor'ide kustutamine, kuna see muudaks ründaja jaoks konfiguratsioonifailidega manipuleerimise olulisemalt raskemaks. Samas muudab see ka administreerimise keerulisemaks. Konfiguratsioonifailide muutmiseks tuleb siis alati uuesti installeerida vastav editor, või, mis on ka parem lahendus, tuleb konfiguratsioonifaile töödelda mõnes teises arvutis ja seejärel ümber kopeerida.

Minimaalne operatsioonisüsteem ei tohiks muidugi muutuda omaette eesmärgiks.

Internetiserveri jaoks tuleb loomulikult paigaldada ka reaalne serveriteenus.

Kas see juhtub ülemise nimekirja lõpus või näiteks punktide 6 ja 7 vahel või ka vahetult pärast 1. punkti, sõltub vastavast installatsioonist. Probleem tekib

siis, kui installeerimine ebaõnnestub puuduvate süsteemipakettide tõttu, kuna sel juhul tuleb puuduvad paketid üles leida ja ise juurde installeerida. Parem on, kui serveriteenuse tootja annab info, millisel määral sõltutakse operatsioonisüsteemist, et minimaalse süsteemi väljatöötamisel saaks juba algusest peale lähtuda asjakohasest infost.

Ka miinimumsüsteemiga arvuti ei ole lõplikult rünnakute eest kaitstud. Eduka rünnaku tõenäoline põhjus on kindlasti serveriteenus, kuid ka miinimumsüsteem ise on veel rünnatav, näiteks TCP/IP pinu, mis peab võrgupakette rakenduse juurde edasi suunama. Peaaegu kõik senised teadaoleva TCP/IP pinu vastu suunatud ründed on puudutanud ainult käideldavust, põhjustades asjassepuutuvate arvutite kokkujooksmise, st arvutisse endasse sissetungimist pole seni veel täheldatud.

Et ka seda ohtu veelgi vähendada, tuleks rakendada muuhulgas ka meedet M 4.98 Side piiramine miinimumini paketifiltritega .

Kontrollküsimused:

- Kas serverite ebavajalikud programmid on desaktiveeritud?
- Kas kõik ebavajalikud võrguteenused on välja lülitatud?
- Kas kontrollitakse regulaarselt, milliseid võrguteenuseid serverid pakuvad?

M 4.96z DNSi desaktiveerimine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: administraator

Internetiserver ei vaja tavaliselt DNSi (*Domain Name System* 'it), et tagada info käideldavus, välja arvatud juhul, kui selle kaudu saadetakse meile, kuid sellisest lahendusest on soovitav loobuda (vt lisaks M 4.97 Ainult üks teenus serveri kohta). Nii kasutataksegi enamikes WWW-serverites DNSi ainult selleks, et kanda vastavatesse logifailidesse IP-aadresside asemel arvutinimesid. Vastavat IP-aadresside muutmist arvutinimedeks saab teha ka hiljem, logifailide analüüsimisel. Logifailide käsitsemine on küll sel juhul pisut keerulisem, kuid logiandmete usaldusväärsus seevastu suurem. IP-aadressi ja arvutinime vastavus pole ei ühene ega staatiline. DNSist loobumine kaitseb ka *DNS-Spoofing* 'u eest (vt M 5.59 DNS võltsimise tõrje) ja suurendab sageli ka internetiserveri jõudlust.

Järgnev kasutusvaldkond näitab võimalikke negatiivseid tagajärgi:

Ründajal on olemas isiklik domeen ja testarvuti. Vastav Test-PC on samaaegselt ka selle domeeni DNS-serveriks. Testarvuti abil loob ründaja ühenduse internetiserveriga. Internetiserver tunneb ühenduspäringu alguses ainult testarvuti IP-aadressi ja üritab DNSi kaudu teada saada testarvuti arvutinime. Sel eesmärgil peab operatsioonisüsteem looma ühenduse DNS-serveriga, mis peab omakorda saama andmeid testarvutist, kuna see on ründajadomeeni DNS-server. Selle asemel, et vastata internetiserveri DNS-serverile, saab ründaja nüüd saata suvalise vastuse otse internetiserverile (kasutades *IP-Spoofing* 'ut, vt G 5.78 DNS-i võltsimine). Sel moel saab ründaja saata andmeid mitte ainult reaalsele DNS-serverile, vaid ka otse internetiserverile. See võimaldab ära kasutada selle operatsioonisüsteemis leiduda võivaid vigu.

Teadmiseks
Kui juurdepääs WWW-serverile peab olema võimaldatud ainult teatud domeenile, nt ainult domeenile *.ee, siis DNSist loobuda ei saa. Siiski on selline juurdepääsukaitse väga nõrk ja seetõttu seda ei soovitata.

Täiendav kontrollküsimus:

- Kas DNS on internetiserveris välja lülitatud?

M 4.97z Ainult üks teenus serveri kohta

Algatamise eest vastutavad: infoturbespetsialist, IT-juht
Rakendamise eest vastutab: administraator

Paljusid IT-süsteemide kitsaskohti ükshaaval ei saa potentsiaalne ründaja ära kasutada. Sageli õnnestub arvutisse edukalt sisse tungida seetõttu, et ründaja kombineerib mitut kitsaskohta. Olenevalt ohuastmest ja teenuste kaitsevajadusest võib seega olla otstarbekas käitada arvutis ainult ühte teenust. Esmajoones puudutab see servereid, mis osutavad teenuseid ka internetikeskkonnale või teistele võõrvõrkudele. Turvalisust saab suurendada näiteks sellega, kui hoida nii veebiserverit kui ka meiliserverit töös eraldi vastavaotstarbelistes arvutites, mis on seadistatud töötama minimaalse süsteemina (vt ka M 4.95 Minimaalne operatsioonisüsteem). Pealegi erinevad teenused ka oma turbeastme poolest. Ründaja tungimine veebiserverisse võib tekitada palju probleeme, eriti kui ta muudab väliste kasutajate jaoks ligipääsetavaid veebilehekülgi. Seevastu konfidentsiaalsele infole ründaja sellise tegevusega siiski ligi ei pääse. Ent olukorras, kus veebiserverit kasutatakse samal ajal ka veel meiliserverina, võib ründaja volitamatult lugeda ka kõiki meile ning selle tagajärjed võivad olla juba palju tõsisemad.

Lahutatud funktsioone saab muuta veelgi kindlamaks, kui jaotada ühe teenuse erinevad ülesanded ära eri arvutite vahel. Näiteks võime oletada, et eksisteerib meiliserver A, mis võtab meile internetist vastu ja suunab need edasi sisevõrku, ning meiliserver B, mis suunab meile sisevõrgust internetti. Kuna internetist tulev sidealgatus on võimalik ainult meiliserverist A, saab ründaja rünnata ainult seda. Meiliserver A ei tohi ise meile internetti saata ja seepärast ei saa seda arvutit ära kasutada ka mitte rämpsposti saatmiseks. Erinevate teenuste jaotamine eri arvutite vahel pakub muu hulgas järgmisi eeliseid:

- arvuteid on kergem seadistada;
- ettelülitatud paketifiltrit on kergem seadistada ja see on turvalisem;
- suurem vastupanu rünnetele;
- suurem avariikindlus.

Suuremast hulgast arvutitest tekkivat administreerimisvaeva saab ületada tsentraalse süsteemihaldusega.

Virtualiseerimine

- Turvalisuse seisukohast kriitiliste teenuste puhul tuleks sama moodi nagu füüsilistes süsteemides ka virtuaalsetes IT-süsteemides käitada ainult ühte teenust. Virtuaalne IT-süsteem ise ei ole siiski sama mis virtualiseerimisserveri teenus. Seega saab ühel virtualiseerimisserveril käitada mitut virtuaal-

set IT-süsteemi. Olenevalt virtualiseerimistehnoloogiast, millel virtualiseerimisserver põhineb (serveri või operatsioonisüsteemi virtualiseerimine), võib ka virtuaalse IT-süsteemi pakutavate teenuste hulk olla piiratud. Iga konkreetse virtualiseerimistoote puhul tuleb eraldi kontrollida, kas see suudab virtualiseerimisserveril osutada erinevaid virtuaalseid IT-süsteemide teenuseid või mitte. Kriteeriumideks on antud juhul isoleerimisvõimaluste tugevus ja virtuaalsete IT-süsteemide kapseldamisvõimalused virtualiseerimisserveril (vt M 3.72 Virtualiseerimistehnika põhimõisted). Mida tugevamalt on virtuaalsed IT-süsteemid virtualiseerimisserveris isoleeritud, seda paremini sobib virtualiseerimistoode erinevate teenuste käitamiseks erinevates virtuaalsetes IT-süsteemides. Alljärgnevad põhimõtted kergendavad esmavaliku tegemist.

- Virtualiseerimisserverites, mis kasutavad operatsioonisüsteemi virtualiseerimislahendust, tuleks tavaliselt sisse seada ainult ühe funktsiooniga virtuaalsed IT-süsteemid. Virtualiseerimisserveris tuleks käitada näiteks eranditult veebiservereid või eranditult meiliservereid, kuid mitte nende rühmade segu. Mõnede operatsioonisüsteemide virtualiseerimistoodete puhul on virtuaalsete IT-süsteemide isoleerimine siiski ka piisavalt tugev, et seda nõuet eirata.
- Serveri virtualiseerimislahendusega virtualiseerimisserverites on tavaliselt lubatud käitada erinevaid teenuseid osutavaid virtuaalseid IT-süsteeme. Seega on olenevalt olukorrast võimalik veebi- ja meiliserverit käitada ühel virtualiseerimisserveril, juhul kui need asuvad üksteisest eraldatud virtuaalsetes IT-süsteemides.

Virtualiseerimisserveris endas tohiks siiski käitada ainult virtualiseerimistarkvara ja sellega otseselt seotud teenuseid (virtualiseerimise haldusteenust jm) ja mitte ühtki muud teenust.

Täiendavad kontrollküsimused:

- kas turvalisuse seisukohast kriitiliste teenuste puhul järgitakse põhimõtet „Üks teenus serveri kohta”?
- kas virtualiseerimistehnoloogia (serveri ja operatsioonisüsteemi virtualiseerimise) puhul on piisavalt arvestatud nende eripäradega, mis puudutavad virtuaalsete IT-süsteemide erinevaid teenuseid ühel virtualiseerimisserveril?
- kas virtualiseerimisserveril käitatakse ainult virtualiseerimistarkvara ja mitte mingeid muid teenuseid?

M 4.98 Side piiramine miinimumini paketifiltritega

Algatamise eest vastutavad: infoturbespetsialist, IT-juht
Rakendamise eest vastutab: administraator

Paketifiltrid on spetsiaalse tarkvaraga IT-süsteemid, mis filtreerivad OSI-mudeli alumiste kihtide infot ja juhivad erireegleid järgides pakette edasi või peatavad nende liikumise (vt M 2.74 Sobiva paketifiltri valimine).

Veebiserverite kaitseks kasutatava paketifiltri konfiguratsioon peab olema võimalikult piirav, et suurendada ründekindlust. Hästi konfigureeritud veebiserver (vt M 4.95 Minimaalne operatsioonisüsteem) peaks küll suutma end ka iseseisvalt rünnete eest kaitsta, kuid veebiserveri tarkvara on siiski palju keerulisem ja veaaltim kui paketifiltri tarkvara, mille kontseptsiooni põhiaspektiks on turve. Paketifilter peaks endast läbi lubama ainult need suhtluskanalid, mis on veebiserveri tööks hädavajalikud. Peale internetist veebiserverisse suunatud kommunikatsiooni tuleb kontrollida ka veebiserverist internetti liikuvat kommunikatsiooni. Paljude rünnete puhul on esmane eeldus see, et rünnatav arvuti peab suutma ise luua uusi ühendusi internetiga. Kui see pole võimalik, lõppevad ka paljud ründed edutult. Näiteks olid 1997. aastal väga populaarsed uudisteserverite vastu suunatud ründed, mille käigus lasi ründaja endale uudiste-deemoni vea abil saata meiliga olulist süsteemiinfot. Kui rünnatud arvutitel ei oleks olnud meilisaatmise volitusi, poleks ründaja vastust saanud ning ründed oleksid jäänud tulemusteta.

Alljärgnevalt on toodud mõned näited erinevate veebiserverite paketifiltrite seadistamiseks.

1. Veebiserver

- Internet võib pääseda veebiserverisse läbi veebiserveri TCP pordi nr 80 või pordi nr 443, kui kasutatakse SSL-i/TLS-i
- Veebiserver võib pääseda internetti pordist nr 80 või SSL/TLS-i, TCP/ack-i jaoks pordist nr 443, kõik muu peab olema keelatud!

2. News-Server

- Newsfeed-Serverid tohivad kasutada News-Serveri TCP porti 119
- News-Server võib pääseda pordist 119 Newsfeed-Serveri TCP-sse/ack-i
- News-Serveril tohib olla juurdepääs Newsfeed-Serveri TCP pordile 119
- Newsfeed-Serverid tohivad pordist 119 pääseda News-Serveri TCP-sse/ack-i 3. Meiliserver (meililüüsi annab kasutada teenusepakkuja):
- teenusepakkuja meiliserver tohib pääseda meiliserveri TCP porti 25
- meiliserver tohib pordist 25 pääseda teenusepakkuja TCP/ack-i meiliserverisse
- meiliserver tohib ligi pääseda teenusepakkuja TCP meiliserveri pordile 25

- teenusepakkuja meiliserver tohib pordist 25 ligi pääseda meiliserveri TCP-le/ack-ile 4. Meiliserver (omapoolne internetti saatmine):
- internet tohib pääseda meiliserveri TCP porti 25- meiliserver tohib pordist 25 pääseda interneti TCP-sse/ack-i
- meiliserver tohib pääseda interneti TCP porti 25
- internet tohib pordist 25 pääseda meiliserveri TCP-sse/ack-i 5. DNS-server:
- Resolvingu DNS-server tohib pääseda Advertisingu DNS-serveri UDP porti 53
- Advertisingu DNS-server tohib ligi pääseda kõikidele Resolvingu DNS-serveri UDP portidele (vajalik ainult olekurežiimita tulemüüri korral)
- Resolvingu DNS-server tohib ligi pääseda oma Forwarderi UDP pordile 53
- Forwarder tohib ligi pääseda kõigile Resolvingu DNS-serveri UDP portidele (vajalik ainult olekurežiimita tulemüüri korral)
- Välisvõrk tohib pääseda Advertisingu DNS-serveri UDP porti 53
- Advertisingu DNS-server tohib pääseda kõigi väliste DNS-serverite UDP ja TCP portidesse (vajalik ainult olekurežiimita tulemüüri korral)
- Sisevõrgul võib olla juurdepääs Resolvingu DNS-serveri UDP pordile 53
- Resolvingu DNS-serveril võib olla juurdepääs kõigile sisevõrgu UDP portidele (vajalik ainult olekurežiimita tulemüüri korral)
- Primaarsel DNS-serveril võib olla juurdepääs sekundaarse DNS-serveri UDP ja TCP pordile 53
- Sekundaarsel DNS-serveril võib olla juurdepääs primaarse DNS-serveri UDP ja TCP pordile 53

Kui rakendatakse üksnes neid reegleid, piirdub internetist tuleva kommunikatsiooniühenduse algatamine ainult lubatud teenustega. Kui kommunikatsioonipartnereid saab piirata veelgi täpsemalt (vt eelnevaid näiteid 2 ja 3), ei suuda ründaja luua otseühendust veebiserveriga.

Teadmiseks
Äsja loetletud reeglite rakendamisel võib tekkida olukord, kus kõik arvutid ei saagi ühendust veebiserveriga, sest ICMP-d ei lasta läbi. Seepärast on soovitatav ICMP Subtype *icmp unreachable* internetist kuni internetiserverini läbi lasta.

Täiendav kontrollküsimus:

- kas regulaarselt kontrollitakse, et paketifiltrite kommunikatsioon oleks vähendatud miinimumini?

M 4.99 Kaitse info muutmise eest pärast üleandmist

Algatamise eest vastutavad: IT-juht, IT turvaosakond

Rakendamise eest vastutavad: administraator, kasutaja

Failid, mis antakse edasi kolmandale osapoolele, on tavaliselt ka nende poolt töödeldavad. Failide koostaja ei pruugi seda soovida. Seega kuluks ära kaitse hilisema muutmise, osalise edastamise või töötlemise eest. Sageli on probleemiks, et info tuleb interneti või muude võrkude kaudu kolmandale osapoolele küll kättesaadavaks teha, kuid seejuures tuleks takistada sajakordset väljaprintimist või jäljetut integreerimist teistesse töödesse.

Selleks on erinevaid lahendusi, mida saab osaliselt ka üksteisega kombineerida. Mõningad näited:

- Digitaalsete allkirjade kasutamine, et takistada failide märkamatut muutmist (vt lisaks M 3.23w Sissejuhatus krüptograafia põhimõistetesse ja M 4.34z Krüpteerimise, kontrollsummade ja digitaalallkirjade rakendamine).
- Autoriõigusi kajastava info lisamine WWW-infole või failidele. See võib olla järgnev: „Teos ja kõik selle osad on kaitstud autoriõigusega. Igasugune autori loata kasutamine väljaspool autoriõiguseseaduse määrusi on keelatud ja karistatav.” Lisaks nt „Copyright (c) 7/1999 by BSI”.
- Failiformaatide kasutamine, mis raskendavad hilisemat muutmist või osalist edasitöötlemist. Selleks võib kasutada nt Postscripti või rakendusprogrammide turvafunktsioone, nt PDF-failide puhul. PDF-dokumentidele saab loomisel määrata juurdepääsupiirangud. Nii saab nt piirata PDF-failide avamist, printimist või kopeerimist. PDF-failide loomiseks ja töötlemiseks kasutatava rakenduse Acrobat Exchange abil saab määrata kahte liiki paroole. Esimesi kasutatakse dokumendi avamiseks, teisi turvaatribuutide muutmiseks. Volitamata avamise eest kaitstud PDF-dokumendid krüpteeritakse seejuures RC4ga. Turvaatribuutide abil saab piirata järgmisi funktsioone:
- printimine,
- dokumentide muutmine,
- teksti või graafika kopeerimine,
- märkmete ja formulariväljade lisamine või muutmine.

Näiteks saab sel moel kerge vaevaga piirata õigusi nii, et keegi ei saaks lõika ja kleebi funktsioonide abil teose sisu ümber tõsta. Kui ekstreemjuhul on takistatud isegi printimine, saab faili lugeda ainult onlain-versioonis. Kahjuks on selline kaitse suhteliselt piiratud, kuna PDF-faile saab avada programmidega, mis neid turvaatribuute eiravad. Kui nt printimine on lubatud, saab dokumendi alati muuta uuesti PDF-failiks, millel puuduvad igasugused piirangud.

Kontrollküsimus:

- Millised turvameetmed on võetud kasutusele, et takistada failide muutmist?

M 4.100 Tulemüür ja aktiivsisu

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: administraator

Tulemüüri kontseptsiooni suurimaks probleemiks on toimetulek probleemidega, mis tekivad aktiivsisu edastamisel kaitstava võrgu arvutitele. Hetkel pole veel kasutuskõlblikke programme, mis pakuksid arvutiviiruste tõrjega võrreldavat kaitset ActiveX-Control'ide, Java-Applet'ite või skriptiprogrammide kahjulike funktsioonide eest. Kaitstavas võrgus asuvat arvutit ohustava aktiivse sisu ohtlikkust ilmestab järgnev näide: Java-Applet või brauser tohib vastavalt Java-spetsifikatsioonile luua võrguühenduse serveriga, millelt see alla laeti. See hetkel veel vähekasutatav võimalus on peamiseks eelduseks, kui tahetakse kasutada võrguarvutit (NC) või muud sarnast, mis peab kasutajapoolse algatuseta serverist programme laadima. Vastava funktsiooni täiemahuliseks toetamiseks, hoolimata paketifiltri kasutamisest, tuleb avada kas palju rohkem porte või siis kasutada dünaamilist paketifiltrit. Kui see on nii, saab Java-Applet'ite abil luua vaevu kontrollitavaid IP-ühendusi. Aktiivsisu saab kontrollida erineval moel:

Aktiivsisu tsentraalne filtreerimine tulemüüris
Tulemüüri komponent (tavaliselt ALG) filtreerib kogu kahjulikuks peetavat sisu nii, et klientarvutisse ei satuks enam potentsiaalselt ohtlikke programme.
Aktiivsisu seotakse erimärgendite abil HTML-lehega. Tavaliselt tuntakse ja eemaldatakse aktiivsisu HTML-leheküljelt vastavate märgendite abil, või siis asendatakse need tekstiga, mis annab kasutajale märku, et sisu on filtreeritud. Probleem seisneb selles, et hetkel kasutatava HTML-spetsifikatsiooni keerukate võimaluste tõttu ei tunne turvaproksid paljusid kustutatavaid märgendeid ära. Lisaks on probleemiks, et näiteks Java-Applet'eid ei pea ilmtingimata edastama failina, mille laiend on .class. Selle asemel saab kasutada kokkupakitud faile, mis on nt laiendiga .jar (Java-arhiiv). See tähendab, et Java-filter peab tundma ka kõiki brauserite poolt toetatavaid Java-failide laiendeid. Täiendatav kahjupotentsiaal tuleneb võimalusest käivitada JavaScripti Javast. Sarnased probleemid esinevad ka Flash-objektide, .NET Assemblies ja muu aktiivsisu puhul. Tuleb ilmtingimata arvestada, et aktiivsisu tuleb filtreerida ka väljaspool veebilehti, nt HTML-meilides.

Detsentraalne kaitse ühendatud klientidel
Aktiivsisu käivitamist tuleb keelata vastavate brauseriseadistustega. Erinevad brauserid toetavad aktiivsisu jaoks rohkemal või vähemal määral lubatud nimekirja strateegiat (*Whitelist Strategy*) (näited: Microsoft Internet Exploreri tsoonimudel, Mozilla brauseriprofiil). Ideaaljuhul peaks brauser pakkuma võimalust teatud tüüpi aktiivsisu eraldi serverite või domeenide puhul lubada või keelata. Seejuures tuleb arvestada, et brauserite kitsaskohtade tõttu saab vastavatest piirangutest mööda minna. Java-Appletid, Acitve-X objektid ja piiratud määral ka Javascript on varustatavad digitaalsete allkirjadega. Allkiri on mõeldud aktiivsisu tervikluse ja autentsuse kaitsmiseks. Kui kasutada lubatakse ainult allkirjastatud aktiivsisu, pakub see suuremat kaitset kahjulike funktsioonide vastu. Selline turvalisus on siiski vaid kaudne, kuna kasutaja ise sõltub omakorda aktiivsisu pakkuja jaoks allkirja andva üksuse usaldusväärsusest. Isegi aktiivsisu käivitamise täielik desaktiveerimine pakub halvaloomulise aktiivsisu eest ainult piiratud kaitset.

Brauseritarkvara arvukate puudujääkide tõttu saab turvaseadeid eirata, mistõttu eesmärgiks seatud kaitse kas puudub või on olemas vaid piiratud määral.

Viirusetõrjetarkvara ja isiklike tulemüüride paigaldamine klientidele
Viirusetõrjeprogrammid võivad kaitsta aktiivsisu poolt automaatselt allalaetavate viiruste, makroviiruste ja Trooja hobuste eest. Need pakuvad kaitset juba tuntud kahjulike programmide eest. Lisainfot viirusetõrjetoodete kohta leiate moodulist B 1.6 Viirusetõrje kontseptsioon . Isiklikud tulemüürid on klientarvutitesse installeeritavad programmid, mis täidavad seal tavaliselt korraga mitut funktsiooni. Lisaks lokaalse paketifiltri funktsioonile pakuvad need ka veel täiendavaid funktsioone. Näiteks võimaldavad osad isiklikud tulemüürid jälgida programme, mis püüavad algatada võrguühendusi. Sellist ühenduse loomist võib lubada või keelata kas siis automaatsete reeglite abil või erandjuhul kasutaja poolt käsitsi. Mõnel juhul pakuvad nad ka nn liivakaste, mis suudavad kontrollida aktiivsisu käivitamist ja piiravad neid, lubades käivitada ainult ohutuid funktsioone. Koostöös viirusetõrjega pakub isiklik tulemüür üsna head kaitset halvaloomulise aktiivsisu vastu. Siiski tuleb arvestada, et nende programmide õige konfigureerimine nõuab lisaaega, mis kulub täiendavale administreerimisele, samuti võib isiklikes tulemüürides leiduda turvaauke, mis ohustavad süsteemi.

Töötajate teavitamine võimalikest ohtudest
Kõigi kolme valiku puhul tuleb kasutajaid täiendavalt teavitada. Lisaks tuleb tagada, et kasutaja kogemata ei desaktiveeriks ning ei eiraks kliendil ühtki punktis 2 ja 3 nimetatud kaitsemeetme jaoks vajaminevat seadistust.

Tsentraalse filtreerimise eelised	**Detsentraalse filtreerimise eelised**

- Lihtne installeerida ja hallata, kuna filtritarkvara tuleb installeerida ainult üks kord. - Lihtne logida ja analüüsida, kuna erinevalt detsentraalsest filtreerimisest ei ole tarvis kokku koguda mitme arvuti logiandmeid. - Erinevalt detsentraalsest filtreerimisest ei saa kasutaja filtreerimistarkvaraga manipuleerida. - ALG aktiivsisu filtriprogrammide näol on tegemist eriotstarbeliste turvatoodetega. Aktiivsisu eest kaitsmine klientidel (nt brauseris) on seevastu sageli lahendatud puudulikult. - Filtreerimistarkvara saab kasutada sõltumatult klientides olevast tarkvarast. Klientides kasutatava tarkvaraga seotud ühilduvusprobleemid on välistatud.	- Tsentraalsest filtreerimisest suurem tõrkekindlus, kuna filtreerimine toimub detsentraalselt. - Kaitse krüpteeritud aktiivsisu eest. Lõppseadmel filtreerimine aitab ära tunda aktiivsisu, kuna see dekrüpteeritakse alles lõppseadmes. - Aktiivsisu käivitamise väljalülitaine ei sõltu tulemüürist. - Ei teki ühilduvusprobleeme, mis võivad tuleneda tsentraalse filtritarkvara kasutamisest ALG'l.

Tabel: tsentraalse ja detsentraalse filtreerimise eelised

Soovitus

Otsus, mida aktiivsisuga teha, sõltub esmajoones asjassepuutuva kliendi kaitsevajadusest. Individuaalse strateegia valimisel võib abi olla järgnevast tabelist:

Kliendi kaitsevajadus	**Soovitus**
Tavaline	Üldist: aktiivsisu desaktiveerimine brauseris ja ainult usaldusväärsete veebilehtede lubamine. Viirusetõrje kliendil (vt lisaks moodulit B 1.6 *Viirusetõrje kontseptsioon*). Aktiivsisu on soovitav filtreerida tulemüüris ja lubada tuleks ainult usaldusväärseid veebilehti (lubatud nimekirja strateegia).

Kõrge	Aktiivsisu desaktiveerimine brauseris ja ainult usaldusväärsete veebilehtede lubamine. Viirusetõrje kliendil (vt lisaks moodulit B 1.6 *Viirusetõrje kontseptsioon*). Aktiivsisu tuleks filtreerida tulemüüris ja lubada tohiks ainult usaldusväärseid veebilehti (lubatud nimekirja strateegia). Lisaks filtreerida küpsiseid (lubatud nimekirja strateegia). Kriteeriumid, milliste veebilehtede jaoks aktiivsisu lubatakse, peavad olema märksa piiravamad kui tavalise kaitsevajaduse puhul. Soovitatav on teha täiendav turvaanalüüs, et tagada sobiva turbeastme saavutamine.
Täiendavad või erinõuded	Isikliku tulemüüri kasutamine kliendil.

Tabel: veebilehtede aktiivsisu käsitlemise soovitused

Teatud protseduuri kasuks otsustamine ja otsuseni viinud põhjused tuleb selgesti mõistetavalt dokumenteerida. Liiga järeleandlik seadistus või täielik aktiivsisu lubamine pole ka tavalise kaitsevajaduse puhul soovitatav. Selleks on halvaloomulise aktiivsisu ning veebibrauseri või operatsioonisüsteemi puudujääkide tulemusel tekkida võivad kahjustused liiga tõsised. Juhul kui teatud rakendused peavad kindlasti kasutama aktiivsisu, tuleb seda võimaldada ainult vastavas serveris.

Brauseripõhiste rakenduste väljatöötamisel või olemasolevate edasiarendamisel, mis vajavad aktiivsisu, tuleb seada kahtluse alla, kas aktiivsisu kasutamine on kindlasti hädavajalik. Sageli saab aktiivsisu asendada serveripoolsete dünaamiliselt genereeritavate veebilehtedega, mille puhul jäävad funktsioonid samaks.

Täiendav kontrollküsimus:

- Kuidas käiakse ümber aktiivsisuga?

M 4.101 Tulemüürid ja krüpteerimine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: IT-turvaosakond, administraator

Kuna internetis pole kunagi ette näha, milliseid teid ja sõlmpunkte andmeedastuseks parasjagu kasutama hakatakse, tuleks andmeid saata võimalusel ainult krüpteeritud kujul.

Läbi interneti kulgeva andmeside krüpteerimiseks on võimalik kasutada kahte erinevat meetodit:

- Turvalüüsis ehk võrguühenduselementides toimuvat krüpteerimist, mida saab kasutada turvaliste alamvõrkude ülesehitamiseks
- Lõppseadmetes toimuvat krüpteerimist, mida saavad kasutajad ise rakendada vastavalt oma vajadustele.

Mõlemal protseduuril on nii oma head kui ka vead, mistõttu tuleb sõltuvalt kasutusvaldkonnast eelistada erinevaid lahendusi.

Turvalüüsis rakendatav krüpteerimine
Andmete vahetamiseks väliste sidepartneritega läbi avaliku võrgu ja/või sidepartnerile juurdepääsu andmiseks oma võrgule võib olla mõistlik rakendada virtuaalsete privaatvõrkude (VPNide) ülesehitamist. Selleks tuleb kõik sidepartnerilt tulevad temani viivad ühendused krüpteerida, et välistada volitamata isikute juurdepääs vastavatele ühendustele. Krüpteeritud ühenduste loomiseks on võimalik kasutada tervet rida erinevaid riist- ja tarkvaralahendusi. Kui omavahel on tarvis ühendada vaid väheseid asukohti, on kõige kindlam ja lihtsam lahendus võtta kasutusele riistavaralised vahendid, mis töötavad asümmeetrilistel krüptograafilistel protseduuridel. Infot VPN-komponentide kaasamisest turvalüüside alla leiate meetmest M 4.224z Virtuaalsete privaatvõrkude integreerimine turvalüüsidesse. Krüpteerimine ja dekrüpteerimine võib aset leida ka erinevates seadmetes. Nii näiteks võib riistvaraline lahendus töötada paketifiltris võtmeseadmena.

See on eriti siis mõistlik, kui läbi selle seadme ei tohiks liikuda ühtki krüpteerimata kommunikatsiooni. Krüpteerimise integreerimine ALG alla pakub veel ka täiendavat eelist lihtsama (tsentraalse) kasutajahalduse näol. Lisaks puudub ründajal, kes on saanud oma kontrolli alla välise infoserveri, võimalus kuulata pealt krüpteeritud sidet.

Lõppseadmetes rakendatav krüpteerimine

Teatud andmete konfidentsiaalsuse kaitseks, eriti meilide saatmisel, on hea lahendus võtta kasutusele mehhanismid, mis pakuvad end-to-end krüpteeringut.

Meiliteenuse jaoks kasutatakse selleks tihti vabavarana kättesaadavat program-

mipaketti PGP (Pretty Good Privacy) (vt M 5.63z GnuPG või PGP kasutamine), juurdepääsuks teistele arvutitele aga Secure-Shell protokolli (SSHd). Usaldusväärseks andmevahetuseks sidepartneritega läbi interneti tuleks kasutada selliseid edastusprogramme ja -protokolle, mis toetavad edastatavate andmete krüpteerimist. Ebaturvalisi, teksti loetaval kujul edastatavaid protokolle nagu Telnet'i ja FTPd tohiks avalikes võrkudes kasutada vaid koos täiendava kaitsega (nt koos tunneldamisega läbi mõne turvalise kanali või ehtsa VPNi). Andmete end-to-end krüpteering seab turvalüüside filtreerimismehhanismide tõhusale kasutusele omalt poolt ette küllaltki suured probleemid. Juhul, kui turvalüüsis on lubatud edastada krüpteeritud andmeid (nt SSLiga), ei ole rakenduskihi filtrid enam suutelised kasutajaandmeid nt viiruste või muu kahjurvara suhtes kontrollima.

Suuri piiranguid kehtestab krüpteerimise kasutamine ka logimisvõimalustele.
Probleemi üks võimalikke lahendusi on lasta andmeliiklus ajutiselt turvalüüsis dekrüpteerida. SSL'i jaoks on olemas nt vastavad proksid, mis lõpetavad turvalüüsis SSL-ühenduse ja muudavad dekrüpteeritud andmevoo kättesaadavaks filtreerimisprotsessidele. Vajadusel on andmeid võimalik lõppseadmele edastamiseks taas krüpteerida. Siinkohal võimalik anda üldkehtivaid soovitusi, mis räägiksid üheselt kas turvalüüsides krüpteerimise kasutamise poolt või selle vastu. Kõik sõltub konkreetsetest vajadustest, mistõttu tuleks olukorda hinnata rakenduse kontekstis.

Turvalüüsis:	Lõppseadmetes:
+ andmete tsentraalne kontrollimine	+ *end-to-end* turve
+ tsentraalne võtmehaldus	+ protokolliprobleemide puudumine
+ detailne *accounting*	+/- sõltuvus kasutajast
- juurdepääs sisevõrgule läbi turvalüüsi	- kontrollivõimalused turvalüüsis puuduvad
- ei võimalda *end-to-end* turvet	- sageli läheb tarvis *Public-Key* -infrastruktuure

Tabel: võimalike lahenduste eelised ja puudused

Juhtudel, kus teatud teenuste või protokollide puhul määratakse kindlaks end-to-end krüpteeringu kasutamine (või antakse selleks luba), võib lõppseadmetes olla vajalik rakendada täiendavaid kaitsemeetmeid. Sellist vajadust tuleks analüüsida täiendava turvaanalüüsi raames.

Kontrollküsimus:

- Kas mõne teenuse puhul rakendatakse end-to-end krüpteeringut? Kui vastus on jah: kas täiendava turvanalüüsi raames on välja selgitatud, kas lõppseadmetes on tarvis rakendada veel ka täiendavaid kaitsemeetmeid?

M 4.105 Unixi turvaline tüüpinstalleerimine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: administraator

Enamik Unix-süsteeme ei vasta kohe pärast standardset installeerimisprotsessi turvalise süsteemikäituse nõuetele. Seda takistavad paljud tootjate poolt lisatud, turvalisuse seisukohast kriitilised teenused ja konfiguratsioonid ning tõsiasi, et need on varustatud liiga laialdaste volitustega. Järgnev ülevaade on toodud näiteks, kuidas muuta standardset installatsiooni turvalisemaks:

- Enne installeerimist tuleks administraatorit piisavalt koolitada, eriti turbeaspektide kohta. Vastava koolituse käigus peaks administraator viima ennast kurssi ka kõikide vastava IT-süsteemi turvalünkadega (vt M 2.35 Teabe hankimine turvaaukude kohta). Siia alla kuulub ka liitumine võimalike meililistidega.
- Pärast installeerimist tuleks süsteemiadministraatori kasutajakonto varustada hea parooliga (vt M 2.11 Paroolide kasutamise reeglid).
- Tuleks kontrollida, milliseid teenuseid IT-süsteemis käitatakse. Seda võib kontrollida nt käsuga *netstat -a | grep LISTEN* . Ebavajalikud teenused tuleb välja lülitada või eemaldada (vt M 5.72 Mittevajalike võrguteenuste desaktiveerimine (Unix)).
- Juhul, kui süsteemi ei rakendata meiliserverina, tuleks meilideemon kui võrguteenus desaktiveerida. Kui meile on tarvis **lokaalselt** kättesaadavaks teha, võib käivitada sednmaili, kasutades *-q15* või siis *Cron* -protsessina: 1 * * * * /usr/sbin/sendmail -q 2>&1 >/dev/null. *Mail-Queue* tühjendatakse regulaarsete ajavahemike tagant ning meilid tehakse lokaalselt kättesaadavaks.
- Installeerida tuleks tootja kõige värskem *sendmail* -versioon (vt M 4.107 Tootja ressursside kasutamine ja M 5.19 Sendmaili turvamehhanismid). Alternatiivse lahendusena võib kasutusse võtta ka mõne ka *Public-Domain* -meiliprogrammi, nt *qmail* . Hetkel kasutatavat *sendmail* -versiooni on võimalik välja selgitada käsuga *telnet localhost 25*.
- Pärast standardse installeerimise lõpetamist tuleks installeerida olemasolevad tootja poolt pakutavad turvapaigad (vt M 4.107 Tootja ressursside kasutamine). Seejärel tuleb ilmtingimata kontrollida, et vastavate *Patch* 'ide installeerimine ei ole endaga kaasa toonud mõne ebasoovitud teenuse sisselülitamise.
- Failisüsteemide importimisele ja eksportimisele tuleb kehtestada piirangud. Tuleb jälgida, et failisüsteeme ei eksporditaks selliselt, et kõik saaks neid kirjutada.
- Juhul, kui *NIS* 'i kasutamisele ei eksisteeri alternatiive, tuleks kasutusele võtta *NIS+* , mis on varustatud laiendatud turvafunktsioonidega.
- Kui peab saama kasutada *tftp* 'd, tuleks see käivitada valikuga *-s* , et igat faili ei oleks võimalik süsteemist kopeerida (vt lisaks M 5.21 telneti, ftp, tftp, rexeci turvaline kasutamine ning M 5.72 Mittevajalike võrguteenuste desaktiveerimine (Unix)).

- *inetd* logimisfunktsioon tuleks aktiveerida valikuga *-t* , et kõik ühenduse loomise katsed kajastuksid ka logis (vt M 5.72 Mittevajalike võrguteenuste desaktiveerimine (Unix)). Palju abi on ka *Public-Domain-Tool* 'i *xinetd* või TCP-Wrapper'i installeerimisest. Nende tarkvaratööriistadega on muuhulgas võimalik juba varakult logida kõiki ühenduse loomise katseid ja seda juba enne, kui vastav deemon *inetd* käsuga käivitatakse.
- Logifaile tuleks kas iga päev või kord nädalas analüüsida. Poolautomaatseks analüüsiks tuleks installeerida analüüsiprogrammid nagu *swatch* , *logdaemon* või *logsurfer* (vt M 2.64 Logifailide kontroll).
- Regulaarselt tuleks läbi viia turvakontrolle, kasutades programme *COPS*, *Tripwire* või *Tiger.*
- Lisaks kõikidele teistele ebavajalikele programmidele tuleks kindlasti desaktiveerida veel ka *rshd*, *rlogind*, *rexecd* (vt M 5.72 Mittevajalike võrguteenuste desaktiveerimine (Unix)). RPC-programminumbrite konverteerimiseks pordiaadressideks lisavad paljud tootjad oma tootele kaasa programmi *rpcbind.* Juhul kui kasutatava platvormi jaoks vastav võimalus eksisteerib, tuleks täiendusena või asendusena rakendada deemonit *portmapper.* Tavaliste kasutajate jaoks tuleks keelata kõikide klientide käivitamist, mis on varustatud nende teenustega. Täiendavad autentimisprotseduurid, mis baseeruvad *host* 'i nimedel, tuleks täielikult kõrvaldada.
- *Telnet* tuleks asendada *ssh* 'ga. *ssh* võimaldab luua tugevalt krüpteeritud ja autenditud interaktiivse ühenduse kahe süsteemi vahel. *ssh* 'd tuleb käsitleda *telnet* 'i, *rsh*, *rlogin* 'i ja *rcp* asendajana. Selle abil on võimalik turvaliseks muuta ka X-Window (vt lisaks M 5.64 Secure Shell (SSH)).
- *Xhost* 'ile tuleks eelistada *xauth*'i – mitte mingil juhul ei tohiks kasutada „ *xhost +* 'i" (vt lisaks M 4.9 X Windowsi turvamehhanismid).
- Konfiguratsioonifailist */etc/inetd.conf* tuleks kustutada kõik ebavajalikud sissekanded (vt M 5.72 Mittevajalike võrguteenuste desaktiveerimine (Unix)).
- Logimisfunktsiooni sisselülitamiseks tuleks kohandada konfiguratsioonifaili */etc/syslog.conf* (vt M 4.106 Süsteemi logimise aktiveerimine (Unix)).
- Loendi kõikidest *world-writable* omadustega failidest ja kataloogidest saab koostada järgmiste käskudega: find / -type f -perm -22 -exec ls -l {} \; ja find / -type d -perm -22 -exec ls -ld {} \; Tulemusi tuleks regulaarselt võrrelda installatsiooniseisundiga.
- Enne kasutuselevõtmist tuleks installeerida programm *Tripwire*, et genereerida installeeritud süsteemi igapäevatöösse ülevõtmisel ülevaade kontrollsummadest. Koostatav ülevaade tuleks salvestada mõnele ülekirjutuskaitsega andmekandjale.
- */var* peaks moodustama ühe suure partitsiooni, et logiandmete pahatahtlik genereerimine ei tooks endaga kaasa Unix-süsteemi seiskumise.

Kõik tehtavad muudatused tuleb hoolikalt dokumenteerida ning tööd tuleb süsteemiadministraatorite vahel kooskõlastada. Vastavat dokumentatsiooni võib koostada nii paberversioonina kui ka süsteemis elektroonilise faili kujul. Dokumentatsiooni peaks ilmtingimata olema võimalik igal ajal lugeda ning seda peab olema võimalik ka värskendada (vt lisaks M 2.34 IT-süsteemi muutuste dokumenteerimine).

Täiendavad kontrollküsimused:

- Milliseid teenuseid kasutatakse IT-süsteemis?
- Kas kõik saadaolevad turvapaigad on korralikult installeeritud?
- Kas kõiki teatavaid muudatusi kajastatakse vahetult ka vastavas dokumentatsioonis ning kas muudatused kooskõlastatakse kõikide süsteemiadministraatorite vahel?
- Kas kõik operatsioonisüsteemi konfiguratsioonis tehtavad muudatused on dokumenteeritud selliselt, et pärast reinstalleerimist on võimalik neist ka aru saada?

M 4.106 Süsteemi logimise aktiveerimine (Unix)

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: administraator

Süsteemi enda Unix-logi *syslog* pakub võimalust registreerida infot, mida genereerib operatsioonisüsteem või rakendusprotsessid. Turbega seotud sündmusi nagu sisselogimiskatseid ehk käsu *su* tarvitamist tuleks kindlasti logida, et seda oleks võimlaik hiljem analüüsida.

Vajaminev deemon *syslogd* käivitatakse reeglina automaatselt ning selle konfigureerimiseks kasutatakse faili */etc/syslog.conf*. Volituste jagamisel tuleb vajalike ettekirjutustega tagada, et selle faili muutmise õigus oleks ainult administraatoritel, ning et logifaile asukohtades */var/log* ja */var/adm* oleks võimalik lugeda ainult süsteemiadministraatoritel. Kõik failis */etc/syslog.conf* tehtavad muudatused tuleb dokumenteerida. IT-süsteemi jaoks tehtava kohandamise käigus tuleks algselt logida kõike ning seejärel võib hakata vastavalt vajadusele erinevate valdkondade logisid välja lülitama. */var* -partitsiooni küllaldase dimensioneerimisega tuleb tagada, et logimisfunktsioonil oleks kasutada piisav salvestiruum. Järgnev konfiguratsioonifaili näide on koostatud SunOS-konfiguratsiooni baasil ning see defineerib erinevate failide põhjalikku logimist.

```
#ident “@(#)syslog.conf 1.3 93/12/09 SMI” /* SunOS 5.0 */
  #
  # Kõik teated saadetakse Loghost ’ile, mis tuleb defineerida failis
  # /etc/hosts.
  #
  # Eraldajana tuleb kasutada TAB’i!
  #
  # Test: . käivitage syslogd valikuga “-d”
  # . pärast antud faili igat muudatust käivitada syslogd kill -HUP’ga
  # . logifail peab eksisteerima juba enne käivitust/taaskäivitust
  # . /usr/ucb/logger ’abil on võimlaik genereerida test-teateid iga facility
  # ja priority jaoks
  #
  *.err;kern.warning;auth.err;daemon.err /dev/console
  *.alert;kern.err;daemon.err operator
  *.alert root
  # kuvab emerg-teateid terminalides (kasutab WALL’i)
  *.emerg *
  #
  kern.info ifdef(‘LOGHOST’, /var/log/kernlog, @loghost)
  user.info ifdef(‘LOGHOST’, /var/log/userlog, @loghost)
  mail.info ifdef(‘LOGHOST’, /var/log/maillog, @loghost)
  daemon.info ifdef(‘LOGHOST’, /var/log/daemonlog, @loghost)
  auth.info ifdef(‘LOGHOST’, /var/log/authlog, @loghost)
  lpr.info ifdef(‘LOGHOST’, /var/log/lprlog, @loghost)
```

```
news,uucp.info ifdef(‘LOGHOST’, /var/log/newslog, @loghost)
cron.info ifdef(‘LOGHOST’, /var/log/cronlog, @loghost)
#
## kõik ülejäänud “local” teated, oma programmide jaoks
local0,local1.info ifdef(‘LOGHOST’, /var/log/locallog, @loghost)
local2,local3,local4.info ifdef(‘LOGHOST’, /var/log/locallog, @loghost)
local5,local6,local7.info ifdef(‘LOGHOST’, /var/log/locallog, @loghost)
#
# kõik alarmid ja kõrgemad kirjutatakse eraldi faili:
*.err ifdef(‘LOGHOST’, /var/log/alertlog, @loghost)
#
# Näide Log levels:
# ——————————
# ‘su root’ failed for .. auth.err
# ROOT LOGIN REFUSED ON . . . auth.err
# ‘su root’ succeeded for.. auth.notice
```

Täiendavad kontrollküsimused:

- Kas failis */etc/syslog.conf* tehtud muudatused on dokumenteeritud?
- Kas on tagatud, et konfiguratsiooni on võimalik muuta ainult süsteemiadministraatoril?
- Kas on tagatud, et logifaile asukohtades */var/log* ja */var/adm* on võimalik lugeda ainult süsteemiadministraatoritel?

M 4.107 Tootja ressursside kasutamine

Algatamise eest vastutavad: IT-juht, IT turvaosakond

Rakendamise eest vastutavad: administraator

Kõik IT-süsteemide ja IT-komponentide tootjad pakuvad oma toodetele erinevaid tugi- ja infoteenuseid. Siia alla kuuluvad nt abi osutamine vigade kõrvaldamisel (tugi, infoliin, uuendid, paigad jne) ning võimalus hankida infot erinevate turvalahenduste kohta (WWW-lehed, uudisegrupid, meililistid jne). Mõned pakutavad võimalused on saadaval tasuta, mõned jällegi mitte. Juba IT-süsteemide ja IT-toodete soetamise käigus tuleks uurida, milliseid tootja pakutavaid tugiteenuseid oleks tarvis kasutama hakata, eriti neil juhtudel, kus sellised teenused toovad endaga kaasa jooksvad kulud. Tuleb tagada, et kõikide rakendatavate IT-süsteemide ja IT-toodete kohta uuritaks regulaarselt, kas tootja on nende kohta avaldanud uut infot võimalike turvalünkade ja nende kõrvaldamise kohta. Eriti oluline on seda nõuet järgida serveri operatsioonisüsteemide puhul, kuna võrreldes mõne üksiku IT-süsteemiga võib potentsiaalne turvalünk serveris endaga kaasa tuua palju suurema kahju.

Kui turvalisuse seisukohast kriitilise tähtsusega uuendid ei pärine otse tootja CD-ROMilt, tuleks need hankida ainult usaldusväärsetest allikatest, nt CERTidest (vt M 2.35 Teabe hankimine turvaaukude kohta). Juhul kui vastavaid faile pakutakse krüpteeritud või allkirjastatud versioonides, tuleks värskendusi kontrollida krüptograafiliste protseduuridega (nt protseduuridega SHA-1, RIPEMD-160, GnuPG), veendumaks, et neid pole manipuleeritud.

Tootja avaldatava turvainfo kättesaadavuse tagamiseks tuleks garanteerida, et kõikidest rakendatavatest operatsioonisüsteemidest ja kõikidest olulistest IT-toodetest säiliks vajalik ülevaade. Selles peaks olema kirjas, milliste WWW-aadresside alt tuleks otsida vastavaid turvavärskendusi ja paiku ehk tootjainfot. Vastavad aadressid on kirjas toodetega kaasasolevas dokumentatsioonis. Tihti viitavad ka tootjate veebilehed otse sellele infole. Veebilingid võivad aga tihti muutuda, mistõttu on oluline neid regulaarselt kontrollida ning vajaduse korral vastavat infot ka värskendada.

Kontrollküsimused:

- Millistest allikatest hangitakse tootjafirma turvapaiku?
- Kuidas tagatakse, et alati oleks käepärast informatsioon kõige värskemate turvapaikade kohta?
- Kuidas kontrollitakse süsteemide paigataset?
- Kas turvapaikade terviklust kontrollitakse krüptograafiliste protseduuridega?

M 4.109z Tööjaamade tarkvara reinstalleerimine

Algatamise eest vastutavad: IT-juht, IT turvaosakond
Rakendamise eest vastutavad: administraator

Töökohaarvutites võib tihti esineda probleeme operatsioonisüsteemide või rakendustega, mille kõrvaldamisega tuleb toime ainult kasutajatugi. Probleemide põhjused võivad peituda nt tarkvaravigades, konfiguratsiooni muutmises, uue tarkvara paigaldamises või arvutiviirustes. Liigse ajakulu vältimiseks tööjaamade haldamisel või vigade otsimisel, et kõrvaldada tööjaamadest eelpool kirjeldatud probleeme, tuleks standardse konfiguratsiooni taastamiseks ette võtta tarkvara taasinstalleerimine. Selle töö jaoks tuleb vastav arvuti esmalt üheselt identifitseerida ja seejärel vastavat dokumentatsiooni või programmi appi võttes välja selgitada, milline tarkvara tuleb sellesse arvutisse installeerida ning milline peab olema selle tarkvara konfiguratsioon. Siin on suureks abiks, kui süsteemid on suures osas üksteisega sarnased, vähemalt neis valdkondades, mis on seotud sarnaste tööülesannete täitmisega. Töökohaarvuti kõvaketas on soovitatav esmalt täielikult formaatida ning alles seejärel tuleks sinna uuesti installeerida kogu vajalik tarkvara ja andmed. Tarkvara on võimalik taasinstalleerida mitmel erineval moel, nt on võimalik kasutada ka spetsiaalseid programme, mis kirjutavad töökohaarvuti olemasoleva konfiguratsiooni üle serveril asuva etteantud konfiguratsiooniga. Siinkohal tuleb arvestada, et sellistele töödele kuluvat aega tuleb vaadelda küllaltki kriitiliselt ja seda kahel põhjusel: seadme uuesti kasutuselevõtmine peaks toimuma võimalikult kiiresti, et vastav IT-süsteem oleks jälle käideldav ning teiselt poolt tuleb tagada, et võrgule ei langeks liigset koormust. Eriti oluline on see koolituseks kasutatavate arvutite puhul ja ühiselt kasutatavate PC-kogudega.

Loomulikult võib taasinstalleerimistöid teha ka „käsitsi”. Sel otstarbel tuleks esmalt läbi viia standardne installeerimistöö. Seejärel tuleks kopeerida arvuti võimalikud eripärad, nagu spetsiaalsed seadmedraiverid, muud konfiguratsioonifailid või spetsiaalne tarkvara. Selleks peavad need aga juba eelkonfigureeritult valmis olema, nt võrgukeskkonnas või mobiilsetel andmekandjatel. Seejärel tuleb kasutada värskendatud viirusetõrjeprogrammi.

Kontrollküsimus:

- Kuidas toimub tööjaamade tarkvara reinstalleerimine?

M 4.113z Autentimisserveri kasutamine kaugpöördussüsteemis

Algatamise eest vastutavad: IT-turbespetsialist
Rakendamise eest vastutavad: administraator

Remote-Access-VPN 'ide (RAS-VPN'ide) kasutamisel tuleks kasutajate suure hulga korral kaaluda erinevaid võimalusi efektiivse kasutajahalduse ülesehitamiseks kaugpöörduse (ingl *Remote Access*) tarbeks. Reeglina tuleb iga RAS-kasutajale varustada süsteemis isikliku identiteediga (operatsioonisüsteemi kasutajakontoga) ning iga sellise kasutajakonto kasutamisel peab aset leidma kasutaja identifitseerimine ja autentimine. Mõningates operatsioonisüsteemides (uuemates Windowsi versioonides) on RAS-funktsioonid integreeritud juba ühise kasutajahaldussüsteemi alla. Keskmise ja suurte võrkude puhul, mis on töökorralduse poole pealt tihti jaotatud mitmeks alamvõrguks (domeenideks, haldusaladeks), eksisteerib tihti probleem, et kasutajate andmeid tuleb hallata igas haldusalas eraldi. Selleks, et ühe alamvõrgu alla kuuluvad kasutajad saaksid ka teist alamvõrku kasutada, tuleb rakendada kas ristvolitusi (*Cross* -sertifikaate, usaldussuhteid) või juurutada tsentraalset toimiv kataloogiteenus. Üheks täiendavaks alternatiiviks on veel võimalus, et kasutajatele luuakse teises alamvõrgus täiendav kasutajakonto, kuid selline lahendus raskendab kastjaandmete haldamist. RAS-kontekstis on välja töötatud spetsiaalseid autentimissüsteeme, mida on võimalik kasutada ka „tavalises" autentimisprotsessides süsteemidesse sisselogimisel. Tüüpilisteks näideteks on RADIUS, TACACS, TACACS+ ja teised LDAP-baasil töötavad kataloogiteenused.

Vastavad süsteemid on enamasti järgneva ülesehitusega:

- Kasutajate autentimisandmeid hallatakse tsentraalses serveris.
- Süsteemi sisselogimist võimaldav programm esitab kasutaja sisestatud autentimisandmete kontrollimiseks vastava päringu autentimisserverile.
- Sisselogimisprotsessi ja autentimisserveri vahel aset leidvas andmesides kasutatakse reeglina mõnda turvatud protokolli.

Selleks peab sisselogimise protsess toetama väliste autentimisserverite kasutamist. Lisaks peab sisselogimisprotsessi konfiguratsiooniandmetesse olema korrektselt sisestatud kasutatava autentimisserveri võrguaadress. Kasutaja, kes soovib ennast süsteemi sisse logida, peab suuresti lihtsustades läbima järgmised etapid, sõltumata sellest, kas ta kasutab sisselogimiseks RAS-ühendust või asub otse LANis:

- Kui ühenduse loomine leiab aset süsteemi või RASi sisselogimisprotsessi vahendusel, kontakteerub viimane autentimisserveriga ja informeerib seda kasutaja poolt laekunud soovist ühenduse loomise kohta. Autentimisserver

saadab sisselogimisprotsessile vastuseks nn *Challenge* 'i, juhul kui kasutatakse *Challenge-Response* -protseduuri ning protsess edastab selle kasutajale.
- Kasutaja identifitseerib ennast *VPN-Client* 'i suhtes nt vastava parooli või Token'i abil.
- Sisselogimisprotsess saadab autentimisandmed (tihti kasutaja jaoks nähtaval kujul) edasi autentimisserverisse.
- Autentimisserver kontrollib kasutajaandmete õigsust ja saadab sisselogimisprotsessile oma kontrolli tulemused.
- Juurdepääs võrgule (*access*) võimaldatakse siis, kui kontrollimine on osutunud edukaks.

Tsentraalselt töötavate autentimisserveritega on võimalik ühelt poolt saavutada autentimisandmete läbivalt ühtne haldamine ning teiselt poolt võimaldab see kasutusele võtta paremaid autentimisprotseduure kui operatsioonisüsteemide standardsed autentimismehhanismid. Eriti tuleks siinkohal mainida kiipkaartidel ja *Token* 'itel põhinevaid mehhanisme. Sõltuvalt süsteemist genereerivad need ühekordseid paroole, mida kuvatakse ekraanil ning mis tuleb kasutajal sisestada paroolina. Keskmistes ja suurtes võrkudes on eriti RAS-valdkonnas soovitatav võtta kasutusele eraldi autentimisserverid, kuna need suudavad pakkuda kasutajate autentimisel palju suuremat turvalisust. Siiski tuleb arvestada, et ka neid servereid on tarvis administreerida ja hooldada. Autentimisserver peab olema võrgukeskkonda paigutatud selliselt, et see oleks üheltpoolt hästi käideldav, kuid teiselt poolt peaks see olema ka piisavalt kaitstud volitamata juurdepääsude eest.

Täiendavad kontrollküsimused:

- Kas RAS-juurdepääsude ning süsteemi ja rakenduste juurdepääsude puhul on tagatud läbivalt ühtlane kasutajahaldus?
- Kas rakendatavad autentimisprotseduurid suudavad täita ettekirjutatud turvanõudeid?
- Juhul kui rakendatakse eraldiseisvaid autentimisservereid: kas vastavaid autentimisservereid käitatakse turvaliselt ning kas need on piisavalt kaitstud volitamata juurdepääsude eest?

M 4.114 Mobiiltelefonide turvamehhanismide rakendamine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: kasutajad

Mobiiltelefone ja sellega seotud pakutavaid teenuseid on võimalik erinevates valdkondades kaitsta kas PIN-koodide või paroolidega. Siia alla kuuluvad:

Juurdepääs SIM-kaardile
SIM-kaarti on võimalik kaitsta volitamata kasutuse eest nelja- kuni kaheksakohalise PIN-koodiga. Vastava PIN-koodi sisestamisega identifitseerib kasutaja ennast kaardi suhtes. Kui SIM-kaart peaks sattuma kellegi kätte, kes ei ole seda volitatud kasutama, on tal võimalik kaarti aktiveerida vaid juhul, kui ta teab ka sinna juurdekuuluvat PIN-koodi. SIM-kaartide väärkasutuse ärahoidmiseks tuleks seetõttu PIN-koodi küsimise funktsioon kindlasti kasutusele võtta, et telefoni sisselülitamisel tekiks kohustus sisestada PIN-kood. PIN-koodi ei tohiks hoida ühes kohas koos mobiiltelefoni või SIM-kaardiga. Tehasest lahkudes on mobiiltelefonidel PIN-koodi küsimine tihti välja lülitatud ning seadmetesse on salvestatud eelseadistatud PIN-kood. PIN-kood tuleks kindlasti ära muuta ja selle küsimine sisse lülitada juba esimese kasutuse käigus. Siin tuleks arvestada, et triviaalsete või liiga kergesti aimatavate PIN-koodide (1111, sünnikuupäev jne) valimist tuleks kindlasti vältida.

Teadmiseks
Enamike mobiiltelefonide nuppude all on lisaks numbritele ära toodud ka tähed. Tähti saab kasutada selleks, et valida endale PIN-koodide asemel hoopis oma paroolid, mida on võrreldes numbritega palju kergem meelde jätta, kuid ka siin kehtib muidugi põhimõte, et need ei tohiks olla liiga lihtsad. Näide: nt paroolile „4AUGEN“ (sks neli silma) vastab PIN-kombinatsioon „428436“.
Pärast kolmekordset vale PIN-koodi sisestamist SIM kaart lukustub. Lukustuse kõrvaldamiseks tuleb sisestada kaheksakohaline avamiskood. Vastavat koodi tähistatakse sageli kas mõistega PUK (PIN Unblocking Key) või Super-PIN. PUK-koodi kümnekordse sisestamise järel muutub SIM-kaart kasutuskõlbmatuks. PUK-kood antakse tavaliselt SIM-kaardiga kaasa ning see on ära märgitud samas koodiümbrikus koos PIN-koodiga. Seda tuleks hoida ülimalt hoolikalt ning kaitsta volitamata juurdepääsu eest. Mitte mingil juhul ei tohi hoida PUK-koodi ühes ja samas kohas koos mobiiltelefoniga.
Lisaks tavapärasele PIN-koodile eksisteerib veel ka PIN2, millega on võimalik tõkestada juurdepääs teatud SIM-kaardi funktsioonidele. Tihiti rakendatakse seda SIM-kaardi konfiguratsiooni kaitsmiseks, et kasutajad ei saaks seda ise muuta, nt teatud kasutuspiirangute kehtestamiseks. Samas võidakse sellega aga kaitsta ka nt firma telefoniraamatut, kehtestades piirangu, et täiendavaid sissekandeid saab teha ainult PIN2 sisestamisel. PIN2 koodil on oma avamiskood (PUK2).

Juurdepääs mobiiltelefonile
Lisaks eelnevale on paljudel juhtudel veel ka võimalik kasutada mobiiltelefoni enda turvakoodi (seadme PIN-koodi), et tõkestada juurdepääs teatud funktsioonidele.

Ka see kood tuleks võimalikult kiiresti ära muuta, st asendada võimalikult individuaalse väärtusega. See tuleks üles kirjutada ning seda tuleks kaitsta volitamata juurdepääsu eest. Seadme PIN-koodi ei pea ilmtingimata sisestama iga kord, kui mobiiltelefon sisse lülitatakse. Sellega võib nt tõkestada mobiiltelefoni kasutamist mõne muu SIM-kaardiga (vargusevastane kaitse). Moodsad mobiiltelefonid pakuvad lisarakenduste abil võimalust kaotuse või varguse korral mobiiltelefoni positsioneerida, kustutada selle andmeid või selle täielikult lukustada. Selleks tuleb valida sobiv rakendus ja see paigaldada. Seotud töötajaid tuleks selle rakenduse kasutamiseks koolitada.

Juurdepääs kõnepostile

Võrguoperaatori juures saab igale sides osalejale luua oma kõneposti, mida saab muuhulgas kasutada ka automaatvastajana. Kuna kõnepostile on võimalik juurde pääseda kõikjalt suvalist lõppseadet kasutades, tuleks seda volitamata juurdepääsu eest kaitsta PIN-koodiga. Kõneposti teenuse sisseseadmisel edastab võrguoperaator kasutajale eelseadistatud PIN-koodi. See tuleks võimalikult kiiresti ära muuta.

Täiendavad paroolid

Lisaks erinevatele eelnevalt kirjeldatud salajastele numbrikombinatsioonidele võib erinevates kasutusvaldkondades tekkida kokkupuude ka veel täiendavate paroolidega. Üheks selliseks näiteks on juurdepääs võrguoperaatori kasutajaandmetele. Näiteks infoliinile helistades ja telefoniarve kohta infot küsides võidakse küsida parooli. Tihti pannakse täiendava paroolkaitse alla ka tasulised teenused nagu infopäringud ja võrguoperaatori poolt tehtavad konfiguratsioonimuudatused. Ka need paroolid tuleks sarnaselt teiste paroolidega hoolikalt välja valida ja turvaliselt hoiule panna. Kõikvõimalike PIN-koodide ja paroolidega tuleks alati ümber käia võimalikult hoolikalt (vt M 2.11 Paroolide kasutamise reeglid).

Teadmiseks

Kurikaelad on viimasel ajal korduvalt katsetanud mobiiltelefonide kasutajate käest telefoni teel nende PIN- ka PUK-koode välja peilida, püüdes jätta endast muljet nagu oleks tegemist võrguoperaatori töötajaga kes helistab ja küsib infot, väites, et seda läheb tarvis mõne tehnilise defekti kõrvaldamiseks. Oma salakoode ei tohi mitte kunagi mitte kellelegi telefoni teel edasi anda!

Mobiiltelefonidele on välja töötatud palju erinevaid turvamehhanisme. Milliseid nendest kasutada, st milliseid nendest on võimalik aktiveerida, sõltub kasutatavast mobiiltelefonist, SIM-kaardist ja võrguoperaatorist. Sel põhjusel tuleks võrguoperaatorite turbega seotud pakkumisi ja seadmete kasutusjuhendeid enne valikut omavahel võrrelda. Firmatelefonide kasutamise puhul on soovitav tähtsamad turvaseaded kindlaks määrata eelseadistusega, millest tuleks veel omakorda koostada ka väike ülevaatlik andmeleht.

Mõned mudelid pakuvad võimalust kasutada ka parooliga kaitstud SIM-lukke. Nii saab nt takistada, et seadet on võimalik pärast vargust muu SIM-kaardiga probleemideta edasi kasutada. Lisaks võib SIM-lukuga takistada, et järelevalveta seadmesse sisestatakse potentsiaalse ohuga SIM-kaart.

Kontrollküsimused

- Kas mobiiltelefonide kasutamiseks on vajalikud turbemehhanismid välja valitud ja kas seadmetele on tehtud eelnevad konfiguratsioonid?
- Milliste turvamehhanismide kasutamine on mobiiltelefonide puhul muudetud kohustuslikuks?
- Kas kasutajaid on teavitatud vajalikest turbemehhanismidest mobiiltelefonide kasutamisel?

M 4.115 Mobiiltelefonide toite tagamine

Algatamise eest vastutavad: administraator, kasutaja

Rakendamise eest vastutavad: administraator, kasutaja

Mobiiltelefonide akud võivad seadet olenevalt telefoni võimsusest elektritoitega varustada piiratud aja jooksul, tavaliselt mõned tunnid. Selleks, et mobiiltelefonid oleksid vajaduse korral alati kasutusvalmis ning et andmed ei läheks muutmälust kaduma, tuleb järgida teatud raamtingimusi.

- Mobiiltelefoni hoiatavaid näitusid, mis informeerivad aku tühjenemisest, ei tohi ignoreerida.
- Kui on ette näha pikemaajalist mobiiltelefoni kasutamist, peaks kaasas olema akulaadija. Kui akulaadija ei ole saadaval, võib mobiiltelefoni vajaduse korral laadida ka PC või sülearvuti USB-liidese andmekaabli kaudu. See kestab üldjuhul oluliselt kauem kui akulaadijaga. Tuleb mõelda ka sellele, et selle laadimisvormiga on võimalik andmeühendus ja andmed võivad välja liikuda või võidakse neid muuta.
- Laadimise käigus tuleks järgida mobiiltelefoni kasutusjuhendis ära toodud soovitusi, eriti neid, mis käsitlevad aku pika kasutusaja tagamist.
- Mobiiltelefoni üleandmisel tuleb tagada, et aku oleks piisavalt laetud. Akude laetust tuleks regulaarselt kontrollida, sest akud tühjenevad aja jooksul ka siis, kui seadet ei kasutata.

Kui on ette näha mobiiltelefoni pikemaajalist kasutamist, nt töölähetustel, võib vajaduse korral kaasa võtta ka laetud varuaku. Varuakut tuleks hoida kaitsvas pakendis, et vältida kahjusid, mis võivad tekkida ülekuumenemisest või tulekahjust, kui aku kontaktid puutuvad kokku elektrit juhtivate materjalidega. Vastava õnnetuse võivad põhjustada ka täiesti igapäevased esemed nagu võtmed ja ketid. Kui akusid ei ole võimalik vahetada, nt selle tõttu, et see on kindlalt sisse ehitatud, võib kasutada ka väliseid akupakette.

Enne aku vahetamist tuleks mobiiltelefon välja lülitada, et mitte kahjustada selle mälu.

Mobiiltelefoni hoiutingimustes ei tohiks valitseda äärmuslikke temperatuure. Eriti vastuvõtlik on äärmuslike temperatuuride suhtes aku, kuid kahjustada võib saada ka mobiiltelefoni ekraan. Seoses sellega, et temperatuur võib autodes öö jooksul või päikese käes parkimisel päris palju kõikuda, ei tohiks mobiiltelefone ja akusid jätta pargitud autodesse.

Selleks, et kaitsta mobiiltelefoni akut, tuleks Bluetooth, IrDA, WLAN, GPS, ja mobiilside-internetiühendus aktiveerida ainult vajaduse korral.

Kontrollküsimused

- Kas mobiiltelefonide toite tagamiseks kasutati piisavaid turvameetmeid?

M 4.116 Lotus Notesi/Domino turvaline installimine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht
Rakendamise eest vastutab: administraator

Lotus Notesi/Domino turvaline installimine eeldab kasutuse raamtingimuste planeerimist, nagu on kirjeldatud meetmes M 2.206 Lotus Notesi/Domino kasutuselevõtu planeerimine . Seejärel installitakse Lotus Notesi/Domino komponendid vastavatesse serveritesse ja klientidesse. Selleks tuleb kindlaks määrata turvalised installimisprotseduurid ja installimiskeskkonna kaitsemeetmed, mis lähtuvad selle turbevajadustest, ning neid ka järgida. Siinkohal on mõistlik vahet teha installimisprotseduuridel, mis puudutavad kogu Lotus Notesi/Domino platvormi uut installimist, ning protseduuridel, mis on seotud kohandamise (software upgrades, patches) ja migratsiooniga.

Uus installimine
Lotus Notesi/Domino uuel installimisel tuleb turbe seisukohast arvestada järgnevaga.

1. Uute installimiste jaoks tuleb kindlaks määrata ja dokumenteerida asjakohased installimisprotseduurid. Selleks tuleb kehtestada nii üldkehtivad protseduurireeglid kui ka näiteks konkreetsed nõuded serverite, serveriteenuste ja klientide installimise kohta. Üldreeglite alla kuuluvad näiteks otsused selle kohta, kes peab algatama uusi installimisi ja kes vastutab nende eest, nõuded installimisprotseduuri kontrollimise ja kasutuselevõtu ning protseduurides kasutatavate konfiguratsioonide kohta (nt neljasilmapõhimõte) ning nõuded tarkvara kasutuselevõtu kohta igapäevastes tööprotsessides.
2. Kui installatsiooniprotseduuride jaoks on üldreeglid juba välja töötatud, saab siinkohal nendele viidata. Kuid ka neil juhtudel tuleb reegleid siiski täiendada, st lisada Lotus Notesi/Domino platvormi kajastavad eripärad.
3. Uute installimiste protseduur peab tagama, et kogu installimisprotsessi dokumenteeritaks piisavas mahus ja et selle kriitilisi osaetappe logitaks piisavalt detailselt. Seda dokumentatsiooni läheb hiljem tarvis installitud komponentide võimalike manipulatsioonide tuvastamiseks ja veaotsinguks.
4. Kui installimiseks kasutatakse automaatseid protseduure, tuleb installimisel kasutatud parameetrite, skriptide jms kohta koostada võimalikult detailne dokumentatsioon. Nii installipakettide kui ka installitavate komponentide kohta tuleb koostada sobiv kontrolli- ja kasutuselevõtuprotseduur.
5. Installimisprotseduuriga tuleb tagada, et pärast installimist oleks installitud kataloogi- ja failistruktuurile võimalik nii operatsioonisüsteemi kui ka haldustööriistade kaudu juurde pääseda ainult selleks volitatud administraatoritel. Selleks tuleb kohandada volituste struktuuri.
6. Domino serverite puhul tuleb tagada, et neile oleks juba alates installimisest füüsiline juurdepääs ainult volitatud administraatoritel ja hooldustehnikutel.
7. Sobiva alusinstallatsiooni väljavalimine: kuna Domino serverit saab rakendada erineval moel, ei tuleks installida mitte ükskõik milline, vaid kasutusvaldkonna jaoks kõige sobivam alusinstallatsioon. Valikusse kuuluvad näiteks eeldefineeritud Domino Utility Server (sõnumside teenusteta, mõel-

dud üksnes rakendusteserveriks), Domino Messaging Server (rakendusteenusteta, mõeldud üksnes sõnumside serveriks) ja Domino Enterprise Server (kõik teenused). Alusinstallatsiooni saab väga üksikasjalikult kohandada installimissuvandiga Customize Domino Server. Sobiva aluskonfiguratsiooni valimine ning selle üksikasjalik kohandamine planeeritud kasutusvaldkonnaga on muu hulgas ka turvalise konfiguratsiooni loomise ja süsteemi karastamise eeldused.

Kohandamine (upgrade) ja migratsioon

Kohandamise (upgrade) all mõistetakse siinkohal üksnes tarkvara kohandamist, st juba kasutatava Notesi/Domino redaktsiooni või üksikute tarkvarakomponentide, k.a Notesi/Domino platvormi jaoks juurde ostetud või enda arendatud komponentide kohandamist.

Migratsiooni all mõistetakse nii tarkvara kohandamist koos tööandmete muutmisega (nt andmehulkade vormingu muutmist, kasutatavate andmebaaside muutmist ja konsolideerimist) kui ka üleminekut mõne muu meili- ja koostööplatvormi kasutamiselt Lotus Notesi/Domino platvormi kasutamisele.

Lotus Notesi/Domino kohandamise (upgrade) ja migratsiooni puhul tuleb turbe seisukohast arvestada järgnevaga.

1. Kohandamise ja migratsiooni jaoks tuleb kindlaks määrata ja dokumenteerida asjakohased installimisprotseduurid
2. Kohandamiste (upgrade) jaoks võib kasutada uute installatsioonide tegemiseks mõeldud kohandatud, st lihtsustatud protseduure.
3. Migratsioonide puhul tuleb keskenduda ka tööandmete käideldavuse, konfidentsiaalsuse ja tervikluse tagamisele.
4. Suuremahuliste kohandamiste ja migratsioonide puhul saab Lotus Notesi/Domino platvormiga seotud töid teha etappide kaupa. Näiteks saab suletud domeene värskendada (update) ka ühekaupa (nt kontsernides või mitme asukohaga ettevõtetes), samuti võib töid teha kihtide kaupa, nt esmalt värskendada kliente ja seejärel serverikomponente. Kõikide protseduuride puhul, kus tööd on jagatud etappideks, võib tekkida oht, et vana ja uue redaktsiooni koostalitlusvõime võib kaduda, mistõttu tuleb neid töid planeerida väga hoolikalt, järgides tootja juhiseid. Kõikideks juhtudeks tuleb välja töötada ka ennistamisstrateegiad.
5. Tuleb arvestada, et pärast kohandamisi (upgrade) ja migratsioone tuleb kohandada ka installitud kataloogi- ja failistruktuuri, et Lotus Notesi/Domino operatsioonisüsteemi jaoks installitud elementidele pääseksid ligi ainult selleks volitatud administraatorid.
6. Et vältida olukordi, kus kasutajad avastavad, et pärast migratsiooni on süsteemis tekkinud ebasoovitud kõrvalmõjud, tuleb uute redaktsioonide muudetud tooteomadusi, eriti mis puudutab replikeerimist ja kliendipoliitikate pushmehhanisme, juba enne kontrollida ja hinnata.

Installimiskeskkonna ja installimisel kasutatavate andmekandjate turve Installimiskeskkondi ja installimiseks kasutatavaid andmekandjaid tuleb alati sobival

viisil kaitsta manipuleerimiste eest ja seda nii enne kui ka pärast installimist (vt M 4.177 Tarkvarapakettide tervikluse ja autentsuse tagamine). See kehtib eriti ka Lotus Notesi/Domino komponentide kohta. Protseduuridest on levinud näiteks installitavate serverite lahtiühendamine võrgust ja tootjafirma kontrollitud terviklusega originaalandmekandjate kasutamine installimisel. Kuna see kõik suurendab haldustööde mahtu ja ei pruugi (eriti suurte institutsioonide või ka tarnijate puhul) vastata levinud tavadele, võib võtta ka teistsuguseid turbemeetmeid. Siiski tuleb kindlasti ka sellise tarkvara puhul, mis hangitakse mitte originaalandmekandjatel, vaid elektroonilisi kanaleid pidi (nt allalaadimise, tootja automaatse tarkvaravärskenduse, meili teel), alati rakendada konkreetseid installimisprotseduure, mis tagaksid, et tarkvara terviklust kontrollitakse piisavalt.

Rakendatavate turbemehhanismide kvaliteet, nt tervikluse kontrollimiseks kasutatavad räsiväärtused, peavad vastama installitavate komponentide turbevajadusele.

Lotus Notesi/Domino tarkvara hankimiseks elektroonilisi kanaleid pidi pakub tootja HTTP-ga allalaadimise võimalust ja ka spetsiaalset allalaadimise apletti (Download Director). Viimane tagab suurema turbe ja vastab tootja sõnul ka infoturbe ühiskriteeriumitega (common criteria) tarkvara allalaadimisele kehtestatud nõuetele. Kuna tootja ise ühtki läbipaistvat mehhanismi komponentide tervikluse kontrollimiseks ei paku, tuleks Lotus Notesi/Domino tavapärasest suurema ja väga suure turbevajaduse korral võtta lisameetmeid, mis välistaksid allalaadimise kompromiteerimise. Tuleb tagada, et allalaadimise ajal oleks juurdepääs (ka administraatori juurdepääs) sihtkataloogile ja -ajamile välistatud ning et terviklust kontrollitaks vastavate räsiväärtustega (hash). Kui institutsioonis kasutatakse installimistarkvara hoidmiseks tsentraalseid lahendusi (installimisajameid, -servereid), tuleb nende lahenduste jaoks ette näha ka andmekandjate turbeastmele vastavad kaitsemeetmed. Siia alla kuuluvad muu hulgas juurdepääsu kaitsemeetmed ning terviklust ja käideldavust tagavad meetmed.

Kui see on tehniliselt ja halduslikult võimalik, tuleks nii installimisajameid kui ka installimisservereid kasutada üksnes piiratud aegadel, st eranditult ainult installimistöödeks.

Kriitilised protsessid installimisel, kohandamisel ja migreerimisel

Lotus Domino serveri installimisel kuulub kriitiliste tööde hulka oluliste tehniliste elementide koostamine domeeni- ja sertifikaadihierarhias, sest nende elementide kompromiteerimine võib viia kõikide Domino/Notesi turbemehhanismide kompromiteerimiseni. Turbe seisukohast tuleb arvestada järgnevaga.

1. Notesi ID-dele, mis selleks otstarbeks koostatakse (Certifier-ID, Server-ID-d, Administrator-ID-d), tuleb anda komplekssed pääsuparoolid.

2. Neid loetletud Notesi ID-sid ei tohi salvestada nime- ega ka aadressiraamatusse, vaid need tuleb salvestada failidesse, mida kaitstakse operatsioonisüsteemi turbemehhanismidega (nt operatsioonisüsteemi tasandil töötava juurdepääsukaitsega) ja täiendavate turvakomponentidega (nt hostil põhineva IDS-iga).
3. Kui Domino serveri puhul plaanitakse kasutada automaatkäivitust, ei tohi serveri ID jaoks rakendada paroolkaitset. Seetõttu tuleb serveri ID-d kaitsta operatsioonisüsteemi pääsumehhanismide ja seiremeetmetega, mis välistavad volitamata juurdepääsu.
4. Sertifikaadihierarhia elementide installimisel tuleb lähtuda Lotus Notesi/Domino domeeni- ja sertifikaadihierarhia kontseptsioonist (vt M 2.207 Lotus Notesi/Domino turvakontseptsioon). Olenevalt Lotus Notesi/Domino turbevajadusest tuleb siinkohal Certifier-ID puhul rakendada võib-olla ka neljasilmapõhimõtet, st mitmeosalist kasutajate vahel ära jagatud parooli.
5. Siinkohal tuleb arvestada, et Lotus Notesi/Domino sertifikaadihierarhiat kaitsvad tehnilised elemendid pole ette nähtud mitte üksnes tervikluse ja konfidentsiaalsuse, vaid ka käideldavuse tagamiseks. Näiteks tuleb kõikide oluliste ID-de (Certifier-ID, Server-ID, Administrator-ID) jaoks ette näha ka nende varukoopiate tegemine. Neid varukoopiaid tuleb hoida süsteemist eraldi ja koos juurdepääsukaitsega.

Laiendatud pääsukontrolli kasutamine (xACL)

Alates Lotus Notesi/Domino versioonist 6 on võimalik Domino kataloogis või laiendatud kataloogis (Extended Directory Catalog) kasutada laiendatud ACL-e (extended ACL või xACL). xACL-idega saab rakendada täiendavaid pääsukaitsevõimalusi, nt delegeerida organisatsiooniüksuste piires haldustegumeid, ja laiendatud kaitset NRPC-, HTTP-, LDAP-, POP3- ja IMAP-pöörduste jaoks. Nii saab nt takistada parooli räsiväärtuse väljalugemist isikudokumentidele tehtava HTTP-pöördusega failides names.nsf. Selleks vajalikke samme kirjeldatakse tootja väljaandes Technote 1244808. xACL-ide kasutust tuleb plaanida ja neid tuleb rakendada kõikide selliste Lotus Notesi/Domino süsteemide puhul, mille konfidentsiaalsust või terviklust puudutavad turbevajadused on kas tavapärasest suuremad või väga suured. xACL-ide aktiveerimisel tehakse süsteemis ACL-ide ANONYMOUS-grupi jaoks automaatselt sissekanne NO ACCESS. Kui ühtki xACL-i ei kasutata, tuleb Domino installatsioonis ANONYMOUS-grupile üldjuhul teha seadistus NO ACCESS. Kui mõnele andmebaasile on tarvis siiski anonüümset juurdepääsu lubada, tuleb see funktsioon eraldi andmebaasi tasandil tööle lülitada.

Kontrollküsimused:

- Kas (Lotus Notesi ja Lotus Domino) kliendi- ja serverikomponentide uute installimiste, kohandamiste ja migratsiooni jaoks on välja töötatud ja dokumenteeritud installimisprotseduurid?
- Kas installimisprotseduuride (k.a kohandamiste ja migratsiooni) puhul rakendatakse varem välja töötatud logimisprotseduure ning kas installatsioonidokumentidest ja -protokollidest tehakse varukoopiad ja kas need arhiveeritakse?
- Kas kõikide uute installimiste, kohandamiste ja migratsiooni puhul nimetatud kriitiliste protsesside jaoks on olemas detailsed nõuded?

- Kas on tagatud, et uute installimiste, kohandamiste ja migratsiooni ajal on juurdepääs asjakohastele kataloogidele ja ressurssidele ainult protsessis osalevatel administraatoritel?
- Kas installimiskeskkond ja installimisel kasutatavad andmekandjad on võimalike manipulatsioonide eest nii enne kui ka pärast installimisprotsessi piisavalt kaitstud?
- Kas laiendatud juurdepääsukontrolli (xACL) kasutamise otstarbekust on hinnatud ning kas seda kontrolli kasutatakse vastava turbevajaduse korral?
- Kas laiendatud juurdepääsukontrolli mittekasutamisel on Domino installatsioonis ANONYMOUS-grupi seadistuseks määratud NO ACCESS?

M 4.128 Lotus Notesi/Domino turvaline käitus

Algatamise eest vastutavad: infoturbespetsialist, IT-juht
Rakendamise eest vastutavad: administraator, erialaspetsialist

Lotus Notesi/Domino turvaline käitamine hõlmab kõiki Lotus Notesi/Domino platvormi funktsioonide töö tagamiseks vajalikke tegevusi. Nende hulka kuuluvad Lotus Notesi/Domino haldus, kohandamine ja migreerimine, regulaarne andmevarundus ja vajaduse korral ka andmete arhiveerimine ning käituse seire ja platvormi turvalisuse tagamisega seotud tegevused. Kohandamisele ja migreerimisele lähedasi tööprotsesse tuleb kasutada ka siis, kui teenuseid muudetakse väljaspool kohandamist ja migreerimist (nt seni kasutamata teenuste aktiveerimine, uute andmebaaside kasutuselevõtt). Siia kuuluvad ka dokumenteerimisnõuete järgimine (k.a süsteemis tehtud muudatuste logimine ja logi arhiveerimine) ning haldustegevuste jaoks ette nähtud kriitilistest nõuetest kinnipidamine (nt neljasilmapõhimõte või teenuste ja komponentide, nagu andmebaaside ja liideste kasutuselevõtu meetmed).

Käituskontseptsioon
Lotus Notesi/Domino turvaliseks käitamiseks on vaja käituskontseptsiooni, mis reguleerib piisavalt detailselt kõiki käitamise jaoks olulisi teemavaldkondi. Käituskontseptsioon peab viitama teistele käitamiseks olulistele kontseptsioonidele (vt M 2.207 Lotus Notesi/Domino turvakontseptsioon).

Andmevarundus
Regulaarne andmevarundus on osa turvalisest käitusest, mistõttu tuleb andmevarunduse kohustus dokumenteerida andmevarunduse kontseptsioonis. See ei ole hädaolukorraks valmisoleku plaani osa, vaid tegemist on platvormi regulaarse käitusprotsessiga, mis tuleb siiski hädaolukorraks valmisoleku plaaniga kooskõlla viia. Kui sedasama andmevarunduslahendust kasutatakse ka arhiveerimiseks, tuleb andmevarunduse kontseptsioon kooskõlastada meetmes M 2.207 Lotus Notesi/Domino turvakontseptsioon .

Kuna Lotus Notes/Domino hoiab infot (nii kasutajaandmeid kui ka siseseid haldusandmeid, konfiguratsiooniandmeid, logi jms) enda andmebaasides, peab andmevarunduse kontseptsioon peale konfiguratsioonifailide (nt notes.ini) hõlmama ka vastavate andmebaaside varundamist. Andmebaaside turbe üldsoovitused leiate meetmest M 6.49 Andmebaasi varundamine .

Arvestada tuleb Lotus Notesi/Domino platvormi iseärasustega:

1. Alates Domino redaktsioonist 5 ja ODS (On-Disc Structure) 41-st toetab Lotus Notes/Domino andmebaasitehingute logimist. See ei ole oluline mitte ainult laiendatud inkrementaalse andmevarunduse tõttu, mis rakendab tehingulogide salvestamist ja järeltöötlust, vaid ka kahjustatud andmebaaside

parandamise seisukohast, milleks kasutatakse tehingulogisid ja varundatud andmete paigaldamist.

2. Tehingute logimine tuleb sisse seada kõikides käideldavuse või tervikluse suhtes suure turbevajadusega andmebaasides ja eelkõige Lotus Notesi/Domino süsteemiandmebaasides. Seejuures tuleb vajaduse korral konfigureerida logimistüübi, kahjustatud andmebaaside automaatse parandamise ning töötamise ja taaskäivitamise jõudlusparameetrid.
3. Domino uuemates versioonides on võimalik Lotus Notesi/Domino andmebaase paigutada DB2 andmebaasi sisse ja Lotus Notesi/Domino platvormi kaudu neile juurde pääseda. Selle võimaluse kasutamisel peab Lotus Notesi/Domino süsteemi turvakontseptsioon sisaldama ka kasutatava DB2 andmebaasi turvet.
4. Mahukate sõltuvussuhetega keerukates käituskeskkondades, mis võivad tekkida näiteks replikeerimisel, ei tohiks andmetest varukoopiaid teha käsitsi, vaid selleks
5. tuleks kasutada asjakohaseid varundustööriistu. Varundatava platvormi tootja tarkvaratööriistad (siin Tivoli Storage Manager ja Tivoli Data Protection for Domino) on tihti kohandatud platvormi iseärasustega, mistõttu on ühildumatuse risk väiksem kui teiste tootjate tööriistade puhul.

Lotus Notesi/Domino platvormi rakenduste väljatöötamine

Kui Lotus Notesi/Domino platvormi tarbeks töötatakse välja rakendusi, kuuluvad platvormi turvalise käitamise juurde ka meetmed rakenduste ülevõtmiseks käitusprotsessi.

Need meetmed ei pea tagama mitte ainult rakenduste õiget vormilist üleandmist, vaid ka seda, et turve oleks tagatud juba rakenduste väljatöötamisel.

Enda välja töötatud tarkvaraga Lotus Notesi/Domino süsteemi tuleb turvata teisiti kui standardsüsteemi, eelkõige on vaja arvestada selliste teemadega nagu „Vana süsteemi jäägid” ja „Enda välja töötatud rakenduste kasutuselevõtt”. Nagu tavaliselt kombeks, tuleb ka Lotus Notesi/Domino platvormi puhul arendus- ja katsetuskeskkond, kvaliteedi tagamise keskkond ning tootmiskeskkond üksteisest sobivalt eraldada. Arendus- ja katsetuskeskkonna ning kvaliteedi tagamise keskkonna jaoks on võimalik kasutada Lotus Notesi/Domino platvormi virtualiseerimist, mille tulemusena vähenevad ka litsentsikulud (vt M 2.393 Infovahetuse reguleerimine). Olenevalt kaitsevajadusest võib eraldamiseks piisata ka üksnes virtualiseerimisest. Keskkondade eraldamisel tuleb võtta arvesse, et arendusklientidega (Domino Designer) ei tohi juurde pääseda tootmiskeskkonnale. Kui tootmise tõttu on erandkorras vaja tagada arendaja juurdepääs tootmiskeskkonnale, peavad käituskontseptsioonis olema kindlaks määratud protseduurid, mis tagavad vastava juurdepääsu seire ja piisava kvaliteedi.

Juurdepääs peab toimuma läbipaistvalt ja olema logi abil mõistetav. Meetmed enda välja töötatud rakenduste ülevõtmiseks tootmissüsteemi peavad tagama järgmist:

1. vastutavad isikud peavad rakenduse ametlikult vastu võtma;
2. rakenduse jaoks tuleb teha piisaval hulgal spetsiaalseid valdkonna-, integratsiooni- ja jõudluskatsetusi;
3. tootmiskeskkonda sisestatud objektid peavad ühtima katsetatud objektidega;
4. tootmiskeskkonda sisestatud objektides ei tohi olla kahjurvara (vt ka B 1.6 Viirusetõrje kontseptsioon);
5. arendamise käigus peab olema arusaadavalt kasutatud Lotus Notesi/Domino platvormi rakenduste väljatöötamise suuniseid (vt M 2.207 Lotus Notesi/Domino turvakontseptsioon).

Lotus Notesi/Domino platvormi jaoks juurde ostetud rakendustele peaksid võimaluse korral kehtima samad kvaliteedinõuded mis enda välja töötatud rakendustele, kusjuures rakenduste väljatöötamise suunise järgimise nõue tuleb asendada vastavate tootjaandmete ja sertifikaatidega.

Rakenduste integreerimine Lotus Notesi/Domino platvormiga
Rakenduste integreerimine Lotus Notesi/Domino platvormiga (vt M 2.493w Litsentsihaldus ja litsentsiaspektid Lotus Notesi/Domino soetamisel) võib platvormi käitamise turvanõudeid täielikult muuta. Rakenduste integreerimine klientprogrammiga võib suurendada Lotus Notesi kliendi kõigi kolme baasväärtuse turbevajadust. See hõlmab ka spetsiaalseid integreerimiskomponente, nt koos SAP-ga välja töötatud Alloyd, millega saab Lotus Notesist SAP-süsteemidele juurde pääseda. Enamasti mõjutab see ka Notesi kliendi konfiguratsiooni ja kasutamist. Kliendi turvalise konfiguratsiooni loomisel tuleb arvestada meetmega M 4.229 Nutitelefonide, tahvel- ja pihuarvutite turvaline kasutamine . Platvormi turvalist käitamist tuleb laiendada kliendi logimise ja analüüsiga, mille keskmes on kliendiga integreeritud rakendused. Rakenduste integreerimiseks serveris saab näiteks Notesi andmete jaoks rakendada DB2 andmebaasi või spetsiaalseid integreerimiskomponente.

Peale nende leidub veel teisigi integreerimislahendusi, nt Domino DIIOP teenus, Domino XML (DXL) ja Domino JSP, mis toetavad eelkõige integreerimist Websphere'i vahevaraga. Selle käsitluse alla kuulub ka institutsiooni või teenusepakkuja veebiteenuste kasutamine Lotus Notesi/Domino vastava liidesega.

Rakenduste integreerimine serveris suurendab Notesi/Domino rakenduste ja teenuste kaitsevajadust vastavalt sellele, milline on integreerimise teel lisatavate rakenduste ja teenuste kaitsevajadus. Sellega tuleb arvestada nii Domino serveri teenuste konfigureerimisel serveris (vt M 1.1 Vastavus normidele ja eeskirjadele) kui ka seiratavate parameetrite ja sündmuste kindlaksmääramisel.

Samuti tuleb kohandada logimiseks vajalikke parameetreid, mida kirjeldatakse meetmes M 4.427 Lotus Notesi/Domino turbe seisukohalt oluline logimine ja analüüs . Rakenduste integreerimist tuleb seega käsitleda kontseptsioonina, nt rakenduste integreerimise suuniste koostamisega meetme M 2.207 Lotus Note-

si/Domino turvakontseptsioon . Suuniste järgimist tuleb integreeritava lahenduse ülevõtmisel tootmiskeskkonda ka kontrollida. Kui Lotus Notesi/Domino (või selle üksikute komponentide) käitamine on väljast tellitud, jääb turvalise käitamise vastutus väljast tellivale institutsioonile, seevastu turvaliseks käitamiseks vajalike eeskirjade järgimise eest vastutab institutsioon ja/või üks või mitu teenusepakkujat.

Väljasttellimise ja osalise väljasttellimise jaoks vajalikke spetsiaalseid turvameetmeid kirjeldatakse IT etalonturbe moodulis B 1.11 Väljasttellimine (Outsourcing) .

Kohandamine ja migreerimine käitamise ajal
Lotus Notesi/Domino turvaliseks käitamiseks tuleb järgida meetmes M 4.116 Lotus Notesi/Domino turvaline installimine esitatud märkusi kohandamise ja migreerimise kohta.

Haldustegevus
Haldusprotsessis tuleb võimaluse korral alati lähtuda halduskäsiraamatust, mis sisaldab meetmes M 2.206 Lotus Notesi/Domino kasutuselevõtu planeerimine nimetatud haldustegevuste dokumentatsiooni. See on hea vahend kriitiliste haldustegevuste piisava kvaliteedi tagamiseks eelkõige väljasttellimise korral.

Halduskäsiraamatu detailsus sõltub Lotus Notesi/Domino platvormi kaitsevajadusest.

Haldustegevuste puhul tuleb tagada halduskäsiraamatu järgimine.
Seda võib teha institutsioonisisese suunise kehtestamisega, väljast tellitavate haldustööde korral saab need teenuslepingutesse kirja panna.

Seire käitamise ajal
Lotus Notesi/Domino platvormi käitamise ajal peab rakendama ka seiret. Lotus Notesi/Domino platvormi turvaliseks käitamiseks olulisi lisaaspekte kirjeldatakse meetmes M 4.427 Lotus Notesi/Domino turbe seisukohalt oluline logimine ja analüüs .

Lotus Notesi/Domino kasutamine üleinstitutsioonilise identiteedihalduse süsteemina Lotus Notesi/Domino sertifikaadihierarhiat (PKI) on võimalik kasutada üleinstitutsioonilise identiteedihalduse alusena. Enamasti avaldab see suurt mõju Lotus Notesi turbevajadusele, sest identiteedihaldus moodustab tavaliselt keskse volituste haldussüsteemi tuuma. Selline olukord nõuab käituses enamasti rangelt turvatud baasväärtustega eraldi Domino serverit, mis võimaldab kasutada vajalikke teenuseid. Lotus Notesi/Domino kasutuselevõtule sertifikaadihierarhia alussüsteemina peab eelnema planeerimine, mida kirjeldatakse meetme M 2.206 Lotus Notesi/Domino kasutuselevõtu planeerimine punktides „Süsteemiarhitektuur

ja selle turbeaspektid", „Lotus Notesi/Domino roll üleinstitutsioonilises identiteedihalduses" ning „Domeenide ja sertifikaatide hierarhia planeerimine".

Käitamise vaatepunktist tuleb sertifikaadihierarhia teenuseid osutava serveri suurendatud turbevajadust võtta arvesse eelkõige sertifikaadihierarhiaga seotud haldusprotsesside ning seire, logimise, analüüsi ja arhiveerimise puhul.

Lotus Notesi/Domino sidumine välise keskse identiteedihaldusega
Notesi/Domino sidumine välise keskse teenusepakkuja identiteedihaldusega (nt Oracle Identity Manager, Microsoft Identity and Access Management, Novell eDirectory) või tootja enda identiteedihaldusega (IBM-i Tivoli Identity Management) muudab Lotus Notesi/Domino sertifikaadihierarhia turbevajadust. Välise identiteedihaldusega ühendust tagava liidese baasväärtuste turbevajadus on tavaliselt suur (oleneb Lotus Notesi/Domino platvormi turbevajadusest). Seda tuleb tööprotsesside, eelkõige halduse, seire, logimise ja analüüsi puhul kindlasti arvesse võtta. Meetme M 6.73 Hädaolukorraplaani koostamine Lotus Notes süsteemi tõrgete puhuks võtmisel tuleb arvestada ka välise identiteedihalduse või välise identiteedihalduse ühenduse rivist väljalangemisega.

Kontrollküsimused:

- Kas Lotus Notesi/Domino platvormi jaoks on olemas dokumenteeritud käituskontseptsioon või sellega võrreldav käitusdokumentatsioon
- Kas andmevarunduse kontseptsiooni puhul on arvestatud turvatava andmebaasi suuruse ja keerukusega?
- Kas Lotus Notesi/Domino keskkonna rakenduste kasutuselevõtu nõuded on dokumenteeritud?
- Kas käitamisega seotud peamistele haldustegevustele kehtivad nõuded on dokumenteeritud?
- Kas CA-protsessi (sertifitseerimisprotsessi) käitavates Domino serverites rakendatakse vastava Domino sertifikaaditaristu kasutamisel ka seiret ja logimist?
- Kas Domino CA (sertifitseerimiskeskuse) kasutamisel teiste rakenduste jaoks väljaspool Lotus Notesi/Domino platvormi arvestatakse Lotus Notesi/Domino suurenenud turbevajadusega?
- Kui Lotus Notes/Domino on ühendatud mõne välise keskse identiteedihaldusega, siis kas seda arvestatakse ka käituskäsiraamatus?

M 4.132 Lotus Notes'i süsteemi seire

Algatamise eest vastutavad: infoturbespetsialist, IT-juht
Täideviimise eest vastutab: administraator

Lotus Notesi/Domino platvormi asjakohane seire aitab tagada vajalikku turvet reaalses tööolukorras. Seire abil saab tuvastada väärfunktsioone ja ründeid. Olenevalt Lotus Notesi/Domino platvormi turbevajadusest tuleb sisse seada sobiv seire ja see asjakohasel viisil dokumenteerida, nt käituskontseptsioonina, nagu kirjeldatakse meetmes M 4.128 Lotus Notesi/Domino turvaline käitus . Lotus Notesi/Domino platvormi seireks võib kasutada välist seiretarkvara, mis kontrollib olulisi parameetreid ja protsesse võrgus, operatsioonisüsteemis ning mõnel juhul ka rakenduses.

Seireks kasutatavat tarkvaratööriista ja kontrollitavat rakendust on üksteisega võimalik tugevalt integreerida enamasti siis, kui kasutatakse sama tootja tarkvaratööriistu (Tivoli tooteperekond). Oma panuse võivad seiresse anda ka erinevad turvakomponendid, nt turvalüüsid, IDSsüsteemid, Content Security seadmed. Siin on tarvis, et turvakomponentide eest ja Lotus Notesi/Domino käitamise eest vastutavad töötajad teeksid omavahel koostööd. Lotus Notesi/Domino platvorm võimaldab kasutada seirefunktsioone nii domeenis (Domino Domain Monitoring) kui ka serveris (Domino serveri seire ja Server Health Monitoring, milleks kasutatakse IBM-i Tivoli Analyzeri baasfunktsioonide integreerimist). Seire võib toimuda ka serveri-, administraatorikonsooli ja Domino Server Monitori kaudu.

Lisaks pakub platvorm mitmesuguseid jõudlust parandavaid seirefunktsioone, nt Domino Configuration Collectorit. Fault Recovery võimaldab kasutada mehhanisme, mis toetavad rikke korral automaatset taastamist ja taaskäivitumist. Selle funktsiooni kasutamine nõuab laiaulatuslikku kontseptsiooni ja parameetrite hoolikat seadistamist.

Täiendavad kontrollküsimused:

- Kas Lotus Notesi/Domino keskkonna käitamise seireks kasutatakse sobivaid seiremehhanisme või -tööriistu? ·
- Kas seiremehhanismide parameetrid on dokumenteeritud?

M 4.133z Sobivate autentimismehhanismide valimine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator

IT-süsteemide identifitseerimis- ja autentimismehhanismid peavad olema sellised, mis lubaksid kasutajaid üheselt identifitseerida ja autentida. Kõigepealt peab aset leidma kasutaja identifitseerimine ja autentimine ning alles seejärel tohib olla kasutajal võimalik IT-süsteemi kasutada. IT-süsteemi kasutamine peab olema võimalik alles pärast kasutaja edukat identifitseerimist ja autentimist.

Autentimisinfo peab olema salvestatud selliselt, et sellele oleks juurdepääs ainult volitatud kasutajatel. IT-süsteemi peab kõikide protsesside puhul olema võimalik tuvastada, milline kasutaja selles osaleb.Enne kasutajaandmete edastamist tuleb sidepartner (arvuti, protsess või kasutaja) üheselt identifitseerida ja autentida.

Kasutajaandmeid tohib edastada alles pärast seda, kui identifitseerimine ja autentimine on edukalt läbitud. Andmete vastuvõtmisel peab olema võimalik nende saatjat üheselt identifitseerida ja autentida. Kõiki autentimisandmeid tuleb kaitsta volitamata juurdepääsu ja võltsimise vastu. Kasutaja autentsuse tõestamiseks on erinevaid tehnikaid.

Tuntumad nende hulgast on järgmised:

- PIN-koodid ehk personaalsed identifitseerimisnumbrid
- Paroolid
- Token 'id, nt pääsukaardid
- Biomeetria

Turbe seisukohast kriitilistes valdkondades tuleks rakendada tugevaid autentimismehhanisme, mille puhul kombineeritakse omavahel kahte autentimistehnikat nagu nt parooli ja tehingunumbrit (ühekordset parooli) või parooli ja kiipkaarti.

Seetõttu nimetatakse seda tihti ka kahefaktoriliseks autentimiseks. Mõlemad kasutatavad lahendused peavad vastama kaasaja tehnilistele nõuetele. Järgnevalt esitatakse erinevad valikukriteeriumid, mida tuleks järgida identifitseerimis- ja autentimismehhanismide valimisel. Mitte kõik turustatavad tooted ei suuda täita kõiki kriteeriume, kuid oma kontekstis tuleks neid siiski arvestada. Paljud IT-tooted, nt operatsioonisüsteemid, sisaldavad lisaks oma põhifunktsioonile veel ka autentimismehhanisme. Siin tuleks kontrollida, kas vastavad pakutavad mehhanismid suudavad täita vajalikke nõudmisi, või on neid võib-olla tarvis lisafunktsioonidega täiendada. Ka selleks otstarbeks sobib kasutada käeolevaid valikukriteeriume.

Autentimisandmete haldamine

Autentimismehhanismil peavad olema turvafunktsioonid, mis võimaldaksid koostada ja muuta kasutajate autentimisandmeid. Sellistele funktsioonidele tohib olla juurdepääs ainult volitatud administraatoritel. Paroolide kasutamisel peaks volitatud kasutajatel olema võimalik oma autentimisinfot etteantud piirides muuta.

IT-süsteem peaks olema varustatud turvatud mehhanismiga, mis lubaks kasutajal muuta oma paroole iseseisvalt. Selle raames peaks olema võimalik määrata

paroolidele minimaalne kasutusiga. Pärast edukat sisselogimist tuleks kasutajale kuvada info tema viimase eduka sisselogimise aja ja koha kohta.

Autentimisandmete kaitsemine muudatuste eest

IT-süsteem peab suutma autentimisandmeid töödeldes neid kogu aeg kaitsta võimaliku nuhkimise, muutmise ja hävitamise eest. See võib olla lahendatud nt paroolifailide krüpteerimisega ja sisestatavate paroolide kirjapildi varjamisega.

Autentimisandmeid tuleb salvestada rakendusandmetest eraldi.

Süsteemi tugi Üleorganisatsiooniliste autentimisprotseduuride kasutamisel tuleks vastavaid lahendusi käitada ainult serveritel, mille operatsioonisüsteemid suudavad pakkuda adekvaatset kaitset võimalike manipulatsioonide vastu. Autentimisprotseduuride valimisel tuleks pöörata tähelepanu sellele, et neid saaks rakendada võimalikult paljudes platvormides.

Autentimisel tekkivate vigade käsitlemine

IT-süsteem peaks suutma pärast kindlat arvu ebaõnnestunud sisselogimiskatseid vastava sisselogimisprotseduuri sulgeda. Pärast ebaõnnestunud sisselogimiskatset peab IT-süsteem suutma vastava kasutajakonto ehk terminali sulgeda või selle ühenduse katkestada. Pärast ebaõnnestunud sisselogimiskatseid peaks IT-süsteem suutma kehtestada uutele sisselogimiskatsetele progresseeruvaid ajalisi piiranguid (time delay). Sisselogimisprotsessi maksimaalset kestust peab olema võimlaik piirata.

Kasutajaandmete haldamine

IT-süsteem peaks suutma siduda kasutajaid erinevate eelseadistustega. Vastavaid seadistusi peab olema võimalik kuvada ja muuta. Kasutajaandmete muutmise võimalust peab saama piirata, lubades seda teha ainult volitatud administraatoritel. Juhtudel, kus kasutajaandmete haldamine peaks toimuma läbi mõne sideühenduse, tuleb seda piisavalt krüptograafiliselt kaitsta.

Kasutaja sissekannete defineerimine

IT-süsteem peab võimaldama turvapoliitika ellurakendamist, st peab võimaldama valida igale kasutajale tema jaoks sobivat turvaseadistust.

Autentimisprotseduuri peab olema võimalik ka laiendada, nt võtta täiendavalt kasutusele tugevaid autentimisprotseduure nagu Token 'eid või kiipkaarte (vt M 5.34z Ühekordsed paroolid).

Kasutajaandmete maht

Lisaks kasutajanimedele ja õiguste profiilidele tuleks kasutajate kohta koguda veel ka muud infot (vt lisaks M 2.30 Kasutajate ja kasutajarühmade määramise protseduurid):

- Kasutajahalduses peaks olema üles märgitud vähemalt kasutaja eesnimi ja perenimi. Lisaks on palju abi ka võimalikust telefoninumbrist ja töökabineti numbrist.
- Selleks, et kasutajaga ühendust võtta, tuleks täiendavalt kajastada ka kontaktinfot nagu meiliaadressi, telefoniumbrit ja tema geograafilist asukohta (aadressi, töökabineti numbrit).

- Lisaks peaks olema ära märgitud ka see, kui pikalt peaks vastava kasutajatunnus kehtima. Kui kasutajatunnus on aegunud, tuleks see sulgeda.

Parooli kvaliteet

Juhtudel, kus paroole kasutatakse autentimiseks, peaks IT-süsteem olema varustatud selliste mehhanismidega, mis täidaksid järgmisi nõudeid (vt M 2.11 Paroolide kasutamise reeglid):

- Tagatakse, et iga kasutaja rakendab vaid isiklikke paroole (koos võimalusega neid ise ka välja valida).
- Kontrollitakse, et kõik paroolid vastaks kehtestatud nõuetele (minimaalse pikkuse järgimine, triviaalsete paroolide vältimine). Parooli kvaliteedi kontrollimist peaks saama individuaalselt reguleerida. Näiteks peaks saama kehtestada ettekirjutusi, et parool peab sisaldama vähemalt ühte viitemärki või keelata teatud tähemärgikombinatsioonide kasutamist.
- IT-süsteem genereerib paroolid, mis vastavad määratletud ettekirjutustele.

Süsteem peab nõuetekohaseid paroole kasutajale välja pakkuma.

- Süsteem peaks kohustama kasutajat regulaarselt parooli muutma. Parooli kasutusiga peab olema reguleeritav.
- IT-süsteem peaks takistama vanade paroolide kasutamist parooli vahetamisel (paroolide ajalugu).
- Parooli sisestamisel ei tohi parool arvutiekraanil näha olla.
- Pärast installeerimist ja kasutajate uuesti sisseseadmist peaks paroolisüsteem nõudma kasutajalt kohustuslikus korras, et see muudaks oma parooli kohe pärast esmakordset sisselogimist.

Biomeetria

Biomeetria all peetakse antud kontekstis silmas isikute automaatset tuvastamist nende kehaliste tunnuste alusel. Biomeetriliste protseduuride rakendamiseks autentimise eesmärgil läheb tarvis täiendavaid lõppseadmeid, mis suudaksid kasutajaid nende iseloomulike tunnuste alusel üheselt tuvastada.

Autentimiseks on võimalik korraldada nii ühe kui ka korraga mitme järgmise biomeetrilise tunnuse põhjal:

- Iiris
- Sõrmejälg
- Näoproportsioonid
- Hääl ja kõneomadused
- Käekiri
- Arvuti klaviatuuri kasutamine

Lisaks suurele hulgale biomeetrilistele tunnustele ja nendel põhinevatele biomeetrilistele protseduuridele eksisteerivad lisaks ka veel suured erinevused konkreetsete saadaolevate biomeetriliste süsteemide ja toodete vahel. Biomeetriliste

kontrolliprotseduuride tööjõudlus on väga erinev. Turvalisuse seisukohast kriitilistes valdkondades tuleb tähelepanu pöörata sellele, et vastav biomeetriline süsteem suudaks pakkuda vastuvõetavat tuvastusprotseduuri, millega kaasneks ka kõrge turvalisus. Selliste süsteemide puhul ei tohi olla võimalik, et igasugused järeleaimamised (nt näomaskid, vahast tehtud sõrmekujutise koopias, sobiva iirisemustriga kontaktläätsed vms) saaksid süsteemi mingil viisil üle kavaldada.

Autentimine Token 'itega

Üks täiendav alternatiiv on autentimiseks kasutatavad Token 'id ehk käepärased andmekandjad, mida kasutatakse turvalise salvestina autentimiseks vajaliku info nagu nt krüptograafiliste võtmete talletamiseks. Tüüpilised näited vastavate Token 'ite kohta on kiipkaardid, USB-mälupulgad või pihuarvutisarnased seadmed ühekordsete paroolide genereerimiseks.

Autentimismehhanismide nõuded kasutajatele

Enne kasutaja iga tegevust peab IT-süsteem kontrollima vastava kasutaja identiteeti. Lisaks peab IT-süsteem suutma takistada kasutajate andmete uuesti sisselugemist, suutma tuvastada võltsitud ja kopeeritud kasutaja autentimisandmeid ning takistama nende kasutamist. IT-süsteem tohib kasutajaandeid kontrollida alles pärast nende täies mahus sisestamist. Iga kasutaja jaoks peab saama eraldi seadistada, millal ja millistest asukohtadest lubatakse tal vastavat IT-süsteemi kasutada.

Autentimismehhanismide logimine

Autentimisega seotud protsesse tuleks mõistlikus ulatuses logida. Administraatorid peaksid logifaile regulaarsete ajavahemike tagant analüüsima.

IT-süsteem peab suutma logis kajastada järgmisi sündmusi:

- Logimisfunktsiooni sisse- ja väljalülitamine.
- Kõiki autentimisandmete haldust võimaldavatele mehhanismidele tehtud ligipääsemiskatseid.
- Edukaid katseid juurdepääsu loomisel autentimisandmetele.
- Kõiki katseid, kus on püütud kasutajate autentimisinfole volitamata juurde pääseda.
- Kõiki katseid, kus on püütud kasutaja-sissekannete haldamisfunktsioonidele volitamata juurde pääseda.
- Kasutajasissekannete muutmised.
- Kõiki teste, mis on sooritatud paroolide kvaliteedi kontrollimiseks.
- Igat autentimismehhanismide kasutust.
- Igat konfiguratsiooni, mis on loodud autentimismehhanismide taasloomiseks spetsiifiliste autentimissündmuste tarbeks.
- Autentimismehhanismide installeerimine.

Iga logi peaks sisaldama kuupäeva, kellaaega, sündmuse liiki, subjekti nimetust ning infot selle kohta, kas vastav tegevus osutus edukaks või ebaedukaks.

Kontrollküsimused:

- Milliseid autentimismehhanisme kasutatakse?

- Milliste kriteeriumite alusel toimus nende väljavalimine?

M 4.134z Sobivate andmevormingute valimine

Algatamise eest vastutavad: IT-juht
Rakendamise eest vastutavad: IT-juht, kasutajad

Erinevate IT-rakenduste jaoks on välja töötatud suur hulk erinevaid andmevorminguid. Reeglina ei ole need kõik aga omavahel sugugi ühilduvad, st pole ükskõik, millist andmevormingut kasutada. Kahjuks ei suuda isegi paljud ühe ja sama kasutusvaldkonna (nt tekstitöötlussüsteemide) IT-rakendused kasutada vastastikku sarnaste toodete andmevorminguid. Probleem suureneb veel seeläbi, et paljud rakendusprogrammid ei suuda pärast versioonivahetust töödelda enam oma eelkäija andmeformaate. Seetõttu tuleb uute rakendusprogrammide soetamisel esmalt kontrollida, milliste andmeformaatide kasutamist programm toetab, ja kas vastavate formaatide puhul on tegemist laialt levinud andmeformaatidega. Kuna paljud olulised protsessid salvestatakse elektrooniliselt pikaks ajaks, on sama tähtis järele uurida, kui pikk on vastavate andmeformaatide kasutusiga.

Üldiselt tuleks enne igat süsteemivahetust uurida, kas kõiki salvestatud andmeid on võimalik töödelda ka uute IT-süsteemide ja IT-rakendustega. Iga rakendusprogrammi kasutuselevõtmisel tuleb välja mõelda, millises andmeformaadis hakatakse salvestama selle programmiga töödeldavaid andmeid. Siinkohal tuleks kindlasti arvesse võtta seda, kes ja millise aja möödudes peab suutma neid andmeid lugeda. Andmevormingute valimisel andmevahetuse tarbeks tuleks välja selgitada, kas vastavad andmeformaadid sisaldavad ka soovimatut lisainfot (vt M 4.64 Ülekantavate andmete kontrollimine enne edastamist/peidetud info kõrvaldamine). Teatud andmeformaatides failid võivad kätkeda endas veel ka täiendavaid turbega seotud ohtusid, nt makrod ja sellest tulenev makroviiruste oht (vt M 4.3 Viirusetõrjeprogrammide kasutamine).

Andmevormingutes kasutatavad krüpteerimisfunktsioonidest tingitud andmeväljad peavad olema muudetava pikkusega, et andmevormingut muutmata saaks kasutada teistsuguste parameetritega krüpteerimisalgoritme.

Näide:
Tekstitöötluse puhul oli mõttekas salvestada Microsoft Winwordis loodud failid rikastatud tekstivormingus (Rich Text Format, RTF). Seda formaati suudab lugeda suurem osa tekstitöötlusprogramme ja selle kasutamine annab kindluse, et vastavad failid ei saa sisaldada makroviiruseid.

Kontrollküsimused:

- Kas on välja töötatud soovitused, milliseid andmevorminguid tuleks kasutada andmevahetuse ning milliseid arhiveerimiseks ja muuks otstarbeks?
- Kas uute programmide soetamisel selgitatakse välja, kas nendega on võimalik kasutada kõiki seni kasutuses olnud andmeformaate?

M 4.135 Süsteemifailide pääsuõiguste andmise kitsendused

Algatamise eest vastutavad: IT turvaosakond, IT-juht

Rakendamise eest vastutavad: administraator

Süsteemifailide ja -kaustade eest vastutab administraator. Vastavad kaustad ja failid on kas olulised kõikide kasutajate jaoks või siis rakendatakse neid administreerimiseesmärkidel. Süsteemifailidele peaks olema juurdepääs vaid süsteemiadministraatoritel. Vastavate pääsuõigustega administraatorite arv tuleks hoida võimalikult väike. Ka kataloogid tohivad kasutajatele anda vaid selliseid privileege, mis on hädavajalikud, ja mitte rohkem. Süsteemifailide pääsuõigusi tuleks jagada võimalikult suurte piirangutega ja vastavate volituste andmine peab toimuma ilmtingimata kooskõlas majasiseste turvaeeskirjadega (vt M 2.220 Pääsu reguleerimise suunised).

Süsteemifailid tuleks salvestada rakendusandmetest ja kasutajafailidest eraldi (vt M 2.138 Struktureeritud andmetalletus). Niimoodi saavutatakse parem ülevaade ning kergendatakse andmetest varukoopiate loomist, samuti aitab see tagada korrektset juurdepääsukaitset. Süsteemifailidele tehtud pöördused tuleb alati logida. Üleliigsed, st mittevajalikud süsteemifailid tuleks süsteemist eemaldada, et neid poleks võimalik ära kasutada rünneteks, ning et vähendada failide hulka, mille puhul tuleb regulaarselt kontrollida nende terviklust. Pääsuõiguste jagamisele piirangute kehtestamisel ei piisa, kui piirangud seotakse ainult ühe kindla programmiga. Lisaks tuleb üle vaadata ka kõikide nende programmide pääsuõiguste andmine, mida on võimalik kasutada läbi selle vastava programmi. Süsteemifailide ja süsteemikaustade terviklust, samuti pääsuõiguste korrektset toimimist tuleks vajaduse korral regulaarselt kontrollida. Paljude operatsioonisüsteemide jaoks leidub selleks spetsiaalseid tööriistu, mis võimaldavad vastavaid kontrollimisi teha kiirelt ja usaldusväärselt.

Kontrollküsimused:

- Kas süsteemifailide pääsuõigusi kontrollitakse regulaarselt?
- Kas kontrollide läbiviimiseks kasutatakse spetsiaalseid tööriistu või loetelusid?

M 4.138 Windows Serveri konfigureerimine domeenikontrollerina

Algatamise eest vastutavad: IT-juht, infoturbe osakond

Rakendamise eest vastutavad: administraator

Domeenikontrollerid pakuvad võrgus Windows Serveri domeeni haldamiseks vajalikke teenuseid, mille hulgas on olulise tähtsusega Active Directory teenus (Active Directory Service, ADS). Reeglina pakub domeenikontroller ka nimeteenust DNS (Domain Name Service), ilma milleta ei ole Active Directory't võimalik kasutada. DNS-is hoiab Windows viiteid olulise tähtsusega Windows Serveri ressurssidele, mille terviklus on Windows Server domeeni korrektseks funktsioneerimiseks olulise tähtsusega.

Kuna domeenikontroller on kasutusel logiserverina, osutab see selleks vajalikku Kerberos'e teenust. Kerberos'e komponendid domeenikontrolleril säilitavad lisaks sellele autentimisprotokolli käigus kasutatavaid salajasi võtmeid. Kuna igal domeenikontrolleril on seetõttu täita tähtis roll ning tema abil salvestatakse kaitset vajavaid andmeid, on konfigureerimisel vajalik tähelepanu pöörata järgmistele aspektidele:

Domeenikontrolleri turvalisus oleneb peamiselt kahest olulisest valdkonnast:

- operatsioonisüsteemi turvalisusest ja Active Directory turvalisusest, mille aluseks on omaenda turvamehhanismid (vt M 3.27 Koolitus Active Directory haldamiseks). Operatsioonisüsteemi turvaseaded tulenevad suurel määral grupipoliitika suunistest, Active Directory turvaseaded vajavad vastavat planeerimist ja rakendamist (vt M 2.229 Active Directory planeerimine ja M 2.231 Windowsi grupipoliitika planeerimine).
- Domeenikontrolleril tohivad koha peal sisse logida vaid vastavaid volitusi omavad administraatorid. Kasutajate tegevust domeenikontrolleril ei tohi lubada. Standardseadistuse järgi ei ole tavalistel kasutajatel seetõttu lubatud domeenikontrolleril lokaalselt sisse logida.
- Domeenikontroller ei tohiks lisaks hädavajalikele domeenikontrolleri standardteenustele, näiteks Active Directory, Kerberos ja DNS, teisi infrastruktuuriteenuseid (nt DFS, DHCP) pakkuda. Turvalisuse seisukohalt pole eriti soovitav kasutada domeenikontrolleril DHCP-serverit (vaata ka Microsofti dokumentatsiooni DNS-i ja DHCP kohta). Mõlemad teenused funktsioneerivad ühtede ja samade volitustega. Seetõttu ei ole – lihtsustatult öeldes – pääsuõigused DNS andmetele enam teostatavad, kui DHCP-teenus muudab DNS-andmeid.
- Domeenikontroller ei tohiks pakkuda (rakendus-) serveriteenuseid, kuna vigade korral serveriprogrammis on võimalik domeenikontrolleri ja sellega koos kogu Windows Server domeeni kompromiteerimine. Domeenikontrollerid tuleks konfigureerida võimalikult turvaliselt. Pärast standardinstalleerimist tuleks kasutada mallifaili hisecdc.inf. Mallifailid paiknevad Windows Server süsteemikataloogis %windir%\security\templates all ning neid on võimalik konfigureerida käsurealt käsu secedit abil või MMC Plug-i kaudu turvamallidesse ja turvakonfigureerimisse ja -analüüsi kaasata ja kasutada. Olenevalt keskkonnast tuleb mallide secdc.inf või hisecdc.inf abil tehtud seadistused sobitada. See võib osutuda vajalikuks, kui võrgus on veel vanu

süsteeme, näiteks OS/2, mis pakuvad vähem turvalisi seadeid. Nõuandeid turvaseadete planeerimiseks võib leida lisaks meetmes M 2.231 Windowsi grupipoliitika planeerimine .

- Haldusandmete vahetamiseks Windows Server domeeni arvutite vahel kasutatava kanali konfiguratsioon peaks olema võimalikult turvaline (vt M 5.89 Turvalise kanali konfigureerimine Windowsis).
- Võimaluse korral tuleks domeenikontrollerit kasutada omarežiimis (native mode), et oleks võimlik täiel määral rakendada kõiki Windows Client'i mehhanisme. Nendeks on näiteks universaalsed grupid, gruppide sahteldamine ning kaugpöörduse pääsuõiguste andmine vastavalt grupikuuluvusele.
- Kui domeenikontrolleri saab nn Active Directory taasterežiimi buutida, on võimalik läbi viia AD muudatusi, kusjuures näiteks vanad seisundid (osaliselt või täielikult) laetakse varundusandmekandjatelt. Neid muudatusi on võimalik teha nii, et need laienevad pärast regulaarset buutimistActive Directory replikatsiooni kaudu kõikidele domeeni teistele domeenikontrolleritele. Seepärast tuleb tagada, et Active Directory taasterežiim oleks kaitstud sobiva parooliga ja tööde teostamine selles režiimis toimuks ainult nelja silma printsiibil. Active Directory taasterežiim baseerub käsuridadel ja trükivead võivad esile kutsuda tõsiseid tagajärgi, näiteks vale Active Directory haru kustutamine või ülekirjutamine. Seepärast pakub nelja silma printsiip lisaks tegevuskontrollile ka turvalisust, kuna sissekandeid kontrollivad kaks isikut.
- Forest Root domeeni (FRD) domeenikontrollerid vajavad FRD erilise seisundi tõttu ka erilist kaitset.

Üldiselt tuleb igale domeenikontrollerile alati tagada füüsiline turvalisus, näiteks paigaldada see serveriruumi.

Kontrollküsimused

- Kas kõikidele domeenikontrolleritele on antud piirangutega pääsuõigused operatsioonisüsteemi tasemel?
- Kas Active Directory pääsuõigused on antud piirangutega?
- Kas kõikidele domeenikontrolleritele on tagatud füüsiline turvalisus?
- Kas igale domeenikontrollerile on installeeritud vaid kavandatud teenused?

M 4.146 Windows'i klient-operatsioonisüsteemide turvaline käitus

Algatamise eest vastutavad: IT-juht, infoturbe eest vastutav töötaja

Rakendamise eest vastutavad: IT-juht, administraator

Pärast installeerimist ja algkonfigureerimist vastavalt eelnevalt kavandatud Windows -kontseptsioonile ja turvadirektiividele toimub Windows -arvutite käitamine reeglina võrgukoosluses. Sellise võrgu turvalisus sõltub ühelt poolt seadistatud konfiguratsiooniparameetritest. Teisest küljest sõltub see aga ka suurel määral töö käigus tehtavate konfiguratsioonimuutuste laadist. Seejuures tuleb erilist tähelepanu pöörata kõrvalefektidele, mis teatud tingimustel võivad tahtmatult viia turvaaukude tekkeni. Windows 'i klientversioonid pakuvad terve rea vahendeid ja mehhanisme, mis võivad olla abiks administraatoritele töötava süsteemi töökindluse säilitamisel.

Windows File Protection on Windows 'i süsteemimehhanism, mis tagab süsteemifailide muutumatu originaalseisundi.

Mehhanism kasutab kahte komponenti:

niinimetatud SystemFileChecker 'it (sfc.exe), mis näiteks kontrollib süsteemi käivitumisel, kas süsteemifailid on säilinud muutmata kujul ning asendab muudetud failid vahemällu salvestatud originaalfailidega. Lisaks sellele on olemas seiremehhanism, mille abil asendatakse süsteemifailid pärast nende ülekirjutamiskatset originaalversiooniga. Mehhanismi saab selliselt konfigureerida, et ülekirjutamine pärast vastavat kinnitust õnnestub ning muudetud fail jääb alles.

Konfigureerimine toimub käsurealt sfc.exe:

Windows 7:

- sfc /SCANNOW : teostab kontrolli kõigi kaitstud süsteemifailide tervikluse üle ning parandab vajadusel probleemsed failid.
- sfc /VERIFYONLY : teostab kontrolli kõigi kaitstud süsteemifailide tervikluse üle. Parandamist ei toimu.
- sfc /SCANFILE : teostab kontrolli antud faili tervikluse üle ning probleemide esinemisel parandab faili. Ette tuleb näidata täielik tee.
- sfc /VERIFYFILE : teostab kontrolli nimetatud faili tervikluse üle. Parandamist ei toimu.
- sfc /OFFBOOTDIR : näitab kätte offline- stardikataloogi salvestuskoha offline- parandusteks.
- sfc /OFFWINDIR: näitab kätte Windows - offline -kataloogi salvestuskoha offline -parandusteks.

Automaatne süsteemi taasloomine. Nimetatud mehhanismi saab kasutada varasema süsteemiseisundi taastamiseks, kui näiteks tarkvara installeerimine ebaõnnestub ning see viib süsteemi ebastabiilsesse seisundisse. Sõltuvalt kohalikest oludest ja eriti juurutatud tarkvara jaotamise strateegiast, võib näiteks automaatse süsteemi taastootmise rakendamisel testimiskeskkonnas olla oma eelised. Alates Windows 7-st leiab kahjustatud süsteemi taastamiseks ette nähtud seaded järgmisest asukohast: Control Panel | Recovery | Open System Restore.

Süsteemi taastamise funktsiooni tohivad kasutada üksnes vastutavad administraatorid.

- Taastatud süsteemi konfiguratsiooni puhul tuleb kontrollida, kas see vastab kehtivatele turvapoliitikatele, et säilitada infokoosluse turve. Eriti hoolikalt tuleb kontrollida, et kõik kriitilised turvapaigad (patches), värskendused (updates) ja seadistused oleksid olemas ning tööle lülitatud. Vajaduse korral tuleb need uuesti installida ja konfigureerida.
- Windows sisaldab käsureal põhineva turvaredaktori secedit.exe ja MMC snap - in Turvakonfiguratsioon ja -analüüs näol vahendeid Windows 'i kliendiarvutite turvasätete konfigureerimiseks. Selle turvakonfiguratsiooni võib salvestada ka andmebaasi, millega saab testida arvuti vastavust. Selleks luuakse kõigepealt MMC snap-in Turvakonfiguratsioon ja -analüüs abil andmebaas (Protseduur/Andmebaasi avamine, uue või olemasoleva andmebaasi nime sisestamine). Selle saab turvamalli abil (infofail, vaata MMC snap-in Turvamallid) installeerida. Valides Protseduur / Arvuti analüüs või Protseduur/Süsteemi konfigureerimine saab andmebaasi seadistuste abil teostada süsteemi analüüsi või konfigureerimist. Andmebaas on failivormis (sdb-fail), mida saab teistele süsteemidele üle kanda. Igatahes on informatsioonist pääsuõiguste kõrvalekallete kohta faili- või registri tasandil vähe abi, sest registreeritakse küll kõrvalekalle, kuid mitte see, milliseid pääsuõigusi see puudutab.
- Windows 'i kliendi turvaseadistused määratakse domeenis käitamisel reeglina kindlaks grupipoliitika direktiivide või ühes objektis olemasolevate seadistuste abil. Sel moel on ka suurte Windows 'i võrkude turvaseadete haldamine efektiivsem ja seda on võimalik teha tsentraalselt. Igapäevases töös on reeglina oodata muudatusi grupipoliitika objektide (GPO) seadistuste osas.

Nimetatud muutused toimuvad tsentraalselt ühel domeenikontrolleril ning jagatakse siis vastavatele arvutitele edasi. GPO -mehhanismi on võimalik konfigureerida selliselt, et perioodiliselt toimub GPO- seadistuste värskendamine, mis annab muudetud seadetele võimaluse mõjusalt toimida (vt M 2.231 Windowsi grupipoliitika planeerimine ja M 2.326 Windows Vista ja Windows 7 grupeerimissuuniste planeerimine).

Süsteemipääsu turvalisust saab suurendada kiipkaardil põhineva sisselogimisega.

Autentimine ei toimu sel juhul kasutajanime ja teatud juhtudel nõrga parooli, vaid sertifikaadi abil, mis on salvestatud kiipkaardile. Windows 'i on võimalik selliselt konfigureerida, et sisselogimine võib toimuda kasutajanime ja parooli või kiipkaardi abil, või ainult kiipkaardi abil. Üldiselt on võimalik kasutada vaid Microsoft 'iga ühtivaid sertifikaate ning kiipkaarte, mida operatsioonisüsteemid Windows toetavad.

Arvutisüsteemi turvalisus sõltub alati ka arvuti ja võrgukomponentide füüsilisest turvalisusest. See peab Windows 'i kliendisüsteemi käitamisel olema tagatud.

Windows 'i kliendisüsteemi turvaliseks käitamiseks tuleb põhimõtteliselt silmas pidada järgmist.

Windows 'i töökindlus sõltub olulisel määral Active Directory töökindlusest.

Siin sisalduvat informatsiooni tuleb ühest küljest kaitsta volitamata muutmise eest ja teisest küljest hoida see konsistentsena. See nõuab eriti just muutuste tegemisel teatud hoolikust. Turvalisuse kavandamisel on tungivalt soovitav mitte ainult kindlaks määrata parameetrite väärtused ja väärtuspiirkonnad, vaid defineerida ka asutusesisesed ja administratiivsed protseduurid, mis on sobilikud kindlaks määratud turvasuuniste rakendamiseks.

Näiteks tuleks ka kindlaks määrata, millised sammud on vaja läbida uue kasutajakonto loomiseks, et vajalikud muutused täielikult sisse viidud saaksid.

Täiendav informatsioon Windows 'i klientide turvaliseks käitamiseks Active Directory 's on kirjeldatud moodulis B 1.0 Infoturbe haldus .

Lisaks Active Directory ja süsteemi turvalisusele, mis oleneb Active Directory's kindlaks määratud parameetritest, tuleb tagada ka olulise tähtsusega süsteemiteenuste töökindlus. Selle juures omab erilist tähtsust DNS, WINS, DHCP, RAS ja Kerberos 'e töökindlus.

Ka siis, kui muudatused toimuvad hoolikalt ja kõikidest ettevaatusabinõudest kinni pidades, ei saa keerulises süsteemis kunagi täielikult välistada turvaaukude esinemist. Seetõttu peab alati toimuma asjakohane süsteemiseire (M 4.344 Windows 7 ja Windows Server 2008 süsteemi seire). Seejuures tuleb seire tugevust ja täpsust kohandada ohutaseme alusel.

Seire liigi ja viisi saab kindlaks määrata ainult igal konkreetsel juhul. Üldiselt peaksid seiresse olema kaasatud ka administraatorite tegevused. Peale selle soovitatakse korrapärast kontrollimist, et avastada süsteemi muudatustega tekkida võivad võimalikud lüngad.

- Ka siin tuleb muutuste tegemisel tagada, et ei rikutaks kehtivaid ja kindlaks määratud turvasuuniseid. Nõuandeid nimetatud teenuste konfigureerimiseks leiab meetmes M 4.246 Süsteemiteenuste konfigureerimine Windows 7 keskkondades ja selles soovitatud meetmetes.
- Windows 'i kliendisüsteemi haldamiseks on Microsoft 'i halduskonsoolis standardina olemas niinimetatud snap-in 'id (MMC snap-ins). MMC-snapin'id kujutavad endast haldusmooduleid, mida on võimalik standardiseeritud liidese kaudu MMC -sse integreerida. Seetõttu tuleb juurdepääs erinevatele MMC snap-in 'idele reglementeerida. Tavakasutajatel peaks juurdepääs süsteemi haldusvahenditele olema üldjuhul keelatud. Erandi moodustab siin siiski MMC snap-in sertifikaatide haldamine, mida tuleb ka ta-

vakasutajatel oma sertifikaatide haldamiseks kasutada. Juurdepääsu üksikutele MMC snap-in 'idele on seejuures võimalik reguleerida GPO -sätete kaudu.

- Haldusvahendid juurdepääsuks arvuti lokaalsele registrile (regedt32 ja regedit) ei peaks olema tavakasutajatele kättesaadavad. Ka seda on võimalik GPO -sätete abil saavutada
- Windows 'i võrgu turvalisus sõltub paljudest faktoritest: turvaaugud võivad tekkida just lisarakenduste tõttu, mis on valesti konfigureeritud või sisaldavad programmeerimisvigu. Tihti tekivad probleemid alles mitmete rakenduste koos käitamisel. Sel põhjusel tuleb enne uue rakenduse sisseviimist teha testimine, mis annab esmast informatsiooni tekkida võivate probleemide kohta. Täielikku töökindlust ei ole võimalik saavutada, kuna vigade testimine kõrvalefektide tõttu teistes rakendustes on raske ja väga kulukas.
- Kuigi muudatuste tegemine toimub hoolikalt ja kõiki ettevaatusabinõusid järgides, ei ole turvaaukude olemasolu komplekssetes süsteemides kunagi võimalik täielikult välistada. Sel põhjusel peaks alati toimuma asjakohane süsteemiseire (vt M 4.344 Windows 7 ja Windows Server 2008 süsteemi seire). Seejuures peab seire põhjalikkus ja täpsus olema vastavusesse viidud võimalike ohtudega. Seire läbiviimise viisi on võimalik kindlaks määrata igal konkreetsel juhul eraldi. Üldiselt tuleks teostada seiret ka administraatorite tegevuse üle. Lisaks sellele on soovitav teha regulaarset kontrolli, et oleks võimalik avastada süsteemi muutuste tõttu tekkida võivad turvaaugud.
- Turvalisuse seisukohalt on ka muutused domeeni struktuuris kriitilised. Seepärast tuleb nende tegemist hoolikalt planeerida. Juba planeerimise algetapis tuleb silmas pidada, et Windows 'i domeenistruktuur (jaotus domeenideks, puudeks, metsadeks) võimaldab tagant järele vaid väheste muutuste tegemist (vt M 2.229 Active Directory planeerimine).

Ka turvalisuse seisukohalt on tähtis, et dokumenteeritaks kõik Windows 'i kliendisüsteemi puudutavad direktiivid, eeskirjad ja protsessid. Selleks tuleks koostada kasutusjuhendid, mida tuleb süsteemi muutuste korral aktualiseerida. Kuna kasutusjuhendid sisaldavad turvalisuse seisukohalt tähtsat informatsiooni, tuleb neid säilitada selliselt, et volitamata isikutel ei oleks neile võimalik juurde pääseda, samas aga tuleks juurdepääs volitatud administraatoritele teha võrdlemisi lihtsaks.

Selleks on võimalik anda vaid üldist laadi soovitusi, kuna süsteemi töökindluse säilitamine sõltub ka kohalikest oludest. Seetõttu tuleb juba Windows -võrgu planeerimisfaasis koostada võrgu turvaliseks funktsioneerimiseks vastavad direktiivid, mis arvestavad ka kohalikke olusid. Mõnikord võib ette tulla, et teatud turvamehhanismide konfigureerimisel ei ole võimalik saavutada optimaalset turvalisust. See võib juhtuda näiteks, kui tuleb edasi käigus hoida „vanu" rakendusi, mis on konfigureeritud vaid nõrga autentimissüsteemi jaoks või juhuks, kui see üldse puudub.

Sel juhul tuleb vastavate tasakaalustavate meetmetega mujal – või organisatoorsel tasemel – garanteerida rahulolu pakkuv turvalisus. Windows -süsteemi

turvalisus tööprotsessis sõltub olulisel määral administraatorite teadmiste tasemest.

Seepärast tuleb süsteemihaldurite koolituses ja täiendkoolituses pidada oluliseks kaitseabinõusid (vt M 3.27 Koolitus Active Directory haldamiseks), kuna potentsiaalseid turvaaukusid võivad avastada ja vältida vaid kompetentsed administraatorid.

Lisaks sellele peavad turvaalast koolitust saama ka tavakasutajad (vt M 3.28 Windowsi klientoperatsioonisüsteemide turvamehhanismide koolitus kasutajatele), et potentsiaalsed ohud oleks teada ja käsutuses olevaid turvamehhanisme osataks õigesti kasutada.

Kontrollküsimused:

- Kas toimub süsteemi protokolli andmete regulaarne kontroll?
- Kas juurdepääs kõikidele administratiivsetele vahenditele on kasutajate jaoks tõkestatud?
- Kas administraatorid saavad regulaarset koolitust?
- Kas on tagatud olulise tähtsusega süsteemiteenuste turvalisus, näiteks DNS, WINS DHCP, RAS või Kerberos ?
- Kas juurdepääs erinevatele MMC snap-in 'idele on reglementeeritud?
- Kas enne uute rakenduste sisseviimist toimub funktsiooni- ja turvatestide läbiviimine?
- Kas toimub asjakohane süsteemiseire?
- Kas enne domeeni struktuuri muutmist toimub hoolikas planeerimine?
- Kas Windowsi klient-operatsioonisüsteemide süsteemiseire tugevus ja täpsus on kohandatud ohutaseme alusel?
- Kas Windowsi klient-operatsioonisüsteemide kasutajatele on tõkestatud juurdepääs kõikidele administraatorite tööriistadele?
- Kas enne uute rakenduste juurutamist Windowsi klientoperatsioonisüsteemidele viiakse läbi funktsioonide ja turvalisusega seotud testid?
- VoIP WLAN-is: kas on tagatud WLAN-i kvalifitseeritud kaitse?

M 4.147z EFS-i turvaline kasutamine Windows ’i keskkonnas

Algatamise eest vastutavad: IT-turvaspetsialist, IT-juht

Rakendamise eest vastutavad: administraator, kasutaja

Windows-is on võimalik kasutada failisüsteemi EFS (Encrypting File System – krüpteerivat failisüsteemi), mis toetab failide ükshaaval krüpteerimist ning mille kasutamiseks tuleb failid vastavalt märgistada. Failide krüpteerimiseks kasutatakse EFS-is hübriidset mehhanismi, st läbisegi nii asümmeetrilist kui ka sümmeetrilist krüpteerimisprotseduuri.

- Puhtakujuliseks andmete krüpteerimiseks rakendatakse kiiret sümmeetrilist protseduuri. Selleks kasutatav võti (nn File Encryption Key, FEK) luuakse juhulikkuse printsiibi alusel.
- FEK -i krüpteerimiseks kasutatakse asümmeetrilist RSA -protseduuri. FEK krüpteeritakse selle kasutaja avaliku võtmega, kes soovib oma faili krüpteerida.

Seeläbi saab FEK-i ja failide dekrüpteerimiseks kasutada vaid selle sama kasutaja privaatvõtit. Alates versioonidest Windows 7 ja Server 2008 R2 saab FEK-d krüpteerida ka Elliptic Curve Cryptosystemi krüpteerimisprotseduuriga (ECC). See protseduur võimaldab kasutada lühemaid võtmeid.

Windows 7-s ja Server 2008 R2-s on kasutusel RSA ja ECC Hybrid, mis tagavad koostalitluse varasemate Windowsi versioonidega. Nende protseduuride võtmepikkust konfigureeritakse järgmises grupipoliitikas: Computer Configuration | Windows Settings | Security Settings | Public Key Policies | Encrypted File System.

Siinkohal tuleks kasutada vähemalt eelseadistusväärtusi:

2048 bitti RSA puhul ja 256 bitti ECC puhul. Olenevalt krüpteeritavate andmete konfidentsiaalsusnõuetest võib võtmepikkuse ka suuremaks seadistada.

Windows salvestab kasutuse käigus kõik krüpteerimiseks ja dekrüpteerimiseks vajalikud võtmed sellisesse põhimälu piirkonda, mida saalimisfaili hulka ümber ei paigutata. Sellega soovitakse välistada võtmete kompromiteerimisvõimalused juhtudel, kus volitamata kolmandatel isikutel õnnestub saada juurdepääs saalimisfailile.

Kriitiliseks võib osutuda selle kombinatsiooni puhul säästurežiimi (hibernation mode) kasutamine, kuna terve põhimälu salvestatakse sellisel juhul kokku ühte faili, mis sisaldab seetõttu ka võtmeid kajastavat infot. Sel põhjusel tuleks vältida EFS -i ja säästurežiimi koos kasutamist Windows ’i versioonide puhul, mis on vanemad kui Windows Server 2008. Eriti oluline on see sülearvutite puhul. Windows Server 2008 puhul saab probleemi lahendamiseks ette võtta saalimisfaili krüpteerimise: Computer Configuration | Windows Settings | Security Settings | Public Key Policies | Encrypted File System. Klõpsake parema hiireklahviga ja

valige Properties ning seejärel märgistage vastav menüü.

EFS -iga krüpteerimiseks saab iga kasutaja määrata, kas soovib seda rakendada failidele või kataloogidele. Kasutajad peavad läbima EFS -i korrektset kasutust käsitleva koolituse ning neid tuleb teavitada võimalikest ohtudest, mis võivad kaasneda sellist liiki krüpteerimisvõimaluste kasutamisega. EFS -i kasutamine tõstab turvalisust. Sellele vaatamata peaksid kasutajad siiski teadma, et kuigi loetaval kujul hoitavad tekstid krüpteeritakse, eksisteerib jätkuvalt oht, et loetaval kujul tekste on võimalik ka pärast nende kustutamist siiski veel taastada. Selleks on, tõsi küll, tarvis spetsiaalset tarkvara ning juurdepääsu vastava arvuti kõvakettale.

Selleks, et EFS -iga krüpteeritud failid privaatvõtme kaotamise korral täielikult kaotsi ei läheks, võib FEK krüpteerida täiendavalt veel ka nn taastamisagendi (Recovery Agent) avaliku võtmega. Seeläbi saab andmeid dekrüpteerida lisaks ka taastamisagendi kasutajakonto alt. Taastamisagendi funktsiooni jaoks saab enamasti kasutada ükskõik millist kasutajakontot.

EFS -i kasutamisel tuleb arvestada järgnevaga:

- EFS on kasutaja jaoks täiesti nähtav. Kuna EFS on kasutajale hästi märgatav, on failide krüpteerimine EFS -iga täpselt nii tugev, kui tugev on iga üksiku kasutajakonto parool. Juhul, kui volitamata kolmandal osapoolel õnnestub end kasutajakonto alt sisse logida, tekib tal ka võimlaus ligi pääseda kõikidele selle kasutajakonto all krüpteeritud failidele. EFS -i rakendamisel on soovitav, et iga kasutajakonto oleks varustatud tugeva parooliga. Kuna Windows võimaldab kasutada isiklikke paroolifiltreid, võib kasutada just seda tehnilist lahendust, et saavutada tugevamate paroolide kasutamine.
- EFS krüpteerib faile, see ei krüpteeri kaustasid. Sellele vaatamata võib krüpteerimisfunktsiooniga siiski märgistada ka kaustasid ning sellisel juhul krüpteeritakse kõik kaustas leiduvad failid ning ka kõik sellesse kausta uuena loodavad failid. Krüpteerimisfunktsiooniga märgistatud kaustas on aga siiski võimalik hoida ka krüpteerimata faile, samuti on võimalik neid sinna tekitada (vt järgmine lõik). Lisaks võivad krüpteeritud failid asuda ka failipuu ükskõik millises alajaotuses ning seetõttu ei ole need ilmtingimata seotud kindla, krüpteerimisfunktsiooniga märgistatud kaustaga.
- Krüpteerimise tunnuseks on faililaiend, mis käitub samamoodi nagu ka kõik teised faililaiendid, st failide ümbertõstmisel laiendid ei muutu. See viib selleni, et isegi siis, kui failid tõstetakse vastavasse, krüpteerimismärgistusega kausta, ei toimu nende krüpteerimine sugugi mitte automaatselt. Seetõttu tuleb Windows Explorer 'is eelseadistusega määrata, et ka kausta juurde tõstetud failid krüpteeritaks. Selleks saab kasutada grupipoliitikaid. Samas jällegi ei kehti see tegevuste kohta, mida juhitakse Windows 'i käsuviibalt.

Kasutajaid tuleb teavitada ohust, et failid, mis tõstetakse krüpteerimismär-

gistusega kausta, võivad jääda ka krüpteerimata.

- Vaatamata sellele, et EFS-il ei ole kaustade krüpteerimise funktsiooni, on siiski soovitav hoida krüpteeritud faile spetsiaalsetes kasutades, st lisada kaustadele krüpteerimismärgistus. See kergendab töötamist krüpteeritud failidega.
- Faili krüpteerimisega ei kaasne juurdepääsu kontrolli kehtestamist. Kolmandatel isikutel on võimalus krüpteeritud failid ära kustutada juhul, kui pääsuõigused seda lubavad. Lisaks üksikute failide krüpteerimisele tuleb seetõttu teha täiendavaid muudatusi ka juurdepääsukontrolli seadistustes.
- EFS -i tsentraalselt juhitud kasutamist on võimalik tagada grupipoliitikatega, mida kasutatakse muuhulgas ka taastamisagentide defineerimiseks.

Sõltuvalt sellest, millist turvalisuse astet on tarvis tagada, võiks järele mõelda, kas vastava konto kasutamistingimustesse tuleks lisada võib-olla nelja silma põhimõte, nt paroolide jagamisel.

- Eraldiseisva taastamisagendi rakendamine ei paku piisavat kaitset administraatorite tegevuse vastu, kuna viimased võivad kasutaja parooli iga hetk taastada selle algsele kujule, et seejärel end ise kasutajana sisse logida, mille tagajärjel tekib neil ligipääs ka vastava kasutaja krüpteeritud failidele.
- Pärast seda, kui taastamisagendi privaatvõti on mõnele andmekandjale ümber salvestatud, tuleks see süsteemist kustutada. Vastavat andmekandjat tuleb hoida turvalises kohas. Juurdepääs andmekandjale peaks olema võimaldatud ainult nelja silma põhimõtet järgides. Võtmest on soovitav luua veel ka täiendav, eraldi turvaliselt hoiule pandav varukoopia.
- EFS-i kasutades on oluline luua kõikidest privaatvõtmetest varukoopiad.

Selleks tuleb andmevarundusprotseduuri kaasata kõikvõimalikud kasutajate võtmeid ja sertifikaate sisaldavad kataloogid, mis liigituvad oma hierarhias valdkonna alla Documents and Settings/.

- EFS-iga krüpteerimiseks saab iga kasutaja määrata, kas soovib seda rakendada failidele või kataloogidele. Kasutajad peavad läbima EFS-i korrektset kasutust käsitleva koolituse ning neid tuleb teavitada võimalikest ohtudest, mis võivad kaasneda sellist liiki krüpteerimisvõimaluste kasutamisega. Siinjuures tuleb tähele panna järgmist.
- EFS-krüpteeritud failide kopeerimine või ümbertõstmine NTFS-ilt FAT/FAT32-le dekrüpteerib failid, sest FAT/FAT32 ei toeta krüpteeringut.

Peale selle eemaldatakse NTFS-õigused, mis failidele olid antud.

- Juhtudel, kus EFS-i rakendatakse nõnda, et kasutajate profiile servereile ei salvestata (puudub roaming profile) kasutatakse sõltuvalt erinevatest lokaalsetest profiilidest ka erinevaid võtmeid nii FEK -i krüpteerimiseks kui ka dekrüpteerimiseks, kuna võtmed salvestatakse (krüpteeritud kujul) kasutaja profiili alla. Sellistel juhtudel on oluline luua kõigist võtmetest varukoopiad.

Tuleb arvestada, et ühes arvutis krüpteeritud andmeid, mis on lindile salvestatud, pole võimalik teise arvutisse sisse lugeda, sest erinevate võtmete tõttu ei õnnestu neid edukalt dekrüpteerida. Krüpteeritud failide ümbertõstmine NTFS-ajamite vahel samas arvutis säilitab krüpteeringu ja samuti NTFS-õigused.

- Ettevõtetes ning ametiasutustes tuleks kaaluda, kas EFS -i sertifikaatide väljastamiseks oleks mõttekas kasutada PKI -d. Viimasega muutub võtmete haldamine ja varundamine märgatavalt lihtsamaks, eriti juhtudel, kus kasutajate profiilid salvestatakse serverile.
- Krüpteerimise eest tuleb kaitsta Windows 'i buutimisfaili autoexec.bat, mille puhul tuleb kasutajatele ära keelata kirjutusõigusega juurdepääs sellele failile. Vastasel korral säilib võimalus Denial-of-Service rünneteks.
- Juhul, kui krüpteeritud faile töödeldakse pärast dekrüpteerimist programmidega, nt tekstiredaktoritega, st muudetakse või prinditakse, luuakse selleks otstarbeks reeglina ajutised failid, mis sisaldavad vastavaid andmeid loetava teksti kujul. Need failid võivad sõltuvalt programmi eripärast jääda alles ka pärast süsteemi töötlemist. Seeläbi võib sõltuvalt salvestuskohast (Temp-kataloog või Spool -valdkond) ja pääsuõigustest tekkida juurdepääs ka volitamata kolmandatele osapooltele.
- EFS -iga krüpteeritud failide suurema turvalisuse tagamiseks tuleks kaaluda krüpteerimismärgistuse laiendamist ka sellistele kataloogidele (Temp, Spool), mis võivad reeglina sisaldada ajutisi faile. Siinkohal tuleks arvestada, kui suuri andmemahtusid nendesse kataloogidesse salvestatakse, ning millised programmid neid katalooge kasutavad. Juhtudel, kus nendes kaustades hoitakse suuri andmehulkasid, mida kasutatakse tihti, võib krüpteerimise tagajärjeks olla jõudluse langus. Tuleks arvestada ka sellega, et Temp-kataloogi krüpteerimisel võib tekkida täiendavaid probleeme seoses värskendustega.
- EFS -iga krüpteeritud andmed krüpteeritakse ja dekrüpteeritakse selles arvutis, kuhu need on salvestatud. See tähendab ennekõike seda, et andmed, mis salvestatakse serverile krüpteeritud kujul, toimetatakse kliendini läbi võrgu mitte krüpteeritud, vaid loetava teksti kujul (SMB -protokoll). Juhul, kui turbenõuete täitmiseks on tarvis, et andmed oleksid kaitstud ka edastamise käigus, tuleb kasutusele võtta täiendavad meetmed võrgus aset leidva side turvamiseks. Selleks võib EFS-i kasutada koos WebDAV-i (Web Digital Authoring and Versioning), SSL -i või IPSec -iga (vt M 5.90 IPSec'i protokolli kasutamine Windowsi keskkonnas).
- Juhul, kui EFS -i rakendatakse lokaalsete kasutajakontode jaoks, tohib Registry krüpteerimist käsuga syskey võimaldada ainult koos parooliga. Ainult niimoodi on võimalik lokaalseid kontoparoole kaitsta „häkkeritööriistade" vastu, mille eesmärgiks on paroolide muutmine.
- EFS kujutab endast soodsat alternatiivlahedust kõikide teiste faile krüpteerivate tööriistade suhtes vaid juhul, kui seda osatakse õigesti kasutada. EFS-i võib nt rakendada sülearvutites, et tasakaalustada puudulikku füüsilist turvalisust, et tagada andmete kaitstust volitamata juurdepääsude vastu, mis suudavad mööda hiilida operatsioonisüsteemi kaitsemehhanismidest. EFS ei pruugi ilmtingimata alati kõikjale sobida, mistõttu tuleks selle otstarbekust vaadelda iga konkreetse juhtumi puhul eraldi.

Alternatiivina või täiendusena EFS-ile võib kasutada ka kõvaketta krüpteerimis-

tarkvara BitLocker (vt M 4.337z BitLockeri Drive Encryption kasutamine). Eriti kehtib see kaasaskantavatele arvutitele (vt M 2.442 Windows 7 kasutamine kaasaskantavates arvutites).

Kontrollküsimused:

- Kas säästurežiim (Hibernation Mode) on EFS -i kasutuse korral arvutites, mille platvorm on vanem kui Windows Server 2008, desaktiveeritud?
- Kas töötajaid on koolitatud, kuidas EFS -i korrektselt kasutada?
- Kas kasutajakontosid kaitstakse tugevate paroolidega?
- Kas EFS -iga krüpteeritud failid on täiendavalt kaitstud veel ka piiravate pääsuõigustega?
- Kas taastamisagendi jaoks on loodud eraldi konto, mille privaatvõtmest on loodud varukoopia ning kas võti on seejärel süsteemist eemaldatud?
- Kas kõikidest privaatvõtmetest luuakse varukoopiad?
- Kas Registry krüpteerimisele käsuga syskey on kehtestatud paroolkaitse, juhtudel, kus EFS -i kasutatakse lokaalsete kontode jaoks?
- Kas Windows'i buutimisfail autoexec.bat on krüpteerimise eest kaitstud?
- Kas takistatakse Windowsi buutimisfaili autoexec.bat krüpteerimist?
- Kas kõiki kasutajaid on koolitatud EFS-i õigesti kasutama?
- Kas EFS-i kasutamine on piisav, et täita asutuse konfidentsiaalsust puudutavaid nõudeid?

M 4.148 Windows 2000/XP süsteemi seire

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator, audiitor

Arvutisüsteemide seire on oluliseks meetmeks nende turvalisuse ja tervikluse tagamisel. Ainult niimoodi on võimalik tuvastada võimalikke turvaaukusid, kehtivate turvapoliitikate rikkumisi ning organisatsiooni seest või väljast alguse saanud ründeid ja nende vastu sobivaid vastumeetmeid käiku lasta. Windows 2000/XP süsteemi seirevajadustega tuleb arvestada juba planeerimisfaasis, et olulised parameetrid saaksid määratletud vastavalt vajadustele. Selleks, et *Windows 2000/XP* süsteemis saaks toimuda seire, tuleb see reeglina esmalt sisse lülitada. Eriti kehtib see failide ja registri seire kohta. Seirekomponentide sisse lülitamiseks ja konfigureerimiseks tuleb kasutada järgnevaid grupipoliitikate parameetreid:

- Seirefunktsioonide üldine sisselülitamine

Seadistamisel saab valida mõistete vahel *No auditing* või *Success* ja/või *Failed*.

Arvutipoliitikad / lokaalsed poliitikad / seirepoliitikad

Parameeter

Soovitus

Protsessi jälgimise seire

Protsessi seire ei ole üldjuhul mõttekas ning see tuleks sisse lülitada vaid *Debugging* eesmärgil.

Õiguste kasutamise seire

Kasutajate õiguste rakendamist tuleks jälgida.

Poliitikate muudatuste seire

Poliitikaseadistuste (*GPO* -de) muutmine on turvalisuse seisukohalt kriitilise tähtsusega tegevus ning seda tuleks jälgida.

Süsteemi kajastavate sündmuste seire

Lülitab sisse buutimisega seotud sündmuste logimise.

Sisselogimisega seotud sündmuste seire

Sisselogimisega seotud sündmuste seire peaks olema lokaalsete arvutite (nt töökohaarvutite) puhul sisse lülitatud.

Sisselogimiskatsete seire

Seire peaks kajastama sisselogimiskaitseid domeenikontrollerisse, mis tegeleb kasutaja autentimisega.

Kontode haldamise seire

Kontode seadistustes tehtavad muudatused on turvalisuse seisukohast olulised sündmused ning neid tuleks jälgida.

Objektidele tehtud pöörduste seire

Funktsioon peaks olema sisse lülitatud, kuna seeläbi on võimalik logida failidele ja registrisse tehtud pöördusi.

Active Directory pöörduste seire

On oluline vaid domeenikontrollerite kontekstis. *AD* -s tehtavaid muudatusi tuleks jälgida.

Tabel: Arvutipoliitikad, lokaalsed poliitikad, seirepoliitikad

- Logifailide seadistused

1. Arvutipoliitikad / lokaalsed poliitikad / kasutajaõiguste andmine
Parameeter
Soovitus
Seire- ja turvalogide haldamine
Nimetatud õigus võimaldab
- konfigureerida auditeerimisseadistusi üksikute objektide (failide, registri , *Active Directory*) lõikes,
- vaadata ja kustutada turvalogi.
Millisele kasutajagrupile (või gruppidele) sellist õigust anda, sõltub suuresti seirekontseptsioonist. Üldjuhul tuleks selle õiguse andmisel rakendada suuri piiranguid. Samas tuleks arvestada ka järgnevaga:
- juurdepääs turvalogile võib olla hädavajalik ka selliste probleemide diagnostikaks ja lahendamiseks, mis ei ole seotud turvalisusega,
- administraatorid suudavad selle õiguse enese jaoks taastada ka juhul, kui see neilt ära võetakse. Seetõttu on soovitav, et vastavad sündmused kajastuksid logis (valik *Audit privilege use*).
2. Arvutipoliitikad / lokaalsed poliitikad / sündmuste logi
- Rakenduslogi säilitusmeetod
- Turvalogi säilitusmeetod

- Süsteemilogi säilitusmeetod

Sõltuvalt logimiskontseptsioonist saab valida
iga . . . päeva möödudes ,
üle kirjutada või
mitte üle kirjutada .
- Rakenduste logi säilitamine . . . päevaks
- Turvalogi säilitamine . . . päevaks
- Süsteemilogi säilitamine . . . päevaks
Päevade arv, juhul, kui säilitusmeetodiks on valitud *Iga . . . päeva möödudes* .
Windows 2000 :
- Külaliskonto alt rakendus-logile juurdepääsemise piiramine
- Külaliskonto alt turvalogile juurdepääsemise piiramine
- Külaliskonto alt süsteemi-logile juurdepääsemise piiramine
Windows XP :
- Lokaalse külaliskonto alt rakenduslogile juurdepääsemise tõkestamine
- Lokaalse külaliskonto alt turvalogile juurdepääsemise tõkestamine
- Lokaalse külaliskonto alt süsteemilogile juurdepääsemise tõkestamine
Külaliskonto juurdepääsude piirangud peaksid olema sisse lülitaud.
- Rakenduslogi maksimaalne suurus
- Turvalogi maksimaalne suurus
- Süsteemilogi maksimaalne suurus
Suurus tuleb valida selline, et sõltuvalt säilitamiseks valitud meetodist oleks alati piisavalt ruumi ka keskmisest suurema süsteemisündmuste arvu kajastamiseks.

Eriti oluline on see turvaprotokolli jaoks, kuna vastasel korral võib süsteemi turvalisuse seires tekkida ajaline lünk.

Ettepanekuid selleks otstarbeks tehtavate seadistuste kohta leiate meetmetest M 2.231 Windowsi grupipoliitika planeerimine ning M 4.244 Windowsi klientoperatsioonisüsteemide turvaline süsteemikonfiguratsioon . Viimased tuleb aga kindlasti viia vastavusse reaalsete tingimustega (testida proovikäituse raames).

Windows 2000 :

Süsteemi väljalülitamine turvalogi maksimaalse suuruse saavutamisel

Tavakasutuse puhul tuleks sellesse suhtuda ettevaatlikkusega. Antud funktsioon on mõttekas suurt turvalisust nõudvates keskkondades, juhul, kui peamiseks eesmärgiks pole mitte käideldavus, vaid tõendite kogumine. Funktsiooni kasutamist tuleb iga juhtumi korral eraldi kaaluda.

Tabel: Logifailide seadistused

Seire raames tuleb reeglina arvestada lisaks ka järgnevate aspektidega:

Andmekaitsespetsialisti ja töötajate esindaja kaasamine

- Planeerimisfaasi tuleks võimalikult varakult kaasata ka andmekaitsespetsialist ja töötajate esindaja, kuna seire käigus kogutakse reeglina ka isikuandmeid kajastavat infot, mille eesmärgiks on turvarikkumiste korral võimalikult üheselt kindlaks teha need põhjustanud isikud.
- Selleks, et seirekomponendid genereeriksid logisissekandeid, tuleb sisse lülitada asjakohaste grupipoliitikate seirefunktsioonid.
- Windows 2000/XP pakuvad seire otstarbel kasutada vaid logimisfunktsiooni: süsteemikomponendid ja rakendused genereerivad omalt poolt seisundit kajastavaid teateid, mis kogutakse kokku kolme logifaili (süsteemi-, rakenduste- ja turvalogisse). Eraldiseisvat online -seire auditeerimisarhitektuuri ei eksisteeri. Kõik logifailid salvestatakse lokaalselt ning nende analüüsimine toimub suures osas käsitsi.
- Logifailide tsentraase kogumiskoha loomiseks ning failide automaatseks analüüsimiseks on võimalik kasutada kolmandate tootjate lahendusi. Juhul, kui võrgu ja süsteemi haldamiseks kasutatakse mõnda tööriista (vt B 4.2 Võrgu- ja süsteemihaldus), on võimalik sõltuvalt toote eripäradest importida Windows 2000/XP logid otse vastava tööriista alla.
- Windows 2000/XP auditeerimisseadistuste alt on võimalik registreerida turvalogis hoitavatele failidele või registri võtmetele tehtavaid pöördusi.

Seireparameetreid tuleb esmalt testida

- Seire käigus toodetakse sõltuvalt konfiguratsioonist suuri andmemahtusid. Lisaks võib intensiivne seire vähendada süsteemi jõudlust. Ekstreemjuhtudel võidakse süsteem seirega nii üle koormata, et tavapärane töö muutub võimatuks. Sel põhjusel tuleb seireparameetreid proovikäitamise raames kontrollida ning vajadusel ka kohandada. Siinkohal tuleb arvestada, et parameetrite kohandamine võib avaldada mõju kogu seirekontseptsioonile, kuna võib selguda, et teatud liiki seireülesandeid pole enam võimalik rakendada. Eriti võib seda esineda siis, kui rakendatakse täiendavaid tooteid,

mis seavad logitavatele sündmustele täiendavaid kõrgeid nõudeid. Näitena võib siinkohal nimetada programme, mille poolt läbi viidav logiandmete automaatne analüüs põhineb käitumises aset leidvate anomaaliate nagu nt võimalike rünnete tuvastamisel.

- Süsteemifunktsioonide seire raames on lisaks soovitav regulaarselt kontrollida ka AD replikeerimist, millega edastatakse konfiguratsioonis aset leidnud muudatusi. Selleks võib ühelt poolt kasutada AD -tööriistasid nagu repadmin.exe või showreps.exe , kuid teiselt poolt tuleks kindlasti kontrollida ka ADS -i logi (Active Directory Service) ja FRS -i logi (File Replication Service), et tuvastada võimalikke veateateid. Replikeerimisel toimunud vigade tagajärjeks on reeglina see, et konfiguratsioonis tehtud muudatusi ei ole võimalik kõikjal üheselt rakendada. Sellega kaasneb oht, et mõnele kasutajale võidakse anda kas ebasobivad või liiga laialdased volitused.
- Süsteemi seires ja logitud andmete analüüsimises mängib tähtsat rolli süsteemiaeg. Eriti neil juhtudel, kus seiresse on kaasatud mitmeid süsteeme, tuleb süsteemiaeg kõikides arvutites kindlasti sünkroniseerida. Alates versioonist Windows 2000 on juurutatud ajateenus W32Time (Windows 'i sisemine kell). See teenus vastutab aja sünkroniseerimise eest.

Active Directory keskkonnas määrab domeeni liikmete sisemise kella kindlaks volitatud domeenikontroller. Windowsi ajateenuse ülesehitus on hierarhiline: Tüvidomeeni (Root Domain) domeenikontroller, mis täidab PDCE FSMO rolli, muutub tsentraalseks sisemiseks kellaks kogu Active Directory infrastruktuurile. Domeenikontrollerit on võimalik konfigureerida käsuga net time /setsntp: selliselt, et see kasutaks sünkroniseerimise otstarbel mõnda välist kella. Väline kell võib asuda nii oma võrgu sees kui ka sellest väljas, kuid eelistada tuleks võrgusisest kella. Juhul, kui kasutatakse väljaspool võrku asuvat kella, peab olema tagatud selle usaldusväärsus. Klient-arvutid, mis ei ole domeeni liikmed, kasutavad standardina Microsoft 'i ajaserverit time.windows.com. Neid on aga võimalik ka ümber konfigureerida, nt käsuga net time või sissekandega (HKEY_LOCAL_MACHINE\ SOFTWARE\Microsoft\Windows\CurrentVersion\DateTime\Servers) selliselt, et need kasutaksid mõnda muud kella.

Täiendavad kontrollküsimused:

- Kas on koostatud ja ellu rakendatud vajadustest lähtuv seirekontseptsioon?
- Kas logimisfunktsioonid on sisse lülitatud?
- Kas olulisi süsteemisündmusi logitakse?
- Kas oluliste süsteemifailide ja registri sissekannete seireseadistusi on konfigureeritud?
- Kuidas tagatakse süsteemiaja sünkroniseerimine?

M 4.149 Windows'i faili- ja ühiskasutusõigused

Algatamise eest vastutavad: IT-juht, IT-turbespetsialist
Rakendamise eest vastutavad: IT-juht, administraator
Järgnevas tabelis on toodud ülevaade failide võimalikest pääsuõigustest.

Kaustadega seotud pääsuõigused	Failidega seotud pääsuõigused
Kaustade lehitsemine	Faili käivitamine
Kaustaloetelu koostamine	Andmete lugemine
Atribuutide lugemine	Atribuutide lugemine
Laiendatud atribuutide lugemine	Laiendatud atribuutide lugemine
Failide loomine	Andmete kirjutamine
Kausta loomine	Andmete lisamine
Atribuutide kirjutamine	Atribuutide kirjutamine
Laiendatud atribuutide kirjutamine	Laiendatud atribuutide kirjutamine
Alamkaustade ja failide kustutamine	
Kustutamine	Kustutamine
Volituste lugemine	Volituste lugemine
Volituste muutmine	Volituste muutmine
Omandiõiguste ülevõtmine	Omandiõiguste ülevõtmine

Tabel: kaustade ja failidega seotud pääsuõiguste ülevaade

Pääsuõiguseid saab rakendada kas failidele või kaustadele. Õiguste saamise käigus on võimalik kanda konkreetse kaustaga seotud õigused edasi failidele ja/või alamkaustadele, mille näol tekib lihtne võimalus muuta teatud failipuu osale kehtivaid pääsuõiguseid, tehes selleks vajaliku muudatuse ainult ühes kohas.

Kataloogi alla kuuluvate objektidega seotud õiguste edasikandmist ehk pärimist saab juhtida järgneva seitsme seadistusvõimlausega:

- ainult see kaust
- see kaust, alamkaustad ja failid
- see kaust, alamkaustad
- see kaust, failid
- ainult alamkaustad ja failid
- ainult alamkaustad
- ainult failid.

Funktsiooniga Only assume permissions for objects and/or containers in this container on lisaks võimalik kehtestada piirang, et õigused ei kanduks puustruktuuri alamvaldkonnale rekursiivselt edasi, vaid kehtiksid ainult konkreetse kataloogi objektidele.

Pärimismehhanismi raames saab objektidega seotud õiguste ülevõtmise juhtimiseks kasutada ka veel kahte täiendavat valikut:

- Funktsiooniga Adopt inheritable parent permissions saab objektidele kehtivate õiguste pärimist lubada ja blokeerida.
- Funktsioonidega Reset permissions in all child objects ja Enable processing of inheritable permissions erzwungen saab päritud õiguste ülevõtmist juhtida alampuu objektide kaupa.

Juhul, kui mõlemad õigused on omavahel konfliktis, kehtetustakse päritud õiguste ülevõtmine kohustuslikus korras. Windows 7 puhul on Programmide pääsuõiguste seadistamine ümber nimetatud Programmide laiendatud turvaseadistusteks ning lisatud on ka täiendavad registrikaardid Seire ja Efektiivsed õigused. Objektidele, st failidele, kaustadele ja programmidele tehtavate pöörduste seireks on võimalik Windows 7 keskkonnas konfigureerida registrikaarti Seire. Selle alt on võimalik nt valvata kaustadele tehtud vigaste pöörduste üle. Seda, st seire alla kuuluva sündmuse tuvastamist, on võimalik määrata kõikidele kaustas leiduvatele kaustadele ja failidele. Kasutajale antud õiguste kontrollimist toetab Windows 7 keskkonnas registrikaart Efektiivsed õigused. Iga faili, kausta jne kohta saab kontrollida, millised on konkreetse kasutaja või kasutajagrupi efektiivsed õigused seoses selle objektiga.

Nimetatud efektiivsed õigused võivad olla ka erinevad, nt pärimismehhanismi tõttu või põhjusel, et kasutaja kuulub korraga mitme erineva kasutajagrupi alla.

Kuna failidega seotud õiguseid eksisteerib suur hulk ning neile lisanduvad veel ka erinevad pärimismehhanismid, muutub pääsuõiguste haldamine kasutajate jaoks vägagi ebaülevaatlikuks.

Seetõttu on tavajuhtudel soovitav kasutada ainult standardseid pääsuõiguste kogumikke:

Kaustad	Failid	Sisu
Täielik juurdepääs	Täielik juurdepääs	Sisaldab kõiki üksikuid õiguseid
Muutmisõigus	Muutmisõigus	Lugemine , käivitamine , täiendavalt ka kustutamine
Lugemine, käivitamine	Lugemine, käivitamine	Lugemine , täiendavalt ka faili käivitamine
Kausta sisu kuvamine	-	
Lugemine	Lugemine	Andmete lugemine, atribuutide lugemine, laiendatud atribuutide lugemine, õiguste lugemine
Kirjutamine	Kirjutamine	Andmete kirjutamine, andmete lisamine, atribuutide kirjutamine, laiendatud atribuutide kirjutamine

Tabel: standardsed pääsuõigused

Windows 'i platvormide kasutust planeerides tuleb välja töötada ka failide ja kaustade pääsuõiguste kontseptsioon, mis määratleks vastavad õigused võimalikult detailselt. Siinjuures tuleb arvestada töökorraldusega kaasnevate ja ettevõtlusega seotud eripäradega. Windows 'i süsteemifailidega seotud õiguseid

on üldjuhul soovitav jagada ainult koos asjakohaste piirangutega. Järgnevate, seadistuste kohta tehtud ettepanekute puhul eeldatakse, et kasutajanimest Peakasutaja (Power-User) on loobutud, põhjusel, et haldamisega seotud ülesandeid ja administraatoritele jagatavaid volitusi käsitleb eraldi seisev administreerimiskontseptsioon.

Sel põhjusel tuleks kasutajanimi Peakasutaja kõikidest pääsuloenditest eemaldada. Lisaks on soovitav administreerimiskontseptsiooniga kehtestada volituste lahutamine, selliselt, et administreerimisega seotud õigused oleksid koondatud eraldi kontode alla. Järgneva näite puhul on lähtutud põhimõttest, mille järgi on kõik haldamisega seotud õigused antud kasutajagrupile Administraatorid. Volitused kehtivad ainult ära märgitud kataloogidele või failidele ning ei ole ette nähtud pärimiseks.

Järgnevas tabelis on välja toodud Windows 7 kasutuskeskkonna kataloogiõiguste määratlused:

Kataloog	Õigused
Süsteemi partitsiooni tüvikataloog	Administraatorid: täielik juurdepääs SYSTEM : täielik juurdepääs Kasutajad: lugemine, käivitamine; kausta sisu kuvamine; lugemine.
\WINDOWS	Administraatorid: eriõigused kausta läbiotsimine / faili käivitamine, kausta sisu loetlemine / faili lugemine, atribuutide lugemine, laiendatud atribuutide lugemine, failide loomine / failide kirjutamine, kaustade loomine / andmete lisamine, atribuutide kirjutamine, laiendatud atribuutide kirjutamine, kustutamine, volituste lugemine. Alamkaustadele on administraatoritel täielik juurdepääs. SYSTEM : sama, mis administraatoritel. Kasutajad: lugemine, käivitamine; kausta sisu kuvamine; lugemine. TrustedInstaller: kausta sisu kuvamine

WINDOWS\SYSTEM32\CONFIG	Administraatorid: täielik juurdepääs SYSTEM: täielik juurdepääs Kasutajad: lugemine, käivitamine; kausta sisu kuvamine; lugemine. LOOJA-OMANIK: täielik juurdepääs TrustedInstaller: kausta sisu kuvamine
WINDOWS\SYSTEM32\SPOOL	Administraatorid: täielik juurdepääs SYSTEM : täielik juurdepääs Kasutajad: lugemine, käivitamine; kausta sisu kuvamine; lugemine. LOOJA-OMANIK : täielik juurdepääs TrustedInstaller : kausta sisu kuvamine

Tabel: Windows 7 kataloogiõiguste määratlused

Ülemises tabelis nimetatud mõiste TrustedInstaller kohta vt M 4.341 Tervikluse kaitse alates Windows 7-st , lõik Windows Resource Protection ja TrustedInstaller.

Järgnevas tabelis on välja toodud Windows 7 kasutuskeskkonna failiõiguste määratlused:

Kataloog/fail	Õigused
Bootmgr BCD	System : lugemine, käivitamine Administraatorid: lugemine, käivitamine TrustedInstaller : täielik juurdepääs
autoexec.bat config.sys	Administraatorid: täielik juurdepääs SYSTEM : täielik juurdepääs Kasutajad: lugemine Vista : lugemine, käivitamine
TEMP	Administraatorid: täielik juurdepääs SYSTEM : täielik juurdepääs Kasutajad: eriõigused

PROGRAMS	Administraatorid: eriõigused kausta läbiotsimine / faili käivitamine, kausta sisu loetlemine / faili lugemine, atribuutide lugemine, laiendatud atribuutide lugemine, failide loomine / failide kirjutamine, kaustade loomine / andmete lisamine, atribuutide kirjutamine, laiendatud atribuutide kirjutamine, kustutamine, volituste lugemine. Alamkaustadele on administraatoritel täielik juurdepääs. SYSTEM : eriõigused nagu administraatoritel TrustedInstaller : täielik juurdepääs Kasutajad: lugemine, käivitamine; kaustade sisu kuvamine, lugemine.
Kasutajad	Administraatorid: täielik juurdepääs SYSTEM : täielik juurdepääs Kasutajad: lugemine, käivitamine; kausta sisu kuvamine.

Tabel: Windows 7 failiõiguste määratlused

Pääsuõiguste kontrollimine toimub sellisel juhul kahes astmes. Ühelt poolt on võimalik pääsuõiguseid siduda võrgu kasutamisõigusega, mis kehtestab piirid, kes tohib võrku pöörduda ja kes mitte. Teiselt poolt toimivad aga ka eelpool kirjeldatud, failisüsteemi tasandi määratletavad failide ja kataloogide juurdepääsuõigused.

Võrgukasutusõigusi saab juhtida ainult järgmiste õigustega:

- täielik juurdepääs,
- muutmine ja
- lugemine

Faili-, kataloogi- ja ühiskasutusõiguste määratlemisel tuleks arvestada järgmiste reeglitega:

- vältida tuleks ühiskasutuse andmist töökohaarvutitele
- samuti tuleks vältida ühiskasutuse andmist domeenikontrolleritele, kuna need sisaldavad endas konfidentsiaalset infot.
- Töökohaarvutitele ja domeenikontrolleritele väljastatud ühiskasutused tuleb põhjendada ja dokumenteerida ning selline tegevus tohib aset leida eranditult ainult pärast riskide hindamist.

- Kõikide ühiskasutusse lubamiste ja seeläbi ligipääsetavaks tehtavate andmete pääsuõigused tuleb välja jagada niis suurte piirangutega kui võimalik.
- Tuleks kaaluda, kas konkreetses olukorras oleks võib-olla mõttekas kasutajakonto Igaüks eemaldada ning kasutada selle asemel hoopis kasutajakontot Autenditud kasutajad.
- Pääsuõiguste kontseptsioon peab olema dokumenteeritud.

Kontrollküsimused:

- Kas on koostatud vajadustest lähtuv volituste ja pääsuõiguste kontseptsioon?
- Kas volituste ja pääsuõiguste kontseptsioonis on arvestatud ka töökorraldusest ja ettevõtlusest tingitud eripäradega?
- Kas kõikides arvutites, mille eelnev vanem operatsioonisüsteem on asendatud mõne uuema Windows 'i versiooniga, on kontrollitud kataloogide ja failidega seonduvaid kasutusõiguseid?
- Kas ühiskasutusse antud kataloogide jaoks seadistatud faili- ja kataloogiõigused sobivad võrgukeskkonnas kasutamiseks? Kas ühiskasutusse lubamisel rakendati võimalikult suuri piiranguid?
- Kas volituste ja pääsuõiguste kontseptsioon on dokumenteeritud?

M 4.151 Internet-PC turvaline installeerimine

Algatamise eest vastutavad: IT-juht, IT-turbespetsialist

Rakendamise eest vastutavad: administraator

Internet-PC installeerimise käigus tuleb vastu võtta rida otsuseid, mis mõjutavad süsteemi turvalisust.

Riistavara

Internet-PC riistavara tuleb komplekteerida selliselt, et see oleks varustatud ainult nende komponentidega, mis on selle kasutamise kontseptsioonis ette nähtud. Vajadusel tuleb sellised ajamid ja liidesed, mida ei ole ette nähtud, nt disketiajamid või sisesed modemid kas eemaldada või desaktiveerida (vt M 4.4 Eemaldatavate andmekandjate draivipilude ja väliste andmekandjate nõuetele vastav kasutamine). Süsteemi BIOS'e boot -järjekord tuleb määrata selliseks, et arvuti püüaks esimese võimalusena ennast käivitada alati kõvakettalt, nt C: A:, C only või Harddisk first/only. Juurdepääs süsteemi BIOSle peaks olema parooliga kaitstud. Neil juhtudel, kus kasutusele võetakse mõni operatsioonisüsteem, mille ei ole kohustuslikku kasutaja autentimist.

Operatsioonisüsteem

Pärast riistvara installeerimist tuleb installeerida kasutuskontseptsioonis ette nähtud tarkvara. Siinkohal tuleks arvestada, et levinud operatsioonisüsteemidel on erinevad turvafunktsioonid. Linux on varustatud nt tõhusate pääsuõiguste ja kasutajate teineteisest lahutamise funktsioonidega. Reeglina tuleks installeerida vaid sellised operatsioonisüsteemi komponendid, mida kindlaksmääratud kasutusvaldkonnas ka tõepoolest vajatakse. Eriti kriitilise pilguga tuleks üle vaadata „Services“ (Windows) ning „Daemons“ (Linux). Internet-PC ei tohiks reeglina internetis teenuseid pakkuda (vt lisaks M 5.72 Mittevajalike võrguteenuste desaktiveerimine (Unix)). Pärast installeerimist tuleb kõik võimalikud standardsed paroolid ära muuta. Linuxi puhul puudutab see eriti root password'i, juhul, kui kasutatav distro peaks seda standardse parooliga varustama. Enne kasutuselevõtmist tuleb installeerida kõik turbega seotud paigad ja värskendused.

Windows-operatsioonisüsteemide kohta leiab asjakohast infot Microsofti veebilehtedelt (www.microsoft.com). Linuxi kasutamise korral tuleks võimalikke paikasid ja värskendusi otsida vastava distro looja käest. Juhul, kui vastava distro looja pakutav info on ebapiisav, tuleks kasutada veel ka täiendavaid infoallikaid, nt aadressil www.linuxdoc.org. Täiendavaid teemakohaseid soovitusi leiate meetmetest M 2.35 Teabe hankimine turvaaukude kohta
M 4.107 Tootja ressursside kasutamine .

Windows-operatsioonisüsteemide kohta kehtivad lisaks eelnevale veel ka järgmised soovitused:

- Paigaldada tuleks kõige värskem Service Pack.
- Ainukese võrguprotokollina tuleks installeerida TCP/IP.
- Internetti pääsemiseks kasutatava TCP/IP protokolliga ei tohiks siduda mitte ühtki teenust

- Õigus failide ja printerite ühiskasutusse andmiseks tuleb desaktiveerida. Mitte ükski Share ei tohiks olla kättesaadav.
- Kui kasutatakse Internet Explorerit, tuleks valikutes Tools | Internet Options | Connections välja lülitada funktsioon Perform system security check before dialling, juhul, kui seda seal pakutakse.
- Kui rakendatava konfiguratsioon seda lubab, tuleks deinstalleerida WSH (Windows Scripting Host). Vastasel korral tuleks WSH'ga seotud failitüübid, nt.vbs ja.js siduda mõne editoriga.
- Microsoft PersonalWeb Server tuleks kas desaktiveerida, võimalusel koguni deinstalleerida.
- Juhul kui rakendatav versioon võimaldab kasutajaid lahutada, tuleks kõik ebavajalikud kasutajakontod, nt Guest kas desaktiveerida või kustutada.

Konto nimega Administrator tuleks ümber nimetada ja varustada tugeva paroolkaitsega.

- Windows 9x/ME kasutamise puhul tuleks kaaluda paroolkaitsega varustatud ekraani pimenduspildi kasutuselevõtmist. See pakub mõningast kaitset volitamata juurdepääsude vastu.
- Kui topeltklikkida faili, mille tüübiks on.reg, peab standardina sellele järgnema funktsioon Edit (avamine editoriga), mitte funktsioon Merge. Windows ME puhul jõuab vastavale dialoogiväljale läbi valikute Tools | Folder Options | File Types.
- Tuleks kaaluda, kas standardsete süsteemi- ja andmekataloogide, st -failide nimetuste asemelt tuleks võtta kasutusele hoopis teistsugused rajanimed (path names). Standardprogrammid otsivad paljudel juhtudel kindla nimega faile standardsetes kataloogides, mistõttu võib selline muudatus endaga kaasa tuua teatud täiendava kaitseefekti. Siiski tuleb arvestada, et selline tegevus võib teatud programmide puhul tekitada probleeme ühilduvusega.

Linuxi kasutamisel tuleks arvestada järgmiste soovitustega:

- Hoiduge inetd deemoni käivitamisest. Sõltuvalt distrost tuleb selle konfigureerimiseks kas muuta kas rc-startfaile või kasutada spetsiaalseid haldustööriistu.
- Hoiduda tuleks Portmap Daemon'i ja Name Service Caching Daemon'i käivitamisest.
- Juhul, kui kasutatav distro installeerib ka spetsiaalsed kaughaldamisteenused, nt linuxconf või swat, tuleks need desaktiveerida.
- Apache ning kogu muu WWW-Server-Software tuleks deinstalleerida.
- Prorammi sendmail ei tohiks käivitada töörežiimis Server. Ka kõik ülejäänud deemonid, mis võimaldavad elektronposti vastuvõttu läbi SMTP protokolli, tuleks kas deinstalleerida või vähemalt välja lülitada. Kui on üleüldse vajalik, tuleks meilide vastuvõtu jaoks kasutada POP3 või IMAP protokolli.
- Üheks täiendavaks turvameetmeks, kuidas internetist tulevatele rünnetele vastu astuda, on võtta kasutusele Linuxi paketifiltri funktsioon ipchains või iptables. Mõned distrod on selleks varustatud juba eelkonfigureeritud pakettidega. Täiendava turvameetmena võib installeerida nn Personal Firewall'i.

Selleks, et vastav lahendus ka toimiks, tuleb seda hoolikalt vastavalt konkreetsele rakendusvaldkonnale ka konfigureerida. Eriti oluline on teha programmile selline seadustus, et see ei hakkaks kasutajaid tüütama sagedaste hoiatustega, millega kasutajad ei oska mitte midagi peale hakata. Täiendavaid asjakohaseid soovitusi leiate meetmest M 5.91 Interneti-PC personaalse tulemüüri installeerimine .

Client -programmid

Lisaks vajaminevale operatsioonisüsteemile tuleks Internet-PCle installeerida vaid sellised täiendavad programmid, mis on vajalikud kasutuskontseptsioonis ette nähtud internetiteenuste kasutamiseks. Kui kasutuskontseptsioon näeb ette World Wide Web'i kasutuse, tuleb installeerida WWW-brauser. Levinumateks brauserprogrammideks on Internet Explorer, Mozilla Firefox, Google Chrome, Safari, Netscape Navigator ja Opera. Soovitusi nimetatud brauserite turvaliseks konfiguratsiooniks leiate meetmest M 5.93 Veebibrauseri turve Internet-PC kasutamisel . Juhul, kui Internet-PC abil on tarvis e-maile saata või vastu võtta, tuleb installeerida kas E-Mail-Client või kasutada mõnda WWW baasil toimivat meiliteenust. Levinud E-Mail-Client'ideks on Outlook, Outlook Express, Mozilla Thunderbird, Netscape Messenger ja KMail. Soovitusi nimetatud programmide turvaliseks konfiguratsiooniks leiate meetmest M 5.94 Meilikliendi turve Internet-PC kasutamisel). Kui kasutuskontseptsioon näeb ette täiendavate internetiteenuste nagu nt News või Instant Messaging kasutamise, tuleb vajadusel installeerida veel ka täiendavaid klientprogramme. Kõik programmid tuleks konfigureerida selliseks, et need pakuksid optimaalset turvalisust ning kasutajaid tuleb õpetada, kuidas neid turvaliselt kasutada.

Tools

Internet-PCde turvalise käitamise tagamiseks tuleb reeglina installeerida veel ka täiendavaid tarkvaratööriistu (tools), mida operatsioonisüsteemid ei sisalda.

Viirusetõrjetarkvara kasutamine on igas Internet-PCs möödapääsmatu. Vastavaid programme on saada erinevatelt tootjatelt. Oluline on see, et vastavaid andmebaase, mille alusel need programmid oma tööd teevad, regulaarselt värskendataks.

Levinud viirustõrje- programmid on selleks varustatud spetsiaalsete funktsioonidega. Siinkohal tuleb arvestada, et juhul, kui Internet-PCd ei ole omavahel võrku ühendatud, puudub ka võimalus nende programmide tsentraalseks juhtimiseks. Täiendavaid soovitusi arvutiviiruste vastase kaitse kohta leiate meetmest M 4.3 Viirusetõrjeprogrammide kasutamine . Internet-PC andmete varundamise kohta eksisteerib erinevaid kontseptsioone (vt M 6.79 Andmete varundamine Internet-PCde kasutamisel). Paljudel juhtudel läheb selle jaoks tarvis siiski eraldiseisvat tarkvaratööriista, mis viib vajaliku varukoopiate tegemise läbi kas automaatselt või poolautomaatselt. Tihti on võimalik andmevarunduseks ja andmete transpordiks majavõrku ja majavõrgust välja ära kasutada ühte ja sama lahendust.

Oluline on siinkohal tagada vajaminevate andmekandjate korrektne haldus.

Interneti teel andmete edastamisel võidakse neid kas volitamata lugeda või ka manipuleerida. Selliste ohtude ennetamiseks võib kasutusele võtta krüpteerimisprotseduurid. Näiteks eksisteerib terve rida tarkvaratööriistu, mis võimaldavad e-mailide krüpteerimist ja digitaalset allkirjastamist. Lisaks eksisteerib võimalus luua turvaline sidekanal mõne tuntud sidepartneriga, kasutades selleks VPNi (virtuaalset privaatvõrku). Juhiseid krüptograafiliste protseduuride kasutuselevõtu planeerimiseks leiate moodulist B 1.7 Krüptokontseptsioon .

Internetis ei tehta infot kättesaadavaks mitte ainult HTML formaadis, vaid kaWord-, Excel-, PowerPoint- või PDF-failidena Juhul kui selliseid faile on tarvis Internet-PCs otse vaadelda, tuleks selleks installeerida vastavad Viewerprogrammid.

Nimetaud Viewer 'id peaksid võimalusel suutma täita ka Makro-käskusid. Võimalusel tuleks Office-tarkvarapaketi installeerimisest Internet-PCle ilmtingimata loobuda. Kui see on aga hädavajalik, tuleks aktiveerida kõik makroviiruste eest kaitset pakkuvad paketti integreeritud funktsioonid.

Kõikidele installeeritud operatsioonisüsteemidele ja tarkvarakomponentidele tuleks juurde installeerida saadaolevad turvalisust puudutavad paigad ja värskendused. Need tuleks hankida usaldusväärsetest allikatest, nt otse tootjatelt (vt lisaks M 4.152 Internet-PC turvaline käitus).

Pärast seda, kui kõik operatsioonisüsteemi ja muu tarkvara komponendid on installeeritud, tuleks vastavast baaskonfiguratsioonist luua kujutis (image). Selle abil on võimalik süsteemi kiiresti taastada, kui installatsioon peaks kas avariide, vigaste konfiguratsioonimuudatuste või manipulatsioonide tagajärjel kasutuskõlbmatuks muutuma (vt lisaks M 6.79 Andmete varundamine Internet-PCde kasutamisel).

Kontrollküsimused:

- Kas operatsioonisüsteemi ebavajalikud teenused ning deemonid on deinstalleeritud või välja lülitatud?
- Kas installeeriti vaid sellised klientprogrammid, mis on vajalikud ette nähtud internetiteenuste kasutamiseks?

M 4.152 Internet-PC turvaline käitus

Algatamise eest vastutavad: IT-juht, IT-turbespetsialist

Rakendamise eest vastutavad: administraator

Internet-PC turvaliseks käitamiseks tuleb rakendada meetmeid, mis tegeleksid süsteemi hooldamisega. Vastasel korral tekib oht, et nt konfiguratsioonis tehtavate muudatuste kohta võivad ilmneda turvalüngad, või et ilmsiks tulnud tarkvaravigasid hakatakse ära kasutama kas sisesteks või väljast tulevateks rünneteks. Internet-PC käitamise raames tuleks tegeleda järgmiste ülesannetega:

Paikade ja värskenduste installeerimine turvalünkade kõrvaldamiseks

Sageli avastatakse tarkvaratoodetes vigu, mis võivad mõjutada turvalisust IT-süsteemides, millesse need tooted on installeeritud. Avastatud puudused tuleb tarkvarast võimalikult ruttu kõrvaldada, et ründajad nii seest kui ka väljast ei saaks hakata neid ära kasutama. Lahendusena avaldavad operatsioonisüsteemide või tarkvarakomponentide tootjad tavaliselt turvapaikasid või värskendusi, mis tuleb vigade kõrvaldamiseks installeerida vastavasse IT-süsteemi. Seetõttu peaksid Internet-PCde administraatorid ennast regulaarselt kursis hoidma võimalike avastatud tarkvara turvaaukudega ning installeerima nende kõrvaldamiseks välja töötud paikasid või värskendusi (vt M 2.35 Teabe hankimine turvaaukude kohta). Nagu igasuguse tarkvara puhul on ka paikade ja värskenduste puhul oluline, et need pärineksid usaldusväärsetest allikatest, võimalusel otse tootja või edasimüüja käest. Lisaks tuleb need enne installeerimist kindlasti ka veel viirusetõrjeprogrammiga üle kontrollida.

Internet-PC regulaarne kontrollimine ja seire

Internet-PC installatsioon ja konfiguratsioon ei ole reeglina mitte staatiline, vaid muutub kasutuse käigus pidevalt. Kasutajatel on nt võimalus märkida ära oma lemmiknetilehekülgi, salvestada oma meile või allalaadimisi ning määrata kindlaid seosed failiformaatide ja nende esitlusprogrammide vahel. Paljud programmid võivad kohati ka iseseisvalt teha olulisi muudatusi oma konfiguratsioonis. Pole ka välistatud, et Internet-PC installatsiooni ja konfiguratsiooni muutumise taga võivad olla koguni ründed või ründekatsed. Seetõttu peavad administraatorid pidevalt kontrollima kas Internet-PC installatsioon ja konfiguratsioon vastavad neile kehtestatud nõuetele ja soovitud väärtustele.

Siinkohal tuleks kontrollida:

- Kas Internet-PC riistavara konfiguratsiooni on säilinud muutusteta?
- Kas süsteemist on vahepeal eemaldatud või on sinna lisatud tarkvarakomponente?
- Kas BIOSi, operatsioonisüsteemi või programmide seadistusi on volitamata muudetud?
- Kas esineb viiteid sellele, et lokaalselt salvestatud andmed ei vasta kehtestud poliitikatele, nt kas esineb kõrvalekaldeid raja- (path) või failinimedes?

Lisaks tuleks aeg-ajalt analüüsida kasutada olevaid logimisfunktsioonide andmeid, nt syslog 'i Linux'i all ning, History 't Internet Exploreris. Vastavad logid võivad anda infot võimalike rünnete, ründekatsete ja Internet-PC väära kasuta-

mise kohta, nt infot keelatud lehtede külastamise kohta. Siinkohal tuleb siiski arvestada, et mõningate nimetatud logidega on võimalik suhteliselt kergesti manipuleerida. Turvapoliitikate teadlikku eiramist tavaliselt keegi väga avalikult sooritada ei julge. Väärkasutuse täiendavaks raskendamiseks võib Internet-PC seetõttu paigaldada ka sellisesse kohta, kus liigub mööda palju juhuslikke pealtnägijaid, nt raamatukokku. Internet-PC seire ja kontrollimise käigus tuleb täita andmekaitseseadustest ja organisatsiooni sisekorrast tulenevaid ettekirjutusi. Seetõttu tuleks vastavate meetmete rakendamine juba võimalikult varakult kooskõlastada töötajate esinduse ja andmekaitsespetsialistiga.

Süsteemi regulaarne reinstalleerimine

Üheks täiendavaks võimaluseks, kuidas soovimatuid muudatusi Internet-PCde installatsioonides ja konfiguratsioonides ära hoida, on neid süsteeme regulaarselt reinstalleerida. Reinstalleerimised ennetavad süsteemide avariisid, mis võivad tekkida kahjustada saanud või ebastabiilse installatsiooni tagajärjel. Internet-PCde reinstalleerimise intervall tuleb kindlaks määrata individuaalselt, võttes aluseks Internet-PCdele kehtestatud terviklusnõuded. Juhtudel, kus vastavaid reinstalleerimisi tuleks läbi viia lühikeste ajavahemike tagant, on soovitav süsteemist luua kujutis (image), mida on võimalik installeerida tervikuna. Vastasel korral võtavad vajalikud tööd liiga palju aega, kuna sellistel juhtudel tuleb kogu süsteem üksikute tarkvarakomponentide ja konfigureerimisparameetrite põhjal uuesti üles ehitada. Reinstalleerimise protseduur peab igal juhul olema kooskõlas Internet-PC andmevarunduskontseptsiooniga (vt M 6.79 Andmete varundamine Internet-PCde kasutamisel). Vastasel korral tekib oht, et reinstalleerimise käigus võivad kaotsi minna ka sellised andmed, mida ei ole võimalik hiljem enam taastada.

Kontrollküsimused:

- Kas on tagatud, et avastatud turvalünkadele välja töötatud paigad ja värskendused installeeritakse võimalikult operatiivselt?
- Kas logiandmeid analüüsitakse regulaarselt et tuvastada võimalikke ründekatseid ja väärkasutust?

M 4.161 Exchange / Outlook turvaline installeerimine

Algatamise eest vastutavad: IT-juht, Infoturbe osakond
Rakendamise eest vastutavad: administraator

Süsteemi tõrgeteta ja turvalise käitamise üheks peamiseks eelduseks on alati tarkvara turvaline installeerimine. Enne Exchange/Outlook tarkvara installeerimist tuleks olemasolevatest e-mailiandmetest luua varukoopia ning see kuhugi kindlasse kohta hoiule panna. Varukoopia tuleb teha nii serveri (nt mõnest varasema Exchange'i versiooni andmetest) kui ka kliendi andmetest.

Käesolevas peatükis tuuakse soovitusi järgnevate *Exchange* 'i teemade kohta:

- installeerimise ettevalmistus
- installeerimine
- installeerimise lõpetamine

Lisaks kajastatakse käesoleva meetme all veel ka soovitusi *Outlook 2000* installeerimise kohta. Viimased puudutavad ennekõike *Outlook 2000* algset konfigureerimist *Microsoft Office 2000 Custom Installation Wizard* 'iga.

Exchange 2000 installeerimise ettevalmistamine
Exchange/Outlook 2000 turvalise käitamise üheks eelduseks on platvormina kasutatava operatsioonisüsteemi, *Windows 2000 Server* 'i või *Professional* 'i turvaline konfiguratsioon. Kindlasti tuleb installeerida kõige värskem *Service Pack* ning kõik saadaolevad turvalisust puudutavad värskendused ja paigad. Täiendavat infot operatsioonisüsteemide *Windows 2000 Server* ning *Professional* turvalise installeerimise, konfigureerimise ja käitamise kohta leiate vastavatest *Windows 2000* moodulitest. Tervikluse tagamiseks on soovitav installeerida *Exchange* -tarkvara kas eraldi partitsioonile või veel parem, eraldi kõvakettale. Failisüsteemina tuleb kasutada NTFS-i. *Exchange Server* 'it on soovitav installeerida domeeni alla *Member* -serverina. Mitte mingil tingimusel ei tohi *Exchange Server* 'it installeerida mõnele domeenikontrollerile, kuna see võib avaldada negatiivset mõju kogu *Windows* -süsteemi turvalisusele.

Mitte mingisuguseid täiendavaid teenuseid Exchange-arvutitel
Turbe seisukohast tuleks eelistada lahendust, mille puhul installeeritakse *Exchange 2000* eraldi serverile. Sellel serveril tuleks võtta kasutusele ainult *Exchange 2000* käitamiseks hädavajalikud teenused.

Eraldiseisva installeerimiskonto kasutamine
Exchange 2000 installeerimiseks ei tohiks kasutada mõnda olemasolevat, administraatoriõigustega kasutajakontot. Kuna installeerimiskontole antakse

pärast installeerimist kõik *Exchange* 'i administreerimisega seotud õigused, on soovitav luua *Exchange 2000* installeerimiseks eraldi kasutajakonto. Sellel installeerimiskontol peavad olema kohapealse arvuti administreerimisõigused ning lisaks peab see olema liige gruppides nimega *Enterprise* ja *Scheme*. Pärast edukat installeerimist tuleks vastav kasutaja administraatorigruppidest *Enterprise* ja *Scheme* eemaldada. Ka kõikide täiendavate *Exchange Server* 'ite installeerimiseks tuleb kasutada iga installeerimise jaoks eraldi kasutajakontot. Seevastu pole täiendavate *Exchange Server* 'ite installeerimiseks enam tarvis administraatoriõiguseid *Enterprise* ja *Scheme*. Nende eraldi kontode puhul on piisav, kui neile on antud täielikud *Exchange*-administraatorite ning domeeniadministraatorite õigused.

Täiendavate *Exchange Server* 'ite järelevalveta installeerimine
Täiendavate Exchange-Serverite installeerimisel on soovitatav kasutada *Exchange* 'i nn järelevalveta installeerimist. Seeläbi väheneb ühelt poolt installeerimisega seotud tööde maht ning teiselt poolt saab seeläbi installeerimistööd mõnele teisele isikule edasi delegeerida. Järelvalveta installeerimise aluseks on *setup* -käivitusfail. Seda on võimalik luua nt järgnevalt: *e:*\. . . *exchange-install-cd*\. . . *setup.exe /CreateUnattend c:**temp**setup.ini* . Sellisel moel loodud käivitusfail *setup.ini* on loetav tekstifail, mis sisaldab erinevate Exchange'i komponentide seadistusi ning seetõttu saab seda kasutada ka installeerimise juurde kuuluva dokumentatsiooni koostamiseks. Installeerimine täiendavale arvutile käivitatakse failiga *e:*\. . . *exchange-install-cd*\. . . *setup.exe /UnattendFile c:**temp**setup.ini*. Käivitusfail võib sisaldada tundlikku informatsiooni, mis kirjeldab Exchange'i komponentide seadistusi. Kui sisaldab, tuleks käivitusfail krüpteerida.

Setup -käivitusfaili krüpteerimine
Tundliku info nagu nt võtmehaldusteenuse paroolide kaitsmiseks volitamata juurdepääsude eest võib käivitusfaili koostada ka krüpteeritud kujul. Seda võimalust tuleks kasutada ennekõike *Exchange* 'i installeerimistööde delegeerimisel. Krüpteeritud käivitusfaili saab luua nt käsuga *e:*\. . . *exchange-install-cd*\. . . *setup.exe /EncryptedMode /UnattendFile c:**temp**setup.ini* . Installeerimise käivitab samamoodi nagu ka krüpteerimata käivitusfaili puhul *e:*\. . . *exchange-in-stall-cd*\. . . *setup.exe /UnattendFile c:**temp**setup.ini.*

Exchange 2000 installeerimine
Exchange 'i installeerimise käigus tuleb arvestada järgmiste turbeaspektidega:

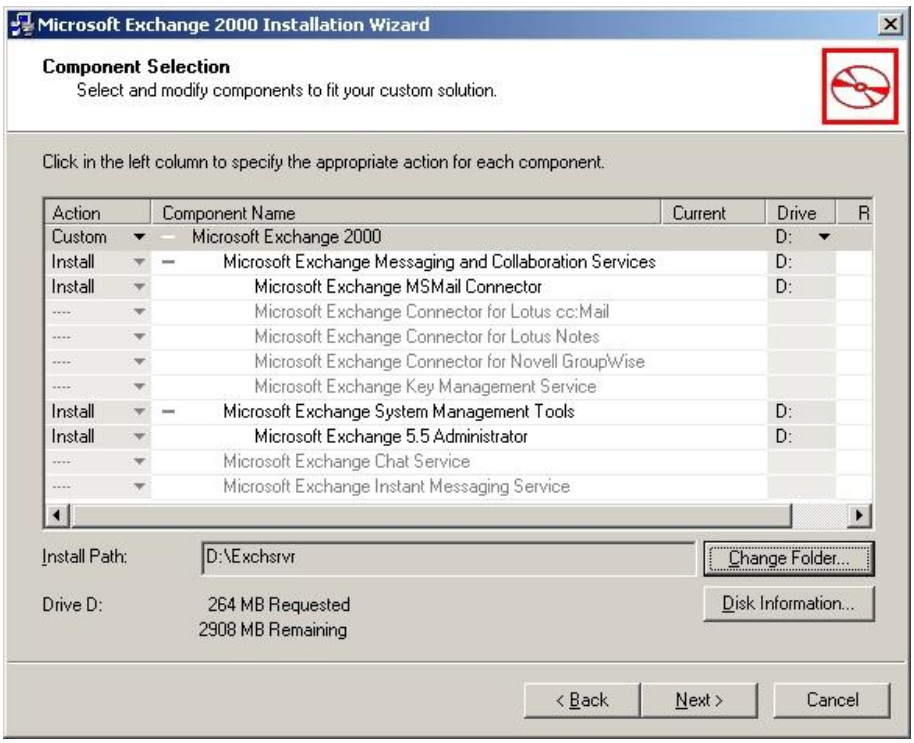
- installeeritavate komponentide valik
- installeerimistee (*path*)
- *Windows 2000* turvagrupi *Pre-Windows 2000 Compatible Access* olemasolu.

Viimase loetletud aspektiga tuleb arvestada vaid juhul, kui domeeni vastav domeenikontroller on tööle pandud koos *Windows 2000* -le eelnenud versioonidega ühilduvate seadistustega. Selle tunnete *Exchange Server* 'ite installeerimise käigus ära installeerimisassistendi vastava teate põhjal, mis liigitab domeeni ebaturvaliste hulka, kuna sellel on seadistused, mis ühilduvad *Windows 2000*- le eelnenud versioonidega.

Joonis: installeerimise rakendusprogramm

Sellisel juhul on soovitav üle kontrollida, kes kuuluvad grupi *Pre-Windows 2000 Compatible Access* alla ning eemaldada sellest grupist kõik liikmed, kes ei pea ilmtingimata selle grupi alla kuuluma.

Installeeritavate komponentide valikul tuleks otsus langetada vaid ülimalt hädavajalike komponentide kasuks. Kui kunagi hiljem on tarvis *Exchange Server'i* funktsioone laiendada, saab puuduvaid komponente alati hiljem juurde installeerida.



Joonis: installeerimisraja määramine

Installeerimisrajaks tuleb määrata uus ning *NTFS* -iga formaaditud partitsioon. Eraldi partitsioon tuleb moodustada, nagu eelnevalt juba mainitud, installeerimise ettevalmistustööde käigus. Oluline on tagada, et loodava *Exchange* -lahenduse infot, mis sisestatakse primaarse *Exchange Server* 'i installeerimisel, ei oleks hiljem võimalik enam muuta.

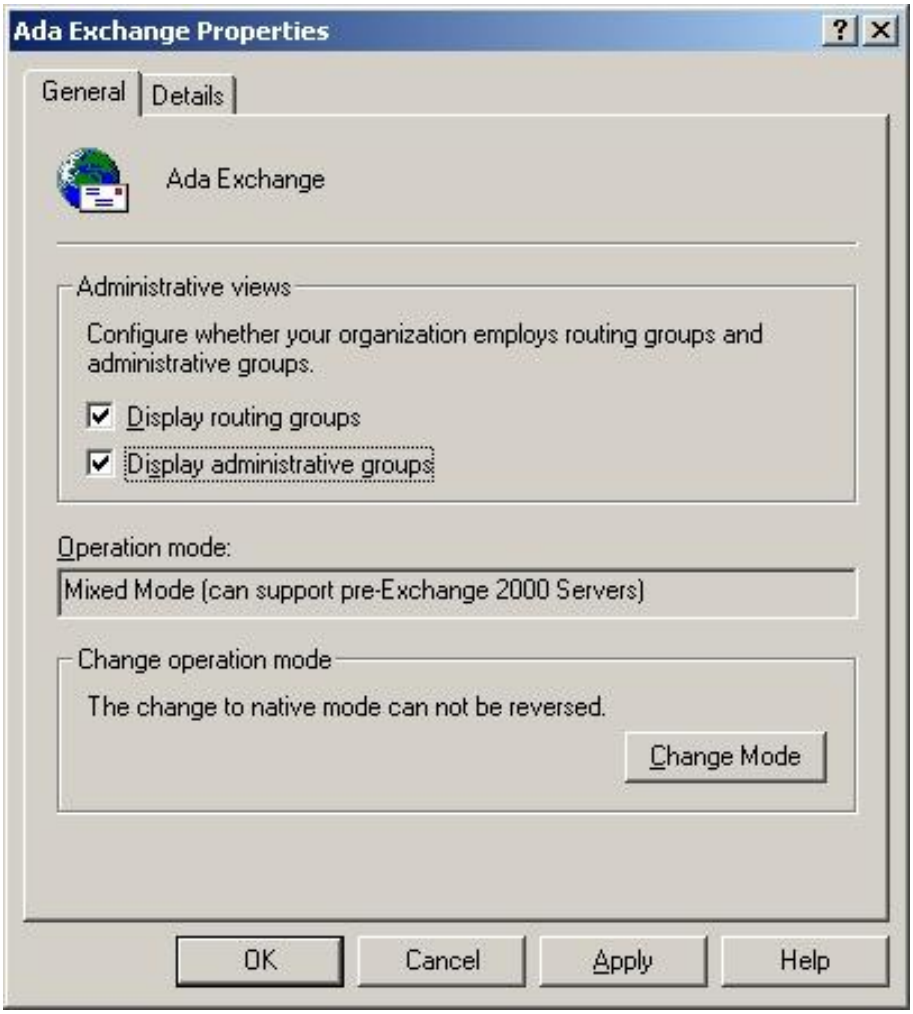
Exchange'i installeerimise lõpetamine

Service Pack 'id, turvavärskendused ja -paigad

Pärast *Exchange 2000* installeerimist tuleb paigaldada kõik *Exchange 2000* -le saadaolevad *Service Pack* 'id, turvavärskendused ja -paigad. Kuna *Exchange 2000* kasutab *Microsoft Internet Information Server'it* (*IIS* -i), tuleb installeerida ka kõik vastavad *IIS* -i *Service Pack* 'id, turvavärskendused ja -paigad. Kõikidel juhtudel kehtib reegel, et *Exchange* -arvutitel käitatavaid teenuseid ja rakendusi tuleb värskendada ning hoida kõige värskemal kujul.

Administratiivsete ja marsruutimisgruppide kuvamine

Pärast *Exchange 2000* installeerimist kehtib standardne seadistus, mille kohaselt administreerimise ning marsruutimisega seotud gruppe ei kuvata. Kuva sisselülitamiseks tuleb *Exchange* -süsteemis kasutada funktsioone *Display administrative groups* ja *Display routing groups* , mis asuvad üldiste seadete all. *Exchange* 'i seadeid saab vaadata *Exchange* 'i enda tööriistaga, mille nimi on *System-Manager*.



Joonis: *Ada Exchange* 'i seaded

Üldteavet *Outlook 2000* installeerimise kohta
Microsoft Outlook 'i installeerides on võimalik valida kolme erineva lahenduse vahel:

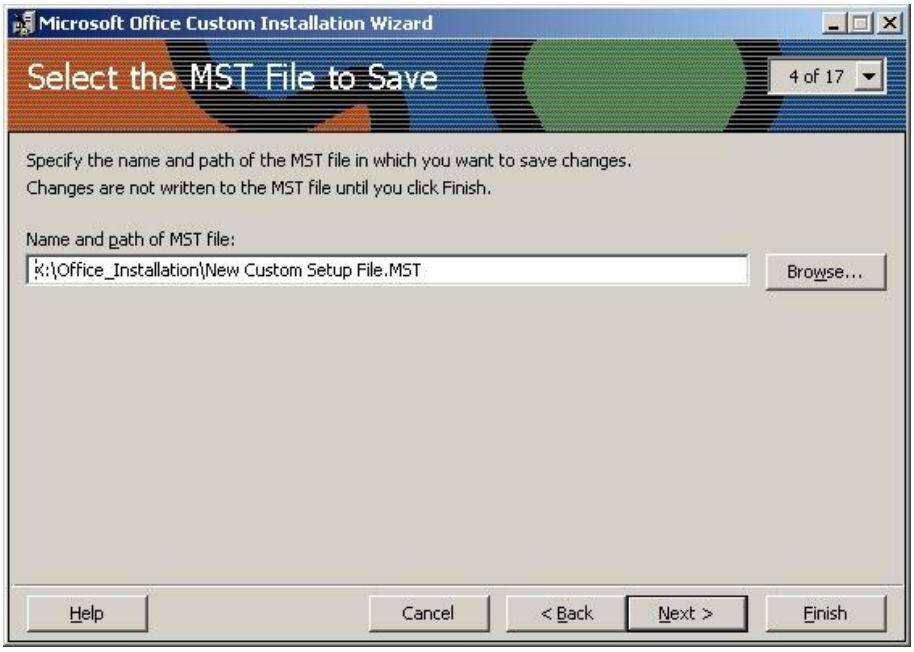
- ilma *Internet-Mail* 'i toeta
- koos *Internet-Mail* 'i toega
- ettevõtte ja töögruppide keskkonna toega, st *Exchange-Client* -lahendusena.

Esimene variant lubab kasutada ainult kontakte, kohtumiste aegasid ja dokumente. Interneti tugi võimaldab saata ja vastu võtta e-maile, milleks kasutatakse meiliprotokolle nagu *POP3* , *SMTP* ja *IMAP* . Selleks, et *Exchange 2000* keskkonnas saaks kasutada spetsiifilisi *Exchange* -funktsioone, tuleb *Outlook*

2000 installeerida eraldi *Exchange - Client* -lahendusena. Viimasest järgnevalt ka pikemalt. *Office 2000 Resource Kit'* i administreerimistööriistadega on võimalik tsentraalselt koostada *Outlook 2000* eelkonfigureeritud versioon, mis võetakse aluseks hiljem aset leidval jaotamise/installeerimisel. Eelkonfiguratsiooniga versiooni loomine aitab kaasa ühtlase turbeastme saavutamisele. Ettevõtetel on soovitav jaotada ainult eelnevalt oludega vastavaks kohandatud ning eelkonfigureeritud *Outlook 2000* versioone. Ettevõtte vajadustele sobiva *Outlook 2000* versiooni koostamiseks kasutatakse *Microsoft Office 2000 Resource Kit* 'i hulka kuuluvat *Custom Installation Wizard* 'it.

Outlook 2000 eelkonfigureerimine *Custom Installation Wizard* 'iga

Office 2000 Custom Installation Wizard pole ette nähtud mitte ainult *Outlook 2000* , vaid kogu *Microsoft Office* 'i paketi eelkonfigureerimiseks. Microsoft *Office 2000* alla kuuluva *Custom Installation Wizard* 'iga töötamise lõpptulemuseks on *Windows Installer Transform - MST* -fail, mis sisaldab installeerimisjuhiseid *Microsoft Installer* 'i tarbeks.



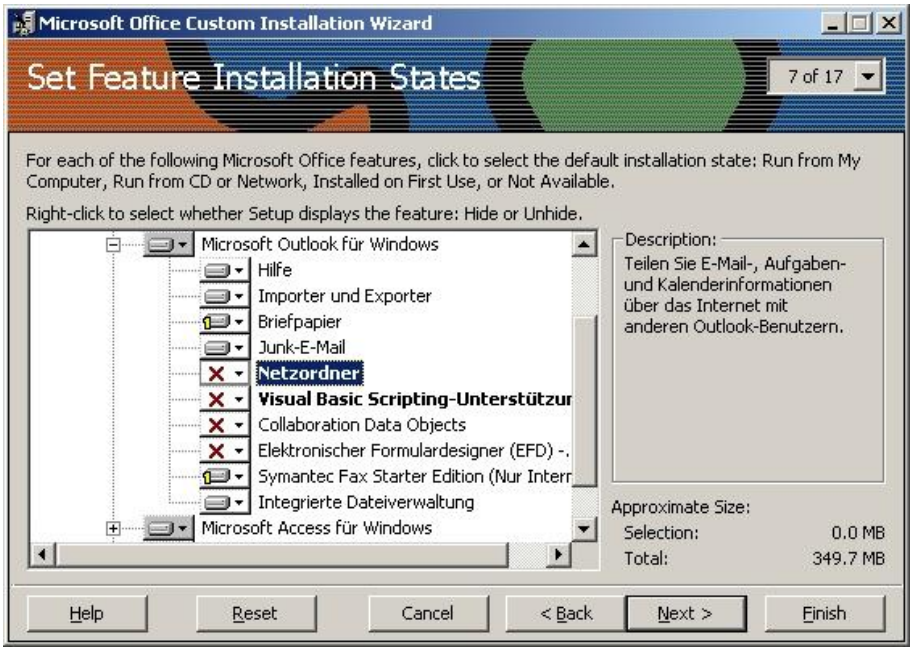
Joonis: *MST* -faili seaded

Custom Installation Wizard pakub uue versiooni installeerimise käigus võimalust, eemaldada süsteemist *Office* 'i komponentide nagu *Outlook* 'i, *Word* 'i, *PowerPoint* 'i, *Excel* 'i ja *Access* 'i vanemad versioonid. *Outlook 2000* installeerimise raames on soovitav eemaldada *Outlook* 'i vanem versioon.

Outlook 2000 jaoks installeeritavate komponentide valik

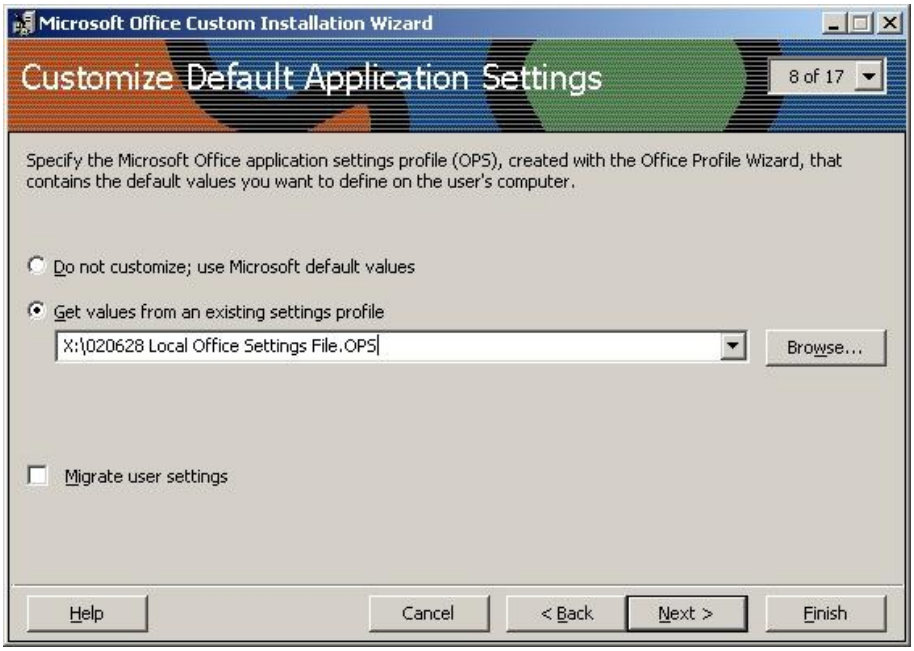
Outlook 'i kasutajate puhul on soovitav loobuda *Electronic Form Designer* 'i (*EFD*) rakendamisest, kuna aktiivsisuga dokumentide kasutamine toob endaga

kaasa täiendava ohuallika organisatsiooni intranetile. See komponent tuleks *Outlook 2000* mugandatud versiooni loomise käigus installeerimispaketist välja jätta. Samuti ei ole soovitav installeerida komponente nagu *Collaboration Data Objects* ja *Netzwork Folder*.



Joonis: rakenduse seadete kohandamine

Installation Wizard pakub võimalust kasutada juba eksisteerivaid *Microsoft Office* 'i seadistusi kohandamise lähteinfona. *Office* -paketi seadistuste eksportimiseks ja ühte faili kokkukogumiseks kasutatakse tarkvaratööriista *Office 2000 Profile Wizard* . Kui *Custom Installation Wizard* 'it kasutades ühtki juba olemasolevat *Office* 'i profiili lähtematerjaliks ei võeta, kasutatakse *Office 2000* standardseid seadistusi. Soovitav on kasutada mõnda juba olemasolevat, sobivalt konfigureeritud *Outlook 2000* installatsiooni profiili (vt M 4.165 Outlook 2000 turvaline konfigureerimine).



Joonis: seadistuste eelkonfigureerimine

Sõltuvalt sellest, millises režiimis Outlook 2000 käitatakse (*Exchange-Client* või ainult *Internet-Mail-Client*), tuleb teha vastavad seadistused.

Režiimis *Exchange-Client* töötava *Outlook 2000* puhul on võimalik seadistada standardseid profiile, *Exchange Server* 'it, isiklikke *Outlook* -kaustasid, *POP3* - ja *SMTP* -protokolle. Standardsete profiilide jaoks saab nt määrata, millised teenused (nt *MS Exchange Server Service*, *Personal Folder Service* või *Address Book Service*) peaksid neisse standardina kuuluma. Isiklike *Outlook* -kaustade (*Personal Folder* 'ite) seadistustes tuleks välja valida optimaalne krüpteerimine (vt M 4.165 Outlook 2000 turvaline konfigureerimine). *POP3* - ja *SMTP* -seadistustes tuleks sisse lülitada parooli turvaline autentimine ja *SSL* -i kasutamine. See eeldab muidugi mõista ka *Exchange Server* 'i enda asjakohast konfigureerimist.

Joonis: *Outlook* 'i installatsiooni kohandamine

Internet-Mail-Client režiimis töötava *Outlook 2000* puhul saab lisaks seadistada ka *POP3* , *SMTP* ja *LDAP* kasutamist. Kõikide protokollide jaoks on soovitav sisse lülitada parooli turvaline autentimine ja *SSL* -i kasutamine. See eeldab muidugi ka serveri enda asjakohast konfigureerimist.

Joonis: *Internet Explorer* 'i kohandamine

Custom Installation Wizard pakub lisaks ka võimalust asendada *Internet Explorer'i* vana versioon versiooniga nr 5. Siinkohal on soovitav koostada *Internet Explorer* 'i tarbeks lisaks ka veel ettevõtte või ametiasutuste vajadustele vastavaks kohandatud brauseritarkvara versioon. Selleks saab kasutada *Internet Explorer Administration Kit'* i (*IEAK*). *IEAK* -ga saab muuhulgas kohandada ka *Internet Explorer* 'i neid internetitsoone, mis mõjutavad otseselt *Outlook 2000* turvalisust seoses e-posti manuste töötlemisega (vt M 4.165 Outlook 2000 turvaline konfigureerimine).

Outlook 2000 installeerimine / tarkvara jaotamine

Pärast *Exchange 2000* süsteemide installeerimist ja konfigureerimist tuleb jaotada *Outlook 2000* kliendid. Klientide installeerimine leiab reeglina aset mõne tarkvarajaotuse mehhanismi abil, mistõttu saab vastavaid *msi-Package* 'eid klientideni toimetada ka *Active Directory* vahendusel.

Outlook 2000 üksikinstallatsioon

Outlook 2000 üksikinstallatsiooni jaoks on kohandatud installatsioonipaketi loomisele kuluv vaev liiga suur. Seepärast võib *Outlook 2000* tarkvara installeerida ka lokaalselt. Sellise installatsiooni puhul tuleks järgida neid samu, eelpool toodud soovitusi (nt jälgida installeeritavate komponentide valikut). Lisaks tuleb juba installeerimise käigus arvestada meetme M 4.165 Outlook 2000 turvaline konfigureerimine soovitustega.

Täiendavad kontrollküsimused:

- Kas *Exchange 2000* serverid on üles seatud füüsiliselt kaitstud keskkonda-

desse nagu serveriruumi või serverikappi?

- Kas administraatoriõiguste ja pääsuõiguste planeerimisel ja ellurakendamisel on arvestatud konkreetsete vajadustega?
- Kas objektidega seotud kasutusõiguseid, juhul kui need võeti üle *Exchange 5.5* tarbeks, on samuti värskendatud?

M 4.162 Exchange 2000 serverite turvaline konfiguratsioon

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator

Pärast *Exchange 2000* installeerimist tuleb tarkvara konfigureerimise teel turvaliseks muuta. Käesolev meetmes antakse soovitusi *Exchange 2000* sobiva konfiguratsiooni kohta. Enne kui administraator alustab pärast *Exchange 2000* installeerimist konfigureerimisega, tuleks rakendada üldisi administreerimissoovitusi, nt sobivate *Exchange* 'i haldusgruppide loomist. *Exchange 2000* konfigureerimisel tuleb ennekõike arvestada järgnevaga:

- administratiivsete meetmete rakendamine,
- juurdepääsuõiguste piiramine,
- *Exchange* -konnektori ja muude komponentide konfigureerimine,
- virtuaalse *SMTP* -serveri ja *POP3* , *IMAP4* ning *NNTP* kommunikatsiooniprotokollide konfigureerimine ja
- logimine.

Algrežiimi (*native mode*) kasutamine
Ühilduvuse tagamiseks vanema versiooniga *Exchange 5.5* töötab *Exchange 2000 Server* pärast installeerimist nn segarežiimis (*mixed mode*). Tuleb jälgida, et *Exchange* -keskkonna nimetusi *native mode* ja *mixed mode* ei aetaks segamini *Windows 2000* domeenikontrollerite sarnaste nimetustega. Exchange-serverit ei ole enamatel juhtudel soovitatav kasutada *segarežiimis*. *Algrežiim* tuleks kasutusele võtta kohe pärast seda, kui kõik *Exchange* -serverid on üle viidud *Exchange 2000* peale või kui *Exchange 5.5* servereid ei ühendata *Exchange* -süsteemiga. Exchange 2000 serveri ümberlülitamine *algrežiimile* toimub *Exchange System-Manager* 'is *Exchange* 'i organisatsiooniobjekti omaduste all. Selleks tuleb registrikaardil *General* klõpsata nupul *Change Mode*. Ümberlülitamine *algrežiimile* kaotab ühilduvuse varasemate versioonidega (*Exchange 5.5* -ga) pöördumatult.

Haldus

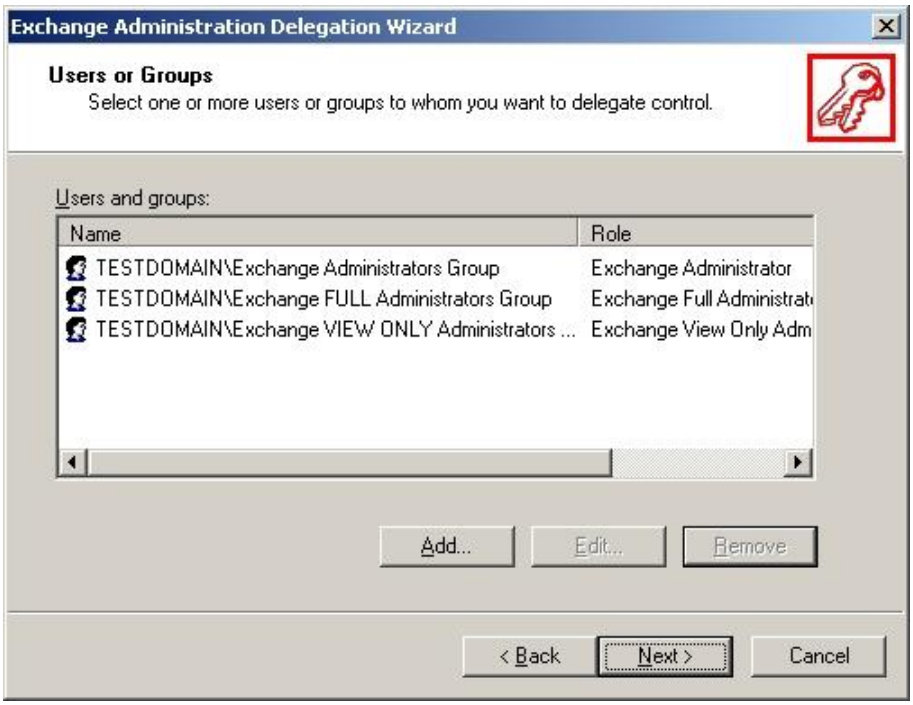
Eraldi kasutajagruppide sisseseadmine *Exchange* 'i haldamiseks
Exchange' i administreerimise saab jaotada mitme administreeriva grupi vahel. Selle aluseks on kolm eelseadistatud *Exchange* 'i administreerimisrolli:

- *Exchange Full Administrator* (*Exchange* 'i täieõiguslik administraator) on mõeldud *Exchange* -info ja *Exchange*- volituste haldamiseks.

- *Exchange Administrator* (*Exchange* 'i administraator) on mõeldud ainult *Exchange* -info haldamiseks.
- *Exchange View Only Administrator* (*Exchange* 'i vaatamisõigustega administraator) on mõeldud ainult *Exchange* 'i info vaatamiseks.

Soovitatav on luua kolm eriotstarbelist turvagruppi, millest igale määratakse üks ülal mainitud *Exchange* 'i rollidest. Administreerimise ülesehitamisel tuleks isikute asemel lähtuda gruppidest: volitused tuleks siduda gruppidega, mitte üksikute kasutajakontodega. See kergendab oluliselt haldamist ja muudab selle ülevaatlikumaks – seeläbi kõrvaldatakse võimalik veaallikas. *Exchange* 'i administraatoreid hallatakse gruppidesse kuulumise alusel.

Rollide määramine loodud administratiivsetele gruppidele toimub delegeerimisassistendi (*Delegation Wizard* 'i) abil *Exchange System-Manager* 'i all.



Joonis: kasutajakontod ja serveripoolsed kasutajaprofiilid

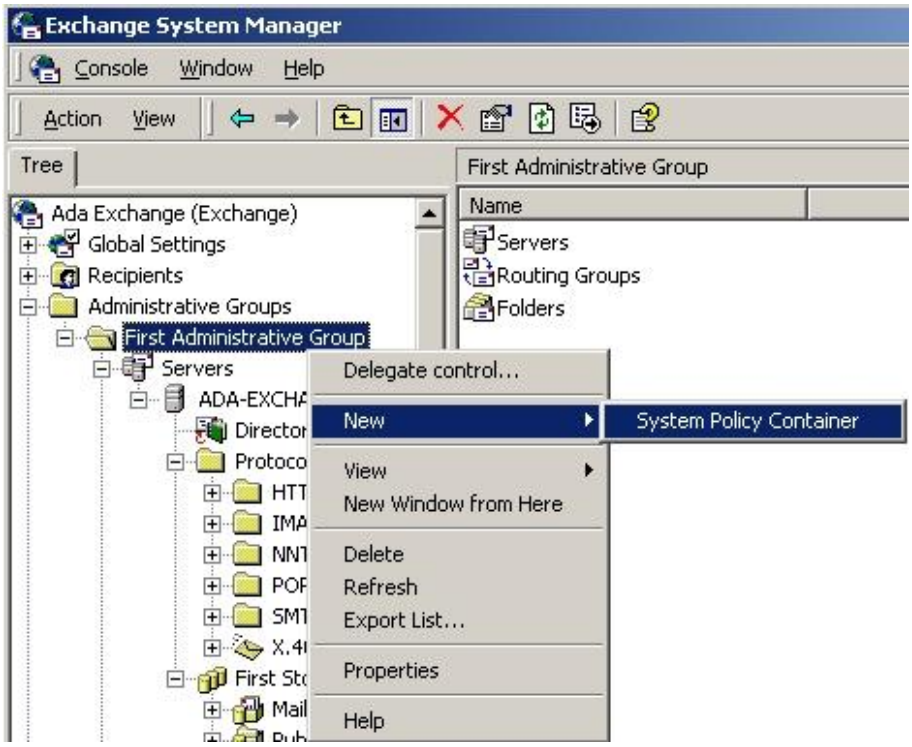
Kasutajakontode ja uudistegruppide loomisel tuleb lähtuda vastavast turvapoliitikast (vt M 2.248 *Exchange/Outlook 2000 turvapoliitika määratlemine*). Esmajoones tuleb siinkohal otsustada, millistele kasutajatele anda *Exchange* -postkast ja kas uudistegrupid võetakse kasutusele või mitte. Soovitatav on kasutada serveripoolseid kasutajaprofiile. Kui kasutajal on serveripoolne profiil, võetakse kasutaja seadistused igal domeeni sisselogimisel üle tööjaama kohalikku konfiguratsiooni (*Registry* 'sse). Seeläbi on võimalik saavutada arvutist sõltumatu juurdepääs *Exchange* -andmetele.

Exchange 2000 teenuste süsteemikontod

Exchange 2000 koosneb mitmest teenusest, mis suhtlevad omavahel. Suhtlemine nõuab Kerberos-protokollil põhinevat autentimist. Teenused töötavad seejuures standardina *Windows 2000* konto *LocalSystem* all. *Windows 2000* muudab nende kontode parooli automaatselt iga 7 päeva järel. *Exchange 2000* serveri integreerimisel *Exchange 5.5* keskkonda tuleb luua kasutajakonto sarnane teenusekonto. Asukoha piires peavad *Exchange* 'iga seotud teenused kasutama suhtlemiseks ühist asukoha-teenusekontot, mille vahendusel toimub ka autentimine. *Exchange 2000* serveri integreerimisest *Exchange 5.5* keskkonna alla tuleks üldjuhul hoiduda. *Exchange* 'i jaoks olulised teenused – esmajoones *Information Store Service*, *Routing Engine Service* ning *System Attendant Service* – töötavad pärast tüüpinstalleerimist konto all nimega *Local System*, millel on kohalikus serveris laiaulatuslikud volitused. Nimetatud *Exchange* -teenuste jaoks saab soovi korral luua eraldi kontod koos kohandatud volitustega. Tuleb aga arvestada, et see võib testimise ja konfigureerimisega seoses olla väga töömahukas.

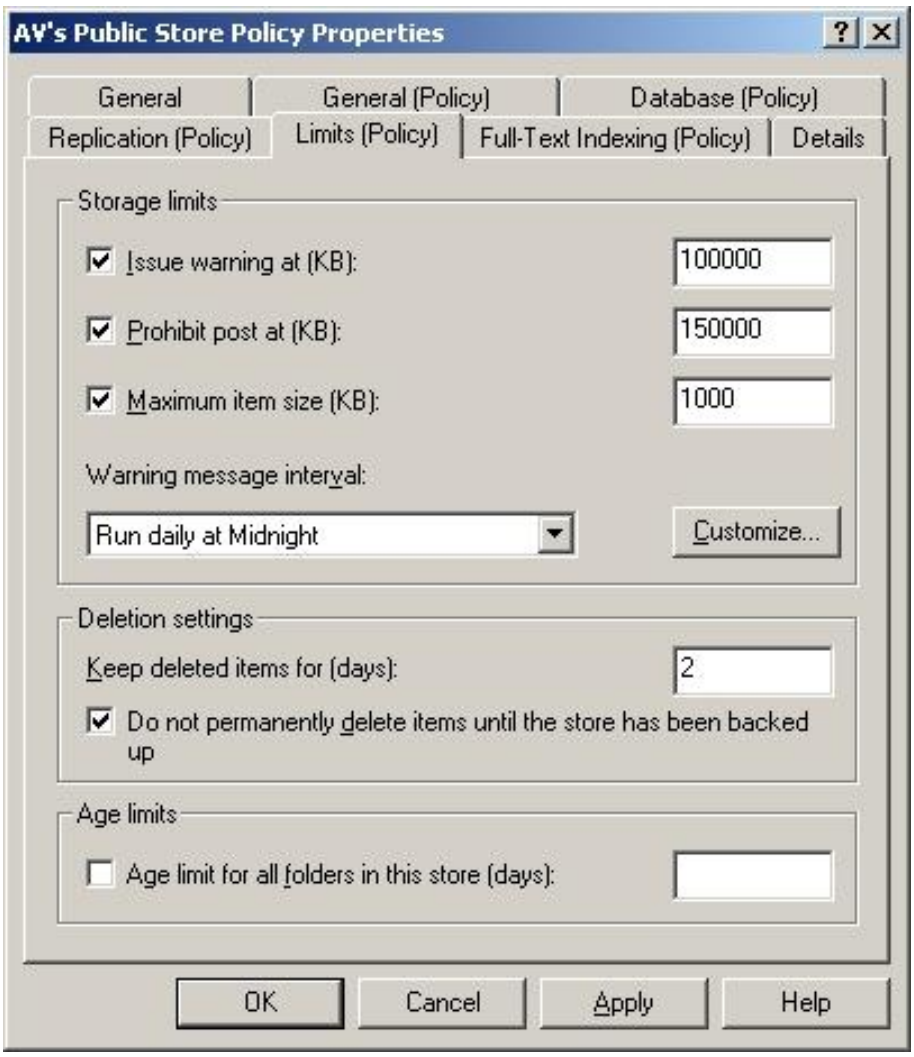
Exchange'i süsteemipoliitikate rakendamine

Exchange 2000 süsteemipoliitika võimaldab samal ajal konfigureerida mitut Exchange-serverit. Süsteemipoliitikaid on kolme erinevat liiki: serveripoliitika, *Mailbox-Store* -poliitika ja avalike kaustade poliitika. Poliitika rakendamine võimaldab ühtset konfigureerimist ja vähendab seega valede konfiguratsioonide ohtu. Seega on soovitatav kasutada *Exchange* 'i poliitikaid ja määratleda need iga defineeritud administratiivse grupi lõikes eraldi.



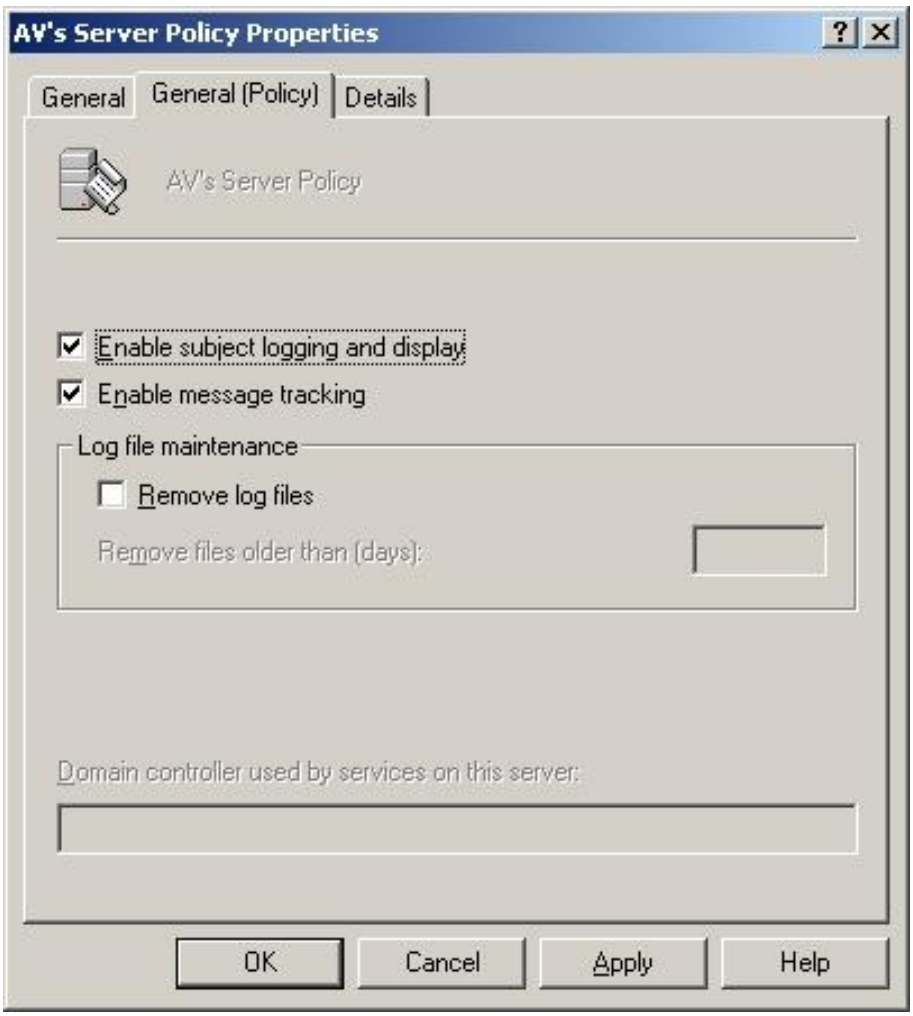
Joonis: *Exchange* 'i süsteemipoliitikad

Mailbox-Store -poliitika ja avalike kaustade poliitika võimaldavad kehtestada salvestamispiiranguid. Limiidi saavutamisel saab väljastada hoiatusi, keelata teadete saatmise või ka saatmise ja vastuvõtmise. Mahupiirangute määramisel tuleks lähtuda ettevõtte/ametiasutuse vajadustest. Lisaks tuleb *Mailbox-Store* -poliitikas ja avalike kaustade poliitikas teha vastavad seadistused, mis lubavad kustutatud teadete lõplikku kustutamist alles pärast varukoopia tegemist.



Joonis: *Mailbox-Store* -poliitikad

Serveripoliitikas tuleks aktiveerida teadete seire- ja logimisvalikud. Selle käigus ei tohi kustutada logifaile.

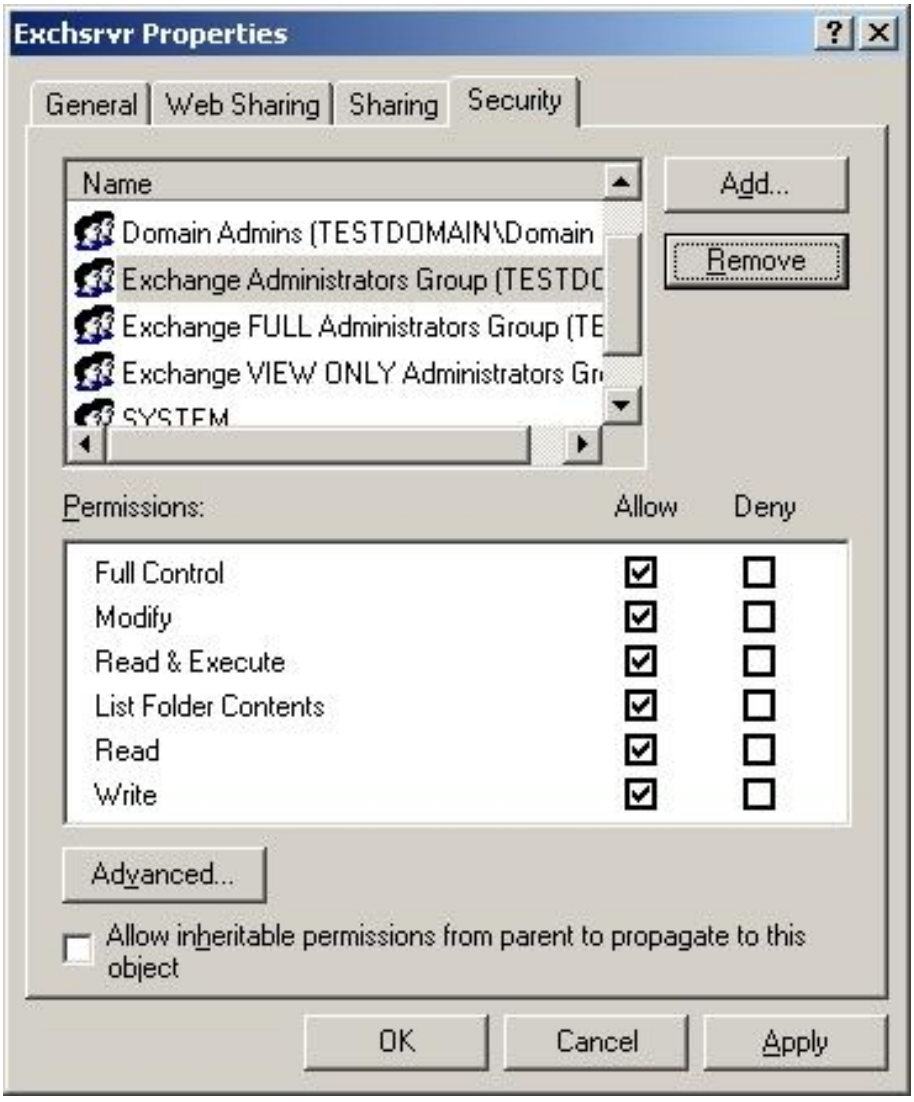


Joonis: juurdepääsuõiguste piiramine

Exchange -kataloogi standardsed *NTFS* -volitused tuleb kohandada selliseks, et selle kataloogi konfidentsiaalsetele andmetele pääseksid ligi ainult volitatud administraatorid ja süsteemikontod (nt andmebaasid ja ülekandeprotokollid). Tüüpseadistusi tuleb seega kohandada järgnevalt:

- Keelata grupi *Everyone* juurdepääs kataloogipuule (st eemaldada olemasolevad volitused).
- Kõik volitused tuleks määrata järgnevatele gruppidele:
- *SYSTEM*
- *CREATOR OWNER*
- *Domain Admins*
- < *Exchange Administrator Groups* > (seadistatud vastavalt eelneva lõigu kirjeldusele).

- Kui plaan näeb ette *Outlook Web Access* 'i (OWA) kasutamist, tuleb autenditud kasutajate grupi (*Authenticated Users*) jaoks tagada lugemis- ja käivitamisõigused.



Joonis: pääsuõiguste piirangute määratlemine

Installeerimise käigus sisse seatud *Exchange* 'i võrgukasutuse ühiskasutusõiguseid tuleb samuti kohandada. Lisaks ülal loetletud pääsuõigustele peab kohalik arvutikonto saama täieliku juurdepääsu nendele ühiskasutusõigustele. Juurdepääsuõigused kontole *Everyone* tuleks enamikel juhtudel volituste hulgast eemaldada.

Muuhulgas seatakse sisse järgnevad võrgu ühiskasutusõigused:

- *\Address* , ühiskasutusse antud kui *Address* . See võimaldab juurdepää-

su aadressigeneraatori *DLL* -failidele. Standardina on administraatoritel ja kohalikul arvutikontol sellele ühiskasutusele täielik juurdepääs. Juurdepääs kontole *Everyone* on pärast installeerimist piiratud lugemisõigusele.

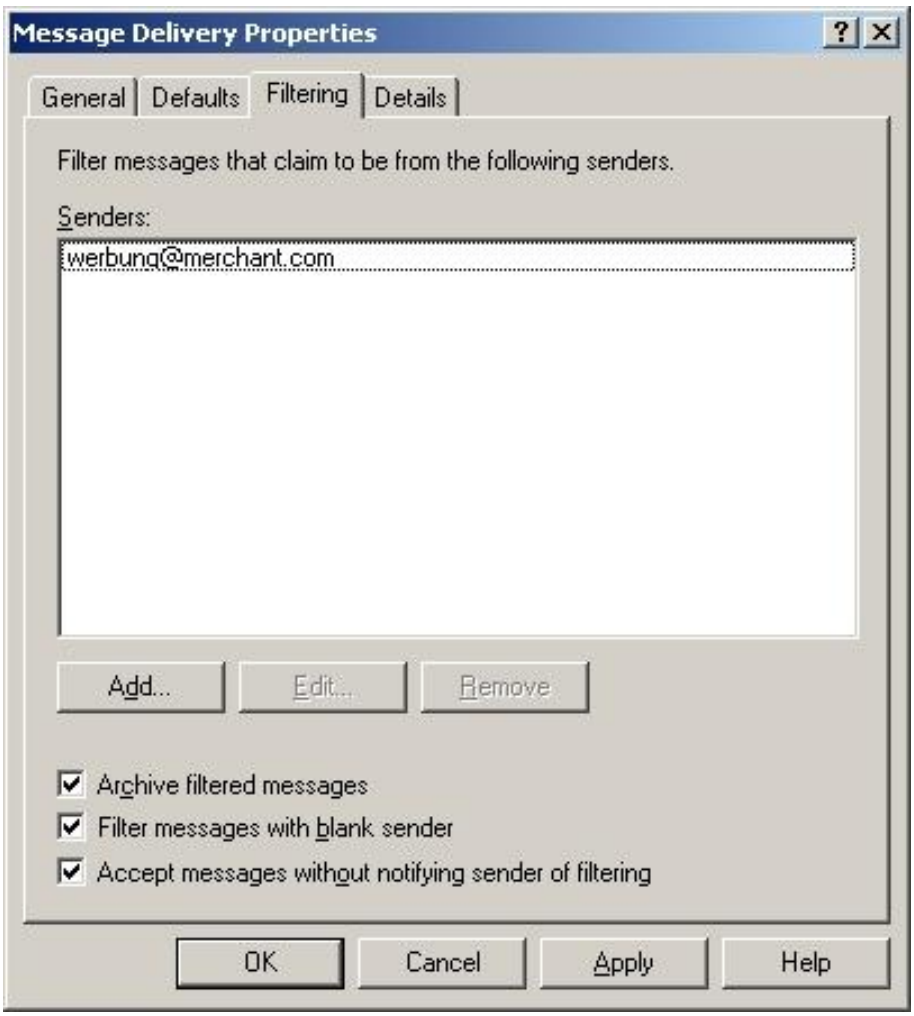
- *\Programs\Exchsrvr\.log* , ühiskasutusse antud kui *.log* . Sellesse kataloogi salvestatakse teadete jälgimiseks olulised logifailid. Logifailid sisaldavad infot meilide saajate, meilide suuruse, saatjate, saatmisaegade ja võib-olla ka meilide teemaribade kohta. Standardina on administraatoritel ja kohalikul arvutikontol sellele ühiskasutusele täielik juurdepääs. Juurdepääs kontole *Everyone* on pärast installeerimist piiratud lugemisõigusele.
- *\Programs\Exchsrvr\Connect\Msmcon\Maildata* , ühiskasutusse antud kui *Maildat$*. See võimaldab juurdepääsu peidetud võrgu ühiskasutusele *MS Mail* konnektoril. Pärast installeerimist on tüüpsättena täielik juurdepääs sellele ühiskasutusele administraatoril, kohalikul arvutikontol ja kontol *Everyone*.

Exchange 2000 objektide juurdepääsuõiguste piiramise kohta leiate lisainfot meetmest M 4.163 Exchange 2000 objektide pääsuõigused .

Globaalsed *Exchange* -seadistused

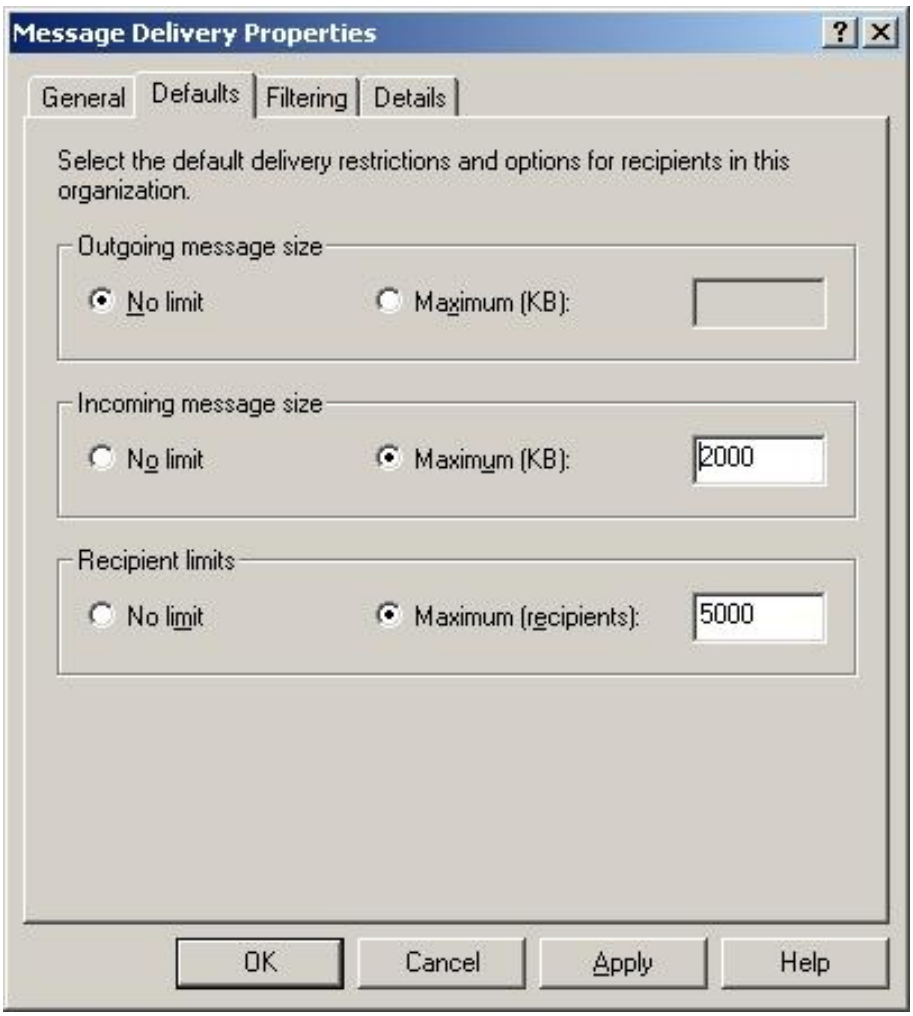
Teadete filtreerimine
Exchange 2000 võimaldab aktiveerida serveripoolset teadete filtreerimist. Kuna blokeerida saab vaid üksikuid saatjaid ja sisufiltreid defineerida ei ole võimalik, on see meede rämpsposti vastu võitlemiseks ebatõhus. Teatud olukordades võib teadete filtreerimine siiski ka kasulik olla. Selle kasutamisel tuleks kõik filtreeritud meilid logida ja mitte informeerida väljafiltreeritud meili koostajat asjaolust, et on aset leidnud meilide filtreerimine.

Välja tuleks filtreerida ka tühja saatjaväljaga meile. Need konfigureerimised tehakse registrikaardis *Filtering* meilide saatmise (*Message Delivery Properties*) all *Exchange* -tervikhalduses.



Joonis: teadete saatmise seadistused

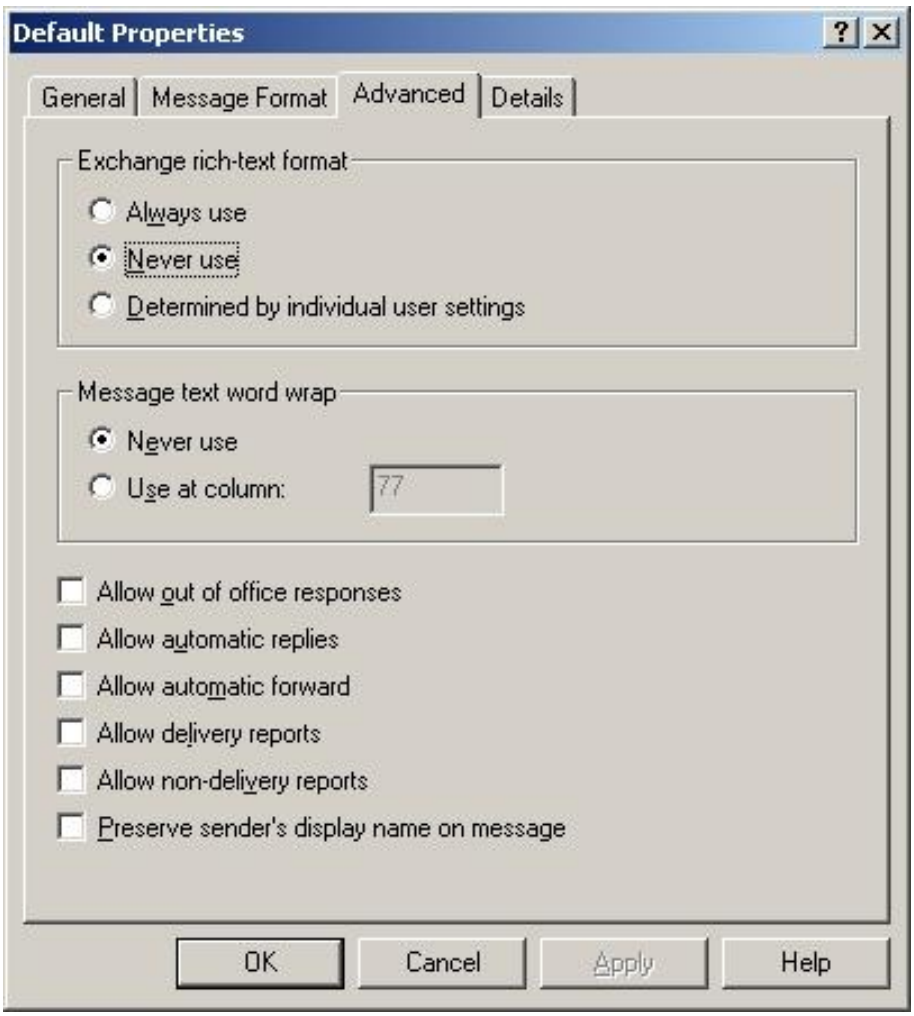
Teate maksimumsuuruse piiramine
Ühe võimaliku meetmena kaitseks *DoS* -rünnete (*Denial of Service*) vastu saab määrata nii saabuvate kui väljuvate meilide jaoks suurusepiirangu. Saabuvate teadete suurust tuleks piirata. Seda saab teha registrikaardis *Defaults* virtuaalse *SMTP* -serveri teadete kättetoimetamise (*Message Delivery Properties*) seadistuste all.



Joonis: teadete kättetoimetamise omadused

Eriteadete käsitsemine

Automaatsed lugemis- ja vastuvõtukinnitused, samuti *Out-of-Office* -teated võivad põhjustada (ka tahtmatuid) *Denial-of-Service* -ründeid. Kui ettevõttes/ametiasutuses pole e-posti kinnituste ja *Out-of-Office* -teadete kasutamine ilmtingimata vajalik, oleks parem selliste eriteadete kasutamine *Exchange* -tervikhalduses täielikult ära keelata. *Exchange* -tervikhalduse tüüpseadistustes (registrikaardis *Advanced*) tuleks kõik eriteadete tüübid desaktiveerida.



Joonis: tüüpseadistused

Exchange -konnektori konfiguratsioon

Mitme serveriga keskkonnas tuleb tagada teadete edastamise turvalisus, mis nõuab marsruutimiskonnektori asjakohast konfigureerimist. Marsruutimisgrupi serverite vahelisi ühendusi konfigureeritakse installeerimisel automaatselt. Üksikute konnektorite seadistusi tuleb siiski kohandada, et tagada kõrgem turvalisus. Tuleb arvestada, et *Exchange* -konnektori konfigureerimine nõuab lisaks *Exchange* 'i administraatoriõigustele ka Windows'i administraatoriõigusi.

Liiasusega ühenduste sisseseadmine

Käideldavuse tagamiseks tuleks sisse seada liiasusega ühendused. Näiteks saab SMTP- või marsruutimisgrupi konnektori kasutamisel määratleda mitu nn *Bridgehead* -serverit (kohalikku ja eemalasuvat). X.400-süsteemidega ühendamisel tuleks kasutata mitut X.400-konnektorit.

Konnektorite üldised piirangud

Kõikide *Exchange* -konnektorite jaoks saab määrata üldised piirangud, mis puudutavad teadete suuruseid. Need suurusepiirangud on üheks *Denial-of-Service* -rünnete eest kaitsvaks meetmeks. Seda tuleb teha vastava konnektori seadistustes, sisupiirangute registrikaardis *Content Restrictions.*

Joonis: sisupiirangud

Lisaks saab *Exchange* -konnektoreid konfigureerida selliselt, et juurdepääs teatud kasutajatele või gruppidele on kas lubatud või keelatud. Seda seadistatakse konnektori seadistustes, saatmispiirangute registrikaardis *Delivery Restrictions*. Kõikide kirjeldatud piirangute mõjumahakkamiseks tuleb Windowsi registris aadressil *HKEY_LOCAL_MACHINE / System / CurrentControlSet / Services*

/ Resvc / Parameters sisestada võti *CheckConnectorRestrictions* andmetüübiga *REG_DWORD* ja väärtusega *1*.

Marsruutimisgrupi konnektor

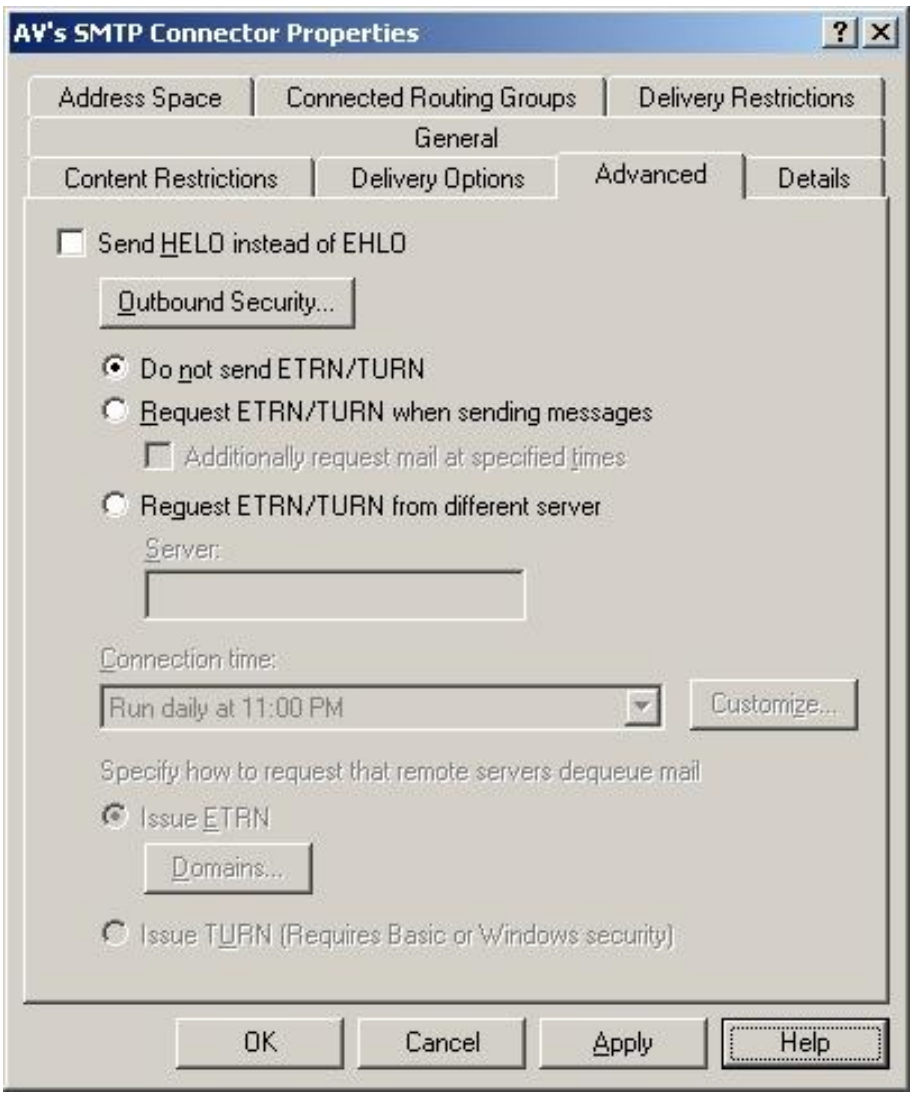
Marsruutimisgrupi konnektorit kasutatakse erinevate marsruutimisgruppide ühendamiseks. Marsruutimisprotokollide standardprotokolliks on SMTP. *Exchange* -serverite käitamisel segarežiimis (*mixed mode*) toimub kommunikatsioon *Exchange 5.5* serveritega RPC vahendusel. Kuna marsruutimisgrupi konnektorid ei võimalda krüpteerimist, tuleks neid konfidentsiaalsete andmete edastamisel läbi ebaturvaliste kanalite kasutada ainult koos *IPSec* -iga. Marsruutimisgrupi konnektori asemel võib kasutada ka *SMTP* -konnektoreid, mis toetavad ka krüpteerimist.

X.400-konnektor

X.400-konnektorit saab kasutada X.400-süsteemidega ühendamiseks. Kuna X.400-konnektor tunneb vaid loetavas tekstivormis paroolidega autentimist ja *HTTP Basic* autentimist, kujutab sellise konnektori kasutamine ebaturvalises sidekanalis endast turvariski. Seetõttu ei soovitata kasutada X.400-konnektoreid.

SMTP -konnektor

SMTP -konnektorit saab lisaks kahe marsruutimisgrupi ühendamisele kasutada ka erinevate *Exchange* -organisatsioonide ühendamiseks ning võõraste (teistsuguste kui *Exchange*) serverite kaasamiseks. Sarnaselt marsruutimisgrupi konnektorile on ka *SMTP* -konnektor ühesuunaline. Väljuvate ühenduste autentimis- ja krüpteerimisseadistusi saab teha vastava konnektori omaduste all (registrikaardis *Advanced*, valikuga *Outbound Security*). Teadete liikluse krüpteerimine on võimalik *TLS* -krüpteerimisfunktsiooni aktiveerimisega. Krüpteerimine tuleks aktiveerida, kui konfidentsiaalseid andmeid soovitakse edastada läbi ebaturvaliste kanalite.



Joonis: lisaseadistused

Kasutada saab kolme autentimisvõimalust: anonüümne juurdepääs, *HTTP Basic* autentimine ja integreeritud *Windows 2000* autentimine. Standardseadistuse kohaselt autentimist ei nõuta (anonüümne juurdepääs). Kui side *Exchange* -serverite vahel toimub *Windows* 'i domeenil (nt marsruutimisgrupi piires), tuleks kasutada integreeritud Windowsi autentimist. *HTTP Basic* autentimist tuleks kasutada eranditult vaid koos *TLS* -iga. Võimalusel tuleks anonüümse juurdepääsu lubamisest hoiduda.

Joonis: väljuvate teadete turvalisus

Muud *Exchange* -konnektorid

Lisaks eelpoolkirjeldatud *Exchange* -konnektoritele on olemas veel mitmeid teisi, nt cc:Maili, *GroupWise* 'i või *MsMail* 'i jaoks. Selliste *Exchange* -konnektorite otstarbekust tuleks hinnata lähtuvalt kasutusvajadusest. Selliste *Exchange* -konnektorite kasutamise korral tuleks seadistada autentimist ja krüpteerimist nõnda, et saavutataks võimalikult kõrge turvalisus (juhul kui selleks on seadistamisvõimalused olemas).

Komponentide konfigureerimine

Front - ja *Back-End* -serverid

Kui kasutaja peab interneti kaudu ligi pääsema oma postkastidele, tuleks kasutada eriotstarbelisi *Front-End* -servereid. *Front-End* -serverid asuvad demilitariseeritud tsoonis (*DMZ*) ja suunavad sisenevad klientühendused *Back-End* -süsteemidesse, kus asuvad kasutaja postkastid. *Front-End* -serverid ise privaatseid postkaste ei sisalda. *Exchange* -serverit saab seadistada *Front-End* -serveriks, aktiveerides serveri omaduste all valiku *This is a Front-End-Server*. Kui seda valikut pole sisse lülitatud, töötab vastav *Exchange* -server *Back-End* -serveri funktsioonides. See on tüüpseadistus.

Autentimine *Exchange* -serverite ja *SMTP-Relay-Host* -ide vahel

Sisenevate ja väljuvate teadete edasisuunamiseks saab ettevõtte demilitariseeri-

tud tsooni sisse seada *SMTP-Relay-Host* 'i. Kui võõrad *SMTP* -serverid suhtlevad demilitariseeritud tsoonis asuva *SMTP-Relay-Host* 'iga loetavas tekstivormis, pole avalikke *SMTP* -ühendusi (väljast kuni *SMTP* - *Relay-Host* 'ini) reeglina võimalik krüpteerida. Demilitariseeritud tsoonis asuva *Relay-Host* 'i ja sisevõrgu serverite vahel tuleks siiski kasutada serverite autentimist. Selleks tuleb *SMTP* -konnektor vastavalt konfigureerida.

Juurdepääs *Exchange* -serverile *HTTP* kaudu (*Outlook Web Access* - *OWA*)
Enamikel juhtudel soovitatakse *OWA* -funktsioonide kasutamisest *Exchange* -keskkonnas loobuda.

MAPI -klientide juurdepääs *Exchange 2000* serverile interneti kaudu
Kasutajale ei tohiks anda interneti kaudu otsejuurdepääsu Exchange-postkastidele ega ka globaalsele kataloogile. Kui seda tahetakse mõnel põhjusel siiski lubada, tuleb selleks konfigureerida tulemüüri: MAPI kasutab side jaoks RPC-d ja dünaamilisi pordimääramisi.

Instant Messaging ja *Chat* -funktsioonide konfigureerimine
Exchange 2000 kiirsõnumi- ja jutufunktsioonide kasutamisel tuleb tagada kasutajate autentimine. Selleks on soovitav kasutada integreeritud *Windows* -autentimist. *HTTP* -autentimise kasutamisest tuleks hoiduda, kuna see nõuab *Windows 2000* all parooli reversiivset krüpteerimist, mida ei tohi mitte mingil juhul aktiveerida. See tähendab seda, et need kasutajad, kes töötavad tulemüüride või *HTTP* -prokside kaudu, ei saa ennast ilmselt autentida.

Outlook-kliendilt Exchange 2000 serverisse kulgeva transpordi konfigureerimine
Klient/server-kommunikatsiooni *Exchange* -transporditeenus toetub *RPC* -dele. *Outlook* 'i ja *Exchange 2000* serverite vahelise suhtluse jaoks toetatakse järgnevaid RPC-mehhanisme:

- *Banyan Vines* : suhtluseks *Banyan Vines* -võrkude kaudu
- *LPC* : kui klient ja server on installeeritud samale arvutile
- *Named Pipes* : ühenduse loomiseks *NetBIOS* -el põhineva *Named Pipes* -protokolli kasutamisel
- *NetBIOS* : ühenduse loomiseks *NetBIOS* -e abil *NetBEUI* , *IPX/SPX* või *TCP/IP* kaudu
- *IPX/SPX* : et toetada originaal *Novell Netware* tööjaamu *IPX/SPX* kaudu ja *Winsock* -liidest
- TCP/IP: *Winsock* -i kasutamiseks *TCP/IP* kaudu

Ühenduse järjekorda saab konfigureerida, mis on eriti oluline heterogeensetes võrkudes. Standardjärjekord on *LPC*, *TCP/IP*, *IPX/SPX*, *Named Pipes*, *NetBIOS*

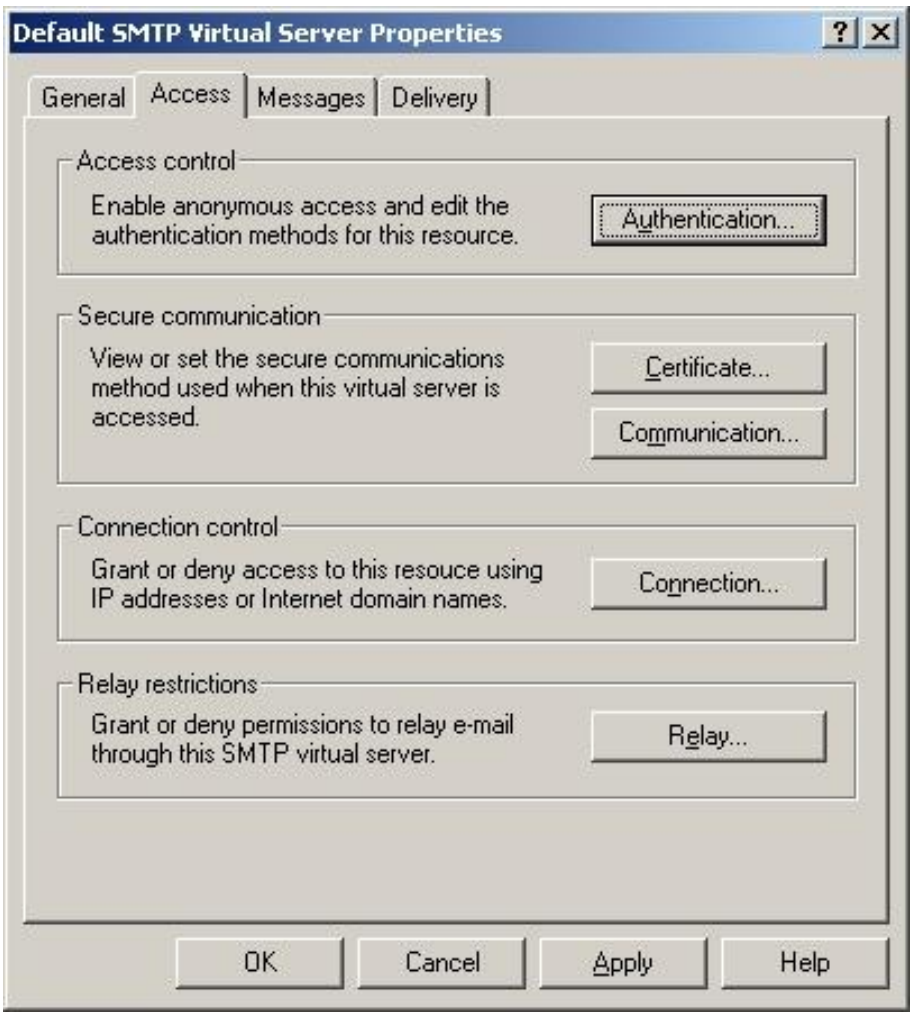
ja lõpuks *Banyan Vines*. Ühenduse järjekorra muutmine toimub Windowsi registreerimisandmebaasi kaudu. Aadressil

HKEY_LOCAL_MACHINE \ *SOFTWARE* \ *Microsoft* \ *Exchange* \ *Exchange Provider*

sisaldab võti *Rpc_Binding_Order* komadega eraldatud *RPC* -suhtlusmeetodite loendit: *ncalrpc* (*LPC* jaoks), *ncacn_ip_tcp* (*TCP/IP* jaoks), *ncacn_spx* (SPX jaoks), *ncacn_np* (*Named Pi-pes* jaoks), *netbios* (*NetBIOS* jaoks) ning *ncacn_vns_spp* (Banyan Vines jaoks). Järjekord tuleks viia vastavusse suhtlusmehhanismidega.

Exchange -transporditeenuse konfigureerimine
Kliendilt *Exchange* -serverile edastatav info peaks olema krüptograafiliselt kaitstud. Andmete krüpteerimise saab aktiveerida registrikaardis *Advanced*. Krüpteerimine on eriti oluline sissevalimisega ühenduse kasutamisel. Autentimiseks tuleks kasutada *Windows 2000* parooliga autentimist. Seda saab samuti seadistada registrikaardis *Advanced*. Kui juurdepääs *Exchange* -serverile peab olema võimalik ka sissevalimisega ühenduse kaudu, tuleks seda võimaldada ainult eraldi kontodele.

Virtuaalsete *SMTP* -serverite konfigureerimine
Exchange 2000 võimaldab määrata mitu virtuaalset *SMTP* -serverit. Turvaseadistused puudutavad siinkohal sisenevate ja väljuvate *SMTP* -ühenduste turvalisust, mille alla kuuluvad autentimine, krüpteerimine, edasisuunamisfunktsioonide piiramine ja IP-aadressidel või domeeninimedel põhinevate juurdepääsuõiguste määramine.



Joonis: juurdepääsuõiguste määramine

Siseneva ühenduse autentimiseks on *SMTP* -serveril (registrikaart *Access* , valik *Authentication*) kolm võimalust, mis on standardseadistuse alusel kõik aktiivsed: anonüümne juurdepääs, *HTTP Basic* autentimine ja integreeritud *Windows 2000* autentimine. Kasutada tuleks kas integreeritud *Windows* -autentimist või *HTTP Basic* autentimist koos *TLS* -krüpteerimisega. Võimalusel tuleks eelistada *Windows* -autentimist. Kui server peab võimaldama anonüümseid *SMTP* -pöördumisi (st, kui tegu on avaliku *SMTP* -serveriga), tuleks demilitariseeritud tsoonis kasutada *SMTP-Relay-Host* 'i.

Joonis: autentimine

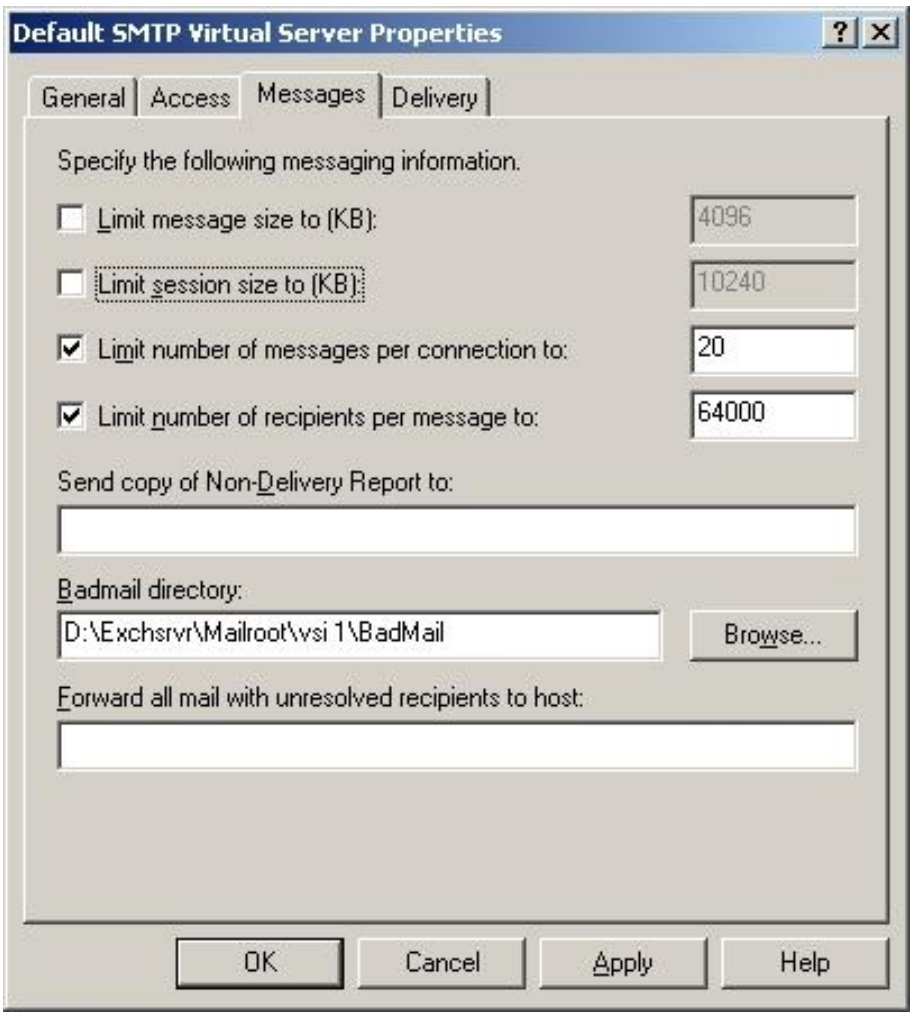
Väljuvate ühenduste autentimiseks on *SMTP* -serveril olemas needsamad eelpool nimetatud kolm võimalust (seadistatavad registrikaardis *Delivery* , valikuga *Outbound security*). Kui ühendusi on tarvis luua erinevate väliste *SMTP* -serveritega, kasutades erinevaid sisselogimisandmeid, tuleks kasutada erinevaid *SMTP* -konnektoreid.

Joonis: väljuvate teadete turvalisus

Kui kaitsmata kommunikatsiooniteede kaudu edastatakse konfidentsiaalseid andmeid, tuleks ühendused krüpteerida. Samuti soovitatakse krüpteerimist, kui kasutatakse *HTTP Basic* autentimist. Sisenevate ühenduste *TLS* -krüpteerimine aktiveeritakse *SMTP* -serveri puhul registrikaardilt *Access*, alal *Secure communication*. Eriti konfidentsiaalsete andmete edastamisel tuleks kasutada 128-bitist krüpteerimist. Tuleb arvestada, et sisenevate ühenduste krüpteerimise aktiveerimiseks läheb tarvis vastavat serveri sertifikaati. Väljuvate ühenduste krüpteerimine saavutatakse *TLS* -i aktiveerimisega registrikaardis *Delivery*, valikuga *Outbound security*. Siinjuures tuleb arvestada, et vastaspool peab loomulikult samuti TLS-i toetama. Kui kõik *SMTP* -serverid, millega konfigureeritav virtuaalne server suhtleb, on teada, tuleks juurdepääsupiirangute määramisel lähtuda IP-aadressidest või domeeninimedest. Võimalusel tuleks eelistada IP-aadressidel põhinevate piirangute kehtestamist. Lisaks oleks kasulik koostada ainult lubatud IP-aadresside (või domeeninimede) nimekiri ning kõikide ülejäänute jaoks tuleks juurdepääs automaatselt ära keelata (nn *default deny policy*). Juurdepääsupiiranguid määratletakse serveri puhul registrikaardis *Access*, alas *Connection control*.

Joonis: Juurdepääsupiirangud

Edasisuunamisfunktsiooni, mida pakutakse teistele *SMTP* -serveritele, saab piirata (serveriseadistuste registrikaart *Access*, nt *Relay restrictions*). Seda tuleks teha volitatud SMTP-serverite nimekirja määratlemisega (*default deny policy*). Teadete suurus, samuti teadete arv ühe ühenduse kohta ja teate vastuvõtjate arv ühe teate kohta on piiratavad vastava virtuaalse *SMTP* -serveri seadistuste kaudu (registrikaart *Messages*). Üldjuhul tuleks piirata suurust, kuna see on üks võimalikest meetmetest, mis aitab kaitsta *DoS* -ründe eest. Maksimaalsed väärtused peaksid seejuures lähtuma vastava ettevõtte/ametiasutuse vajadustest.



Joonis: virtuaalserveri maksimaalsed väärtused

Exchange 'i *SMTP* -teenus logib *SMTP* -ühenduse loomisel ennast standardina sisse bänneriga, mis sisaldab muuhulgas infot tarkvara versiooni kohta. Seega tuleks selline info kindlast bännerist eemaldada, nt *IIS-Metabase* tarkvaratööriistaga *MetaEdit*. Bänneri info ei tohiks sisaldada mitte mingisuguseid andmeid, mis lubaks teha järeldusi kasutatava tarkvara ega ka tarkvara versiooni kohta.

POP3, IMAP4 ja NNTP võrguprotokollide konfigureerimine

Juurdepääs *Exchange* -serverile võib muuhulgas aset leida *POP3*, *IMAP4* või *NNTP* protokollide toel. Kui mõni organisatsioon otsustab nende protokollide kasuks, tuleks vastavalt seadistada ka autentimist ja krüpteerimist, lisaks tuleks määrata IP-aadressidel või domeeninimedel põhinevad juurdepääsupiirangud. Seda saab teha vastava protokolli seadistuse all. Kasutajast lähtuvaid seadistusi,

nt *POP3-/IMAP* -juurdepääsu aktiveerimist/deaktiveerimist tehakse *MMC-Snap-In* 'iga *Active Directory Users and Computers* (registrikaardis *Exchange advanced*, valikuga *Protocol settings*| *Protocols*).

Autentimine
Autentimismehhanismina tuleks *HTTP Basic* autentimise asemel eelistada integreeritud *Windows* -autentimist. *HTTP Basic* autentimist tuleks kasutada ainult koos *TLS* -krüpteerimisega. *NNTP* -protokolli kasutamiseks tuleb järele mõelda, kas serverile tohiks lubada anonüümset juurdepääsu. Kõikidel juhtudel on soovitav määratleda *NNTP* -protokolli jaoks avalikustatavate teadete maksimumsuuruse piirangud (registrikaardis *Settings*).

Krüpteerimine
Kui kaitsmata sidekanalite kaudu edastatakse konfidentsiaalseid andmeid või kui kasutatakse *HTTP Basic* autentimist, on soovitav ühendused krüpteerida. Sissetulevate ühenduste *TLS* -krüpteerimise saab aktiveerida protokolli seadistuste all registrikaardis *Access*, alal *Secure communication*. Eriti konfidentsiaalsete andmete edastamisel tuleks kasutada 128-bitist krüpteerimist. Tuleb siiski arvestada, et sisenevate ühenduste krüpteerimise aktiveerimiseks läheb tarvis vastavat serveri sertifikaati.

Juurdepääsupiirangud
Juurdepääsupiirangute defineerimisel tuleks lähtuda kas IP-aadressidest või domeeninimedest, juhul, kui klientide hulk on tuvastatav.

Teate formaat
HTML -formaadis teated võivad sisaldada ka aktiivseid elemente, mis võivad kujuneda kliendi jaoks turvariskiks. Seepärast tuleks *POP3* ja *IMAP4* kaudu edastatavad teated vormindada tavalisteks tekstiteadeteks (*message body as plain text*, registrikaart *Message Format*). *Rich-Text* -formaati (RTF-i) ei tohiks kasutada.

Logimine
IT-turvalisuse seisukohast tuleb *Exchange* -süsteemi käitamist logida.

Täiendavad kontrollküsimused:

- Kas enne konfigureerimist määratleti marsruutimisgrupid?
- Kas *Exchange 2000* installatsiooni administratiivsed grupid on määratletud?
- Kas organisatsioonisiseselt on selge, kas meilikontodele juurdepääsemiseks lubatakse kasutada ka *Outlook Web Access* 'i?

M 4.163 Exchange 2000 objektide pääsuõigused

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: administraator

Exchange 2000 turvalisuse tagamisel on muuhulgas määravaks ka *Windows 2000 Active Directory* turvalisus. *Exchange 2000* installatsiooni üheks oluliseks koostisosaks on *Active Directory* skeemi laiendamine, mille käigus lisatakse kataloogiteenuse alla nii otseselt *Exchange*'iga seotud objekte kui ka täiendavaid atribuute juba olemasolevatele objektidele. Tähtsamad objektid on järgnevad: *Mailbox, Custom Recipient, Distribution List, Connectors, Public Folder* ja *Server.* Nende objektide alla salvestatakse suures osas nii isikuandmeid kui ka organisatsiooni puudutavaid andmeid, need juhivad meilide liikumist ning peavad seetõttu olema kaitstud volitamata juurdepääsude eest. *Exchange*-objektide kasutust puudutavate pääsuõiguste jagamine on keskseks teemaks *Exchange*-installatsioonide turvalisuse tagamisel. Juurepääsu reguleeritakse *Access Control List*'ide (*ACL*-ide) abil. *Exchange*-objektidega seotud pääsuõiguste jagamine leiab *Active Directory*'s aset tavapärasel moel. Seetõttu palume teil siinkohal tutvuda järgnevate, *Windows 2000 Server*'it ja *Active Directory*'t käsitlevate moodulitega:

- M 2.229 Active Directory planeerimine
- M 2.230 Active Directory halduse planeerimine
- M 2.231 Windowsi grupipoliitika planeerimine

Konfigureerimistööriistad

Nagu *Windows 2000* puhul tavaks, võetakse *Exchange 2000* objektide administreerimiseks kasutusele nn *Microsoft Management Console* (*MMC*) ja sinna juurde kuuluvad *Snap-In*'id: *Exchange System, Exchange Message Tracking System* ja *Exchange Advanced Security*. *Active Directory* info kuvamiseks võib kasutada utiliiti *ADSI Edit*.

Pääsuõiguste administreerimine

Pärast *Exchange 2000* standardset installeerimist administraatorikonto alt on nii domeeni- kui ka *Enterprise*-administraatoritel *Exchange*'i üle piiramatud administraatoriõigused. Sellist olukorda ei tuleks aga soosida, kuna vastasel juhul ei õnnestu administreerimisülesandeid üksteisest selgelt lahus hoida. Sel põhjusel on installeerimiseks soovitav kasutada eraldi kasutajakontot nagu on kirjeldatud meetmes M 4.161 Exchange / Outlook turvaline installeerimine . Organisatsiooni ning administreerivate gruppide tasandil tuleks volituste jagamiseks kasutada alati utiliiti *wizard for allocation of administration rights to Exchange* objects, mis asub *Exchange'i System Manager*'i all.

Exchange 2000 kasutamisega seotud kasutajaõiguste konfigureerimine

Exchange 2000 kasutamisega seotud kasutajaõiguseid saab siduda individuaalsete kasutaja- ja grupikontodega (liikuge vastava kasutaja objektide seadistamise all registrikaardile *Security*). Volituste jagamisel tuleks alati eelistada varianti, mille puhul lähtutakse gruppidest. Järgmised volitused peaksid reeglina olema

antud vaid Exchange-administraatoritele:

- A*dd PF to Admin Group* määrab, kas kasutajakontole on antud volitus, mis lubab lisada avaliku kausta mõne administreerimisega tegeleva grupi alla.
- *Administer Information Store* määrab, kas kasutajakontole on antud volitus, mis lubab hallata andmesalvestit.
- *Create named Properties in the Information Store* määrab, kas kasutajakontole on antud volitus, mis lubab koostada enda poolt antava nimetustega omadusi (nt kuvanime, eesnime, perenime, kustutatud sissekannete märgistusi jms).
- *Create Public Folder* määrab, kas kasutajakontole on antud volitus, mis lubavad tekitada hetkel valitud asukohta avalikke kaustasid.
- *Create Top-Level Public Folder* määrab, kas kasutajakontole on antud volitus, mis lubab tekitada avalikke kaustasid kaustade hierarhia kõige ülemisel tasandil.
- *Full Store Access* määrab, kas kasutajakontole on antud volitus, mis lubab kasutada andmesalvesti andmebaase täies mahus.
- *Mail-Enable Public Folder* määrab, kas kasutajakontole on antud volitus, mis lubab siduda avaliku kaustaga e-mailiaadresse.
- *Modify Public Folder ACL* määrab, kas kasutajakontole on antud volitus, mis lubab muuta avaliku kausta *ACL*-e.
- *Modify Public Folder Admin ACL* määrab, kas kasutajakontole on antud volitus, mis lubab avaliku kausta *ACL*-e administraatorite jaoks muuta.
- *Modify Public Folder Deleted Item Retention* määrab, kas kasutajakontole on antud volitus, mis lubab kindlaks määrata ajavahemiku päevades, mille vältel peavad avalikes kasutades kustutatud objektid säilima.
- *Modify Public Folder Expiry* määrab, kas kasutajakontole on antud volitus, mis lubab määrata avalikes kaustades hoitavatele objektidele vanusepiirangu.
- *Modify Public Folder Quotas* määrab, kas kasutajakontole on antud volitus, mis lubab kehtestada avalikele kaustadele suurusepiirangu.
- *Modify Public Folder Replica List* määrab, kas kasutajakontole on antud volitus, mis lubab muuta avaliku kausta duplikaatide loendit. Administraatoril peab olema see volitus nii administreerimisgrupi tasandil kui ka avaliku kausta andmebaasi tasandil, sest ainult nii saab ta edukalt dublikaati luua ja avalike kaustade dubleerimist hallata.
- *Open Mail Send Queue* määrab, kas kasutajakontole on antud volitus, mis lubab kuvada andmesalvesti sissetulevate ja väljaminevate meilide ootejärjekordi.
- *Read All Metabase Properties* määrab, kas kasutajakontole on antud volitus, mis võimaldab lugeda kogu *Internet Information Services Metabase* infot.
- *Remove PF from Admin Group* määrab, kas kasutajakontole on antud volitus, mis lubab avalikku kausta administreerimisega tegeleva grupi alt eemaldada.
- *View Information Store Status* määrab, kas kasutajakontole on antud volitus, mis lubab kuvada andmesalvesti seisundit kajastavat infot. Seisundit

kajastav info näideteks võivad olla muuhulgas andmed hetkel sisselogitud kasutajate ja neile võimaldatavate ressursside kohta.

Mailbox-salvesti
Kõikides *Exchange 2000* serverites on soovitav kasutada „*lockdown*“-skripti (*edslock.vbs*). Sellega kõrvaldatakse rakendamisel tehtavad vead ning piiratakse juurdepääsud lokaalsete serverite *mailbox-store*'dele.

Privaatsete postkastide pääsuõigused (Mailbox)
Kasutajale tema privaatpostkasti jaoks jagatud standardseid pääsuõiguseid ei ole reeglina tarvis enam kohandada, kuna lugemisvolitused ja täielik juurdepääs antakse seeläbi vaid postkasti omanikule. Siiski tuleks arvestada, et neid õiguseid ei jagataks mitte *Exchange System Manager*'i vahendusel, vaid kasutataks *MMC-Snap-In'i Active Directory Users and Computers* vastava kasutajakonto omaduste all (registrikaart *Exchange Advanced*).

Avalike kaustadega seotud pääsuõiguste piiramine
Pärast *Exchange 2000* installeerimist standardselt sisse seatud pääsuõigused lubavad kasutajatel, kes kuuluvad gruppi igaüks (*Everyone*), koostada *Outlook*'i vahendusel uusi avalikke kaustasid. Seda õigust tuleks aga nii palju kui võimalik piirata, kuna avaliku kausta omanikul on muuhulgas võimalus lisada sinna kausta ka selliseid dokumente, mis võivad endas kanda aktiivsisu. Kuna viimasega võib kaasneda turvarisk, tohiks uute avalike kaustade loomise õigus olla vaid vähestel isikutel. Seetõttu on soovitav anda järgmised õigused ainult usaldusväärsetele isikutele:

- *Create Top-Level Public Folders*
- *Create Public Folders*
- *Create Named Properties*

Lisaks tuleks kasutajagrupilt igaüks (*Everyone*) ära võtta administreerimisvolitused (nt õigus muuta *ACL*-e või teisi kaustaga seotud omadusi). Õigused nagu *Create Public Folder, Create Top Level Public Folder, Modify Public Folder ACL, Modify Public Folder Admin ACL* jagatakse kasutajatele *Exchange System Manager'*i abil vastava avaliku kausta omaduste all (registrikaart *Security*). Täiendavaid avalike kaustadega seotud pääsuõiguseid jagatakse läbi registrikaardi *Permissions*. Seal on võimalik valida kolme funktsiooni vahel: *Client permissions, Directory rights* ja A*dministrative rights*.

Organisational Forms Libraries (OFL) turvaseadistused
Organisatsiooniblankettide raamatukogud luuakse kohustuslikus korras teadetekausta moodustamisel. Need pärivad kaustakonfiguratsiooni seadistuse ning kasutajaõigused. Süsteemikausta tasandil (mis on varjatud), asub organisatsiooniblankettide raamatukogu. Standardina on ainult sellel administraatoril, kes vastava organisatsiooniblankettide raamatukogu lõi, õigus selle raamatukogu alla *Outlook*-blankette registreerida. *Outlook*-blankettide registreerimisvolitusi on soovitav jagada vaid suurte piirangutega, kuna blanketid võivad olla varustatud aktiivsisuga. Kui

vastavat volitust on tarvis anda veel ka täiendavatele kasutajatele, saab selle kindlaks määrata *Exchange System Manager*'i abil: täiendavate kasutajate lisamiseks tehke *EFORMS REGISTRY* all parem hiireklõps vastava organisatsiooniblankettide raamatukogu kausta peal, valige *Properties*, liikuge edasi registrikaardile *Permissions* ja klõpsake valikul *Client Permissions*.

Send on behalf jt sarnaste õiguste jagamine

Kasutajatele asendajaid määrates on olulised järgnevad *Exchange 2000* kasutamisega seotud õigused: s*end as, send on behalf* ning *receive as*. Neid õiguseid jagatakse *MMC-Snap-In*'iga *Active Directory Users and Computers* vastava kasutaja omaduste all (send as ja receive as läbi registrikaardi *Security* ning *send on behalf* läbi registrikaardi *Exchange General*). Reeglina on soovitav volituse „*send as*" jagamisest üldse loobuda. Kui tekib siiski vajadus, tuleks selle asemel võimaldada volitust „*send on behalf*", mida rakendatakse ka siis, kui keegi kasutaja määrab oma *Outlooki* seadistustes registrikaardi all *Delegation* kellegi teise kasutaja enda asetäitjaks. Need õigused on suurel määral seotud turvalisusega. Õiguseid send on behalf ja receive as tuleks jagada ainult koos suurte piirangutega ning õigust *send as* ei tohiks üldse mitte kellelegi anda.

Täiendavad kontrollküsimused:

- Kas *Exchange*-administraatori tööülesanded on määratletud ning kas neile on sisse seatud vastav kasutajagrupp?
- Kas *Exchange*-objektidega seotud pääsuõiguste kindlaksmääramisel on lähtutud turvasuunistest?
- Kas *Exchange*-objekte jagatakse *Active Directory* replikeerimise raames sobivalt?

M 4.165 Outlook 2000 turvaline konfigureerimine

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator, kasutaja

Pärast seda, kui *Outlook 2000* on institutsiooni raames installeeritud või laiali jaotatud, tuleb ette võtta klienttarkvara konfigureerimine, mis võimaldaks *Exchange/Outlook* keskkonda turvaliselt käitada. Reeglina tuleb selleks rakendada meedet M 5.57 Rühmatarkvara/meiliklientide turvaline konfiguratsioon . Järgnevalt on toodud soovitusi spetsiaalselt *Outlook 2000* kohta, mille raames käsitletakse muuhulgas järgmisi teemasid:

- *Outlook 2000* konfigureerimist võimaldavad administreerimistööriistad
- aktiivsisu *Outlook 2000* keskkonnas
- e-mailide allkirjastamine ja krüpteerimine
- filtreerimisreeglid rämpsposti vastase abinõuna
- makrode käsitsemine *Outlook 2000* keskkonnas
- *Outlooki* andmete turvaline hoidmine
- *Outlooki* objektide juurdepääsukaitse (*Outlooki* kaust tervikuna ning selle üksikud objektid nagu ülesanded või kontaktid)
- e-mailide manuste käsitsemine
- spetsiaalsete teadete käsitsemine (*Out-of-Office* -teated või kättesaamise kinnitused)
- side turvalisus *Outlook 2000* vaatevinklist
- *Outlook 2000* SR-1 turvavärskenduse kasutamine.

Lähtutakse sellest, et *Outlook 2000* on *Exchange 2000* suhtes tööle pandud kui *MAPI-Client* , mitte kui *Internet-Mail-Client*.

Üldised soovitused

Exchange/Outlook -keskkonna seadistusi peaksid nii palju kui vähegi võimalik tegema administraatorid. Kasutajate endi seadistusi tuleks lubada vaid erandjuhtudel, kui administraatoritel ei võimalik seadistusi teha. Administraatorite tehtavaid tsentraalseid seadistusi tuleb kaitsta kasutajate võimalike muudatuste vastu, et vältida väärkonfiguratsioonide teket, mis võib nõrgestada üleüldist soovitud turbeastet. Kahjuks ei ole see kõikide seadistuste puhul võimalik. Juhtudel, kus see on võimalik, leiate järgnevast tekstist ka asjakohased viited.

Platvormina kasutatava operatsioonisüsteemi turvaline konfiguratsioon

Outlook 2000 turvalise konfiguratsiooni eelduseks on platvormina kasutatava operatsioonisüsteemi konfiguratsiooni turvalisus. Töökohtades, kus on operatsioonisüsteemina kasutusel *Windows 2000* , tuleb ilmtingimata rakendada vastavat meedet. Klientide üldiseks konfigureerimiseks ja administreerimiseks võimaldab *Windows 2000* kasutada poliitikate mehhanismi. Neid poliitikaid on soovitatav kasutada, et rakendada tsentraalse administreerimise võimalusi.

Haldamiseks kasutatavad tööriistad

Outlook 2000 administreerimine ja konfigureerimine võib aset leida järgnevatel erinevatel aegadel: juba enne *Outlook 2000* tarkvara laialaijaotamist ja installeerimist (tehes nn eelkonfiguratsiooni) või alles siis, kui *Outlook* on juba laiali jaotatud. *Outlook 2000* haldustööriistadega, nt *Custom Installation Wizard'* i abil on administraatoril võimalus tsentraalselt luua *Outlook 2000* tarkvarast hilisema laialijagamise ja installeerimise tarbeks eelkonfigureeritud versioon. Keskmistel ja suurtel ettevõtetel ning asutustel on *Outlook 2000* klientide konfigureerimiseks ja haldamiseks soovitatav kasutada haldustööriistu. Haldustööriistade kasutamine lihtsustab administraatorite tööd ning aitab kaasa ühtlaselt kõrge turbeastme saavutamisele. Väikeste ettevõtete ja asutuste puhul tuleks analüüsida, kas haldustööriistade rakendamine on mõttekas või mitte. Administraatorid võivad kasutada järgnevaid tarkvaratööriistu:

- *Custom Installation Wizard*: läbi *Custom Installation Wizard'i avaneb võimalus rakendada Outlook 2000* installeerimisel spetsiaalseid installeerimispakette, mis on kohandatud institutsiooni vajadustele. Lisaks saab installeerimispakette kasutada veel ka selleks, et määrata kindlaks klientidele tehtavate seadistuste konfiguratsioon ning kehtestada, milliseid *Outlook* 'i komponente tohib installeerida. Selle abil on administraatoril võimalik mõningaid järgnevalt kirjeldatavaid soovitusi ellu rakendada juba enne installeerimist.
- *OutlookSecurity.oft* on mall, mille abil saab *Exchange* -serveris genereerida turvaseadistusi ning selle otstarbeks on turvet puudutavate värskenduste kohandamine.
- Administreerimismall *Outlk9.adm* defineerib süsteemipoliitika *Windows 2000* grupipoliitika objektide tarbeks, mis võimaldab rakendada *Outlook* 'i turvaseadistusi klientidel üle terve organisatsiooni tsentraalselt, st neid *Active Directory* kaudu seadistada ja kehtestada.

Kasutajaprofiilide rakendamine

Kui ühte arvutit kasutab mitu isikut, saab igale kasutajale luua oma *Outlook'* i profiili koos sinna juurde kuuluvate spetsiaalsete seadistustega. Sellisel juhul peab erinevad *Outlook'* i profiilid looma administraator ning administraator peab need ka üksteise suhtes turvaliseks muutma. Kasutajaprofiile võib salvestada nii serverile kui ka kliendi alla. Reeglina on soovitatav kasutada serveripoolseid kasutajaprofiile. Kui kasutaja logib ennast mõnda *Windows 2000* domeeni, laetakse need kliendi registrisse (täpsemalt asukohta *HKEY_CURRENT_USER*) (vt M 4.162 Exchange 2000 serverite turvaline konfiguratsioon). Siinkohal tuleb arvestada, et kui kasutatakse serveripoolseid profiile, pole võimalik töötada *offline* -režiimis, mille puhul eksisteerivad andmed arvutis lokaalse koopiana. Kui seda aga ilmtingimata soovitakse, tuleb *Outlook* 'i profiilid salvestada klientide alla. Siinkohal tuleb arvestada, et profiilis tehtavad muudatused kehtivad ainult lokaalsele arvutile, mis võib kaasa tuua olukorra, kus üks töötaja peab erinevates arvutites töötama erinevate profiilide all. Ka neil juhtudel, kus *Outlook* 'i profiilid salvestatakse lokaalselt, on siiski soovitatav, et kasutajaprofiilide loomisega tegeleksid *Exchange*'i administraatorid, kes need ka laiali jaotavad, kuna seeläbi tagatakse turvaline ja ühtne eelkonfiguratsioon. *Exchange*'i administraator peab selleks otstarbeks loo-

ma *Custom Installation Wizard* 'iga profiilifaili (*outlook.prf*). See profiil tuleb hiljem kopeerida *Windows 2000* süsteemikataloogi, reeglina sihtarvuti asukohta *\Winnt* ning seda tuleb kasutada uute kasutajaprofiilide loomisel mallina.

Konfidentsiaalsete andmete kaitse *Outlook 2000* keskkonnas

Outlook 'i kajastavaid andmeid tuleb hoida turvaliselt

Outlook 'i andmeid hoitakse ennekõike *Exchange* -serveri postkasti kaustas. Sellele vaatamata on *Outlook* 'i andmeid võimalik salvestada ka lokaalselt, kliendi alla, kasutades nt *offline* -kaustu (st serveripoolse postkastikausta lokaalse koopiana) või kui kasutaja on lokaalselt loonud oma enda personaalsed kaustad. Klientide juures hoitavad *Outlook* 'i andmed on reeglina seotud suuremate riskidega kui serverile salvestatud andmed, kuna esimesel juhul vastutab nende kaitse eest ka kasutaja. Privaatkaustade turvalisuse konfigureerimisega (nt failidega seotud juurdepääsuõigused) peab kasutaja tegelema ise. Seetõttu tuleb *Outlook* 'i turvapoliitikas määratleda, kas *Outlook* 'i andmeid tohib kasutajate arvutisüsteemides hoida või mitte. Üldjuhul on soovitatav mitte salvestada *Outlook* 'i andmeid klientide alla. See välistab aga omakorda ka *offline* -failidega töötamise võimaluse. Kui *offline* -failidega töötamisest pole võimalik loobuda, tuleks arvestada järgnevate, lokaalselt salvestatud *Outlook* 'i kaustade kaitseks ette nähtud võimalustega. *Outlook* salvestab andmeid personaalsetesse kaustadesse (.pst-failidesse) ning *offline* -kaustadesse (.ost-failidesse), mis asuvad sel juhul kliendi lokaalsel kõvakettal. Tuleb arvestada, et täiendavaid andmeid salvestatakse veel ka süsteemikataloogidesse, *Outlook* 'i installatsioonikataloogidesse ning *Windows 2000* kasutajaprofiilide alla (reeglina asukohta *C:\Documents and settings* \ \ *Application data* \ *Microsoft* \ *Outlook*). Seetõttu tuleb nende suhtes kehtestada piirangutega juurdepääsuõigused.

Lokaalsete *Outlook* 'i kaustade andmevarundus

Kui kasutaja arvutisse salvestatakse personaalseid *Outlook* 'i kaustu, tuleb andmekadude vältimiseks ka need kaustad kaasata andmevarunduse alla. See kehtib ka *offline* -kaustade kohta.

Lokaalsete *Outlook* 'i kaustade krüpteerimine

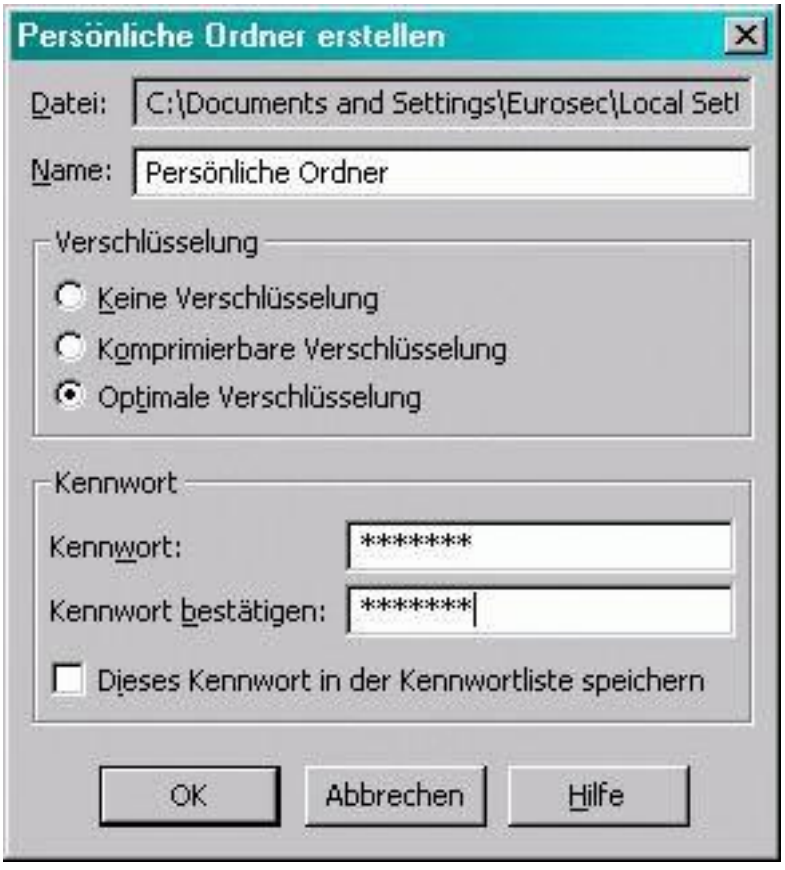
Lokaalseid *Outlook* 'i kaustu (st personaalseid ja *offline* -kaustasid) on soovitatav krüpteerida.

Offline -kausta krüpteerimise saab sisse lülitada *Tools* | *Services* | *Microsoft Exchange Server* | *Properties* all, mis asub registrikaardil *Advanced*, täpsemalt *Offline folder file settings* all. Personaalsete kaustade krüpteerimist saab konfigureerida vaid kaustade loomise käigus ning seda ei saa tagantjärele muuta. Kausta loomiseks liikuge valikusse *Tools* | *Services* | *Add*: valige loetelust *Available information services* funktsioon *Personal folders* ning klõpsake valiku kinnitamiseks OK. Teile avaneb dialoogiaken *Create personal folders* , kuhu teil tuleb sisestada loodava kausta nimi. Seejärel saab vastava kausta konfiguratsiooni menüüs valida juba vastavad krüpteerimisfunktsioonid. Krüpteerimisvõimalustena saab *Outlook 2000* puhul valida kas tihendatud või optimaalse krüpteerimise vahel. Soovitatav on kasutada optimaalset krüpteerimist. Mõlema krüpteerimisviisi puhul tuleb arvestada, et kuna nende mehhanismid on teadaolevalt nõrgad, ei suuda need tagada kõrgete konfidentsiaalsusnõuete täitmist. Täiendavaks kaitseks on soovi-

tav salvestada nii *offline* -kaustad kui ka personaalsed kaustad eraldi kataloogi alla ning kehtestada sellele kaustale piirangutega juurdepääsuõigused. Vastavale kataloogile tohib olla juurdepääs vaid selle kasutajal. Kaustadesse salvestatud info kõrgema konfidentsiaalsuse tagamiseks on võimalik kasutusele võtta kas *Windows 2000* failisüsteemi krüpteerimine (EFS) või kasutada selleks täiendavaid tooteid.

Ärge kasutage lokaalselt hoitavate Outlooki personaalsete kaustade puhul paroolkaitset

Personaalsete kaustade tarbeks on võimalik sisse lülitada paroolkaitse, kuid selle kasutamine ei ole siiski mõttekas. Nimetatud paroolkaitse on nõrk ning seda on võimalik internetis leiduvate tööriistadega lahti muukida. Kui organisatsiooni turvapoliitika nõuab, et paroole tuleb lisaks muule veel ka tsentraalselt deponeerida, võib öelda, et paroolkaitsega saavutatav turvalisuse tõus on nii väike, et selle rakendamiseks kuluv administreerimisega seotud vaev on ressursi raiskamine. Seetõttu on soovitatav paroolkaitse rakendamisest loobuda.



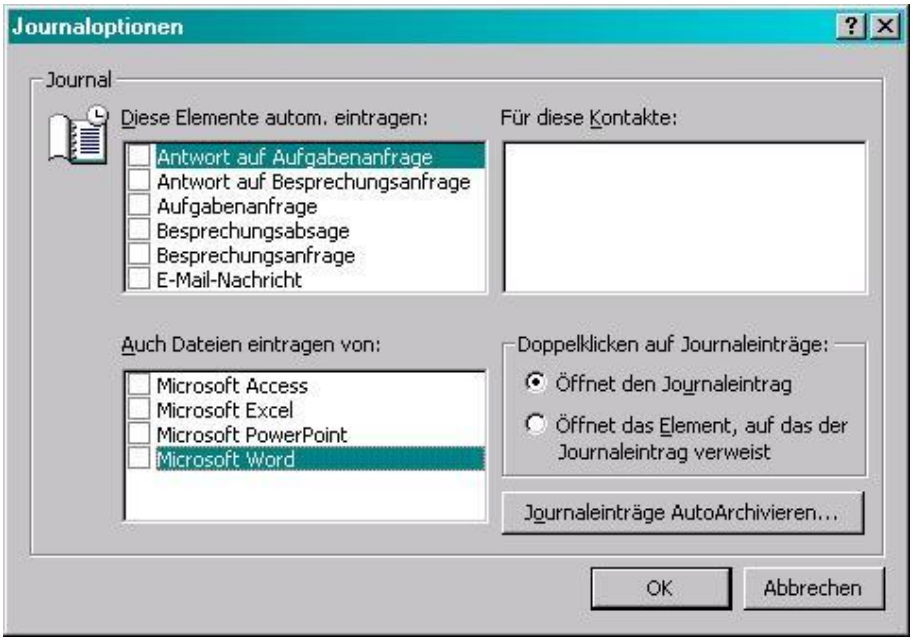
Joonis: lokaalsete kaustade krüpteerimine

Tsentraalsete *Outlook* 'i kaustade pääsuõigused

Exchange 'i keskkonnas saab personaalseid kaustu teistele kasutajatele kättesaadavaks muuta. Selleks on kokku kasutada kaheksa volituste astet, alates kõige kõrgemast astmest nr 8 (kausta omaniku volitused) kuni seadistuseni „volitused puuduvad“.Enamikel juhtudel on soovitatav kehtestada pääsuõiguste jagamisel piiranguid ja jagada korraga ainult selliseid volitusi, mida ka tõepoolest tarvis läheb. Turvalise baasseadistusena on soovitatav juurdepääsu võimaldada ainult omanikule endale. Eriti oluline on tagada, et kasutajale nimega *Standard* ei antaks mitte mingisuguseid volitusi. Tuleks arvestada, et hierarhias kõrgemal asuvate kaustade pääsuõigused pärandatakse edasi struktuuri hierarhias madalamal asuvatele kaustadele.

Outlook 2000 Journal 'i turvaline käsitsemine

Journal registreerib ajaliselt tegevusi, mille sooritamiseks on kasutatud *Outlook 2000*. Siia alla ei kuulu mitte ainult saadetud ja vastu võetud meilid, kohtumiste kokkulepped ja tööülesanded, vaid ka need tegevused, mida sooritati kontaktide ja *Office* -dokumentidega. *Journal* 'i sissekandeid saab teha käsitsi ning neid saab genereerida ka automaatselt. Turvalisuse seisukohalt tuleks arvestada, et *Journal*'isse käsitsi või ka automaatselt tehtud sissekanded võivad sisaldada konfidentsiaalseid andmeid ning dokumentide otseteid. Seetõttu on soovitatav loobuda sissekannete automaatsest genereerimisest. Seda saab konfigureerida registrikaardis *Settings*, valikute alt *Tools* | *Options*, liikudes funktsioonile *Journal Options*: mitte üheski valikukastis ei tohiks olla linnukest. Kui sissekanne tehakse käsitsi ning vastavale *Outlook* 'i kaustale on juurdepääs ka teistel kasutajatel, on soovitatav lisada sissekandele märgistus *Private* . Sellisel juhul märgistust *Private* kandvaid sissekandeid teistele kasutajatele ei kuvata. Siinkohal tuleb arvestada, et tegu on vaid väga lihtsakoelise kaitsemehhanismiga, mis suudab tõkestada vaid „juhuslikku lugemist“. Töökorralduslike turvapoliitikatega tuleks määratleda, millist tüüpi faile tohib *Journal* 'i sissekannetesse lisada otseteedega.



Joonis: *Journal* 'i valikud

Isiklike andmete kaitsmine süsteemiadministraatorite suhtes

Lokaalselt salvestatud *Outlook* 'i andmeid (.pst-failid) saavad administraatorid igal ajal lugeda. Konfidentsiaalsust saab administraatorite suhtes seetõttu tagada ainult krüpteerimisega. Selleks võib kasutada *Outlook* 'i enda (nõrka) krüpteerimismeetodit või siis mõnda failidel baseeruvat krüpteerimissüsteemi (*Windows 2000* all EFS-i või mõnda lisatoodet). Kui kasutate *Windows 2000* EFS-i, tuleb arvestada, et defineeritud taastamisagendil on juurdepääs krüpteeritud infole. Standardse installatsiooni puhul on taastamisagendina defineeritud automaatselt administraator. Failidega töötavat krüpteerimismehhanismi kasutades on soovitatav koostada turvapoliitika, mis käsitleb kasutatavate võtmete deponeerimist, et võimaldada ligipääsu krüpteeritud andmetele ka avariiolukordades.

Outlook 'i / *Exchange* 'i side turvamine

Autentimine

Autentimismeetodit, mida *Outlook 2000* kasutab *Exchange* -serveri suhtes *MAPI* -kliendina, saab seadistada valikute alt *Tools* | *Services* | *Microsoft Exchange Server* | *Properties,* registrikaardis *Advanced*, andmeväljas *Network Security Logon*. Soovitatav on mitte kasutada automaatseid sisselogimismehhanisme nagu *NT Password Authentication* või *Distributed password authentication*, vaid määrata seadistuseks *None*. Viimasel juhul palutakse kasutajal, kui too pöördub *Exchange* serveri poole, sisestada oma kasutajanimi ja parool.

Joonis: *Network Security Logon*

Kui *Outlook 2000* kasutatakse *Exchange*-serverisse või mõnda teise e-mailiserverisse pääsemiseks *POP3/IMAP4/SMTP*-kliendina, on soovitatav kasutada meetodit *Logon by means of Secure Password Authentication* (*Tools| Services | Internet e-mail | Properties | Server*), juhul kui vastav e-mailiserver selle kasutamist muidugi toetab. Täiendavalt on soovitatav posti väljasaatva serveri puhul kasutada seadistust *Server requires authentication*, mille konfigureerimine leiab aset täpselt samas kohas. Lisaks tuleks seadistuse all ära märgistada kontrollkastike sisselogimine läbi parooli turvalise autentimise (*SPA, Secure Password Authentication*). Sealjuures peab posti väljasaatev server olema konfigureeritud selliselt, et süsteem nõuaks autentimist. Mitte mingil tingimusel ei tohi salvestada kasutaja parooli, st kontrollkastikesest 'salvesta parool' (*Save password*) tuleb märgistus kindlasti eemaldada. Vastasel korral esineb oht, et salvestatud paroole võib õnnestuda kasutajasüsteemi lokaalse juurdepääsu käigus avalike, internetis saada olevate tööriistadega välja lugeda.

Kommunikatsiooni krüpteerimine

Kui *Outlook 2000* kasutatakse *Exchange* -serveri *MAPI* -kliendina, saab selleks kasutatavat RPC-kommunikatsiooni (*Remote Procedure Call*) kliendi ja

Exchange-serveri vahel kaitsta krüpteerimisega. Seda, kas vastavad andmeside krüpteerimist kasutatakse või mitte, peab määratlema *Outlook* 'i jaoks koostatud turvapoliitika. Krüpteerimist on soovitatav kasutada eriti siis, kui *Outlook* -klientide ja *Exchange* -serveri vaheline side liigub läbi ebaturvaliste võrkude. *RPC* -krüpteerimise saab sisse lülitada *Tools* | *Services* | *Microsoft Exchange Server* | *Properties* all, mis asub registrikaardil *Advanced*, täpsemalt *Activate encryption* all. Soovitatav on sisse lülitada mõlemad pakutavad funktsioonid, st nii *If a network connection is used* kui ka *If a dial-up connection is used*, kuna sellega tagatakse mõlema juurdepääsu versiooni side turvalisus. Kui rakendatakse IP baasil töötavaid protokolle nagu *POP3*, *IMAP4* ja *SMTP*, tuleks kasutusele võtta *SSL/TLS*. Selle sisselülitamiseks liikuge valikutesse *Tools* | *Services* | *Internet* | *e-mail* | *Properties* registrikaardis *Advanced* ning märgistage kontrollkastike *This server requires a secure connection (SSL)* .

Aktiivsisu *Outlook 2000* keskkonnas

Meilides võib reeglina esineda kahte tüüpi aktiivsisu:

- skriptidena HTML-meilides
- aktiivsisuna meilide manustes.

Aktiivsisu kontrollimatu teadlik ning mitteteadlik käivitamine võib kujutada endast ohtu *Outlook* 'i klientidele, lokaalsetele arvutitele ning tervele võrgule. *Outlook 2000* saab aktiivsisu kaitseks konfigureerida järgnevalt.

Turvatsoonide konfigureerimine

Microsoft Internet Explorer 'i turvatsoonide seadistused on olulisteks piiranguteks ka aktiivsisu käivitamisele *Outlook 2000* keskkonnas. Need määratlevad *Outlook 2000* käitumise e-mailide vastuvõtmisel ning veebilehtede kuvamisel (nt HTML-e-maili sisu kuvamise). Tuleb arvestada, et turvatsoonide seadistused ei keskendu otseselt *Outlook 2000* eripäradele, vaid kehtivad lokaalsele süsteemile. Seetõttu mõjutavad igasugused muudatused alati ka kõiki teisi programme, mis neid seadistusi kasutavad (nt *Microsoft Internet Explorer*'it). *Outlook* 'i e-maile saab liigitada kas turvatsooni *Internet* või *Restricted Sites*. Soovitatav on meilid liigitada turvatsooni alla *Restricted Sites*, milleks tuleb liikuda valikusse *Tools* | *Options* registrikaardil *Security* ning valida alalõigust *Zone* funktsioon *Secure content*. Tsooni seadistust tuleks kohandada vastavalt järgnevatele soovitustele. Turvatsoone võib üldjuhul konfigureerida läbi *Windows 2000* grupipoliitikate, võttes aluseks kas vastavate arvutite või kasutajate grupi või siis otse kliendi all *Outlook 2000* keskkonnas. Läbivalt ühtlase seadistuse saavutamiseks on soovitatav turvatsoone konfigureerida vaid läbi *Windows 2000* poliitikate. Täiendavaks eeliseks on sellisel juhul veel ka võimalus kaitsta tehtud seadistusi või muudatusi kasutaja poolt tehtavate muudatuste vastu. Kasutajatele keskenduvaid interneti turvatsoonide seadistusi saab kehtestada poliitikaga *User Configuration* | *Windows Settings* | *Internet Explorer Maintenance* | *Security* | *Security Zones and Content Filters policy*. Kaitsmaks tehtud seadistusi võimalike kasutajapoolsete muudatuste vastu, saab rakendada poliitikat *Computer Configuration* | *Administrative Templates* |

Windows-Components | *Internet Explorer* | *Security Zones: Users cannot modify settings*. Lisaks on soovitatav kasutada poliitikat *Computer Configuration* | *Administrative Templates* | *Windows-Components* | *Internet Explorer* | *Security Zones: Users cannot add or remove sites*, et kasutajatel ei tekiks võimalust muuta tsoonide kehtimisalasid.

Ou*tlook 2000* keskkonnas saab turvatsoone konfigureerida valikute all *Tools* | *Options* registrikaardil *Security*, kuid seda ainult juhul, kui *Outlook* 'i lokaalne turvapoliitika lubab sellist konfigureerimist.

Joonis: turvaseadistused

Internet Explorer 'i väljavalitud turvatsooni saab liikuda läbi valiku *Zone settings*. Tsooni jaoks tuleks malliks võtta kõrge turbeaste (*High*) ning seejärel tuleks hakata seda järgneva tabeli põhjal mugandama (funktsiooniga *Customise*

Security Level).

Valik	Seadistus
Run ActiveX control elements which are secure for scripting	desaktiveeritud
Initialise and run ActiveX control elements which are not secure	desaktiveeritud
Run ActiveX control elements and plug-ins	desaktiveeritud
Download signed ActiveX control elements	desaktiveeritud
Download unsigned ActiveX control elements	desaktiveeritud
Logon	sisestuse nõue (*prompt*)
File download	desaktiveeritud
Font download	desaktiveeritud
Java permissions	Disable Java
Active Scripting	desaktiveeritud
Allow inserts via script	desaktiveeritud
Scripting of Java applets	desaktiveeritud
Access data sources beyond domain boundaries	desaktiveeritud
Permanence of user data	desaktiveeritud
Display mixed content	desaktiveeritud
Install desktop objects	desaktiveeritud
Client certificate selection not requested if there is no certificate or only one certificate	desaktiveeritud
Allow META REFRESH	desaktiveeritud
Start programs and files in an IFrame	desaktiveeritud
Move subframes between different domains	desaktiveeritud
Send unencrypted form data	desaktiveeritud
Drag and drop or copy and paste files	desaktiveeritud
Access rights for software channel	kõrge

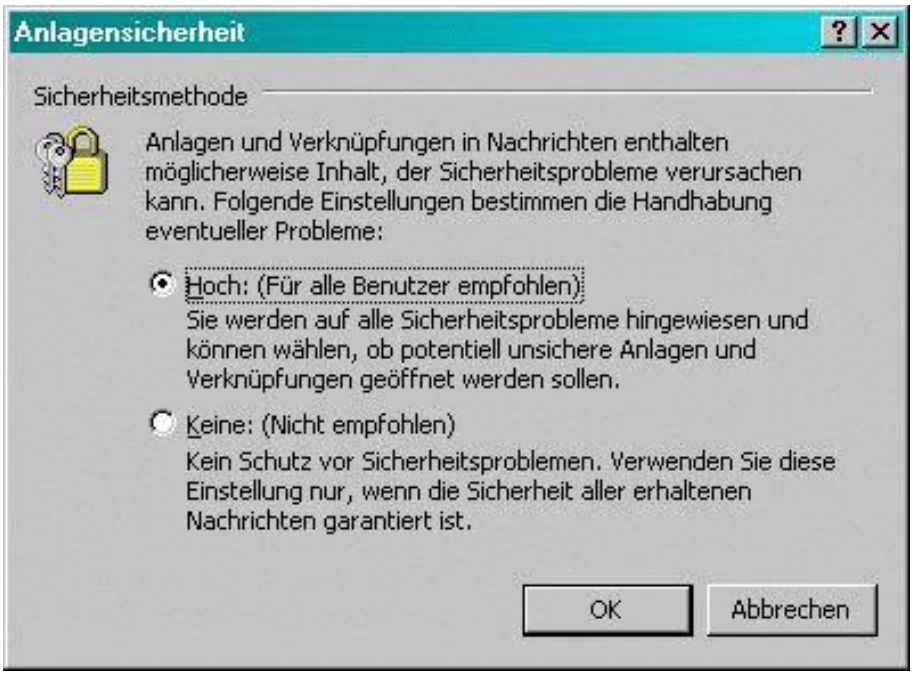
Tabel: *ActiveX* -juhtelementide ja *Plugin* 'ide seadistamine

Tuleb arvestada, et tsoonile kehtestatud piirangud kehtivad kõikidele programmidele, mis kasutavad *Internet Explorer*'i turvatsoone. Näitena toodud konfiguratsioon on väga suurte piirangutega, kuna eesmärgiks on luua olukord, mis välistaks igasuguse aktiivsisu käivitamise *Outlook* 'i keskkonnas. Kui sellist tsoonide seadistust rakendatakse läbi *Internet Explorer*'i ka netilehekülgedele, võib juhtuda, et netilehti ei õnnestu enam korrektselt kuvada, juhul kui need sisaldavad kas skripte või muud aktiivsisu. Hetkel ei ole võimalik defineerida

täiendavaid turvatsoone, mistõttu tuleb turvatsooni *Restricted Sites* kohandada *Outlook*'i piirangutega seadistulele.

Potentsiaalselt ohtlike failimanustega ümberkäimine

Meilidele lisatud manused ei tohi automaatselt avaneda. Automaatse avamise takistamiseks tuleb valida manuste turvalisuse konfiguratsiooni astmeks kõrge (*High*), liikudes valikutesse *Tools* | *Options* | *Security* ning sealt edasi funktsioonile *Attachment Security*).



Joonis: manuste turvalisus

Manustega seotud turvalisuse tõstmiseks võimaldab *Microsoft* kasutada turvavärskendust *Outlook 2000 SR-1 E-Mail Security Update International Release*. Kasutuse praktilisuse seisukohast pole see aga soovitav, kuna värskendusega kaasneb paljude funktsioonide piiramine. E-mailidega kaasnevate potentsiaalselt ohtlike manuste kontrollimiseks ja väljafiltreerimiseks võib enamatel juhtudel soovitada *E-Mail-Gateway* filtrit või tulemüüri. Kui aga meile krüpteeritakse, kaotavad *E-Mail-Gateway*'des rakendatavad filtrid oma toime. Sellisel juhul võib meilifiltreid rakendada klientides, mis peaksid meile pärast nende dekrüpteerimist kontrollima. Võimalike lokaalsete meilifiltrite rakendamise otstarbekuse üle tuleb otsustada iga juhtumi puhul eraldi. Tuleb arvestada, et filtritarkvara laialijagamise, installeerimise ja hooldamise läbi kasvab administreerimistööde maht. Täiendavat kaitset võivad

pakkuda nn *Personal Firewall*'id ehk tulemüürid. Personaalsed tulemüürid võimaldavad kehtestada manuste käivitamisele piiranguid operatsioonisüsteemi tasandil ning loovad käivitatavatele meilimanustele karantiinialad või liivakastid (kontrollitava käivituskeskkonna). Ka siin tuleb vastava toote kasutamise otstarbekus hoolikalt läbi analüüsida, kuna selle rakendamisega suureneb administratiivsete tööde maht.

Lokaalselt installeeritavate toodete nagu meilifiltrite või personaalsete tulemüüride kasutamisest on soovitatav loobuda juhul:

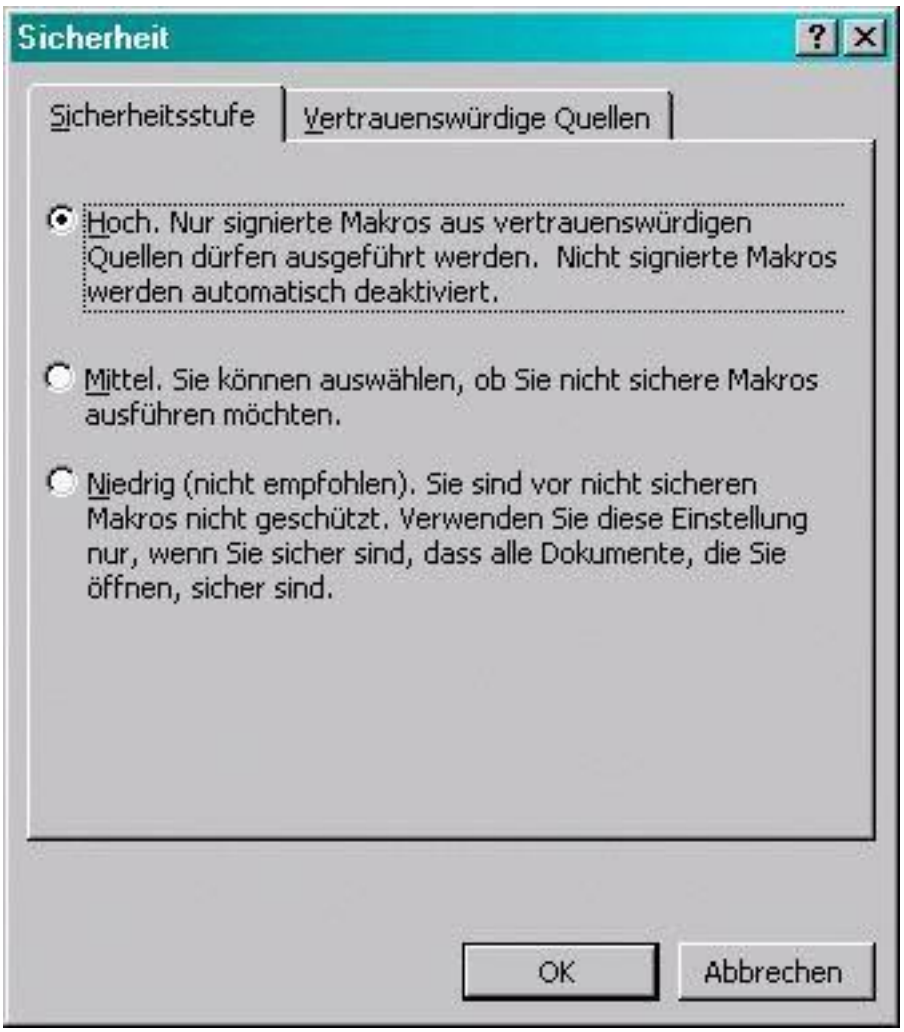
- kui neid ei konfigureerita ega hallata tsentraalselt või
- kui etteantud konfiguratsiooni on kasutajal endal võimalik muuta või
- kui konfigureerimistööd peab tegema kasutaja.

Eelvaateakna desaktiveerimine

Eelvaateakna (*preview*) ehk Outlooki *auto-preview* funktsiooni kasutamisel kuvatakse e-post automaatselt, st meilide võimalik aktiivsisu käivitatakse automaatselt. Seetõttu on soovitatav eelvaateaken ja automaatne eelvaade desaktiveerida. Selleks tuleb *Outlook* 'is välja lülitada funktsioonid *View* | *Preview Pane* ja *View* | *Auto-Preview*.

Turvaseadistused makrode töötlemiseks *Outlook* 'i keskkonnas

Visual Basic (VBA) jaoks on soovitatav lülitada makrode turvaaste kõige kõrgema peale (*High*), tehes vastava seadistuse valikutes *Tools* | *Macro* | *Security* | *Security Level*. Seeläbi käivitatakse ainult allkirjastatud makrod, mille signatuure on võimalik vastavate sertifikaatide abil kontrollida. Usaldusväärsete sertifikaatide loendit saab näha asukohas *Tools* | *Macro* | *Security* | *Trustworthy Sources*.



Joonis: turvaaste

Tuleb arvestada, et ka siin kasutatakse *Microsoft Internet Explorer* 'i vastavat *Authenticode* -seadistust. Muudatused mõjutavad seega kõikide nende programmide tööd, mis seda seadistust kasutavad. Usaldusväärsete väljastajate loendit on soovitav hallata tsentraalselt ning selle laialijagamiseks tuleks kasutada *Windows 2000* grupipoliitikaid. Sinna juurde kuuluv poliitika on kasutajapoliitika, mis tähendab, et erinevatele kasutajagruppidele saab määrata erinevaid eelseadistusi. Poliitika asub grupipoliitika objekti all asukohas *User Configuration / Windows Settings / Internet Explorer Maintenance / Security / Authenticode Settings*. Eelseadistustele on soovitav kehtestada tõke, mis ei lubaks kasutajatel neid ise muutma hakata, milleks tuleb *Authenticode* -seadistustes sisse lülitada funktsioon *Enable trusted publisher lockdown option*.

Joonis: *Authenticode* -seadistused

Tuleb arvestada, et makrode seadistused kehtivad ainult VBA makrodele ning ei kehti *Visual Basic Script* 'ile (selle piirangud kehtetustakse läbi turvatsooni seadistuste). Juhtudel, kus kasutajad tegelevad ise usaldusväärsete väljastajate loendi koostamise ja muutmisega, on täheldatud järgmist käitumist: kui avatakse mõni signeeritud VBA makro ja kui sinna juurde kuuluv sertifikaat pole kantud usaldusväärsete väljastajate loendisse, saab kasutaja ise otsustada, kas lisada vastav sertifikaat sinna loendisse või mitte. Olemasolevate sertifikaatide loendit saab kasutaja ka kustutada. Vastavad otsused puudutavad turvalisust ning reeglina ei peaks neid langetama kasutajad. Ettevõtete ja ametiasutuste puhul ei ole niisugune lahendus soovitatav.

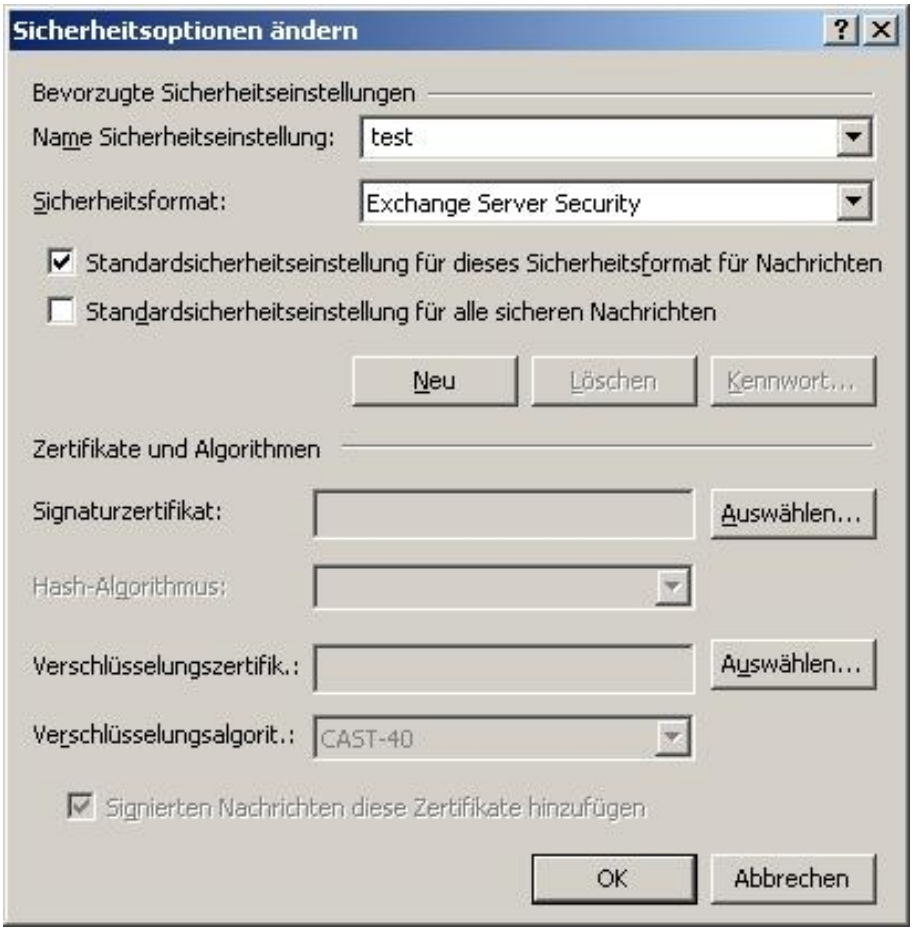
Meilide digitaalsed allkirjad ja meilide krüpteerimine

Meilide krüpteerimiseks ja dekrüpteerimiseks saab *Outlook* 'is kasutada reeglina kahte mehhanismi:

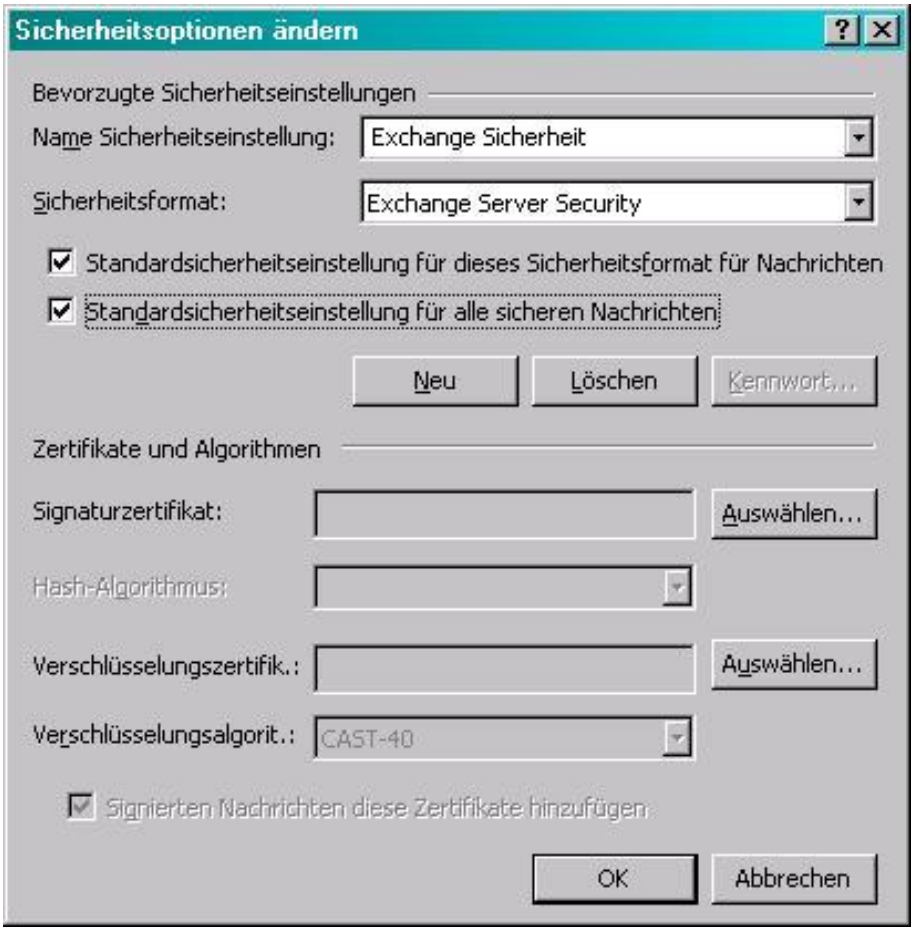
- *Exchange Server Security*
- *S/MIME*

Seadistus *Exchange Server Security* eeldab, et kasutusel on ka *Windows 2000 Key Management Services*. Seda seadistust on soovitav kasutada homogeenses *Windows 2000* keskkonnas. Kui keskkond ei ole homogeenne või kui meile soovitakse krüpteerida läbi mõne *Windows* 'i domeeni, on soovitatav võtta kasutusele S/MIME. E-mailide digitaalsete allkirjade krüpteerimise ja dekrüpteerimise seadistusi saab määrata asukohas *Tools* | *Options*, registrikaardis *Security*, valikuga *Security settings*. Turvaseadistuste dialoogiväljal tuleb määratleda ka

turvaseadistuse nimetus. Lisaks saab funktsiooniga *Security Format* valida *S/MIME* ja *Exchange Server Security* vahel. Siin saab välja valida sertifikaadid, mida tuleks kasutama hakata, kui signatuure luuakse ja krüpteeritakse. Samuti on võimalik konfigureerida, milliseid algoritme tuleb signeerimiseks ja krüpteerimiseks kasutada. Sertifikaatidele ja algoritmidele kohustuslikud seadistused tuleb defineerida ettevõtte või ametiasutuse *Outlook* 'i turvapoliitikaga. Kui kasutatakse erinevaid turvaseadistusi, peab ühe konfiguratsiooni jaoks olema ära märgistatud kontrollkastike *Standard setting for this security format for messages*. Sellega määratakse kindlaks väljavalitud turvaformaadi tüüpseadistused. Kui kasutusele võetakse nii *Exchange Server Security* kui ka *S/MIME*, võib aktiveerida kontrollkastikese *Standard setting for all secure messages*, mis määrab väljavalitud turvaseadistused mõlema turvaformaadi jaoks tüüpseadeteks. Sellisel moel on võimalik samu sertifikaate ja protseduure rakendada nii *Exchange Server Security* kui ka *S/MIME* jaoks. Eelduseks on muidugi asjaolu, et tegemist on ühilduvate sertifikaatide ja protseduuridega.



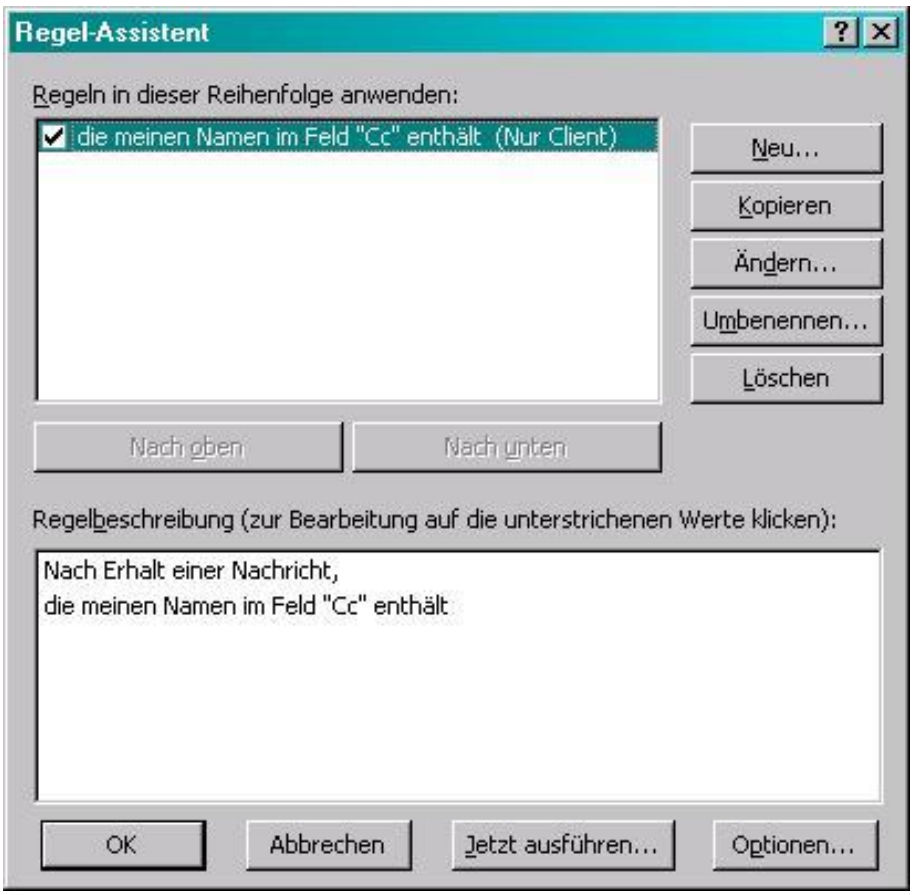
Joonis: turvaseadistuste muutmine



Joonis: standardsed turvaseadistused

E-mailide filtreerimisreeglite konfigureerimine

Ebasoovitud meilid (nn *spam* ehk rämpspost) võivad segada produktiivset töötamist. *Outlook 2000* pakub võimalust rämpsposti spetsiaalsete meilifiltritega välja filtreerida. Filtreerimisreeglite seadistamist ei ole soovitatav jätta kasutaja hooleks, kes teeksid seda *Outlook 2000* klienttarkvara all. Filtreerimine peaks aset leidma serveris. Serverilahenduse eeliseks on ühelt poolt asjaolu, et sellisel juhul filtreeritakse meile pidevalt ning teiselt poolt tõsiasi, et sellega väheneb administratiivse töö maht. Kui serveripoolset filtreerimist siiski ei taheta, on soovitatav, et administraator looks vastavad filtreerimisreeglid tsentraalselt. Kasutajatel on seejärel võimalik need endale importida läbi valikute *Tools* | *Rules Wizard* | *Options*. Kasutajate loodavaid reegleid tuleks sellistel juhtudel kasutada ainult täiendustena.



Joonis: *Rules Wizard*

Piirangutega asendaja volitused

Outlook/Exchange lubab määrata asendajaid (nt puhkuse või haiguslehel viibimise ajaks), kes saavad üle võtta meilidega töötamise, tegutsedes algse kasutaja nimel. Vastavad asendajad saavad juurdepääsu postkastile või vastava kasutaja üksikutele *Outlook*'i kaustadele ning neil on võimalik meile saata põhimõttel „. . . ülesannetes“. Asendajate puhul on soovitatav, et nende volitused defineeriks eranditult postkasti administraator, mitte kasutajad. Sellega vähendatakse andmekao ja konfidentsiaalsuse kadumise ohtu, mis võivad olla tingitud väärkonfiguratsioonide tekkest. Asendajatele on võimalik anda pääsuõigusi eraldi kõigi *Outlook* 'i kausta komponentide (kalendri, kontaktide, sissetulevate meilide jne) lõikes. Konfiguratsioon tehakse vastavate objektide omaduste all. Asendajatele kehtivad reeglid tuleks sisse kirjutada ettevõtte või ametiasutuse üldkehtivatesse poliitikatesse. Postkastide administraatorid saavad volitust *Send on behalf* konfigureerida utiliidiga *Active Directory Users and Computers*.

Kasutajatele saab asendajaid määrata valikutega *Properties* | *Exchange General* | *Delivery Options*. Vajadusel saab asendajate volitusi *Outlook 2000* keskkonnas määrata ka valikutest *Tools* | *Options* registrikaardis *Delegations* , klõpsates lisamisvalikul *Add*. Sellisel juhul saab asendajaid valida aadressiraamatu alusel.

Igale kasutajale, kes on saanud seoses mõne võõra postkastiga asendaja volitused, antakse automaatselt saatmisõigus *Send on behalf* . See tähendab, et asendajatel on võimalik kasutada andmevälja kellelt (*From*), et lisada sinna vastav nimi. Meilide vastuvõtjatele ilmub sellisel juhul viide „ *On behalf of* “ ning lisaks konto omaniku nimele ilmub *From* -reale ka asendaja nimi.

E-maile ei tohi automaatselt edasi saata ega ümber paigutada

Reegliassistenti (*Rules Wizard* 'it), mille abil reeglid kehtestatakse, saab kasutada ka selleks, et meile automaatselt mõnele teisele kasutajale edasi saata või teatud kindlatesse kaustadesse ümber tõsta. Läbimõtlemata edasisaatmine ja ümbertõstmine võib aga endaga kaasa tuua ohu, et andmed võivad kas kaduma minna või siis kannatab nende konfidentsiaalsus. Niisugused olukorrad võivad tekkida näiteks siis, kui meilidega edastatakse ootamatult konfidentsiaalseid teateid või juhul, kui sellele kaustale, kuhu e-mailid ümber paigutatakse, pole kehtetustatud piirangutega pääsuõigusi. Seetõttu on soovitatav elektronposti mitte automaatselt edasi saata ega ka kuhugi ümber tõsta.

Täiendavad turvameetmed kasutajatele

Kui saatja e-mailil on eraldi kuvanimi, nt *BSI Mailing list*, kuvab *Outlook 2000* mitte alati täieliku meiliaadressi, vaid ainult kuvanime, ehk siis antud juhul nime *BSI Mailing list* . Selle *Outlook 2000* omadusega kaasneb oht, et manipuleeritud meiliaadressid võivad jääda tuvastamata ning tagajärjeks võib olla konfidentsiaalsete andmete edasitoimetamine isikutele, kel puuduvad vastavad volitused. Seetõttu on soovitatav saatja meiliaadressi (või siis vastuvõtja meiliaadress, kui kasutatakse vastamisfunktsiooni *Answer*) kindlasti täies pikkuses kuvada ja see üle kontrollida. Meiliaadresside vaatamiseks tuleb teha topeltklõps kuvatava nime peal kas andmeväljal „ *From* “ või „ *To* “. Selle kontrolli peab läbi viima kasutaja. Kui meili päritolu kohta esineb kahtlusi, tuleks kontrollida meili päiseinfot (*heather data*). Vastava info leiab andmeväljalt *Internet Headers*, valikute alt *View* | *Options*. Lisaks täiendavale infole saatja kohta saab siin vaadata ka meili liikumise teekonda ehk seda, kuidas see on saatjalt adressaadini toimetatud. Sellele vaatamata tuleb arvestada, et kurikaeltel on võimalik oma meiliga kaasas olevat päiseinfot muuta.

Outlook 2000 laiendatud funktsioonide desaktiveerimine

Outlook - *Formulardesigner* kujutab endast arenduskeskkonda *Workflow* -rakendustele, mis töötavad *Outlook* -kataloogide baasil. Seeläbi võivad tekkida turvaprobleemid, kuna *Formulardesigner* 'iga on võimalik kasutada nt *ActiveX* juhtelemente. Meilide tavakasutajatele pole neid võimalusi tarvis. Seetõttu on soovitatav *Outlook* 'i *Formulardesigner* klientide jaoks desaktiveerida. Selleks on kaks võimalust. Võib koostada kohandatud installatsioonipaketi, (*Customized Installation*), millest tuleb *Formulardesigner* välja jätta (vt lisaks M 4.161 Exchange / Outlook turvaline installeerimine). Teiseks võimaluseks on *Formulardesigner*'i desaktiveerimine läbi vastava registriseadistuse. Selleks tuleb *HKEY_USERS* \ *.DEFAULT* \ *Software* \ *Microsoft* \ *Office* \ *9.0* \ *Outlook* all luua *REG_DWORD* nimega *NoOutlookFormsDesigner*. Väärtuseks peab olema määratud *1*, et *Formulardesigner* ei oleks enam kättesaadav. Registrisse tehtud sissekanne kopeeritakse seejärel automaatselt kasutajate registriharudesse. Kui *Outlook* 'i uuesti laiali jaotatakse, on soovitatav kasutada kohandatud installatsiooni. Olemasolevate installatsioonide jaoks saab registrisse tehtud sissekannet jaotada *Windows 2000* grupipoliitikate kaudu.

Folder-Add-In 'ide ja *COM-Add-In* 'ide keelamine

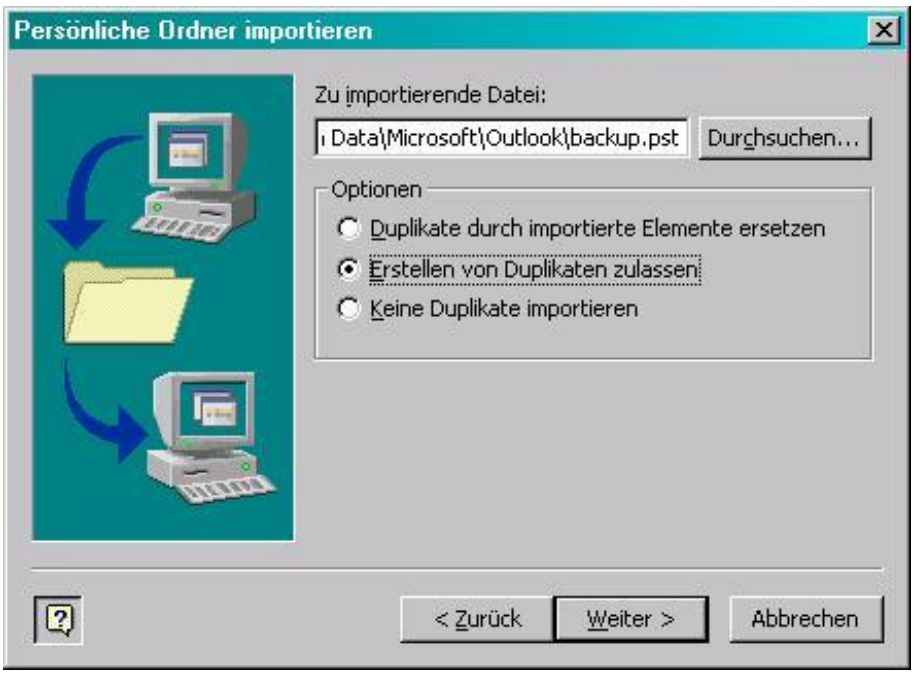
Standardina lubab *Outlook 2000* oma kasutajatel iseseisvalt *Add-In* 'e juurde

installeerida, et laiendada *Outlook* 'i funktsioone (*Add-In-Manager* ja *COM-Add-Ins* valikutes *Tools* | Options, registrikaardil *Other* lõigus *General* | *Extended Options*). Kuna selle käigus kaasatakse reeglina käivitatavaid koode kas *EXE* - või *DLL* -failidena, peavad täiendused alati läbima kasutuselevõtu protsessi. Töökorralduslike reeglitega peab olema tagatud, et töötajad ei laeks internetist ega kasutaks oma Add-In 'e.

Kausta *Deleted Items* automaatne tühjendamine

Kustutatud objektide kausta automaatne tühjendamine *Outlook* 'i töö lõpetamisel on seotud nii eeliste kui ka puudustega. Peamisteks eelisteks on asjaolud, et seda funktsiooni kasutades ei jää kausta alles „kustutatud" konfidentsiaalset infot ning andmete jaoks ei lähe tarvis täiendavat salvestusruumi. Põhiliseks puuduseks on aga tõsiasi, et seda funktsiooni kasutades võib tekkida andmekadu. Kustutatud objektide kausta (*Deleted items*) tuleks automaatselt tühjendada neis keskkondades, kus tuleb tihti ette konfidentsiaalsete andmete edastamist meili teel. Automaatse tühjendusfunktsiooni saab sisse lülitada valikute alt *Tools* | *Options* registrikaardil *Other*, märgistades kontrollkastikese *Clear "Deleted Items" folder on program termination*. Sellistel juhtudel on soovitatav, et süsteem kuvaks ka enne sisu lõplikku kustutamist ka vastava hoiatuse. Selle sisselülitamiseks tuleb valikute all *Tools* | *Options* registrikaardil *Other* | *Advanced Options* ära märgistada kontrollkastike *Display warning before final deletion of items*.

PST -failide importimiseks ei tohi kasutada funktsiooni *Replace duplicates with imported items*
PST -failide importimisel (nt varukoopiate või arhiiviimportimisel) võivad tekkida andmekaod värskete andmete ülekirjutamisel vanemate andmeversioonidega, kui importimisviisardiks valitakse funktsioon *Replace duplicates with imported items*. Seepärast on soovitatav funktsioon *Replace duplicates with imported items* välja lülitada. Siinjuures tuleb arvestada, et duplikaatide genereerimisel ei väljasta süsteem sellekohast hoiatust, mis tähendab, et kõik võimalikud liigsed duplikaadid tuleb vajadusel kasutajatel endil üles leida ja käsitsi ära kustutada.



Joonis: *Import Wizard*

Outlook 2000 e-mailide turvavärskendus

Microsoft 'i poolt soovitatav turvavärskendus suurendab e-mailidega ümberkäimise turvalisust. Installeerimise eelduseks on installeeritud *Office 2000 Service Pack 1* või *1a*. Pärast turvavärskenduse installeerimist on *Outlook* funktsioonid seoses meilide manuste kasutamisega väga piiratud juhul, kui Outlook on konfigureeritud kui *Internet-Mail-Client* ning kui e-maile hoitakse personaalsetes (.pst) kaustades. Seetõttu tuleb iga juhtumi puhul eraldi kaaluda, kas vastava turvavärskenduse rakendamine on mõttekas või mitte. Üldised nõuanded on järgmised:

- Bürookeskkondades, kus kasutajad saadavad meilidega tihti nt *Office* 'i dokumente, võib selle installeerimist soovitada.
- Töökeskkondades, kus programmide arendajatel ja administraatoritel on tarvis ka käivitatavaid faile saata, ei ole selle installeerimine soovitatav. Sellistel juhtudel tuleb siiski rakendada täiendavaid kaitsemeetmeid potentsiaalselt ohtlike käivitatavate meilimanuste vastu (nt viirusefiltreid, personaalset tulemüüri).

Kui turvavärskendus installeeritakse keskkonda, mille kasutatakse *Outlook* 'i *Exchange-Client* funktsioonides, saab *Exchange* 'i administraator selle kasutamist reguleerida. Sellisel juhul võib turvavärskenduse installeerimist soovitada. Turvavärskendusel on järgnev mõju:

- *e-mailide manuste turvalisus*: kasutajatele tõkestatakse juurdepääs meilide manustele, mis võivad sisaldada ohtlikku käivitatavat koodi (nt .EXE, .BAT, Skripts, vt tabel allpool). *Outlook* tõkestab sealjuures juurdepääsu täielikult nii, et vastavaid manuseid ei saa ka salvestada. Seda, kas e-maili manus blokeeritakse või mitte, otsustab *Outlook* faili nimelaiendi põhjal.
- *Objekti mudeli kaitse*: sellega nõutakse kasutaja sekkumist niipea, kui mõni väline programm püüab tekitada endale juurdepääsu Outlooki aadressiraamatule või püüab iseseisvalt hakata meile saatma (ILOVEYOU tüüpi viiruse analoog). See tähendab, et olukordades, kus kasutaja sessiooni vältel leiab taustal aset programmi pooltjuhitud meilide saatmine, tuleb iga kord, enne kui e-mail välja saadetakse, kasutajal sellesse protsessi sekkuda. Reeglina sellist lahendust ei soovita.
- *Kõrgendatud standardsed turvaseadistused*: seeläbi tõstetakse Outlooki turvatsooni turvalisuse standardseadistused astmelt *Internet* astmele *Restricted Sites* . Samaaegselt lülitatakse selle tsooni sees välja aktiivne *Skripting*.

Pärast turvapaiga installeerimist pole kasutajatel enam võimalik teatud liiki e-maili manustele ligi pääseda (nn *security level 1 files*). Siia alla kuuluvad järgnevas tabelis toodud failitüübid. Sellist lahendust võib küll IT-turbe seisukohast väga positiivseks pidada, kuid praktikas kaasnevad sellega tihti suured puudused piiratud funktsioonide näol. Selleks et usaldusväärsete allikate poolt edastatud, turvaklassi nr 1 liigitatavaid e-maili manuseid oleks ka edaspidi võimalik vajadusel kätte saada ja salvestada, tuleb need saatjatel mõnda teise failiformaati pakkida (nt ZIP-formaati).

Tähistus	**Eelseadistusega määratud failide nimelaiendid**	**Soovitatavad laiendid**
Level 1	.ADE, .ADP, .BAS, .BAT, .CHM, .CMD, .COM, .CPL, .CRT, .EXE, .HLP, .HTA, .INF, .INS, .ISP, .JS, .JSE, .LNK, .MDB, .MDE, .MSC, .MSI, .MSP, .MST, .PCD, .PIF, .REG, .SCR, .SCT, .SHS, .URL, .VB, .VBE, .VBS, .WSC, .WSF, .WSH	Soovitatav on mitte ühtegi sissekannet sellest loetelust kustutada. Vajadusel saab seda nimekirja täiendada. Muudatused jõustuvad ainult juhul, kui andmed salvestatakse *Exchange* -serverile. Kui andmeid hoitakse mõnes lokaalses kaustas, pole võimalik täiendavaid failide nimelaiendeid defineerida.

Level 2	puudub	*Office* 'i failid: .DOC, .DOT, .XLS, .XLT, .MDZ, .POT, .PPT, .WIZ, .OFT, .PST, .EML Tihendatud failid: .ZIP, .ARC, .ARJ, .CAB Multimeediafailid: .AVI, .MPEG, .IVF, .MP3, .WAV Internetilehed: .HTM, .HTML

Tabel: failiformaadid

Turvapaigaga defineeritakse täiendav turvaklass, nn failid, mis kuuluvad turvaklassi nr 2, mida ei ole enam võimalik otse e-maili seest avada. Nende failide edasitöötlemiseks tuleb need esmalt kuhugi salvestada. Seda, millised failid liigitatakse turvaklassi nr 2, peab defineerima ja seadistama administraator. Turvaklassi nr 2 on soovitatav liigitada vähemalt järgmist tüüpi failid (vt ka ülemist tabelit):

- *Microsoft Office* failiformaadid
- kokkupakitud failiformaadid
- multimeedia failiformaadid
- Internetilehed.

Täielik nimekiri lokaalse arvuti alla salvestatud failiformaatide liigitusest koos installeeritud rakendustega asub registrivõtme all *HKEY_CLASSES_ROOT*. Administraator võiks soovitavalt just nende registrikannete alusel defineerida *Level 2* turvaklassi failide loetelu. Nende e-maili manuste puhul, mis ei liigitu ei turvaklassi 1 ega 2, kehtivad tavalised kasutustingimused. Kasutajalt küsitakse, kas ta soovib vastavat manust avada või salvestada. Turvavärskenduse kohandamiseks ja klientidele laialijagamiseks on soovitatav appi võtta *Outlook Security Template* (*OutlookSecurity.oft*).

Eriteadete käsitsemine

Automaatselt toimivad lugemis- ja vastuvõtukinnitused võivad viia tahtmatute *Denial-of-Service* -rünneteni. Olukorras, kus organisatsiooni e-mailipoliitika vastavate kinnitusfunktsioonide kasutamist konkreetselt ette ei näe, on soovitatav lugemis- ja vastuvõtukinnitusest loobuda. Selleks tuleb sisse lülitada funktsioon *Never send a reply*, mis asub valikute all *Tools* | *Options* registrikaardil *Settings*, kasutades valikut *E-Mail Options* | *Follow-up Options*.

Joonis: *Follow-up*

Automaatselt loodavad eemalolekuteated edastavad üheltpoolt informatsiooni töötaja eemalviibimise kohta organisatsioonist väljapoole, kui teiselt poolt võivad need kujuneda ka lähtepunktiks *Denial-of-Service* tüüpi rünnetele. Seetõttu peaks iga organisatsioon otsustama, kas selliseid funktsioone kasutada või mitte. Eemalolekuassistenti saab konfigureerida menüüs *Tools* | *Out of Office Assistant*. Eemalolekuassistenti saab ka Outlooki klientide jaoks desaktiveerida, milleks tuleb menüüs *Tools* | *Options* | *Other* | *Advanced Options Add-In Manager*, eemaldada märgistus kastikesest *Exchange Extension Commands*.

e-maili formaat

Meilide saatmiseks ei ole soovitatav kasutada HTML-formaati, kuna see võib vastuvõtjale tähendada potentsiaalset turvariski. Meiliformaati saab valida menüüst *Tools* | *Options* registrikaardis *e-mail-Format*. Formaadiks on soovitatav seadistada ainult tekst (*Text Only*). Tuleb arvestada, et antud seadistus ei paku kaitset sissetulevate HTML-e-mailide vastu. (Teadmiseks: *Outlook 2000* -le järgnenud programmiversiooni saab seadistada nii, et kõik sissetulevad e-mailid konverteeritakse sisenedes ümber puhtasse tekstiformaati).

Joonis: e-maili formaat

Vältige *Word* 'i kasutamist meiliredaktorina

Kui meiliredaktorina kasutatakse Microsoft Wordi, koostatakse meilid *RTF* -formaadis (*Richt-Text-Format*). Sellega kaasneb oht, et kõik e-mailirakendused ei pruugi RTF-formaadis teadete kuvamisega hakkama saada. Halvimal juhul võivad seeläbi meilide teatud osad kaduma minna. Kuna turvaprobleem kaasneb ka makrodega, soovitatakse *Word* 'i kasutamisest meiliredaktorina loobuda. Selleks tule menüüs *Tools* | *Options* registrikaardil *e-mail-Format* desaktiveerida kontrollkastike *Process e-mail with Microsoft Word*. Ametiasutuses ja ettevõtetes tuleks mõne poliitikaga kehtestada kõigile ühtsed reeglid, millist tohib redaktorit e-mailide jaoks kasutada.

Täiendavad aspektid

Kui meilide krüpteerimiseks kasutatakse S/MIME krüpteeringut, võetakse krüpteeritud meilid reeglina ka andmevarundusse üle krüpteeritud kujul. Tagamaks, et need andmed on hiljem käideldavad, nt millegi taastamiseks pärast avarii-

olukorda, tuleb andmevarundusse kaasata ka krüpteerimisel kasutatud võtmed. Täiendavat infot leiate selle kohta meetmest M 6.82 Avariiplaani koostamine Exchange-süsteemi avarii puhuks .

Peakategooria loetelu taastamine kustutatud ülesannete, kontaktide ning kalendri ja *Journal* 'i sissekannete puhul

Ülesannete, kontaktide, kalendri ja *Journal* 'i sissekannete tegemisel on võimalik need liigitada kategooriate alla. Kategooriaid saab valida eeldefineeritud kategooriate nimekirjast ning saab defineerida ka uusi kategooriaid. Enda poolt defineeritud kategooriad jäävad alles ka siis, kui sissekanded ülesannete, kontaktide kohta või kalendri sissekanded on juba ära kustutatud. Seepärast tuleks ebavajalikuks muutunud kategooriad ära kustutada, eriti juhtudel, kus nende põhjal on võimalik teha järeldusi konfidentsiaalsete sissekannete kohta. Kategooriate nimekirja saab vaadata asukohas *Edit* | *Categories* | *Main Category List*. Seal on võimalik ka kategooriaid ükshaaval kustutada või taastada kogu peakategooria nimekiri selle esialgsel kujul, mis eemaldab kõik lisatud kategooriad.

Joonis: peakategooria nimekiri

Tundliku detailse info eemaldamine oma e-maili päisest

Väljasaadetavate e-mailide päised (*headers*) võivad sisaldada infot, mida ei peaks võib-olla väljapoole levitama. Siia alla kuulub nt info operatsioonisüsteemi ja kasutatava meiliserveri meilitarkvara kohta Seda tuleb konfigureerida serveri poolel, vt kisaks M 4.162 Exchange 2000 serverite turvaline konfiguratsioon .

Viirusetõrjetarkvara kasutamine

Kõikidel juhtudel on soovitatav kasutada viirusetõrjetarkvara. Suurimat kaitset pakub lahendus, milleks on *Gateway-Client* -kombinatsioon, mis sisaldab nii serveri- kui ka kliendipoolseid komponente. Lahendus peab tagama, et e-maili kõik manused läbiksid kontrolli. See kehtib ka tihendatud ja krüpteeritud manuste kohta.

Tarkvara ja süsteemi hooldamine

Vastutavad administraatorid peaksid ennast regulaarselt läbi interneti kursis hoidma võimalike uute *Exchange/Outlook 2000* kitsaskohtadega. Pakutavad turvapaigad tuleks esmalt mõnes testimiskeskkonnas läbi katsetada ning alles siis igapäevasesse kasutusse üle võtta.

Täiendavad kontrollküsimused:

- Kas turvaklassi nr 2 kuuluvate failitüüpide nimekiri on koostatud?
- Kas kasutajaprofiilid on loodud?
- Kas internetist otsitakse regulaarselt infot *Exchange/Outlook 2000* tarkvara puhul ilmsiks tulnud turvaaukude kohta?

M 4.166 Exchange/Outlook 2000 turvaline käitamine

Algatamise eest vastutavad: IT-juht, IT-turbespetsialist
Rakendamise eest vastutavad: administraator

Pärast *Exchange/Outlook 2000* installeerimist ja konfigureerimist tuleb kasutusele võtta meetmed, mis tagaksid süsteemi turvalise käitamise. Siinkohal tuleb arvestada järgmiste, turvalisuse seisukohast oluliste aspektidega:

- organisatsiooni turvapoliitikate rakendamine (vt M 2.248 Exchange/Outlook 2000 turvapoliitika määratlemine),
- platvormina kasutatava operatsioonisüsteemi turvaline käitamine (vt M 4.146 Windows'i klient-operatsioonisüsteemide turvaline käitus),
- administratiivsed aspektid,
- tarkvara ja süsteemi hooldamine,
- viirusetõrje,
- süsteemi seire,
- andmevarundus ja
- avariikindlus ehk kahjude ohjamine avariide korral.

Administratiivsed aspektid

Administreerimisel ja volituste jagamisel tuleks alati lähtuda põhimõttest 'võimalikult vähe privileege' (*least privilege*). See kehtib ennekõike *Exchange* 'i administraatorite kohta: iga administraator peab saama ainult sellised volitused, mis on vajalikud tööülesannete täitmiseks. *Windows* 'i ja *Exchange* 'i administraatorite tööd tuleks nii palju kui võimalik lahutada. Samas tuleb ka tõdeda, et see ei ole alati täies mahus võimalik. Teatud tööülesannete täitmiseks läheb ka *Exchange* 'i administraatoritel tarvis Windows 2000 lokaalseid administraatoriõigusi (nt *Exchange* 'i teenuste käivitamiseks ja peatamiseks).

Tarkvara ja süsteemi hooldamine

Turvalise käitamise üheks oluliseks eelduseks on kõikide turvalisuse seisukohast oluliste remondipakettide, värskenduste ja turvapaikade paigaldamine. Seetõttu on oluline, et administraatorid hoiaksid ennast pidevalt kursis *Exchange 2000* ja *Windows 2000* kohta avaldatud turvaaukudega ning astuksid võimalikult kiireid samme vastuabinõude rakendamiseks. Kindlasti ei tohiks *Service Pack* 'i, *Update* 'i või *Patch* 'i paigaldada otse töökeskkonda, vaid neid tuleb eelnevalt testimiskeskkonnas katsetada. Niimoodi on võimalik kindlaks teha, kas nendega kaasnevad võimalikud soovimatud kõrvalmõjud. Sellele lisaks tuleks regulaarselt kontrollida terviksüsteemi konfiguratsiooni, et teha kindlaks, kas see vastab jätkuvalt kõigile ettekirjutustele ning turvanõuetele.

Viirusetõrje

Üheks suurimaks ohuks meilisüsteemide turvalisele käitamisele on olukorrad, kus

süsteemi võivad sattuda viirused, ussviirused ning kõikvõimalikud teised pahavara vormid. Süsteemi kaitseks tuleks installeerida viirusetõrjetarkvara, mille võrdlusandmebaasi uuendatakse regulaarselt. Täiendavat infot viirusetõrje valdkonna kohta leiate moodulist B 1.6 Viirusetõrje kontseptsioon ning meetmetest M 4.33 Viirustõrjeprogrammi kasutamine andmekandjate vahetamisel ja andmete edastamisel ja M 6.23 Käitumisreeglid arvutiviiruste esinemisel .

Süsteemi seire
Igapäevaste tööprotsesside jooksva turvalisuse tagamiseks ning igasuguste ohtude varajaseks tuvastamiseks tuleks *Exchange* -süsteem kaasata pideva seire alla.

Andmevarundus
Selleks, et andmeid saaks võimalikult kiiresti taastada, nt pärast mõne süsteemi avariid, tuleb *Exchange* -süsteemi andmetest teha regulaarselt varukoopiaid (vt M 6.32 Regulaarne andmevarundus ja M 6.49 Andmebaasi varundamine). Varukoopiate loomiseks võib kasutada *Windows 2000 Backup Utility* 't (vt M 6.78 Andmete varundamine Windowsi klientsüsteemides). Varundamisprotsessi tuleks kaasata vähemalt *Mailbox Store*, *Public Store* ja *Transaction Logs*. Andmevarunduse liik (täielik või inkrementaalne) ei mängi siinkohal olulist rolli. Kuna *Exchange/Outlook* -süsteemid vajavad korralikuks toimimiseks *Windows 2000 Active Directory* 't, tuleks ka see varundusse kaasata (vt lisaks M 4.146 Windows'i klient-operatsioonisüsteemide turvaline käitus). Lisaks on soovitatav postkastides ja avalikes kaustades hoitud kustutatud *Exchange* -objektid jäädavalt kustutada alles pärast teatud arvu päevade möödumist ning vastavate varukoopiate loomist. Selliseid seadistusi saab teha kõikide üksikute andmesalvestite lõikes. Lisaks on soovitatav jätta postkastide kustutatud sisu esialgu teatud aja jooksul lõplikult kustutamata (standardne seadistus on 30 päeva). Vastavad väärtused peaksid seejuures lähtuma kas ettevõtte või ametiasutuse vajadustest. Andmebaaside varundamiseks ja nende sisu taastamiseks võimaldab *Exchange 2000 Server* kasutada omaenda programmiliidest API (*Esebcli2.dll*). See võimaldab *Windows 2000* andmevarundusprogrammil teha vastavaid andmevarundus- ja taastamistöid *online* -töörežiimis, st ilma et *Exchange* -teenuseid oleks tarvis sulgeda. *Online* -andmevarundust on soovitatav kasutada sagedaste (iga päev tehtavate) varukoopiate loomiseks. *Exchange 2000 Server* installatsiooni *offline* -andmevarunduseks tuleb *Exchange* -teenused esmalt sulgeda. Seejärel tuleb *Exchange* -kataloogist (nt *c:\Programme\Exchsrvr*) koos kõikide alamkataloogidega teha varukoopia. Sellega kaasatakse kõik *Exchange* -serveri binaarsed andmed, muuhulgas ka MTA-de ja *Gateway* -konnektorite meilide ootejärjekorrad. Sellist andmevarundusmeetodit on soovitatav kasutada vähem sagedaste (iganädalaste) varukoopiate loomiseks.

Andmevarundusprotsessi automatiseerimiseks tuleb vastavalt seadistada *Windows 2000 Server* 'i konfiguratsiooni. Kui ühtki teist andmevarundust automatiseerivat mehhanismi organisatsiooni raames ei kasutata, on soovitatav kasutada just seda, Windowsi oma andmevarundusmehhanismi.

Andmevarunduse puhul tuleb arvestada ka klientidega. Lokaalsete kasutajasüsteemide alla salvestatud andmed nagu personaalsed *Outlook* 'i kaustad tuleb

samuti andmevarundusse kaasata. Erilist tähelepanu vajab selliste andmete varundamine, mis on kaitstud kas krüpteeringu, juurdepääsu piiravate paroolide või muude mehhanismidega. Reeglina tuleb sellistel juhtudel luua varukoopiad ka konfidentsiaalsetest pääsuandmetest, et tagada nende olemasolu vastavate andmete taastamisel.

Avariikindlus

Exchange 2000 turvaliseks ja katkestusteta käitamiseks peab *Global Catalog Server* olema alati ligipääsetav. Exchange 2000 serveri võimaliku avarii tagajärgede minimeerimiseks saab Exchange-andmeid partitsioonide loomise teel laiali jaotada erinevatele serveritele. Sellisel juhul puudutab ühe serveri avarii ainult teatud osa andmetest. Partitsioonide loomist tuleb planeerida ja rakendada vastavalt vajadustele. Kui avalikes kaustades hoitavad andmed peavad olema alati täies mahus kättesaadavad, tuleks luua replikaadid, mis võimaldaksid jaotada andmeid erinevatele serveritele. Ühe serveri avarii korral saab jätkuvalt kasutada teiste serverite all hoitavaid replikaate. Niinimetatud klasterdamisega on võimalik käitada mitut füüsiliselt eraldi toimivat serverit korraga ühe virtuaalse serverina. Ühe serveri tõrke korral toimub automaatne *Failover* ja klastri ülejäänud serverid võtavad avariilise serveri ülesanded enda kanda. Kas seda funktsiooni kasutada või mitte, tuleb otsustada iga juhtumi puhul eraldi. Kõrgete käideldavusnõuete puhul tuleks järele mõelda, kas *Exchange* -süsteemiterviku jaoks võiks sisse seada liiasusega ühendused ning vahest tuleks varustada liiasusega ka väljuvad/sissetulevad ühendused (vt M 4.162 Exchange 2000 serverite turvaline konfiguratsioon). Avariide ennetamiseks peaks eksisteerima rakendatav avariiplaan (vt M 6.82 Avariiplaani koostamine Exchange-süsteemi avarii puhuks).

Kaitse *Denial-of-Service* (*DoS*) tüüpi rünnete vastu

DoS -rünnete vastaseks kaitseks on soovitav kehtestada piirangud teadete ehk salvestusruumi maksimaalsele suurusele. See kehtib ennekõike sissetulevatele ühendustele. Täiendavaks kaitsemehhanismiks on meilide filtreerimine. Sellega ei ole küll võimalik ära hoida suurelt ette võetud rämpspostiründe id, kuid üksikute saatjate väljafiltreerimiseks on see mehhanism täiesti sobiv.

Täiendavad kontrollküsimused:

- Kas *Exchange* -süsteemi avarii puhuks on koostatud avariiplaan?
- Kas *Exchange* 'i, *Outlook* 'i ja *Active Directory* andmetest luuakse regulaarselt varukoopiaid?
- Kas administraatorid hoiavad end pidevalt kursis uute ilmsiks tulnud turvaaukudega?

M 4.168 Sobiva arhiivisüsteemi valimine

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: IT-juht, arhiivi haldaja

Arhiivisüsteemi valiku langetamisel tuleb lähtuda arhiveerimise kontseptsioonis (vt lisaks M 2.243 Arhiveerimiskontseptsiooni väljatöötamine) ette antud tingimustest. Üldjuhul seatakse arhiivisüsteemile järgmised miinimumnõuded, mida tuleb kindlasti täiendada ka individuaalsete, organisatsiooni eripära kajastavate nõuetega:

- Ühendamine olemasoleva süsteemikeskkonnaga – arhiivisüsteemil peaksid olema vajalikud liidesed olemasoleva süsteemikeskkonnaga ühendamiseks (võrgu-, serveri-, klient-, süsteemihaldusliidesed). Süsteemid, mis võimaldavad andmeid sisestada ja väljastada, nagu nt skannerid, tekstitöötlus, printerid jne, ei kuulu tavaliselt arhiivisüsteemi alla, vaid tehakse kättesaadavaks rakenduste tasandil.
- Ühendamine dokumendihaldussüsteemiga – arhiivisüsteemil peaksid olema vajalikud liidesed dokumendihaldussüsteemiga ühendamiseks.
- Dokumentidest erinevate versioonide loomise võimalus – arhiivisüsteem peaks võimaldama salvestada dokumentidest erinevaid koopiaid (versioone).
- Arhiveeritud andmete juurdepääsu kaitse – arhiivisüsteemi enda funktsioonide abil peaks olema võimalik kaitsta arhiveeritud andmeid volitamata juurdepääsude vastu. Seda peaks saama teha ette antud volituste kontseptsiooni alusel.
- Mitmeastmeline, töörollidel põhinev volituste kontseptsioon – töörollidel baseeruva volituste andmise puhul ei anta pääsuõiguseid mitte konkreetsetele kasutajatele, vaid seotakse need eelnevalt defineeritud kasutajagruppidega (rollidega). Vastupidiselt tavapärastele volitusi omavatele gruppidele arvestatakse rollipõhise juurdepääsumudeli puhul ka võimalike rollikonfliktidega. See tähendab nt, et ühel ja samal isikul ei saa olla võimalik täita korraga nii administraatori kui ka revidendi ülesandeid.
- Logimine – arhiivisüsteem peaks võimaldama logimisfunktsiooni kasutamist, mis aitaks mõista kõikvõimalikke arhiveerimisega seotud protsesse (vt M 4.172 Arhiivipöörduste logimine). Logimise puhul peab olema võimalik defineerida sündmusi, mida peetakse kriitilisteks ning süsteem peaks suutma nende esinemisest teavitada administraatorit.
- Eraldi kasutajakonto loomine revisjoniks – arhiivisüsteemis regulaarselt läbiviidavaks revisjoniks peab olema võimalik luua eraldi kasutajakonto, millele antakse revidendile vajalikud õigused. Konkreetsed õigused tuleb kehtestada igal organisatsioonil iseseisvalt. Revisjoni jaoks antakse vastavale kasutajakontole konfiguratsiooni- ja logiandmetega tutvumiseks lugemisõigus (read-only).
- Arhiivisüsteemi laiendamisvõimalused – arhiivisüsteemi peaks saama laiendada selliselt, et nõudmiste muutudes oleks seda võimalik kohandada uutele tingimustele. Laiendamisvõimalus puudutab eelkõige rakendatavaid salvestikomponente ja andmekandjaid, kuid ka igasuguseid muid riistavaramuudatusi, samuti arhiivisüsteemi tarkvara ja kasutuslitsentse.
- Andmepöörduste lühike reaktsiooniaeg – arhiivsüsteemidelt nõutakse üldjuhul lühikesi reaktsiooniaegu ning suurt ribalaiust soovitud dokumentide

edastamisel ja kättesaadavaks tegemisel. Vajalikud nõuded tuleb välja töötada organisatsiooni eripärade alusel. Siinkohal tuleb lisaks ühendamisele olemasoleva süsteemikeskkonnaga arvestada veel ka eeldatava kasutusaktiivsusega. Kindlaksmääratud nõuded mõjutavad otseselt arhiveerimisandmekandjate ja salvestiajamite valikut. Samuti võivad kehtestatud nõuded mõjutada ka vahesalvestuskomponentide valikut ja nende dimensioonimist.

- Arhiveerimisandmekandjate piisav salvestiruum – arhiveerimiseks kasutatavad andmekandjad peavad olema küllaldase salvestiruumiga. Mälumahtude planeerimisel tuleks arvestada vajadusega dokumentidest erinevate versioonide salvestamiseks ning ka prognoositava andmemahuga.
- Süsteemi juhitud arhiveerimisandmekandjate pealepanek ja väljavõtmine – enamikel juhtudel peaks arhiivisüsteemid toetama süsteemi juhitavat andmekandjate pealepanekut ja väljavõtmist nende lugemisseadmetest. Selle nõudega tagatakse, et arhiivi andmekandjaid saab kasutada ainult pärast kontrollitult vallasrežiimi lülitamist (unmount) kooskõlas vastavate pääsuõigustega, ning et andmekandjate kasutamine kajastuks ka logimissüsteemis. Sama kehtib ka arhiveerimisandmekandjate lülitamise kohta sidusrežiimi. See on vajalik, et tagada arhiveerimisandmekandjate ühesugune kasutamine. Avariiolukordadeks on harilikult kõikides arhiivisüsteemides ja ajamites loodud ka võimalused arhiveerimisandmekandjate käsitsi väljavõtmiseks.
- Arhiveerimisandmekandjate salvestiruumi täituvuse seire – kasutatavate arhiveerimisandmekandjate järelejääv mälumaht peab olema kogu aeg seire all. Salvestiruumi kahanemisest allapoole piirväärtust peab süsteem kas teavitama või alarmeerima.
- Alarmeerimine ja teavitamine – arhiivisüsteem peab võimaldama edastada süsteemiteateid hierarhias kõrgemal asetsevatele süsteemihalduskeskkondadele. Juhul kui ühendusi süsteemihalduskeskkonnaga ei planeerita, peaks teavitamine olema võimalik kas SMSi, e-posti või SNMP vahendusel.
- Standardite järgimine – kooskõla erinevate standarditega kergendab erinevate üksikkomponentide koostalitlusvõimet. See on vajalik, kuna tuleb arvestada ka võimalusega, et seadmete kasutusea jooksul võib tekkida vajadus erinevaid üksikkomponente välja vahetada või süsteemi laiendada.

Standardid on olulised järgmistes valdkondades:

- arhiveerimiseks kasutatavad andmekandjad ja salvestusprotseduurid (vt M 4.169 Sobiva arhiveerimis-andmekandja valimine),
- failide formaadid ja tihendusprotseduurid (vt M 4.170 Dokumentide arhiveerimiseks sobivate andmevormingute valimine),
- dokumendihaldussüsteemid (vt M 2.259z Üldise dokumendihaldussüsteemi kasutuselevõtt).

Andmete kaitsmiseks tuleks kaaluda krüpteerimise digitaalsete allkirjade kasutuselevõttu. Vastavad lahendused ei toimi aga mitte läbi arhiveerimissüsteemi, vaid rakenduste tasandil, nt dokumendihaldussüsteemi kaudu. Erandiks on siinkohal vaid arhiveerimisandmekandjate baas-krüpteerimine arhiivisüsteemi poolt. Sellega püütakse tõkestada arhiveerimisandmekandjate kasutamist väljaspool arhiivisüsteemi. Etalonturbe rakendamise seisukohast vastavat baas-krüpteeringut ei nõuta.

Kontrollküsimused:

- Kas kõik arhiivisüsteemile esitatavad nõuded on dokumenteeritud?
- Kas väljavalitud arhiivisüsteem suudab täita kõiki talle seatud nõudeid?

M 4.169 Sobiva arhiveerimis-andmekandja valimine

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: IT-juht, administraator

Elektrooniliste dokumentide pikaajaline arhiveerimine eeldab selleks sobilike arhiveerimisandmekandjate kasutamist.

Arhiveerimiseks kasutatavate andekandjate valikul tuleks pöörata tähelepanu järgnevale:

- Kui suurt andemahtu on tarvis arhiveerida?
- Millised keskmised reaktsiooniajad tuleb tagada?
- Kui suur on keskmine korraga toimuvate andmepäringute hulk?
- Milliseid säilitamiskohustusi on tarvis vastava andmekandjaga täita?
- Kas andmeid tuleb salvestada „revisjonikindlalt"?

Järgnevates lõikudes kirjeldatakse enamlevinud arhiveerimisandmekandjaid ja nende kasutusvaldkondi. Andmekandjates rakendatakse üldjuhul kas magnetilisi, magnetoptilisi või optilisi salvestustehnoloogiaid. Järgnevates lõikudes tuuakse välja vastavate tehnoloogiate head ja vead. Kõik kirjeldatud arhiveerimisandmekandjad, kuhu peale saab infot kirjutada, on väga vastuvõtlikud kõikvõimalikele füüsilistele kahjustustele, mida võivad põhjustada

- vesi,
- tuli ehk kuumus,
- andmekandja kriimustamine lugemisseadmes kas võimaliku määrdumise või eelneva mahakukkumise tõttu,
- andmekandja kortsumine või katkemine lindiajamis,
- sabotaaž ja vargused.

Arhiveerimiseks kasutatavaid andmekandjaid tuleb hoida hoolikalt ning kaitsta äsja loetletud ohtude eest. Lisaks tuleb tagada, et andmekandjatele ei oleks võimalik ilma volituseta juurde pääseda. Andmekandjate kaitsmiseks on olenevalt elektroonilise arhiivi konkreetsest kasutusvaldkonnast soovitatav rakendada moodulites B 2.5 Andmekandjate arhiiv ja B 2.7 Kaitsekapid .

Digitaalsed magnetilised süsteemid

Magnetiliste salvestussüsteemide puhul saavutatakse salvestusefekt magnetilise baasmeediumi sihipärase lokaalse mõjutamisega. Asetleidnud magnetiseerimist suudab lugemisseade edasi anda ning seeläbi muudetakse salvestatud andmed uuesti loetavaks. Magnetvälja korduva rakendamise abil on võimalik salvestatud andmeid ka muuta. See võib toimuda ettekavatsetult, kasutades vastavat lugemis-/kirjutamisseadet või siis kogemata tugevate väliste magnetväljadega (nt elektromagnetiliste väljadega, mis tekivad trafode või suurte lindikerade läheduses).

Magnetilised andmekandjad on tundlikud rünnete suhtes, mis pannakse toime tugevate magnetväljade abil. Magnetiseeritud andmekandjaga, mis on üldjuhul toodetud plastist ja kaetud (magneetumisvõimelise) metallilise pinnakattega, kaasnevad isegi ka hoolikal ümberkäimisel pikemas perspektiivis alati teatud muudatused. See võib olla tingitud nt materjalide lagunemisest (plastmaterjali pehmendajate vananemisest), üleskobrutamisest (seotise katkemisest plastmaterjali ja metalli vahel), või (metallikihi) oksüdeerimisest. Selleks rakendatava tehnoloogia tõttu on magnetlinte võimalik alati uuesti üle kirjutada ehk siis ka kustutada, mistõttu sobivad need ilma täiendavate kaitsemeetmete rakendamiseta vaid lühiajaliseks arhiveerimiseks, kus pole vaja tagada dokumentide kaitsmist võimalike muudatuste ehk taaskirjutamise vastu. Harilikult sellest tingimusest piisab, et välistada selliste andmekandjate kasutamist revisjonikindla arhiveerimise tagamisel. Sellele vaatamata võib magnetilisi andmekandjaid rakendada andmevarunduse otstarbel ja vahesalvestuse vahenditena. Revisjonikindlust on võimalik tagada suure vaevaga, kui rakendada täiendavalt krüptograafilisi protseduure, mis suudavad tuvastada andmete võimalikku muutumist (nt allkirjastamisega).

Tüüpilised magnetilised salvestid on kõvakettad, disketid ja (magnet-) lintandmekandjad:

- Disketid – hetkel mõõdus 3,5 tolli, varem mõõdus 5,25 tolli ja suuremad, suudavad andmeid mahutada vaid 1,44 MB. Diskettide kasutamist arhiveerimisandmekandjatena soovitatakse ainult väga väikeste arhiivide puhul, kus pole tarvis tagada revisjonikindlat (kirjutuskaitsega) arhiveerimist.
- Kõvakettad – neis on tavaliselt salvesti ja selle kirjutamis- ning lugemisseade pandud kokku ühte kompaktsesse seadmesse. Seetõttu võib kõvaketastel ette tulla mehaanilisi avariisid, nt lugemisseadme ajami rikkiminekuid. Füüsikalise kapseldamisega saavutatakse magnetsalvestite ruumiline kokkusurumine väiksemale pinnale, luues ka tõhusama kaitse tolmuosakeste vastu, mistõttu on kõvakettad võrreldes diskettidega varustatud mitme lugemiskirjutus-komponendiga. Kõvaketastel on üldjuhul suur salvestiruum, väike reaktsiooniaeg ja suur andmeedastuskiirus. Kõvaketastes kasutatava salvestustehnoloogia tõttu ei sobi need dokumentide pikaajaliseks revisjonikindlaks arhiveerimiseks. Seevastu kasutatakse kõvakettaid laialdaselt arhiivisüsteemi enda andmekandjatena ja vahesalvestussüsteemides.
- Magnetlindid – koosnevad tavaliselt pooli peale keritud magnetlindist, mida juhitakse sekventsiliselt üle lugemis-kirjutuspea. Magnetlint ja selle kirjutus-lugemis-komponent ei ole üksteisega ühendatud. Magnetlinte iseloomustab nende tehnoloogilise eripära tõttu väga pikk käitlemisaeg ning väga madal andmeedastuskiirus. Nende salvestustihedus ja ruumivajadus on siiski võrreldavad kõvaketastega. Magnetlindid sobivad suurte andmehulkade salvestamiseks, mida on tarvis kasutada kas ainult harva või teatud korduvate ajavahemike möödudes. Seetõttu sobivad need varukoopiate tegemiseks, mille puhul ei oodata mitte pikaajalist, vaid pigem lühiajalist stabiilsust. Kuna ka magnetlintide sisu on võimalik nii üle kirjutada, kustutada kui ka magnetväljade juhusliku mõju tõttu muuta, ei sobi need andmete revisjonikindlaks salvestamiseks.

Järgnevas tabelis on toodud lühike ülevaade magnetiliste salvestite sobi-

vusest elektrooniliseks arhiveerimiseks:

Salvesti	Formaat ja mahtuvus	Standard	Kasutusotstarve
Diskett	3,5 - 5,25 tolli, kuni 1,44 MB	de facto	lühiajaline kasutus väga väikestes arhiivides, ei ole revisjonikindel
Kõvaketas	2,5 - 5,25 tolli, rohkem kui 100 GB	tootjate normid	lühiajaline kasutus väikestes arhiivides ja *Cache* -süsteemides, ei ole revisjonikindel
Magnetlint	rohkem kui 80 GB	tootjate normid	keskmise pikkusega kasutus keskmise suurusega arhiivides, ei ole revisjonikindel

Tabel: Magnetiliste salvestite kasutusotstarbed

Digitaalsed optilised süsteemid

Magnetilistes salvestisüsteemides saavutatakse salvestamisefekt seeläbi, et alusmeediumi optilist käitumist on võimalik sihipäraselt muuta. Salvestusprotsess leiab reeglina aset alusmeediumi muutmise teel, milleks töödeldakse või simuleeritakse alusmeediumi kihti („maasse“) sihipäraselt vastavaid süvendeid (ingl *Pits*), mis tekitavad lugemisprotsessi käigus reeglina erineva optilise käitumise, kui neid loeb selleks konkreetselt teele suunatud laserkiir. Antud protsessi tulemusena on võimalik interpreteerida bitimustreid. Kui lugemisprotsess leiab kõikide optiliste salvestusvahendite puhul aset reeglina ühtmoodi (kasutatava laseri lainepikkus võib siiski erineda), siis salvestusprotsessi puhul eksisteerivad tehnoloogiate vahel suured erinevused:

- CD-ROM - CD-ROM'ide (*Compact Disk Read Only Memory*) loomine toimub mehaaniliselt, st vastava *Master* -andmekandjaga töödeldakse sellele vastav tempel. CD-ROMile salvestatud andmeid ei ole reeglina hiljem enam võimalik muuta (WORM). Selliste andmekandjate tootmine on majanduslikult tasuv vaid suure tükiarvu korral. Arhiveerimise otstarbeks antud andmekandjad ei sobi, kuna elektroonilistes arhiivides luuakse neid ainult väga vähesel arvul ning see ei tasu end majanduslikult ära. Siiski on ka erandeid, nt „aastakäiguarhiivid“, mis lisatakse suure tiraažiga ajakirjadele. CD-ROMide jaoks on välja töötatud mitmeid standardeid, mida täidavad paljud tootjad. Enamlevinud salvestimahuks on 650 MB.

- *CD-Recordables* (CD-Rid) - CD-Rid on varustatud vastupidiselt CD-ROMidele veel ühe täiendava kihiga (reeglina kas tsüaniinist või ftaloksüaniinist kihiga), millesse töödeldakse (kõrvetatakse) laseri abil punktid, mille hilisema lugemise käigus tekib teatud valguspeegeldus, mis on sarnane CD-ROMiga. Enamlevinud salvestimahuks on 700 MB. Kord juba sisse „kõrvetatud“ punkte ei ole enam võimalik kustutada. Eeliseks võrreldes andmekandja mehaanilise tembeldamisega on individuaalne kohandamisvõime. CD-Ridel on järgnevalt ära toodud puudused. CD-Re on võimalik piiratud arv kordi ka hiljem muuta, kuna põhimõtteliselt on võimalik CD-Ri pinnale ülekõrvetamisega tekitada täiendavaid põletuspunkte ning saavutada seeläbi kas soovitud muutus andmete koostises või CD-Ril olevate andmete kustutamine. Sellele vaatamata ei ole võimalik juba vastava punkttöötluse läbinud pindasid enam tagasi muuta. CD-Rid ei ole seetõttu vastupidiselt laialt levinud arusaamale sugugi „tõelised“ *Write-Once* ehk WORM andmekandjad, vaid ainult andmekandjad, mida ei saa kustutada. Vigase kõrvetusprotsessi tulemusena võib tekkida valguspeegelduse petlik esilekutsumine, mis võib olla väga harvadel juhtudel tingitud ka vahekihi ajutusest reageerimisest. Seetõttu tuleb CD-Re mõne päeva möödudes kontrollida, et selliseid efekte välistada. CD-Ride puhul eksisteerib väga väike jääkoht, et pealispinna spontaanse kristalliseerumise tagajärjel võivad salvestatud andmed juhuslikult muutuda. CD-ROMid on küll ühekordselt kirjutatavad, kui nende puhul on ka võimalus kirjutada sinna andmeid erinevate seansside (ingl *sessions*) käigus. Ahiveerimise otstarbel tuleks sellest võimalusest kindlasti loobuda, kuna see võib mõjuda negatiivselt kõige esimesena plaadile salvestatud andmete loetavust ja korrektsust.
- *CD-Rewritables* (CD-RWd) - CD-RWd kasutavad sarnaselt CD-Ridele vahekihti, kuid siin on see toodetud mõnest keerulisemast materjalist nagu hõbe, indium, antimon või telluur, mida on võimalik sihipäraselt viia kahte erinevat moodi valgust peegeldavasse seisundisse. See sõltub kasutatava laseri intensiivsusest. CD-RWd on seetõttu mitmeid kordi ülekirjutatavad ehk kustutatavad ning vigaste ajamisüsteemide puhul võib see toimuda ka kogemata. Seetõttu ei sobi neid kasutada arhiivides, kus on tarvis tagada andmete revisjonikindel salvestamine. Enamlevinud salvestimahuks on 700 MB. Arhiveerimis-andmekandjana iseloomustavad CD-RW-tehnoloogiat samasugused puudused nagu CD-Ri. Vigase kõrvetusprotsessi tulemusena võib tekkida valguspeegelduse petlik esilekutsumine, mis võib olla väga harvadel juhtudel tingitud ka vahekihi ajutusest reageerimisest. Seetõttu tuleb CD-RWsid mõne päeva möödudes kontrollida, et selliseid efekte välistada. CD-RWde puhul eksisteerib väga väike jääkoht, et pealispinna spontaanse kristalliseerumise tagajärjel võivad salvestatud andmed juhuslikult muutuda.
- DVD - DVD-andmekandjaid (*Digital Versatile Disk*) võib pidada CDde (*Compact Disk* 'ide) tehnoloogiliseks edasiarenduseks. DVDd võimaldavad kasutada palju suuremat salvestustihedust, sõltuvalt tootjast 4,7 kuni 17 GB. DVD formaat ei ole vastupidiselt CDle standardiseeritud, mistõttu levivad hetkel erinevad DVD variandid. Mõningate DVD variante puhul on võimalik andmeid salvestada kahte erinevasse kihti, mida loetakse eraldi, kasutades selleks erinevalt fokuseeritud lasereid (*Dual Layer DVD*). DVDsid on saadaval ka DVD-R (*VD-Recordable*) formaadis. Ootused püsivad, et tulevikus ilmub ka DVD-RW formaat. Elektroonilise arhiveerimise jaoks on siinkohal huvitav, sarnaselt CDga variant *DVD-Recordable*, kuna see loob võimalu-

se revisjonikindlaks salvestamiseks, pakkudes samal ajal ka suurt salvestiruumi. Samas tuleb aga ka siin arvestada samasuguste ülekirjutuskaitset puudutavate piirangutega nagu ka CD-R'i puhul.

Lisaks laialt levinud CD- ja DVD-andmekandjatele leidub elektroonilise arhiveerimise jaoks ka veel teisi standardiseeritud optilisi andmekandjaid, mida kasutavad suurte salvestisüsteemide tootjad.

Järgnev tabel annab ülevaate võimalike saadaolevate andmekandjaformaatide kohta ja loetleb ka neid käsitlevad standardid:

Formaat	Salvestiruum	Norm
3,5 tolli		ANSI X3.213
CD (5,25 tolli)	650 - 700 MB	ISO 9660
DVD (5,25 tolli)	4.7 - 17 GB	ISO 13346
5,25 tolli, RW	1 - 2.6 GB	ISO 10089
5,25 tolli, WORM	1 - 2.6 GB	ISO 9171, ANSI X3.191, ANSI X3.211, ANSI X3.214
12 tolli	2.6 - 16 GB	sõltub tootjast, pole normeeritud
14 tolli, WORM	6.8 - 25 GB	ANSI X3.200 ja ISO/IEC 10885

Tabel: Saadaolevad andmekandjaformaadid

Loetletud andmekandjate puhul kasutatav tehnoloogia sarnaneb peamiselt CD-Ri (DVD-Ri) ja CD-RW (DVD-RW) puhul kasutatava optilise lahendusega. Peamised erinevused seisnevad selles, kuidas töödeldakse vajalikke usaldusväärseid materjale ning selles, milliseid lisagarantiisid annavad oma toodetele erinevad tootjad. Erinevad tootjad lubavad, et ülekirjutatavate andekandjate puhul säilivad andmed stabiilsetena 10 kuni 100 aastat ning WORM-andmekandjate puhul vastavalt 30 kuni 100 aastat, andes ka erinevaid soovitsu optimaalsete kasutustingimuste kohta. Ka eelpoolkirjeldatud WORM-andmekandjate puhul ei saa nende puhul kasutatava tehnoloogia tõttu välistada, et seni kasutamata jäänud alasid võib olla võimalik hiljem siiski üle kirjutada. Seetõttu ei ole ka siin tegemist „tõeliste“ *Write-Once* andmekandjatega, vaid ainult andekandjatega, mida ei ole võimalik kustutada. Vastavad tootjad pakuvad reeglina müüa mitte üksikuid andmekandjaid vaid terveid salvestisüsteeme, millesse on reeglina integreeritud ka automaatne andmekandjate haldussüsteem. Sellistes lahendustes on andmekandjad tavaliselt mehaaniliselt vastava tootjalahendusega sobivaks kohandatud ning ümbritsetud spetsiaalse korpusega, mis võimaldab neid kasutada ka robotsüsteemides (*Jukebox* 'ides)

Salvesti	Formaat ja mahtuvus	Kasutatavus arhiivides	Revisjoni-kindlus

CD-ROM	5,25 tolli, 650 MB	ei soovitata	jah
CD-R	5,25 tolli, 700 MB	väiksed arhiivid	jah*
CD-RW	5,25 tolli, 700 MB	väiksed arhiivid	ei
DVD	5,25 tolli, 4 - 17 GB	ei soovitata	jah
DVD-R	5,25 tolli, 4 - 17 GB	keskmised arhiivid	jah*
DVD-RW	5,25 tolli, 4 - 17 GB	keskmised arhiivid	ei
ISO 9171-WORM andmekandjad	5,25 tolli, 1,3 - 2.6 GB	keskmised kuni suured arhiivid	jah*
ISO 10089-RW andmekandjad	5,25 tolli, 1,3 - 2.6 GB	keskmised kuni suured arhiivid	ei
12 tolli RW, tootja eripäradega	12 tolli, 2.6 - 16 GB	suured arhiivid	ei
12 tolli WORM, tootja eripäradega	12 tolli, 2.6 - 16 GB	suured arhiivid	jah*
14 tolli, tootja eripäradega	14 tolli, 6.8 - 25 GB	suured arhiivid	pole teada

(* arvestades kasutatavat tehnoloogiat, ei saa vastavate andmekandjate ülekirjutamist täielikult välistada. Sellele vaatamata liigitatakse WORM andmekandjad enamasti revisjonikindlate andekandjate hulka kuuluvaks).

Tabel: Ülevaade optiliste andmekandjate sobivusest elektrooniliseks arhiveerimiseks

Magnetoptilised süsteemid

Magnetoptiliste (MO) salvestustehnoloogiate puhul toimub salvestatud andmete lugemine sarnaselt optilist laadi andmekandjate lugemisega seeläbi, et andmekandjat kombitakse laserkiirega. Vastupidiselt CD-laadsetele andmekandjatele ei saavutata optilist efekti siiski mitte pealispinna sisse töödeldud süvendite abil, vaid magnetkihi abil, mille osakesed hakkavad magnetkiire kokkupuute ja peegeldumise tagajärjel toimina polarisatsioonifiltritena. Pealispinna polarisatsiooni on võimalik ülitäpselt mõjutada seeläbi, et tekitatakse magnetväli, mis mõjub ainult ühele kindlale (taas kord laseri poolt) spetsiaalselt ülessoojendatud salvestialale. Salvestusprotsessi käigus varustatakse vastavad alad andmekandja pealispinnal sihipäraselt erinevate polarisatsioonidega.

Järgnev tabel annab ülevaate võimalike saadaolevate andmekandjaformaatide kohta ja loetleb ka neid käsitlevad standardid:

Formaat	Salvestiruum	Norm
3,5 tolline formaat	128 - 256 MB	ISO norm 10090
5,25 tolli, RW	1,3 - 9,1 GB	ANSI norm X3.212
5,25 tolli, WORM	1,3 - 9,1 GB	ISO/IEC 11560, ANSI norm X3.220

Tabel: Andmekandjate formaadid

Ka äsjakirjeldatud WORM-andmekandjate puhul ei saa kasutatava tehnoloogia tõttu välistada, et seni kasutamata jäänud alasid võib olla võimalik hiljem siiski volitamatult üle kirjutada (kõrvetada). Seetõttu ei ole ka siin tegemist „tõeliste“ *Write-Once* andmekandjatega, vaid ainult andekandjatega, mida ei ole võimalik kustutada. Magnetoptilisis süsteeme iseloomustab kõrge pikaajaline stabiilsus (tootjate andmetel rohkem kui 30 aastat) ning suur salvestiruum (kuni 9,1 GB ühe andmekandja kohta).

Järgnevas tabelis on tood lühike ülevaade magnetoptiliste salvestite sobivusest elektrooniliseks arhiveerimiseks.

Salvesti	Salvestiruum	Kasutatavus arhiivides	Revisjonikindlus
3,5 tolline formaat	128 - 256 MB	ei soovitata	ei
5,25 tolli, RW	1,3 - 9,1 GB	keskmised arhiivid	ei
5,25 tolli, WORM	1,3 - 9,1 GB	keskmised arhiivid	jah*

(* arvestades kasutatavat tehnoloogiat, ei saa selliste andmekandjate ülekirjutamist täielikult välistada. Sellele vaatamata liigitatakse WORM andmekandjad enamasti revisjonikindlate andekandjate hulka kuuluvaks).

Tabel: Elektroonilise arhiveerimise võimalikud andmekandjad

Sõltumata sellest, mis liiki andmekandja kasuks on otsustatud, tuleks alatai järgida põhimõtet, et pärast igat salvestust tuleks läbi viia ka verifitseerimine. Ühelt poolt peaks see toimuma süsteemi initsiatiivil, et kontrollida, kas salvestamisprotsessi käigus loodud andmete puhul on tegemist algmaterjali täpse koopiaga. Teiselt poolt peaks aga ka arhiivi haldaja ise pisteliste kontrollide käigus välja selgitama, kas kõik arhiveerimiseks ettenähtud andmed on ka tõepoolest arhiveeritud, või on mõnd andmed väära konfiguratsiooni tõttu kahe silma vahele jäänud.

Kontrollküsimused:

- Kas arhiveerimise otstarbeks välja valitud andmekandjad on sobivad eeldatavate arhiveeritavate andmehulkade katmiseks?
- Kas väljavalitud arhiveerimis-andmekandjad sobivad pikaajaliseks arhiveerimiseks?
- Kas väljavalitud arhiveerimis-andmekandjad ühilduvad piisavalt teiste IT-süsteemidega ja on nendega piisavalt koostalitusvõimelised?

M 4.170 Dokumentide arhiveerimiseks sobivate andmevormingute valimine

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: IT-juht, administraator

Elektrooniliste dokumentide arhiveerimiseks tuleb välja valida sobivad andmevormingud. Andmete formaat peab suutma tagada arhiveeritud andmete võimalikult originaalilähedase reprodutseerimise ning tagama algse dokumendi jaoks valitud seisunditunnuste (nt paberformaadi, värvide, logode leheküljenumbrite, vesimärkide, allkirjade) säilimise. Mitte kõik hetkel kasutatavad andmevormingud ei ole selleks ühtemoodi sobivad, kuna nende sobivus sõltub suuresti arhiveeritavate andmete kasutusotstarbest ja sellest, millisel andmekandjal neid hoitakse. Andmekandja liigi ja andmeformaadi vahetumisel pole alati võimalik tagada, et kõik eelneva andmekandja struktuuritunnused taastataks nende algsel kujul. Kuna enamikul juhtudel pole võimalik ette näha, millist algdokumendi omadust on hilisemate reproduktsioonide puhul tarvis tõestada ning kui suurt tõendamisvõimet on tarvis kindlustada, arhiveeritakse dokumente tavaliselt korraga erinevates elektroonilistes andmevormingutes. Sellega seatakse eesmärgiks võimalikult paljude originaaldokumendi omaduste kajastamine.

Konvertimisprotsessi nimetatakse tihti tõlgendamiseks.

Sobivate andmevormingute valimisel on määrava tähtsusega järgmised kriteeriumid:

- Andmeformaat peaks jääma pikaks ajaks kasutusse.
- Dokumendi struktuuri peab olema võimalik üheselt interpreteerida.
- Dokumendi sisu peab olema võimalik elektrooniliselt töödelda.
- Seadustest tulenevad ettekirjutused peavad olema täidetud.
- Andmeformaadi grammatika ja semantika peab olema põhjalikult dokumenteeritud, et hilisem üleviimine saaks toimuda tõrgeteta.
- Originaaldokumendi tunnused (elektroonilised või paberil) peavad olema hiljem üheselt tõestatavad ka siis, kui originaaldokumenti pole enam olemas.

Graafilise kuvamise struktuur

Üldjuhul on lisaks strukturaalselt kuvatavale (struktuuri kirjelduskeeles) versioonile paberdokumentide puhul arhiveeritud veel ka dokumendi graafiliselt kuvatav versioon. Olenevalt olukorrast võivad lisanduda veel ka elektroonilised allkirjad dokumendi autentsuse tõestamiseks. Järgnevates lõikudes kirjeldatakse tüüpilisi andmeformaate ning arutletakse nende sobivuse üle elektrooniliseks arhiveerimiseks.

Struktuuriformaadid

SGML

SGML (standard generalized markup language) on dokumentide kirjeldamise keel, mis kirjeldab elektrooniliste dokumentide loogilist struktuuri ja nende sisu. SGML on muudetud standardiks ISO-normiga 8879. Lisaks struktuurile (süntaksile) kirjeldab SGML eriti veel ka elektroonilise dokumendi struktuurielementide

semantikat. SGML ei jäljenda aga dokumente nende konkreetse esitluse ja formaadi kuvamise teel.

SGMLi tähtsamad omadused on järgmised:

- SGML-elementide semantika defineeritakse eraldi nn DTDga (document type definition). DTD on dokumendivahetuse aluseks institutsioonide ehk rakenduste vahel.
- SGML sobib struktureeritud tekstidokumentide sõltumatuks kuvamiseks ja salvestamiseks, kuna layout-infot käsitletakse dokumendi sisust eraldi.
- SGMLi võib kasutada dokumendihaldussüsteemides vahetult struktuuride kuvamiseks.

SGML formaati võib kasutada elektrooniliste dokumentide pikaajaliseks arhiveerimiseks. Arhiveerimisel tuleks muu hulgas siiski ilmtingimata arhiveerida ka semantika spetsifikatsioon (DTD). Kuna SGML ei sisalda ühtki infot layout'i kohta, on soovitatav lisaks SGML-dokumentidele arhiveerida ka originaaldokumendi graafiline kujutis, nt TIFF-formaadis.

HTML

HTML (hyper text markup language) on elektrooniliste dokumentide struktuuri kirjeldav keel. HTML koosneb SGML-kirjelduselementidest ning see on muutunud dokumentide kuvamise ja vahetamise standardiks World Wide Webis. HTML võimaldab dokumentide jaoks kasutada vaid väga piiratud struktuuritunnuste valikut, mistõttu tuleb seda mõista kui spetsiaalset SGMLi, mis sisaldab ka DTDd.

HTMLi tähtsamad omadused on järgmised:

- HTMLis saab dokumendi osasid liita hüperlinkide abil kokku üheks tervikliikuks dokumendistruktuuriks. Selle abil on võimalik jooksvasse teksti kaasata pilte ja tekstiosi, mis asuvad füüsiliselt laialijagatuna kusagil teistel serveritel. Tänu dünaamilisele ühendusviisile on võimalik, et tervikdokumendi osad võivad muutuda ka ilma dokumendiomaniku teadmata, kuna juurde lisatud alapeatükkide või piltide lingid võivad olla kas muudetud või kättesaamatuks tehtud.
- HTML on fikseeritud olemasolevate struktuuritunnuste peale. Niinimetatud HTML-sildi puhul ei saa individuaalselt täiendada ega ka laiendada ei selle süntaksit ega ka semantikat.
- Põhjusel, et HTML ei ole just väga paindlik, tuleb nõuete muutumise korral ilmtingimata uuesti läbi töötada HTML-standard. Viimastel aastatel on seda regulaarselt teinud vastutav standardiseerimiskomitee (W3C-konsortsiumi). Lisaks võtavad veel omal soovil täiendusi ette ka HTML-brauserite tootjad. Ka tulevikus peab arvestama, et seda keelt täiendatakse kindlasti veel edasi.

HTML-formaati ei soovitata kasutada pikaajalise arhiveerimise otstarbel. See ei sobi arhiveerimiseks, kuna selle vähene paindlikkus nii süntaksi kui ka semantika puhul annab alust oletada, et HTML-standardile hakatakse looma üha uusi täiendusi ja seda suhteliselt lühikeste vaheaegade tagant. Lisaks ei sobi see formaat arhiveerimiseks veel ka seetõttu, et HTML-dokumentide dünaamiline struktuur on

selline, mis nõuab kogu tervikdokumendi arhiveerimist, st arhiveerida tuleb lisaks ka kõik lingitud pildid, alamdokumendid ja ristviited. HTML-dokumentide arhiveerimisel ei tohi eksisteerida aktiivseid linke mittearhiveeritud dokumentidele, kuna ei ole võimalik tagada, et sellised väljaspool asuvad dokumendiosad ka veel tulevikus alles on, kui dokumenti kunagi reprodutseerima hakatakse.

XML

HTMLi funktsiooniliste piirangute tõttu lõi W3C võimaluse, kuidas kasutada ära SGML-keele eeliseid, ilma et tuleks kaasata kogu süsteemi täit keerukust. XML töötati välja SGMLi baasil.

XMLi tähtsamad omadused on järgmised:

- XMLis on võimalik vastupidiselt HTMLile defineerida uusi silte ja atribuute. Seeläbi on võimalik kohandada kirjeldavate elementide süntaksit ja semantikat.
- Analoogselt HTMLiga on ka siin võimalik integreerida dokumendi struktuuri alla linke. Niimoodi on võimalik lihtsaid dokumente viidata ja kaasata dokumentidesse nt pilte.
- Uuemad veebibrauserid suudavad XMLi kuvada juba otse. Kuvamiseks läheb tarvis eraldi layout'i definitsiooni kirjelduskeeles XSL (extensible stylesheet language).

XML-formaati võib kasutada elektrooniliste dokumentide pikaajaliseks arhiveerimiseks. Siiski tuleks arhiveerimisel ilmtingimata arhiveerida ka semantika spetsifikatsioon (document type definition, DTD) ja vajaduse korral ka XSL-keeles kirjeldatud layout-info.

PDF

PDF (portable document format) on dokumendi vorming, mille puhul on lisaks elektrooniliste dokumentide struktuuriinfole kaasa salvestatud ka olulisem layout-informatsioon. PDFi arendas välja firma Adobe, võttes aluseks andmeformaadi nimega PostScript. Dokumendi esitlusviisi kirjeldab andmejada, mis sisaldab tervet hulka graafilisi objekte. Läbi selle kirjelduse on dokument täielikult fikseeritud. Dokumendi esitlusviis määratakse kindlaks dokumendi loomis hetkel ja pärast seda jääb see fikseerituks. Võrreldes pildi kuvamisega (pikslites kuvamisega) vajavad PDF-formaadis dokumendid enamasti oluliselt vähem salvestiruumi. PDFi rakendamise eesmärk on tagada elektroonilise dokumendi esitlusviisi sõltumatus selle loomiseks kasutatud rakendustarkvarast, riistvaraplatvormist ja operatsioonisüsteemist. Seetõttu sobib PDF-formaat eelkõige selliste dokumentide arhiveerimiseks, mille puhul nähakse ette nende paberkuju edasiandmist, ehk siis kirjade ja äridokumentide arhiveerimiseks. Spetsiaalselt pikaajalise arhiveerimisega kaasnevate nõuete täitmiseks loodi PDF/A standard ISO 19005-1:2005. PDF/A (A tähistab arhiveerimist) defineerib stabiilse PDFi alamversiooni, mis võimaldab arhiveeritavaid dokumente kirjeldada selliselt, et kõik vajaminev info sisaldub juba dokumendis endas ning et see info oleks tervikuna olemas, üheselt mõistetav, käideldav ja äratuntav. PDF/A formaati võib kasutada elektrooniliste dokumentide pikaajaliseks arhiveerimiseks. Siin tuleks kontrollida, kas dokumendid täidavad PDF/A spetsifikatsioone.

Pildiformaadid

TIFF

TIFF (tagged image file format) vormindust kasutatakse rasterdatud piltide arhiveerimiseks. TIFF-fail koosneb faili päisest ja pildiinfost. Faili päis sisaldab silte, kuhu on salvestatud foto omadused, nt selle eraldusvõime või kasutatud tihendamismeetod.

TIFFi tähtsaimad omadused on järgmised:

- Pildiinfot on võimalik ilma kadudeta salvestada nii mustvalgena kui ka hallides variatsioonides, kuid seda vaid juhul, kui valitakse 24-bitiline värvisügavus (truecolor). Ainult selles valikus on võimalik edasi anda kõiki halle toone. Värviinfo võimalikult originaalilähedaseks jäädvustamiseks ja salvestamiseks tuleb aga siiski regulaarselt häälestada vastavaid optilisi andureid, et värviinfo ei muutuks valeks, nt värvinihke tõttu. Selleks võib teha nt värvivõrdlusi, võttes võrdlusvärviks valge.
- Kõik levinud graafika- ja esitlusprogrammid toetavad TIFF-formaadi kasutamist. Lisaks selle toetavad seda vormingut ka arhiivi- ja töövoosüsteemid.
- TIFF on levinud andmeformaat faksiseadmetes.
- Pildiandmeid on võimalik salvestada tihendatud kujul. TIFF ühildub suure osa tihendamisprotseduuridega (compression).

Alljärgnevalt veidi kahest levinumast tihendamisprotseduurist:

1. ITU/CCITT – grupp nr 4: ITU-tihendus kasutab TIFFi sisendformaadina. Tavaliste tekstidokumentide puhul saavutatav tihendustegur on 1 : 40. Seetõttu sobib see ideaalselt mustavalgetele dokumentidele. Tihendamisel ei teki kadusid. ITU-tihendus on ülemaailmselt arhiveerimise otstarbel standardiseeritud.
2. JBIG – kaovaba tihendusprotseduur TIFF-formaadis mustvalgete piltide tihendamiseks. See on standardiseeritud ISO/IEC standardiga nr 11544. Võrreldes ITU 4. grupi tihendusega töötab see kuni 70% efektiivsemalt. JBIG ei ole hetkel nii laialt levinud kui ITU-protseduur ja kõik tootjad selle kasutamist ei toeta. TIFF-formaat sobib tihendatud kujul piltide ja dokumentidest loodud piltkujutiste pikaajaliseks arhiveerimiseks. Soovitatav on kasutada tihendamisprotseduure, mis ei tekita kadusid, nt ITU/CCITT gruppi nr 4, et vajaminevat salvestiruumi võimalikult minimeerida.

GIF

Vormindust GIF (graphics interchange format) kasutatakse rasterdatud piltide arhiveerimiseks.

GIFi tähtsamad omadused on järgmised:

- Kõik levinud graafika- ja esitlusprogrammid toetavad GIF-formaadi kasutamist. Lisaks toetavad seda vormingut ka veel arhiivi- ja töövoosüsteemid.

- Konvertimine GIF-formaati on seotud kadudega, sest väikse failisuuruse saavutamiseks läheb teatud pildiinfo kaduma.
- GIF-formaadi kasutamine rakendustes eeldab kohustusliku litsentsi olemasolu. GIF-formaati ei soovitata kasutata pikaajalise arhiveerimise otstarbel, kuid seda võib rakendada lühiajaliseks ning keskmise pikkusega arhiveerimiseks.

JPEG

JPEG arendas välja Joint Photographic Experts Group ja see sobib eriti hästi värvilistele ja hallides toonides piltidele. Selles valdkonnas on JPEG-tihendamine ka palju efektiivsem kui ITU 4. grupi tihendusprotseduurid. JPEGd on võimalik teatud parameetrite abil erinevalt konfigureerida. Olenevalt seadistustest on võimalik saavutada erinevaid tihendusastmeid. Siiski tuleb arvestada ka võimalike kadudega.

JPEG tähtsamad omadused on järgmised:

- Kõik levinud graafika- ja esitlusprogrammid toetavad JPEG-formaadi kasutamist.
- JPEG-formaati konvertimine on seotud teatud tihendamisetappides mõningate kadudega ning väiksema failisuuruse saavutamise eesmärgil võib oluline pildiinfo kaduma minna.

JPEG-formaat sobib piltide ja dokumentidest loodud piltkujutiste pikaajaliseks arhiveerimiseks. Revisjonikindla arhiveerimise tagamiseks on soovitatav tihendusastme valikul kasutada mõnda sellist astet, mis ei tekita kadusid.

Audio- ja videoformaadid

Audio- ja videofailide digitaalsel töötlemisel tekivad ka juba lühiajaliste salvestite puhul küllaltki suured andmehulgad. Efektiivne tihendamine on siinkohal seega küllaltki oluline. Kaovabad tihendamisprotseduurid suudavad hetkel saavutada audio- ja videofailide tihendusastmena suhte 2 : 1. Palju rohkem on kasu tihendamisprotseduuridest, mis saavutavad tihendusastme 200 : 1, kuid nende töös tekivad kaod. Tihendamisprotseduuri tõttu tekkiv, mõnikord ka märkimisväärne andmekadu on olukord, millega lihtsalt lepitakse, st vähemalt nii kaua, kuni vahe pole kas inimsilmaga märgatav, või kuni see pole liialt häiriv. Kaovabade tihendamisprotseduuride sobivus video- ja audiomaterjali arhiveerimiseks tuleks iga kord rakenduse alusel üle kontrollida. Alljärgnevalt on välja toodud mõningad enamlevinud formaadid.

MPEG

ISO raames vastutab rahvusvaheliste digitaalsete liikuvate piltide tihendamisprotseduuride väljatöötamise eest Motion Pictures Expert Group (MPEG).

Hetkel on olemas kolm teadaolevat protseduuri:

- MPEG1: seda formaati on kolmes erinevas kihis. Kiht 3 on tuntud lühiformaadina MP3 ning levinud audioandmete tihendamisel.
- MPEG2: seda formaati kasutatakse hetkel videoandmete salvestamiseks DVDdele ja tegemist on aktsepteeritud standardiga.

- MPEG4: see formaat on hetkel veel väljaarendamisel ja selle lõplik standardiseerimine ei ole veel läbi viidud.

ITU H.261

Aastal 1990 esitles ITU standardit tähistusega H.261, mis on mõeldud videosignaalide kodeerimiseks. Standardile H.261 vastavat kodeeringut arendati ja optimeeriti edastuse jaoks ISDN-kanalites.

ITU H.263

ITU standard H.263 on standardi H.261 edasiarendus, mis pärineb aastast 1995/96. Algselt töötati seda välja andmeedastuskiiruste jaoks, mis on aeglasemad kui 64 kbit/s. Selline piirang tänapäeval enam ei kehti. Võrreldes standardiga H.261 on märgata palju parema tihendamisvõime juures ka märgatavalt paremat pildikvaliteeti.

Kontrollküsimused:

- Kas on kindlaks määratud, milliseid andmeformaate kasutatakse?
- Kas rakendatavate andmeformaatide süntaks ja semantika on arhiveeritud?
- Kas standardsetesse formaatidesse konvertimisel tekkiv andmekadu on vastuvõetav?
- Kas väljavalitud andmeformaadi omadused on planeeritud arhiveerimisaja kestuseks piisavad?
- Kas revisjoninõuetele vastava arhiveerimise tagamiseks rakendatakse kaovabasid pilditihendamisprotseduure?

M 4.171 Arhiivisüsteemi indeksiandmebaasi tervikluse kaitse

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: IT-juht, administraator

Arhiivisüsteemi korrektseks toimimiseks on ülimalt oluline, et indeksiandmebaas oleks terviklik. Indeksiandmebaasi on salvestatud viited kõikide arhiveeritud dokumentide kohta. Indeksiandmebaasi puuduvad või kahjustatud sissekanded võivad viia selleni, et arhiveeritud dokumente pole enam võimalik üles leida, või on see võimalik ainult väga suure vaevaga, samuti on suuresti häiritud nende dokumentide sidumine igapäevaste tööprotsessidega. Seetõttu tuleb arhiivisüsteemi tõrgeteta töö kindlustamiseks tagada indeksiandmebaasi terviklus ja võimalus seda kontrollida.

Tervikluse tagamisel võiks arvestada järgmiste soovitustega:

Indeksisissekannete varukoopia hoidmine

Olenevalt arhiivi suurusest tuleks ette näha järgmisi astmeid:

- Väikeste arhiivide puhul, kus andmeid tekib juurde vähe ja kus andmepäringute reaktsiooniaja nõuded ei ole kõrged, piisab, kui indeksiandmebaasist tehakse varukoopia kord päevas. Varukoopiate tegemine peaks vastama nõuetele moodulis B 1.4 Andmevarunduspoliitika .
- Arhiivide puhul, kus andmeid tekib juurde palju ja kus indeksiandmebaasi päringute reaktsiooniajale esitatavad nõuded on kõrged, peaks ka indeksiandmebaas ise olema varundatud, st peegeldatud. Täiendavalt tuleb ka siin teha iga päev vastavad varukoopiad. Peegeldatud andmebaasi osad peaksid asuma erinevates tuletõkketsoonides.

Regulaarne tervikluse kontroll

Indeksiandmebaasi tuleks regulaarselt (vähemalt kord nädalas, suurte arhiivide puhul iga päev) kontrollida, kas see on terviklik ja kõikvõimalikest mõjudest puutumata. Kõik indeksiandmebaasis viidatud dokumendid peavad olema arhiivi andmekandjatelt ülesleitavad. Tervikluse rikkumised tuleb dokumenteerida ja võimalikult kiiresti kõrvaldada.

Varukoopiate taastatavuse kontrollimine

Regulaarsete ajavahemike tagant (nt kord kuus) tuleks lisaks veel ka kontrollida, kas indeksiandmebaasist loodud andmevarundused on loetavad ning kas nendest on võimalik andmeid taastada. Liiasusega varustatud andmebaaside puhul tuleks kontrollida, kas ühe osa avarii puhul toimub funktsioonide ülevõtmine korrektselt või mitte.

Kõik regulaarse tervikluskontrolli tulemused tuleks samuti arhiveerida, et andmete muutumine oleks ka veel hiljem arusaadav.

Kontrollküsimused:

- Kas arhiivisüsteemi indeksiandmebaasist tehakse regulaarselt varukoopaid?
- Kas varukoopiatest andmete taastamise võimalikkust kontrollitakse regulaarselt?
- Kas keskmiste ja suurte andmebaaside puhul on indeksiandmebaas varundatud, nt peegel-andmebaasina?
- Kas peegeldatud andmebaasiosasid hoitakse erinevates tuletõkketsoonides?

M 4.172 Arhiivipöörduste logimine

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: IT-juht, administraator

Elektroonilisse arhiivi tehtud pöördused tuleb logida. Selle eesmärk on mõista arhiivis aset leidnud tegevusi ja luua eeldused võimalike vigade korrigeerimiseks.

Järgnev loetelu annab ülevaate võimalikest sündmustest, mida on logimise abil võimalik tuvastada:

- andmete konfidentsiaalsuse/tervikluse kadu kasutaja vea tõttu,
- väär pääsuõiguste haldus,
- serveri väljalülitamine jooksva töö käigus,
- õiguslike raamtingimuste rikkumised arhiivisüsteemide kasutamisel,
- defektsed andmekandjad,
- salvestatud andmete hävimine,
- andmekadu andmekandja täitumise tõttu,
- andmete või tarkvaraga manipuleerimine,
- andmekandjate volitamata kopeerimine,
- krüpteerimismooduliga manipuleerimine,
- krüptograafiliste võtmete kompromiteerimine,
- arhiivi andmekandjate volitamata ülekirjutamine ja kustutamine.

Logimise detailsus sõltub ühelt poolt sellest, millisel määral on tarvis arhiivis salvestatud dokumente mõista ning mil määral on tarvis tagada nende autentsust. Teiselt poolt jällegi tuleb järgida ka organisatsioonis kehtestatud nõudeid, nt andmekaitsenõudeid.

Kui vähegi võimalik, tuleks logides kajastada vähemalt järgmisi andmeid:

- pöörduse kuupäev ja kellaaeg,
- klientsüsteem, kust vastav pöördus sooritati,
- arhiivi kasutaja ja tema rakendatud kasutajaroll,
- sooritatud tegevused,
- võimalikud veateated või koodid.

Logifailide säilitamiskohustuse kestus tuleks kindlaks määrata arhiveerimiskontseptsioonis. Logifaile tuleb organisatsiooni sisenõudeid järgides regulaarselt analüüsida, et tuvastada võimalikke väärkasutusi ja süsteemi vigu. Analüüsimine võib toimuda kas käsitsi või vastava analüüsitarkvara kaasabil. Juba eelnevalt tuleks defineerida, milliseid sündmusi loetakse kriitilisteks, st olukorrad, millest tuleb kindlasti teavitada mõnda administraatorit. Info sellistest sündmustest peaks laekuma võimalikult kiiresti, nt vastavate süsteemihalduskeskkondade vahendusel. Lisaks on oluline, et vastav teavitusprotsess leiaks aset rollipõhiselt, mitte isikupõhiselt. Kui olukorrast teavitav e-kiri saadetakse nt ainult ühele konkreetsele isikule, võib see teatud olukorras jääda ka täiesti tähelepanuta, kuna vastav isik ei pruugi ilmtingimata alati oma töökohal viibida.

Järgmisi sündmusi tuleks arhiveerimisprotsessis liigitada tüüpiliste kriitiliste sündmuste alla, mistõttu tuleks neid ka pidevalt logida, need peaksid olema seire all ning nende esinemisest tuleks viivitamata teavitada:

- arhiivi andmekandjate kopeerimine,
- arhiivisüsteemi andmekandjate kopeerimine,
- andmehulkade kustutamine või nende kustutamist lubav märgistamine,
- arhiivisüsteemi andmekandjate lülitamine vallasrežiimi,
- arhiivi andmekandjate eemaldamine arhiivisüsteemist,
- arhiivi andmekandjate lisamine,
- arhiivi andmekandjate lülitamine sidusrežiimi,
- vead või probleemid arhiivile tehtud pöörduste puhul,
- süsteemivead ja ajalõpud,
- katastroofistsenaariumid (tulekahju, lubamatu temperatuur, vesi jne), mida üldjuhul tuvastavad välised andurid.

Pärast info laekumist vastava olukorra tekkimise kohta tuleks seda kohe kontrollida ja vajaduse korral käivitada eskalatsiooniprotsess. Harilikult tuleks esimese eskalatsiooniastmena informeerida IT-juhti. Olenevalt organisatsiooni eripäradest võib eskalatsiooniprotsess ka teisiti välja näha.

Kontrollküsimused:

- Kas arhiivisüsteemi sündmusi logitakse?
- Kas logimisel järgitakse seadusi ja organisatsioonisiseseid ettekirjutusi?
- Kas logi kajastab ka sellist infot, milliseid andmekandjaid on jukebox'ist välja võetud ja juurde pandud?
- Kas turvarikkumistele järgneb olukorrast teavitamine?
- Kas turvarikkumiste jaoks on välja töötatud eskalatsioonireeglid?

M 4.173 Arhiveerimise regulaarsed talitlus- ja taastetestid

Algatamise eest vastutavad: IT-juht, arhiivi haldaja

Rakendamise eest vastutavad: IT-juht, administraator, arhiivi haldaja

Arhiveerimise käigus võib tekkida erinevatel põhjustel andmekadusid, mis võivad olla tingitud probleemidest andmekandjate, riistvara ja programmide tööga. Seetõttu tuleb ilmtingimata teha regulaarselt talitlus- ja taasteteste. Andmekandjatel võib esineda sarnaselt kõigi muude arhiveerimiseks kasutatavate komponentidega kulumisnähtusid ja sel põhjusel tuleks vähemalt kord aastas kontrollida, kas neil hoitav info on loetav ja terviklik. Juhul kui arhiveerimiseks kasutatavas andmekandjas leitakse mõni viga, tuleb viivitamata hoolitseda selle eest, et vigasel andmekandjal hoitav info saaks varukoopiate abil uuesti taastatud. Olukordades, kus vigased andmekandjad peab välja vahetama, tuleb sealt pärast koopia tegemist salvestatud andmed turvaliselt kustutada või vajaduse korral andmekandjad hävitada (vt M 2.167 Andmete kustutamiseks või hävitamiseks sobivate lahenduste valik).

Kogu asjakohane protseduur tuleb dokumenteerida. Kõiki riistvarakomponente, eriti arhiivi mehaanilisi detaile tuleb regulaarselt kontrollida, et nende töös ei esineks tõrkeid. Ainult niimoodi on võimalik tagada, et arhiveeritud andmehulgad vastavad neile seatud käideldavusnõuetele ning et andmete lugemisel ja kirjutamisel säilib ka nende terviklus. Ka arhiveerimisprotseduuris endas võib tekkida vigu. Võimalikud põhjused on konfigureerimisvead, tarkvara ebakorrektne toimimine (nt pärast uute programmide kasutuselevõttu), probleemid salvestitega või muudatused ja vead protsessi juhtimises. Seetõttu tuleb kord päevas kontrollida, kas kõik arhiveerimisprotsessid on kulgenud veatult. Sellega võivad tegeleda administraatorid, kes peaksid analüüsima logifaile ja kontrollima pisteliselt ka arhiveerimiseesmärgil loodud andmekandjaid. Indeksiandmebaaside puhul hädavajalikke tervikluse kontrolle kirjeldatakse meetmes M 4.171 Arhiivisüsteemi indeksiandmebaasi tervikluse kaitse .

Kontrollküsimused:

- Kas kõiki arhiveerimise andmekandjaid kontrollitakse regulaarselt, et need oleksid loetavad ja terviklikud?
- Kas arhiivi mehaanilisi detaile kontrollitakse regulaarselt, et nende töös ei esineks tõrkeid?
- Kas andmehulkade kontrollimine ja logifailide analüüs leiab aset iga päev?

M 4.176 Autentimismeetodite valimine veebilehtede jaoks

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: administraator

E-kaubandust ja e-riiki puudutavate teenuste puhul, samuti isikutuvastust nõudvate veebilehtede või ka lihtsalt mõningase juurdepääsupiirangu kehtestamisel veebilehte teatud osale läheb tarvis kasutajatele suunatud identifitseerimis- ja autentimismehhanisme. Sõltuvalt konkreetsetest vajadustest, kui tugevalt on tarvis kaitsta kas dokumente volitamata juurdepääsu eest või millise kvaliteediga autentimist soovitakse kasutada, tuleb välja valida sobiv meetod. Autentimismeetodi valik ja põhjused, miks ühe või teise lahenduse kasuks otsustati, tuleb dokumenteerida.

Autentimismeetodid HTTP puhul

Protokoll HTTP/1.1 võimaldab kasutajaid autentida kahel erineva moel:

- Esimene meetod on nn Basic-Access- autentimine. Selleks edastab klient oma kasutajatunnuse ja Base64 -kodeeringuga varustatud parooli HTTP-Request'i nn Authorization Header 'is serverile. Base64 on meetod binaarandmete kodeerimiseks 7-bitise ASCII koodiga, mida kasutatakse siinkohal viitemärkide edastamiseks läbi HTTP-liidese. Parool pole seetõttu kohe esmapilgul loetav, kuid potentsiaalsel „pealtkuulajal" on võimalik seda siiski probleemideta välja selgitada, kuna see ei ole krüpteeritud. Sel põhjusel on antud autentimise liik rakendatav parimal juhul vaid väga nõrkade konfidentsiaalsusnõuete puhul.

- Teine HTTP-autentimismeetod on Digest -autentimine. Selle autentimisliigi puhul peab kasutaja parool serveris loetaval kujul olemas olema. Klient saab serverilt juhusliku stringi, niinimetatud Challenge 'i. Selle Challenge 'i ja kasutajalt saadud parooli abil arvutab klient kindlaksmääratud protseduuriga nn Digest 'i, mis saadetakse seejärel autentimise otstarbel edasi serverile. Kuna serveril on olemas nii tema poolt genereeritud juhuslik string kui ka kasutaja parool, on serveril samuti võimalik välja arvutada vastav Digest ning viia läbi vastav autentimine. Kuna Digest -autentimisviisi puhul ei saadeta parooli võrgu kaudu, sobib antud meetod ka juba veidi kõrgema kaitsevajaduse rahuldamiseks.

Eelnimetatud autentimismeetodite kasutamisel on probleemiks serveril hoitavate parooliandmete turvalisus: Digest -autentimsimeetodi rakendamisel tuleb kasutajate autentimisandmeid hoida veebiserveril loetava teksti kujul. Basic -autentimismeetodi rakendamisel tuleb enamatel juhtudel salvestada parooli räsiväärtus. Neil põhjustel on eriti oluline kaitsta serveril hoitavaid paroolifaile volitamata juurdepääsude eest. Lisaks HTTP-autentimisele eksisteerib veel üks võimalus, kuidas juurdepääsusid HTTP-protokolli vahendusel kaitsta: autentimist ei vii

läbi mitte veebiserver ise, vaid hoopis serveripoolne rakendus. Selleks sisestatakse kasutajatunnus ja parool tavalistesse HTML blankettidesse ning rakendus kontrollib nende õigsust. Antud lahendusi võib tihti kohata veebilehtede puhul. Siiski tuleks sellistel juhtudel alati arvestada, et paroolid ja PIN-koodid, mis edastatakse läbi interneti loetava teksti kujul, on ka soovimatutele osapooltele kergesti loetavad. Lisaks muidugi veel ka tõsiasi, et ka kõik andmed, isegi kui need tehakse kättesaadavaks ainult läbi autentimist nõudvate päringute, edastatakse krüpteerimata kujul. Mõned veebilehed identifitseerivad kasutajaid spetsiaalsete küpsistega, mis salvestatakse brauseritesse. Kuna HTTP kasutamisel edastatakse ka küpsised loetava teksti kujul, ei sobi ka see meetod kaitsmist vajava info juurdepääsu autentimiseks. Põhjusel, et küpsistega on seotud veel teisigi turvaprobleeme, tuleks selle meetodi kasutamisest üldjuhul loobuda.

SSLi kasutamine

Juhtudel, kus e-kaubandust ja e-riiki puudutavate veebilehtede puhul seatakse suuremad nõudmised autentimise turvalisusele ja edastatavate andmete konfidentsiaalsusele, tuleks andmeedastuste turvamiseks rakendada SSLi (vt M 5.66 TLS-i/SSL-i kasutamine). SSLi on võimalik rakendada kahes töörežiimis: esimese variandi puhul on sertifikaadiga varustatud ainult server. See on kasutajale vajalik selleks, et ta saaks tuvastada, kas ta on tõepoolest ikka „õige“ serveriga ühendatud ning võimaldab pärast krüpteeritud ühenduse loomist turvaliselt edastada autentimisinfot ja rakendusandmeid. Serveri sertifikaat sisaldab lisaks sertifitseerimiskeskuse nimele veel ka selle serveri nime, millele see kehtib. Sertifikaat võib olla väljastatud juur-sertifitseerimisüksuse (Root-CA) poolt, kuid võib olla ka ise genereeritud, nt mõne OpenSSL paketis sisalduva tarkvaratööriista abil. Sertifikaate, mis ei ole väljastatud juur-sertifitseerimisüksuse poolt, kuid mis on brauseritele teada, ei aktsepteeri brauserid reeglina mitte automaatselt, vaid kasutajatel tuleb konkreetselt veel kinnitada, et süsteem peaks kõnealust sertifikaati aktsepteerima. Teise variandi puhul on ka kasutaja varustatud sertifikaadiga, mis peab klient-arvutis kohapeal olemas olema ja saadetakse autentimise eesmärgil brauseriga edasi serverile. Selle lahenduse eelduseks on asjaolu, et sertifitseerimiskeskused, kelle sertifikaate sel otstarbel kasutatakse, peavad olema usaldusväärsed. Põhjus, miks antud lahendust praktikas eriti tihti ei kohta, seisneb selles, et antud lahenduse rakendamine on seotud väga suure vaevaga. Serveri konfigureerimine on küllaltki lihtne: lisaks veebiserveri konfigureerimisele SSLi kasutamiseks, tuleb hankida ja juurutada SSL-serveri sertifikaat. Töö hulk, mis on seotud iga üksiku kasutajaga on aga seevastu suhteliselt suur: iga kasutaja peab olema varustatud SSL-klient-sertifikaadiga, mis tuleb installeerida kasutaja brauseri alla. Sellega kaasneb teatud langus kasutusmugavuses, kuna üks suuremaid eeliseid tavalise WWW-kasutuse juures seisnebki just selles, et juurdepääs on võimalik praktiliselt ükskõik millisest arvutist. Juhul, kui klient-sertifikaate rakendatakse autentimise otstarbel, muutub kasutusvõimaluste paindlikkus tunduvalt piiratumaks, kuna vajaminev klient-sertifikaati ei ole kõikjal kohapeal olemas. Mõningatel juhtudel võib see aga olla ka taotluslik, nt intranet-veebiserveri kasutamisel.

Üheks sagedasti rakendatavaks kasutajate autentimismeetodiks veebilehtede puhul on kombinatsioon blanketipõhisest autentimisest ja SSLiga krüpteeritud andmeedastusest. Selle meetodiga on võimalik saavutada, juhul kui valitud SSL protokoll on piisavalt tugev, mõistliku töövaevaga (kasutajate haldamine veebirakenduses ja veebiserveri juurdepääsu SSLi põhise turbe juurutamine) täiesti vastuvõetav turbeaste, mis sobib ka kõrgemate turvanõuete rahuldamiseks.

Järgmine tabel annab ülevaate kasutajate autentimisvõimalusest veebiserveri-tes:

Meetod	Turbe-aste	Juurutamise keerukusaste	Serveriga kaasnevad kohustused	Kommentaarid
Standardne autentimine	Madal	Madal	Kasutajate haldamine	Autentimisinfo ja andmed edastatakse krüpteerima-ta kujul!
Blanketil põhinev autentimine ilma and-meedastuse turbeta	Madal	Madal kuni keskmine	Juurutamine vastava rakenduse alla	Autentimisinfo ja andmed edastatakse krüpteerima-ta kujul!
Digest autentimine	Keskmine	Madal	Kasutajate haldamine	Andmed edastatakse krüpteerima-ta kujul.
Blanketil põhinev autentimine koos SSLiga	Kõrge	Keskmine kuni kõrge	SSLi tugi serveris, juurutamine vastava rakenduse alla	Autentimisinfo ja andmed edastatakse krüpteeritud kujul!

Sertifikaadil põhinev autentimine koos SSLiga	Kõrge	Kõrge	Serveri sertifikaatide installeerimine. Sertifikaatide haldamine, Public Key infrastruktuur.	Kasutatakse peamiselt turvaliste transaktsioonide sooritamiseks läbi interneti.

Tabel: Kasutajate autentimisvõimalused veebiserverites

Lisaks eelnevatele pakub veel ühte meetodit Microsoft Internet Information Server, mida rakendatakse Windowsis kasutajate sisselogimise puhul. Antud meetod töötab vaid siis, kui kliendina rakendatakse Microsoft Internet Explorerit.

SSL-ühenduse loomisel lepitakse kasutatav krüpteerimisrežiim kokku kliendi ja serveri vahel. Kasutada olevate algoritmide seas leidub aga ka selliseid, mida ei liigitata enam turvaliste alla. Eriti tuleb aga tähelepanu pöörata sellele, et on olemas ka null-krüpteerimisrežiim, mille puhul krüpteerimist ei toimu. Veebiserveri konfigureerimisel SSLi kasutamiseks tuleb arvestada, et server ei tohiks aktsepteerida mitte ühtki nõrka algoritmi, eriti aga null-krüpteerimisrežiimi. Vastasel juhul võib tekkida olukord, kus näiliselt luuakse küll turvaline ühendus (kasutatakse HTTPSi), kuid tegelikult on see kas liiga nõrk või jääb üleüldse krüpteerimata. Igal potentsiaalsel ründajal võib olla soov sellist situatsiooni sihilikult esile kutsuda, et seeläbi nii autentimisandmeid kui ka muud informatsiooni pealt kuulata. Seetõttu tuleks veebiserveri SSL-konfigureerimise käigus kindlasti null-krüpteerimisrežiimi ja nõrkade algoritmide kasutamine välja lülitada.

Täiendavad kontrollküsimused:

- Kas on dokumenteeritud, mille põhjal langetati otsus rakendatava autentimismeetodi kasuks?
- Kas SSL-konfiguratsioonis on null-krüpteerimisrežiimi ja nõrkade algoritmide kasutamine välja lülitatud?

M 4.177 Tarkvarapakettide tervikluse ja autentsuse tagamine

Algatamise eest vastutavad: IT-juht, IT turbespetsialist

Rakendamise eest vastutavad: administraator, muudatuste haldur

Ebaturvalistest allikatest pärit programmide käivitamine võib endaga kaasa tuua märkimisväärseid kahjusid. Kahjurvara (malware) võib nt installeerida arvutisse paroole nuhkima hakkavaid programme, Trooja hobuseid või tagauksi, samuti võib tagajärjeks olla andmete kustutamine või nende kahjustamine.

Tüüpilised kahjurvara allikad on nt programmid, mis jätavad endast mulje, nagu oleks tegemist kas ekraani pimenduspildi, viiruseskanneri või mõne muu abiprogrammiga, mida saadetakse võltsitud aadresside alt laiali väga paljudele meiliadressaatidele. Tihti võib ka juhtuda, et kasutajad laadivad programmid hooletusest internetist alla ja installeerivad need ilma kontrollimata. Kaks näidet, mille puhul võib väita, et kahju vältimiseks oleks piisanud lihtsalt digitaalsete allkirjade kontrollimisest, on esiteks juhtum 2002. aasta märtsist, kui OpenSSH-projekti raames manipuleeriti ftp-serveril levitamiseks hoitud OpenSSH paketti, ja teiseks sarnane juhtum septembrist 2002, mil sama asi juhtus meiliserveri sendmail levitamisega. Mõlemal juhul smuugeldati levitatavatesse pakettidesse sisse Trooja hobused, mis võisid endaga kaasa tuua arvuti kompromiteerimise neis arvutites, kus neid pakette kompileeriti. Mõlematel juhtudel oleks olemasolevate digitaalsete allkirjade kontrollimine suutnud tõestada, et vastavaid pakette on manipuleeritud. Isegi kui ühekski muuks otstarbeks krüpteerimis- või allkirjastamistehnikaid ei kasutata, tuleks siiski kaaluda nende rakendamist vähemalt sellises ulatuses, nagu siinses meetmes kirjeldatud.

Üldjuhul tuleks tarkvara installeerida ainult siis, kui on teada, et see pärineb usaldusväärsest allikast, eriti siis, kui installeeritav tarkvara ei ole mitte andmekandjal, vaid laetakse alla internetist. Eriti kehtib see värskenduste ja paikade kohta, mida tavaliselt enam andmekandjatel ei väljastata. Suurem osa tootjatest ja levitajatest pakuvad kontrollimiseks vastavaid kontrollsummasid, mis lubavad veenduda vähemalt tarkvarapaketi tervikluses. Kontrollsummad avaldatakse kas tootja kodulehel või saadetakse e-posti teel. Allalaetud programmi või arhiveeritud faili tervikluse kontrollimiseks peab vastav programm kontrollima, kas avaldatud kontrollsumma ja programmi poolt kohapeal genereeritud kontrollsumma langevad kokku või mitte. Juhtudel, kus tarkvarapakettidega on kaasas ka kontrollsummad, tuleks need üle kontrollida enne installeerima asumist. Kontrollsummad ei suuda edastada infot autentsuse kohta. Seetõttu varustatakse paljudel juhtudel nii programmid kui tarkvarapaketid digitaalsete allkirjadega. Digitaalsete allkirjade kontrollimiseks vajaminevad avalikud võtmed avaldatakse kas tootjate kodulehtedel või avaliku võtme serverites. Kontrollsummasid genereeritakse tihti kas programmiga PGP või GnuPG. Kui kontrolli tulemusel selgub, et tegemist on konkreetse tootja kehtiva allkirjaga, võib vastavat tarkvarapaketti pidada usaldusväärsemaks kui selliseid tarkvarapakette, millele on lisatud vaid kontrollsumma. Linuxi levitajate hulgas laialt levinud paketihaldussüsteemi RPM (Redhat Package Manager) on sarnaselt Debiani levitajate paketihaldussüsteemiga vastav kont-

rollifunktsioon juba integreeritud. Mõnedel juhtudel ei võrdle kontrollsummasid isegi operatsioonisüsteemi või rakendustarkvarasse sisseehitatud uuendusmehhanismid. Kui vähegi võimalik, tuleks kontrollsummade võrdlus läbi viia alati enne ükskõik millise tarkvarapaketi installeerimist. Mõningad kontrollsummade võrdlused võivad nõuda ka kasutaja sekkumist, kuna tootjad teevad selleks vajaminevad kontrollsummad, allkirjad või sertifikaadid kättesaadavaks erinevate põhimõtete alusel. Sel põhjusel tuleb tihti verifitseerimisprotsess läbida nt tootja kodulehel käsitsi, või kohandada paikade ja muudatuste tarkvaras vastavat URLi. Kõikidel juhtudel, mil tarkvarapaketid on varustatud digitaalsete allkirjadega, tuleks neid kindlasti enne paketi installeerimist kontrollida.

Üks tõsine probleem digitaalsete allkirjade rakendamise juures on kasutatavate võtmete endi autentsuse kontrollimine. Juhul kui avalik võti ei sisalda teadaoleva usaldusväärse isiku või asutuse (nt trustcenter) digitaalset allkirja, ei paku vastava privaatvõtmega genereeritud allkirjad sugugi erilist kindlustunnet, et vastava tarkvarapaketi taga on tõepoolest loodetud arendaja, tootja või levitaja. Sel põhjusel tuleks avalikke võtmeid, kui need pole sertifitseeritud, hankida võimalikult mõnest muust allikast kui tarkvarapaketti ennast, nt mõnelt tootja CD-ROMilt, mõnest teisest peegelserverist, kus vastav pakett on samuti allalaetav või avaliku võtme serverist. Kontrollsummade kontrollimiseks vajalikud programmid peavad kohapeal olemas olema. Administraatorid peaksid olema kontrollsummade ja digitaalsete allkirjade tähendusest ja kaalukusest piisavalt informeeritud. Lisaks peaks administraatoritel olema piisavalt aega, et vastavaid programme oma igapäevatöös kasutada ja ennast vastavate programmide käsitsemisega kurssi viia. Paikade ja värskenduste hankimisest e-posti teel tuleks loobuda ja seda koguni mitmetel põhjustel. E-kirjade päritolu on ilma täiendavate turvamehhanismideta vaid väga raskesti tuvastatav ja adressaadid on tihtilugu võetud institutsiooni jaotusloenditest, mille aadressid on kergesti aimatavad. Pealegi võivad paigad ja värskendused olla ka väga suuremahulised. Paljud ettevõtted ja asutused on piiranud e-kirjade manuste maksimaalset suurust ning mõningatel juhtudel on kehtestatud koguni keeld võtta käitusfaile vastu e-kirja manusena.

Lisaks koormavad väga suured andmemahud liigselt e-posti süsteeme. Seetõttu pole tarkvaramuudatuste hankimine e-kirja teel, eriti kui on tegemist turvapaikadega, piisavalt kindel ettevõtmine. Mõned tootjad pakuvad oma klientidele võimalust, et muudatused ja paigad toimetatakse kliendini ka andmekandjal. Ka neil juhtudel tuleks vastavaid paikasid ja värskendusi kindlasti kontrollsummade või digitaalsete allkirjade põhjal kontrollida, kuna postisaadetiste saatjaandmeid ja CDdele või DVDdele peale kantavaid tootjafirma logosid on võimalik kerge vaevaga võltsida. Lisaks tuleks tarkvaravärskenduste ehtsuse kontrollimisel arvestada ka erinevate infoallikatega, nagu nt tootja kodulehel avaldatud infoga, tootja uudiskirjadega jms. Mõningad tootjad on määratlenud kindlad tsüklid ja ajad, mille saabudes avaldatakse süstemaatiliselt uut infot võimalike muudatuste kohta.

Kontrollküsimused:

- Kas rakendatavate tarkvarapakettide puhul on kontrollitud võimalike kontroll-

summade ja digitaalsete allkirjade olemasolu?

- Kas enne seda, kui tarkvara institutsioonis kasutusele võetakse, kontrollitakse ka selle terviklust ja autentsust?
- Kas kontrollsummade ja digitaalsete allkirjad kontrollimiseks vajalikud programmid on kohapeal olemas?
- Kas tarkvarapakettide olemasolevaid kontrollsummasid või digitaalseid allkirju on kontrollitud?

M 4.198z Rakenduse installeerimine chroot -puuri

Algatamise eest vastutavad: infoturbespetsialist, IT-juht
Rakendamise eest vastutab: administraator

Turvalisuse suurendamiseks võib rakenduse installida nn *chroot* -puuri. Süsteemikäsuga *chroot()* piiratakse Unixis rakenduse juurdepääs kataloogipuu teatud osale. See on võimalik, sest kõik pöördused, mida rakendus ja rakenduse poolt avatud rakendused failisüsteemi suunavad, lähtuvad kataloogist, mis määrati funktsiooniga *chroot()* . See kataloog muutub virtuaalse kataloogipuu juureks, mida nimetatakse *chroot* -puuriks või *chroot* -vanglaks. Hierarhias sellest kõrgemal asuvatele kataloogidele ja failidele ligi ei pääse. Näiteks saab sellega serveril mitu teenust üksteisest eraldada. Peale süsteemikäsu *chroot()* on olemas ka samanimeline programm, mida saab kasutada mis tahes rakenduste käivitamiseks sellises *chroot* -puuris. Näiteks kui ründajal õnnestub oma programmikood käivitada rakenduse protsessialas, suudab see piirata otsest kahju, sest sellisel juhul ei pääse ründaja operatsioonisüsteemile ligi. *Chroot* -puurist on võimalik ka välja murda. Selleks peab ründaja esmalt märkama, et ta asub *chroot* -puuris. See pikendab ründeks kuluvat aega. Selle aja jooksul on võimalik, et rünnet märgatakse ja võetakse vastumeetmeid. *Chroot* -puur peab sisaldama kõiki rakenduse käivitamiseks vajalikke faile. Millised need failid on, tuleb välja selgitada olemasoleva dokumentatsiooni abil. Tavaliselt on need järgmised failid ja kataloogid: *dev*, *lib*, *usr/bin*, *var*, *var/run*, *etc* ning rakendusepõhised failid ja kataloogid. Kui rakendus kavatsetakse installida *chroot* -puuri, peab jätma piisavalt aega planeerimiseks ja katsetamiseks. Installimisel tuleb dokumenteerida:

- *chroot* -puuri juurkataloog ja
- *chroot* -puuris saadaolevad operatsioonisüsteemi komponendid.

Eriti oluline on see, et *chroot* -puuri paigaldataks mõned *device file* 'id, lisaks läheb tarvis failide */etc/passwd* ja */etc/group* kohandatud versioone. Nendest failidest tuleb eemaldada kõik ebavajalikud andmed, välja arvatud andmed kasutaja ja grupi kohta, mille all peab rakendus töötama. Olenevalt operatsioonisüsteemist on võimalik, et faili peavad alles jääma ka mõned muud sissekanded.

Täiendavad kontrollküsimused:

- Kas *chroot* -puuri konfiguratsioon on piisavalt põhjalikult dokumenteeritud?
- Kas *chroot* -puuri on kopeeritud kõik vajalikud failid?

M 4.199 Ohtlike failivormingute vältimine

Algatamise eest vastutavad: administraator, infoturbespetsialist

Rakendamise eest vastutavad: administraator, kasutaja

Praeguseks on meilidest saanud peamine viiruste ülekandmise viis. Tavaline, manusteta tekstimeil on ohutu. Ohtlikuks muutub olukord alles siis, kui avatakse meilides olevad manused, mis põhinevad HTML-il või juhivad meili saaja lingi kaudu manipuleeritud veebilehekülgedele. Põhimõtteliselt saab meilile lisada nii palju ja mis tahes tüüpi manuseid kui soovitakse. Liiga suur arv manuseid mõjutab aga meiliprogrammi või meiliserveri käideldavust (vaata G 5.75 Ülekoormus siseneva meili tõttu). Suuremat ohtu kujutavad endast aga manused, mis sisaldavad täitmisprogrammi ja mis võivad seetõttu põhjustada etteaimamatuid kõrvalmõjusid.

Manused

Täitmisprogrammi sisaldavad manused võivad põhjustada etteaimamatuid kõrvalmõjusid. Seepärast tuleb potentsiaalselt ohtlike failivormingutega ümberkäimiseks koostada vastavad eeskirjad. Tähtis on, et kõik asjaosalised oleksid probleemist teadlikud ja käituksid vastavate failivormingutega ettevaatlikult. Kahjurvarakoodide mittetahtliku käivitamise vältimiseks tuleks meiliprogramm seadistada nii, et manuseid ei avataks automaatselt, vaid et programm hoiataks kasutajat või vähemalt küsiks, et kas vastav fail tuleb avada. Operatsioonisüsteem või meiliprogramm peaks olema sisse seatud nii, et faili esitatakse esialgu ainult vaaturis (Viewer) või mõnes teises esitusprogrammis, mis ei käivitaks võimalikke programmikoode nagu makrosid ja skripte. Kui kasutaja saab potentsiaalselt ohtliku manusega meili, peaks ta esmalt kindlaks tegema, kas meili saatjaks on usaldusväärne allikas. Seda on võimalik teha saatjapoolse krüptograafilise allkirja ja vastuvõtjapoolse allkirjakontrolliga. Lisaks peaks võimalike ohtlike manuste saatja hoolitsema ka selle eest, et tema saadetud manused oleksid ikkagi ohutud. Selle juurde kuulub vähemalt aktuaalsete kahjurvarakoodide allkirjadega varustatud viirustõrjeprogrammiga skannimine.

Ohtlikud failivormingud

Ohtlike failivormingutega ümberkäimiseks võib luua mitmeid reegleid. Tähtis on aga, et kõik asjaosalised oleksid probleemist teadlikud ja käituksid vastavate failivormingutega ettevaatlikult. Kindlaim võimalus on keelata probleemseid failivorminguid avada või filtreerida neid meililüüsis. See aga toob kaasa aktsepteerimisprobleeme nii klientide kui töötajate seas. Parim lahendus on ühest küljest töötajad probleemiga tuttavaks teha ja neid kaasa mõtlema innustada, teisest küljest aga aidata neid tehniliste vahenditega, näiteks vähendada ohupotentsiaali vastavate konfiguratsioonide ja turvavahenditega (vt M 2.224 Trooja hobuste tõrje ja M 5.69 Aktiivsisu tõrje).Järgmisena antakse hinnang mõningatele failivormingutele.

Hinnangud aga võivad iga hetk muutuda, näiteks kui tootja lisab tootele mõne uue funktsiooni, mis viib ootamatute kõrvalmõjudeni, või kui keegi need kõrvalmõjud avastab.

- Selle hinnanguga tuleb käsitleda Office'i pakette (Microsoft Office, Office Strater, Libre Office või Open Office), mis sisaldavad makrokeelt, näiteks Word, Excel, Powerpoint (.DOCX,.XLSX,.PPTX, ODT jne) ja kõiki dokumente, mis võivad sisaldada tõlgendatavaid/täidetavaid koode, näiteks PDF,

CHM. Eriti kriitiliselt tuleb suhtuda täitmisprogrammidesse (näiteks.COM, .EXE,.PIF) või skriptikeelde (Windowsis.VBS,.JS,.BAT ja Unixis perl - või shell -skriptid), registreerimisfailidesse (.REG), aga ka ekraanisäästjatesse (.SCR). Ettevaatusabinõuna tuleks kõigile nendele failitüüpidele määrata „ohutu" standardrakendus, millega need küll avatakse, aga mille keskkonnas ei ole viirustel võimalik kahju tekitada. Näiteks tuleks kõik failitüübid nagu *.VBS, *.JS, *.BAT avada lihtsa tekstiredaktoriga, mis ei toeta makrot.

- Lisameetmetega võib lubada ka: HTML-i, kui on paigaldatud JavaScripti filter või teised turvameetmed, RTF-i (COM-Object filtriga), ZIP-i (siinkohal peaks aga kasutajaid hoiatama, et selles sisalduvad failid võivad olla ohtlikud), PDF-i (tuleb jälgida, et lõpparvutis oleks vaikimisi kasutusel PDF-Reader, mitte Adobe Acrobat).

Meilipommiks võib osutuda näiteks kokkupakitud manus, mis loob pärast lahtipakkimist suurel hulgal alamkatalooge või võtab palju kõvakettaruumi.

Pakkimisprogrammiga kokkupakitud faile (arhiive) ei tohiks kunagi ilma kontrollimata lahti pakkida. Siia alla kuulub sisukorraülevaade, kokkupakitud faili liik ja suurus ning viirustõrjeprogrammiga kontrollimine. Iseend lahtipakkivaid arhiive (näiteks .EXE) ei tohiks kunagi avada, sest nende sisu pole võimalik enne lahtipakkimist kontrollida.

HTML-meilid

Üha rohkem meile on tänapäeval HTML-vormingus. Tihtipeale on see tüütu, kuna kõik meiliprogrammid ei suuda seda vormingut kuvada. Kuna HTML-meil võib sisaldada JavaScripti või VisualBasicu koodi, võib ainuüksi meili kuvamine viia programmis soovimatute tegevusteni. HTML-lähteteksti paigaldatud piltide kaudu on võimalik rämpsposti saatjale meiliprogrammist tagasisidet anda. Kui meili paigutatud pilt laaditakse kirja näitamisel internetiallikast alla, teab spämmija, et tema meili on loetud, ning saab kinnituse, et vastuvõtja aadress on olemas ning et vastuvõtja loeb rämpsposti. Meilikliendis tuleks HTML-objektide automaatne laadimine keelustada. Erinevate turvaaukude koosmõjul on meiliprogrammides ja brauserites ikka ja jälle tekkinud turvaprobleeme HTML-vormingus meilidega (vt G 5.111 Meilide aktiivsisu kuritarvitamine). Põhimõtteliselt ei tohiks võimalusel HTML-vorminguga ja aktiivsisudega meile saata. Lisaks tuleks valida meiliprogramm, kus HTML-vormingus meilid on äratuntavad, et kasutaja neid teadmatusest ei avaks. Peale selle tuleks kontrollida võimalust meilides olevat aktiivsisu näiteks turvalüüsis filtreerida. Asutuses tuleb anda juhtnööre, kuidas HTML-vormingus meilidega käituda.

HTML-vormingus meili saabudes tuleb kindlaks teha:

- kas saata need muutmata kujul kasutajatele edasi ja koolitada kasutajad selliseid meile vastutustundlikult ja turvaliselt kasutama,
- kas teisaldada need serveri vahenditega tekstivormingusse ja saata alles siis vastava märkega kasutajale (sellisel juhul võib teave kaduma minna),

- kas saata need erilisele töökohale, kus saajal on võimalik kirja vastavate turvanõuetega vaadata (meilide mahust olenevalt võib see kaasa tuua suuri kulusid).

Kõiki kasutajaid tuleks sellest probleemist teavitada. Kes tahab kindel olla, seadistab meiliprogrammi nii, et tavapäraselt näitab programm meile ainult tekstina.

Kontrollküsimused:

- Kas meiliprogrammid ja serverid konfigureeriti nii, et HTML-sisust ja probleemsetest manustest tulenev oht on vastavalt määratud infoturbenõuetele minimeeritud?
- Kas ohtlike failivormingutega ümberkäimine on reguleeritud?
- Kas kõik kasutajad teavad, kuidas ohtlike manustega käituda?

M 4.200z USB-salvestuskandjatega ümberkäimine

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: Administraator

USB-liides võimaldab paljusid lisaseadmeid ühendada personaalarvutitega.

Näideteks on siin kõvakettad, CD/DVD-kirjutajad ja mälupulgad. USB-mälupulgad koosnevad USB-pistikust ja salvestuskiibist. Vaatamata suurele salvestusmahule on nad nii käepärased, et neid toodetakse näiteks võtmehoidjakujulisena ja nad mahuvad igasse püksitaskusse. Kaasaegsetes operatsioonisüsteemides on suurte infohulkade salvestamiseks mõeldud USB-seadmetele draiverid juba sisse ehitatud, nii et nende kasutamiseks ei ole enam vaja tarkvara installeerida.

Üldiselt käib see meede mitte ainult USB-salvestuskandjate, vaid üldiselt kõikide USB-seadmete kohta, mis suudavad andmeid salvestada. Muuhulgas võib ka USB-printereid ja USB-kaameraid andmete salvestamiseks “kuritarvitada”. Eriti käib see selliste “intelligentsete” USB-seadmete kohta nagu seda on pihuarvutid (PDA), mis ühilduvad suvalise USB-identiteediga, kui need on spetsiaalse tarkvaraga varustatud.

USB-salvestuskandjate abil saab informatsiooni ja programme kontrollimatult sisse ja välja laadida. Seepärast tuleb USB-salvestuskandjatega üldjoontes täpselt samamoodi ümber käia kui tavaliste salvestuskandjatega. USB-salvestuskandjate kasutamist on väga raske takistada, kui USB-liidest kasutatakse teiste seadmete jaoks. Nii tarnitakse näiteks sülearvuteid, mille puhul saab hiire ühendamiseks ainult USB-liidest kasutada. Seetõttu ei ole enamikel juhtudel mõttekas kasutada“USB-lukku” või liidest muid mehhaanilisi meetmeid rakendades desaktiveerida.

Seetõttu tuleks liideste kasutamist operatsioonisüsteemi tasemel vastavaid õigusi andes või lisaprogrammide abil reguleerida. Alternatiivina võib kontrollida seadmete lisamist. Andmesalvestite ühendamisel väliste liidestega laaditakse sageli operatsioonisüsteemist draivereid või operatsioonisüsteemi tuuma mooduleid või luuakse sisestisi konfiguratsioonifailidesse (näit. Windows-Registry), mida on võimalik kindlaks teha. Pärast seda, kui muudatused on tuvastatud, võib selle kohta näiteks protokollfaili koostada või sellest administraatorit informeerida. Seda kõike saab teha siiski vaid lisatarkvara kasutades. Selleks on vaja kas enda poolt väljatöötatud süsteemi või väljastpoolt soetatud toodet.

Kontollküsimus:

- Kas USB-salvestuskandjatega ümberkäimiseks on kehtestatud reeglid?

M 4.201 Marsruuterite ja kommutaatorite turvaline lokaalne aluskonfiguratsioon

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: Administraator

Kõik marsruuteri ja kommutaatori konfiguratsioonitööd (vaata M 2.279 Marsruuterite ja kommutaatorite turvapoliitika koostamine *)* tuleb teha vastavalt punktile M 2.281 Marsruuterite ja kommutaatorite süsteemikonfiguratsiooni dokumenteerimine ja vastavalt sellele ka dokumenteerida ja kommenteerida.

Operatsioonisüsteem
Kuna marsruuterid ja kommutaatorid omavad võrgus suurel hulga kommunikatsioonipartnereid ja seega ka ründajaid, tuleb operatsioonisüsteemi valikul, sisseseadmisel ja hooldamisel olla eriti hoolikas. Esmalt on oluline saada ülevaade vajalikest ja pakutavatest funktsioonidest. Valiku eesmärk peaks olema võimalikult stabiilse versiooni kasutamine. Siinkohal tuleb jälgida, et versiooni vanusega suureneb tavaliselt ka rünnakuvõimaluste arv (vallutatavus). Samas võib väga uus versioon (eriti uute funktsioonidega) töötada ebausaldusväärselt ja vigadega. Kahtluse korral on enamasti targem kasutada vanemat versiooni, loomulikult juhul, kui see vastab veel nõudmistele. Vanemale versioonile tuleb aga paigaldada uusimad turvapaigad (vt M 2.273 Turvalisust mõjutavate paikade ja värskenduste kiire paigaldamine). Versioone, millele enam turvapaiku ei toodeta, ei tohiks enam kasutusele võtta.

Offline -aluskonfiguratsioon
Enne kui marsruuter või kommutaator ühendatakse tootmisvõrku, tuleb luua turvaline aluskonfiguratsioon. Paljud seadmed väljastatakse tootja poolt vaikimisi seadistusega, mis võimaldavad selle eelkõige kiirelt tööle seadistada võimalikult paljude funktsioonidega ja peaaegu ühegi turvameetmeta. Seetõttu peab vaikimisi seadete kontrollimine ja aluskonfigureerimine toimuma väljaspool võrku või selleks vastavalt sisseseatud eriti turvalises testvõrgus. Tihti on võimalik koostada konfiguratsioone haldusarvutis vastavate programmide abil ja näiteks mälukaardiga vastavale seadmele kanda. Kui kas või üks ülekanne on võrgus võimalik, tuleb see teostada testvõrgus või administratsioonivõrgus. Konfiguratsiooni juures tuleb jälgida, et kõik haldus- ja konfiguratsioonitööriistad (konsool, veebiliides, välised konfiguratsiooniprogrammid) ei kuva kogu vajalikku informatsiooni. Võib juhtuda, et süsteemikäsk marsruuteri ja kommutaatori konfiguratsiooni kuvamiseks ei näita kõiki seadistusi. Seetõttu on oluline olemasoleva dokumentatsiooni alusel kontrollida, et kõik vajalikud seadistused oleks teostatud. Kasuks tuleb aluskonfiguratsiooni jaotamine kahte ossa:

- lokaalne konfiguratsioon: kontrollida tuleb konfiguratsiooniparameetreid, mis puudutavad seadet ennast (näiteks kasutajakontod või kasutajaõigused, pa-

roolid, protokolliandmed, konsooli ligipääsu seadistused ja jadaliidesed jne). Vastavaid samme on kirjeldatud allpool.
- võrgukonfiguratsioon: kontrollida tuleb konfiguratsiooniparameetreid, mis puudutavad seadme funktsioone võrgus (näiteks teenused ja protokollid, pääsuloendi *ACL* loomine, *VLAN* -id jne). Vastavaid samme on kirjeldatud punktis M 4.202 Marsruuterite ja kommutaatorite turvaline võrguaaluskonfiguratsioon .

Kasutajakontod ja paroolid

Võimalused kasutajakontode loomiseks ja õiguste jagamiseks on tootjati erinevad (mõnikord on suured erinevused ka erinevatel seadmete või tarkvaraversioonide vahel). Seetõttu on aktiivsete võrguosade haldamiseks soovitatav luua iga seadme jaoks vastav detailne kavand, mis lähtub etteantud õiguste kavandist. Mõningate tootjate (näiteks *Cisco*) marsruuteritel ja kommutaatoritel on seadmete haldamiseks juba tootja poolt loodud erinevate õigusastmetega kasutajakontod. Teised seadmed omavad haldamiseks ainult ühte kasutajakontot, mis on tootja poolt eelnevalt paigaldatud. Eelseadistatud kasutajakontodel on enamasti tuntud standardnimed ja paroolid. Mõningatel juhtudel on halduskonto seadistatud üldse ilma paroolita. Vastavatelt veebilehtedelt saab tootjaomaseid standardkontosid ja paroole alla laadida. Seadme kasutuselevõtul tuleks neid standardkontosid võimalusel muuta. Igal juhul tuleb muuta standardkonto paroolid. Mittekasutatavad kasutajakontod tuleb deaktiveerida. Pärast seda tuleb vastavalt õiguste kavandile luua ettenähtud kasutajakontod ja määrata nende õigused. Kahjuks salvestatakse paljude aktiivsete võrguosade paroolid avatekstina konfiguratsioonifaili. Juhul kui see on nii, tuleb konfiguratsioonifaile eriliselt kaitsta volitamata ligipääsu eest. Kus on võimalik, tuleb paroolid krüpteerida. Edasisi aspekte on kirjeldatud punktides M 1.43 Võrgu aktiivkomponentide turvaline paigutus , M 4.204 Marsruuterite ja kommutaatorite turvaline haldus ja M 6.91 Marsruuterite ja kommutaatorite andmete varundus ja taaste .

Sisselogimisaken

Sisselogimisel näitab enamik seadmeid üsna põhjalikku sisselogimisakent. See aken sisaldab tihtipeale informatsiooni, mis võib ründajale kasulik olla (näiteks mudeli- või versiooninumber, tarkvara versioon või turvapaikade tase). Kui seade võimaldab, tuleks sisselogimisaken asendada sobitatud versiooniga, mis eelnevalt mainitud informatsiooni ei sisaldaks. Aken ei tohi mingil juhul sisaldada seadme mudeli- ja versiooninumbrit ega operatsioonisüsteemi versiooni. Sisselogimisel tuleks kuvada järgnevat informatsiooni:

- Igasugune ligipääs on lubatud ainult volitatud isikutele.
- Kõiki töid tehakse vastavalt turvanõuetele.
- Seade on ühendatud kesksete kontrollmehhanismidega, nagu näiteks võrguhaldussüsteem (NMS), mis tuvastab ja protokollib turvanõuete rikkumised.
- Turvanõuete rikkumisi karistatakse distsiplinaarselt või karistusseadustiku alusel.

Protokollimine

Võrguosadele protokollimisest tulenevad turvameetmed ja ajainformatsiooni sidumine *NTP* abiga on kirjeldatud punktis M 4.205 Marsruuterite ja kommutaatorite töö logimine .

Liidesed

Marsruuteri mittekasutatavad liidesed tuleb deaktiveerida. Kõik mitte kasutuses olevad kommutaatorite pordid tuleb kas deaktiveerida või paigutada selleks loodud kinnistamata *VLAN* -i.

Konfiguratsiooni varundamine

Aluskonfiguratsiooni konfiguratsioonifail moodustab kogu järgneva konfiguratsiooni baasi. Nii seadme vaikeseadistusest kui ka failidest, mis on saadud aluskonfiguratsiooni tulemusel, tuleks teha varunduskoopia. Konfiguratsioonifailide varundamist kirjeldatakse lähemalt punktis M 6.91 Marsruuterite ja kommutaatorite andmete varundus ja taaste .

Täiendavad kontrollküsimused:

- Kas seadistamine toimus turvareegleid järgides?
- Kuidas loodi õiguste kavand marsruuteri ja kommutaatori kasutajakontodel?
- Kuidas näeb välja seadme sisselogimisaken?

M 4.202 Marsruuterite ja kommutaatorite turvaline võrgu-aluskonfiguratsioon

Algatamise eest vastutavad: IT-turvanõunik, IT-juht
Rakendamise eest vastutavad: Administraator

Kaugpöördus

Aktiivsete võrguosade haldamiseks läbi võrgu kasutatakse standardvõimalusena tihti *Telnet* 'i. Tihtipeale on olemas haldusvõimalus ka *SNMP*- või *HTTP* -liidese kaudu. Kõigi nende protokollide puuduseks on asjaolu, et nii kasutajanimed ja paroolid kui ka kasulikud andmed kantakse võrgus üle avatekstina (vaata G 2.87 Ebaturvalised protokollid avalikes võrkudes). Seetõttu tuleb halduseks kasutada kas eraldi haldusvõrku (*Out-of-Band-Management*) või tohib kasutada ainult protokolle (näiteks *ssh2*), mis toetavad turvatud autentimist ja krüpteeritud andmeedastust. Kui *SNMP* -d soovitakse kasutada väljaspool haldusvõrku, tohib kasutada ainult *SNMPv3*.

Autentimisserver

Suurtes võrkudes tuleks marsruuterid ja kommutaatorid konfigureerida autentimisserverite kasutamiseks nii, et kasutataks ühekordseid paroole. Sellekohased näited on RADIUS või TACACS+. Edasised aspektid on kirjeldatud punktis M 4.204 Marsruuterite ja kommutaatorite turvaline haldus .

Haldusliides ja haldusvõrk

Mõningad seadmed võimaldavad konfigureerida omaenda loogilist haldusliidest. Kommutaatorite korral tuleks sellele liidesele omistada oma *VLAN*, mida kasutatakse ainult halduseesmärkidel (*Out-of-Band Management*) ja millega on ühendatud ainult haldusliidesed. Marsruuteritel ja kommutaatoritel tuleks pääsuloend (*ACL*) konfigureerida nii, et ligipääs haldusliidesest ja haldusjaamast oleks lubatud defineeritud protokollidega. Kõik mittevajalikud teenused tuleb haldusliideses deaktiveerida. Edasisi samme haldusvõrgu loomiseks (*Out-of-Band-Management*) leiab punktist M 4.204 Marsruuterite ja kommutaatorite turvaline haldus .

Ebavajalike võrguteenuste deaktiveerimine

Aktiivsete võrguosade tootjad panevad ennekõike rõhku komponentide võimalikult lihtsale kasutuselevõtule ja konfigureerimisele. Seetõttu on vaikeseadistustes tihtipeale aktiveeritud hulk teenuseid. Aktiveeritud peaksid olema ainult seadme käitamiseks vajalikud teenused. Mittevajalikud teenused tuleb marsruuteritel ja kommutaatoritel välja lülitada, kuna need kujutavad endast kõrgendatud riski. Seadistused järgnevates tabelites näidatud teenustele kehtivad tihti kogu süsteemile ja mitte ainult üksikutele seadme liidestele/portidele. Reeglina ei tohi need teenused olla ebakindlatest võrkudest kättesaadavad. Seda tuleb kindlustada vastavate pääsuloenditega (Access Control List). Järgnevas tabelis on toodud osa teenuseid, mida võib tihti aktiivsetelt võrguosadelt leida. Iga teenuse juures

on soovitus, kuidas vastava teenusega tavaliselt käituda.

Teenus	Kirjeldus
FINGER	Teenus *Finger* näitab hetkel seadme sisselogitud kasutajaid. See ei oma praktilist väärtust ning tuleks seega deaktiveerida.
BOOTP	Mõningad marsruuterid ja kommutaatorid toetavad BOOTP-i (*Bootstrap-Protocol*) nii serverina kui ka kliendina. Sellega on teistel komponentidel võimalik sellelt seadmelt buutida. BOOTP ei oma ühtegi funktsiooni autentimiseks ega krüpteerimiseks ja tuleks deaktiveerida.
HTTP	Suurt hulka marsruutereid ja kommutaatoreid on võimalik hallata *HTTP* kaudu. See teenus tuleks avalikes võrkudes deaktiveerida ja võtta kasutusele ainult eraldatud haldusvõrkudes .
SNMP	*SNMP* on haldus- ja võrguhaldusprotokoll. Kuni versioonini *SNMPv2* (kaasa arvatud) ei ole turvafunktsioonid piisavad. *SNMPv3* omab tugevamaid autentimis- ja krüpteerimissuvandeid. Seda süsteemi tuleks võimalusel kasutada ainult eraldatud haldusvõrgus. *SNMPv1* ja *SNMPv2* ei tohi mitte mingil juhul olla kasutatavad väljaspool eraldatud haldusvõrke.
TELNET	*Telnet'* i kasutatakse tihti marsruuterite ja kommutaatorite standardse haldusliidesena. See teenus tuleb asendada SSH-ga (vaata all). Avalikes võrkudes ei tohi *Telnet* 'i aktiivsete võrguosade haldamiseks kasutada.

NTP	Võrguaja protokoll (*Network Time Protocol*) *NTP* on kasutuses süsteemiaja sünkroniseerimiseks. Mõningad marsruuterid ja kommutaatorid võivad toimida teistele seadmetele ajaserverina. *NTP* ei oma turvafunktsioone ja ei tohiks seega olla kasutatav avalikes võrkudes. Tuleks installeerida võrgusisene *NTP* server, millele pääsetakse ligi haldusvõrgu kaudu.
DNS	Mõned marsruuterid ja kommutaatorid toetavad nimede kustutamiseks *DNS* -teenust, näiteks seoses protokollimisega. Nimede kustutamine ei ole aktiivsete võrguosade juures tavaliselt vajalik ja ei paku ka erilist kaitset. Seetõttu tuleks *DNS* deaktiveerida.
CDP	*CDP* on *Cisco* marsruuterite ja kommutaatorite vaheline teise kihi (*Layer 2*) litsentsitud protokoll. Vähemalt lõppseadmete portidel tuleks see deaktiveerida.
TFTP	Mõningad marsruuterid ja kommutaatorid võimaldavad buutimist *TFTP* -serverilt. *TFTP* ei paku turvamehhanisme. Seda funktsiooni tuleks kasutada ainult juhul kui *TFTP* -server on installeeritud eraldatud haldusvõrku.
SSH1	*SSH1* on *Secure Shell* protokolli vananenud variant, millel on turvaaugud. Seda ei tohiks seetõttu kasutada. Kui seade ei paku muud varianti kui *SSH1* , võib ligipääs toimuda ainult eraldatud haldusvõrgu kaudu.
SSH2	*SSH2* on turvaline asendus *Telnet'* ile, mida saab avalikes võrkudes kasutada marsruuterite ja kommutaatorite haldamiseks. Ikkagi on soovitatav *SSH* ligipääs vastavate *ACL* -idega kindlustada.

Tabel: Aktiivsete võrguosade teenused

Lisaks tuleks järgnevate seadistustega arvestada esmajoones marsruuterite liidestel avalikes võrkudes, aga ka kommutaatorite liidestel.

Siinkohal ei saa aga üldiseid käitumisjuhiseid anda, vaid jagatakse soovitusi

erinevateks aspektideks. Kui kindlatel juhtudel nendest soovitustest kõrvale kaldutakse, peaks alati teada olema, miks seda tehakse.

Teenus	Kirjeldus, seadistus
IP source routing	See funktsioon lubab IP-paketil sihti viivad marsruuterid ette määrata. Seda funktsiooni saab kasutada erinevat sorti rünnakute jaoks. Seetõttu tuleks see funktsioon deaktiveerida.
IP directed broadcast	Seda funktsiooni saab kasutada *DOS* -rünnakuteks. Seetõttu tuleks see funktsioon deaktiveerida.
ICMP redirects	*ICMP* -funktsiooni saab kasutada informatsiooni saamiseks võrkude kaudu. Seetõttu tuleb see funktsioon vähemalt marsruuterite võrguvälistes liidestes deaktiveerida.
ICMP unreachable notifications	*ICMP* -funktsiooni saab kasutada informatsiooni saamiseks võrkude kaudu. Seetõttu tuleb see funktsioon vähemalt marsruuterite võrguvälistes liidestes deaktiveerida.
ICMP mask reply	*ICMP* -funktsiooni saab kasutada informatsiooni saamiseks võrkude kaudu. Seetõttu tuleb see funktsioon vähemalt marsruuterite võrguvälistes liidestes deaktiveerida.

Tabel: Teenuste seadistamine

Aadressi võltsimise vältimine

Servamarsruuterid (*edge router*) moodustavad ülemineku sisevõrgust välisvõrku. Servamarsruuteritel tuleks sisse seada turvameetmed, mis takistavad *IP* -aadressi võltsimise (vt G 5.48 IP-aadressi võltsimine). *IP*- aadressi võltsimist saab takistada näiteks vastava pääsuloendi (*ACL*) sisseseadmisega. Üks võimalik näide on järgnev meetod:

- Võrguvälise liidese juures blokeeritakse sellised paketid, mille saatja *IP* -aadress asub sisevõrgus.
- Sisevõrgu liidese juures blokeeritakse sellised paketid, mille saatja *IP* -aadress ei asu sisevõrgus.

Vähemal teise meetodiga blokeeritud pakettide puhul on vajalik protokollimine ja vajadusel vastutava süsteemihaldaja teavitamine. Asjaolu, et üks sisevõrgu osa saadab võltsitud pakette, on juba selge märk sellest, et tegemist on kas konfiguratsiooniveaga või isegi turvaprobleemiga.

Loopback -liides

Mõningad marsruuteri mudelid (näiteks *Cisco* marsruuterid) pakuvad *Loopback*-liidese sisseseadmise võimalust. *Loopback*- liidesele määratud *IP* -aadressi saab marsruuter kasutada *Syslog*- i, *NTP* -protokollide või tähtsate haldusteenuste lähteaadressina. Sellega on võimalik saavutada marsruuteri parem turvalisus, kuna *IP* -paketti lähteaadressiks on alati *Loopback*- liidese *IP* -aadress.

Marsruutimise protokollid

Kasutada tuleks ainult marsruutimisprotokolle, mis võimaldavad krüpteeritud autentimist. Demilitariseeritud tsoonides ei tohi kasutada dünaamilisi marsruutimisprotokolle, vaid sisse tuleb seada staatilised marsruuterid. Marsruutimisprotokollide kasutamine tuleks lisaks kindlustada pääsuloendi (*ACL*) sisseseadmisega (vt M 5.112 Marsruutimisprotokollide turvaaspektide arvestamine).

Pääsuloend (*Access Control Lists*)

Pääsuloendi (ACL) kasutamist marsruuteritele ligipääsu piiramiseks ja pakettide filtreerimiseks kogu võrgus on kirjeldatud meetmes M 5.112 Marsruutimisprotokollide turvaaspektide arvestamine .

Täispuu

Täispuu protokolli (*Spanning Tree Protocol*) (*STP*, *IEEE 802.1d*) kasutavad kommutaatorid ja sillad (*Bridges*) selleks, et vältida võrgusiseste silmuste tekkimist *OSI* teisel kihil. Välja saadetakse *BPDU* -d (*Bridge Protocol Data Units*), mis määravad süsteemistardi juursilla (*Root-Bridge*) (*MAC* -aadressil ja prioriteedil põhinevalt) ja topograafilised muudatused. See protokoll ei võimalda autentimist. Vähemalt lõppseadmete portidel tuleks *STP* deaktiveerida. Konfiguratsioonis peab olema kindlalt määratletud juursild (*Roto-Bridge*).

Virtuaalkohtvõrk ja *trunking*

Trunking võimaldab *VLAN* -i laiendamist üle mitme kommutaatori. *Trunking'u* juhtimine realiseeritakse standardi *IEEE 802.1q* või erinevate piiratud *trunking* -protokollide kaudu. Seejuures reserveeritakse kommutaatorite vaheliseks kommunikatsiooniks üks füüsiline port (magistraalport). Seda loogilist ühendust kommutaatorite vahel nimetatakse magistraaliks (*Trunk*). Magistraalpordid (*Trunk Ports*) pääsevad kõigile *VLAN* -idele ligi. See tähendab, et ligipääs ühele magistraalpordile võimaldab ligipääsu selle magistraali (*Trunk*) kõigile *VLAN* -idele. Mõningad

seadmed pakuvad ka võimalust ühe magistraalpordi ligipääsu kindlatele *VLAN* -idele piirata („ *VLAN Pruning* “). Kui kommutaator sellist seadistust võimaldab, siis tuleks seda ka kasutada. Lõppseadmete portidel tuleks *trunking* deaktiveerida. Vaikeseadistusega *VLAN* -i ei tohi kasutada tootmis- *VLAN* -ina. Kasutades Cisco autoriõigustega kaitstud *VTP* (*VLAN Trunking Protocol*) protokolli, tuleks kasutada ka *VTP* poolt toetatavat autentimist.

Vabad pordid

Mittekasutatavatele portidele tuleks sisse seada eraldi *VLAN* (kinnistamata *VLAN*). Võimalusel tuleks mittekasutatavad pordid deaktiveerida, kuna *VLAN* pordi määramine pakub ainult vähesel määral lisakaitset. Kui soovitakse kindlad pordid erinevate seadmete ühendamiseks vabaks jätta, tuleks vastavatele portidele paigaldada kaitse, mis alles pärast sisselogimist võimaldab ligipääsu võrgule. Sellise ligipääsukaitse saab paigaldada näiteks *IEEE 802.1x* standardi abil. Tänaseks kasutavad 802.1x standardit juba paljud kommutaatorid ja enamus arvutite operatsioonisüsteeme. Peale selle esineb veel rida autoriõigustega kaitstud lahendusi, mille korral lõppseadmed kas *MAC* -aadressi põhjal või teiste mehhanismide abil autenditakse aktiivsete võrguosade suhtes enne, kui ligipääs võrgule avatakse.

Täiendavad kontrollküsimused:

- Milliseid teenuseid ja protokolle kasutatakse administreerimiseks/haldamiseks?
- Kas mittekasutatavad teenused ja protokollid on deaktiveeritud?
- Kas loodi eraldatud administratsioonivõrk?

M 4.203 Marsruuterite ja kommutaatorite konfigureerimise kontroll-loend

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: Administraator

Järgneva konfiguratsiooni kontroll-loendi alusel on võimalik kontrollida marsruuterite ja kommutaatorite tähtsamaid turvalisust mõjutavaid seadistusi. Siinkohal tuleb aga silmas pidada ka asjaolu, et marsruuterite ja kommutaatorite konfiguratsioon sõltub paljuski nende kasutustingimustest. Näiteks tuleb servamarsruuterite korral arvestada *ACL* -i, *IP* -aadressi võltsimise vastase konfiguratsiooni ja muu taolise seadistamisega. Seetõttu tuleks järgnevat tabelit kasutada ainult juhisena. Turvameetmeid, mis kehtivad marsruuteritel, tuleb kasutada ka kommutaatoritel, mis toetavad marsruutimisfunktsioone ja kasutavad neid.

Marsruuterite ja kommutaatorite konfigureerimise kontroll-loend

Marsruuteri ja kommutaatori turvadirektiivide loomine
Operatsioonisüsteemi kontrollimine ja vajadusel uuendamine
Marsruuteri ja kommutaatori konfiguratsioonid tuleb salvestada väljaspool võrku, varundada ja kaitsta volitamata ligipääsu eest (*TFTP* -serveri kasutamine ainult koos *Out-of-Band-Management'* iga (eraldi haldusvõrk)).
Konfiguratsiooni dokumentatsioon ja kommentaarid
Paroolide konfigureerimine kõigile ligipääsudele (konsool, *VTY* , jne)
Seansi aegumise sisseseadmine
Ärge kasutage triviaalseid paroole
Paroolide krüpteeritud salvestamine
Konsooliühenduse füüsilise ligipääsukaitse sisseseadmine
Süsteemi haldamiseks tuleb *TELNET* asendada *SSH* -ga
Autentimiseks kasutada kas *RADIUS* -t või *TACACS+*
Haldusligipääsude piiramine (näiteks *SSH* , *SNMP* , *TELNET*) *ACL* -i kaudu, *SNMP* ja *TELNET* -i kasutamine ainult koos *Out-of-Band-Management* 'iga (eraldi haldusvõrk), SNMP korral tuleb muuta *Community-Strings* 'e
Ebavajalike võrguteenuste deaktiveerimine
Marsruuterite mittevajalikud liidesed tuleb välja lülitada, kommutaatorite mittevajalikud pordid tuleb asetada kinnistamata *VLAN* -i või samuti deaktiveerida.
Kriitilised liidesed ja protokollid tuleb blokeerida
Lülitage protokollimine sisse
Seadetel tuleb sisestada täpne kellaaeg (võrgusisene *NTP* -server)
Ajainformatsiooni sidumine protokollimisega
Protokollimisandmete analüüs, kontroll ja varundus peavad lähtuma turvadirektiividest

SNMP tuleb võimalusel deaktiveerida, kasutada võib seda ainult koos *Out-of-Band-Management* 'iga (haldusvõrk) või kasutades *SNMPv3*
Vaikeseadistuse kontroll
Sisselogimisakna sisseseadmine
CDP deaktiveerimine lõppseadmete portides
Spetsiaalselt kommutaatoritele:
VTP -d kasutades: kasutage autentimist
Trunk-Negotiation 'i deaktiveerimine lõppseadmete portides
Vaikimisi *VLAN* -i kasutamine on keelatud
Eraldi *VLAN* -i sisseseadmine kõikidele magistraalportidele
Kinnistamata- *VLAN* -i sisseseadmine kasutuses mitteolevatele portidele
STP (*Spanning Tree* / täispuu) deaktiveerimine lõppseadme portides
Juursilla (*Root-Bridge*) kindlaksmääramine
Spetsiaalselt marsruuteritele:
Ülevõrgulise andmevoolu kommunikatsioonimaatriksi loomine
Ligipääsuloendite kaudu ülevõrgulise andmevoolu piiramine, ühtlustades seda kommunikatsioonimaatriksiga
Tundmatute aadresside blokeerimine pääsuloenditega (ACL)
Kui vajalik (eriti demilitariseeritud tsoonis): turvaliste marsruuterite konfiguratsioon
Marsruutimisprotokollide terviklusmehhanismide konfiguratsioon

---

Täiendav kontrollküsimus:

- Kas pärast komponentide sisseseadmist võeti kontroll-loendi alusel ette seadistuste kontroll?

M 4.204 Marsruuterite ja kommutaatorite turvaline haldus

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: Administraator

Marsruuterite ja kommutaatorite haldamiseks on erinevaid ligipääsuvõimalusi. Sõltuvalt ligipääsumeetodist tuleb luua mitmeid turvameetmeid. Suuremate võrkude puhul on soovitatav marsruuterid ja kommutaatorid siduda kesksesse võrguhaldussüsteemi, kuna vastasel juhul ei ole võimalik garanteerida turvalist ja efektiivset haldust. Süsteemihalduseks kasutatud meetodid tuleks määrata turvajuhendis ja haldustegevus tohib toimuda ainult sellest juhendist lähtuvalt. Kõik mittekasutatavad haldusliidesed tuleks deaktiveerida. Järgnevalt kirjeldatakse mõningaid punkte, mida peaks haldamise juures järgima. Lisaks tuleks haldusligipääsu piiramiseks sisse seada pääsuloend (*ACL*) (vt M 5.111 Marsruuterite pääsuloendite konfigureerimine).

Kaughaldus

Suur osa aktiivseid võrguosasid võimaldab *Telnet* 'i kaudu kasutada kaughaldust. *Telnet* 'i kasutamise ohuks on aga asjaolu, et kõik autentimisandmed, kaasaarvatud kasutajanimed ja paroolid, edastatakse avatekstprotokollina, mis võimaldab nuhkida ja andmesidet lugeda (vt G 2.87 Ebaturvalised protokollid avalikes võrkudes). Tihti kasutatakse kaughalduseks *SNMP* -d. *SNMPv1* ja *SNMPv2* ei paku samuti piisavat kaitset ühenduse kindlustamiseks. Alles *SNMPv3* pakub turvamehhanisme, mis võimaldab kasutuse ka väljaspool turvatud haldusvõrke. Marsruuterite ja kommutaatorite kaughalduse korral peab igal juhul sidet turvama. Seda saab saavutada näiteks *SSH* kasutamisel *Telnet* 'i asemel (vaata M 5.64 Secure Shell (SSH)) või eraldi *LAN* -segmentide loomise kaudu, mida kasutatakse ainult halduseesmärkidel. Mitte mingil juhul ei tohi kaughaldus toimuda (ebaturvaliste) välisvõrkude kaudu. Sellega tuleb arvestada juba turvajuhiste kindlaksmääramisel. Ka sisevõrgus tuleb ebaturvalisi protokolle kasutada nii vähe kui võimalik.

Veebiserver

Paljud seadmed võimaldavad teha haldustöid *HTTP* abil brauseri liidese kaudu. Marsruuteril või kommutaatoril on käivitatud *HTTP* -server ja ligipääs toimub suvalise veebibrauser klientprogrammi kaudu. Veebiserveri ligipääsuseadistused ei ole kõikide tootjate puhul ühtsed. Ideaaljuhul peaks ligipääs olema vaikeseadistustes deaktiveeritud. Samas on võimalik seda teenust kasutada kaitseta ja kasutajainformatsiooni sisestamata. Seda tuleb seadme kasutusele võtmisel kontrollida ja vastaval juhul tuleb konfiguratsiooni muuta. Nagu ka *Telnet* 'i korral edastatakse *HTTP* -s kasutajanimed ja paroolid avatekstina. Peale selle on teada hulk rünnakuid, mis kasutavad erinevate tootjate *HTTP* -serverite nõrku kohti. Seetõttu on soovitatav *HTTP* -teenust süsteemihalduseks mitte kasutada. *HTTP* -server tuleks võimaluse korral süsteemi esmase konfiguratsiooni ajal deaktiveerida. Erand on lubatud juhul kui ligipääs toimub eraldatud haldusvõrgu kaudu. Mõningad seadmed pakuvad lisaks *HTTP* -le võimalust ka üle *HTTPS* -i veebiliidesele ligi pääseda. Kui selline võimalus esineb, tuleks eelistada *HTTPS* -i *HTTP* -le. Kasutades veebiliidest tuleb tähele panna, et kõik konfiguratsioonivõimalused ei ole sel moel

ligi pääsetavad.

Haldusvõrk (*Out-of-Band-Management*)

Vähendamaks kaughalduse riske, pakuvad mõningad seadmed võimalust luua süsteemihalduseks loogiline port (haldusliides). Kommutaatorite korral tuleks sellele pordile omistada oma *VLAN*, mida kasutatakse ainult halduseesmärkidel (*Out-of-Band Management*) ja millega on ühendatud ainult haldusliidesed. Haldusvõrk tuleks teistest võrkudest täielikult eraldada. Seeläbi kompenseeritakse protokollide nagu *Telnet* või vananenud *SNMP* variantide puudujäägid nagu näiteks sisselogimisinformatsiooni krüpteerimata edastamine. Pääsuloendid (ACL) tuleb konfigureerida sedasi, et ligipääs haldusliidesele ja haldusjaamale oleks lubatud. Kõik mittevajalikud teenused tuleb haldusliidese jaoks deaktiveerida.

Võrguhaldussüsteemid

Aktiivsed võrguosad seotakse tavaliselt keskse võrguhaldussüsteemiga. Lisaks eelnevatele lõikudele tuleb siinjuures järgida ka turvanõudeid, mis on märgitud punktis B 4.2 Võrgu- ja süsteemihaldus .

Keskne autentimisserver

Seadmel konfigureeritava lokaalse ligipääsu ja õiguskontrolli asemel saab seda teostada ka kesksel serveril. Suurte võrkude puhul, millel on suur hulk aktiivseid võrguosi, tasub lokaalne konfiguratsioon end ainult osaliselt ära. Halduseks ja paljude paralleelsete õiguste hooldamiseks vajaminevad ressursid on sel juhul väga suured. Kesksel serveril seevastu hallatakse kõik ligipääsud ja õigused ühtselt. Oluline informatsioon ei ole enam salvestatud seadmetel endil ja neid ei ole vaja enam ükshaaval hooldada. Kogu informatsioon on krüpteeritult ühes andmepangas ja nii on neid võimalik ülevaatlikult hallata. Selline server pakub lisaks ka laiendatud protokollimisvõimalusi, näiteks on võimalik dokumenteerida sisselogimise ja ligipääsude arv ja aeg ning edastatud andmemahud. Näideteks on siinkohal RADIUS ja TACACS+ (*Terminal Access Controller Access Control System*). Paljude aktiivsete võrguosadega komplekssetes võrkudes tuleks autentimine kindlustada keskse autentimisserveri kaudu. Juhul kui autentimisserverit ei ole võimalk kasutada (näiteks serveri rikke või võrguprobleemide korral), tuleks siiski konfigureerida lokaalne ligipääs. See tuleb kindlustada ainult selleks otstarbeks loodud parooliga. Lokaalsete ligipääsude korral, mis ei loodud spetsiaalselt selle jaoks, et autentimisserverit ei ole võimalik kasutada, tuleks autentimisserverit ikkagi kasutada, kuna vastasel juhul pääsevad kasutajad, kes lokaalselt sisse logivad, autentimisest ja järelvalvest mööda.

Õiguste haldamine kasutajakontode ja süsteemikäskluste jaoks

Õiguste haldamine võib vastavalt tootjale toimuda erinevatel tasanditel ja erinevate teralisuse astmetega (*Granularity*). Süsteemikäskluste õiguste haldamisel, mis võivad olla ligipääsetavad ainult kindlatele kasutajatele või gruppidele, võib need võtta kokku ühel õigustasandil. See on juba näiteks *Cisco* poolt konfigureeritud kahele astmele:

- Süsteemikäskluste liigitamine vastavalt õigusastmetele.
- Kasutajakontode liigitamine vastavalt õigusastmetele.

Ligipääsu õigusastmele kaitstakse parooliga. Kasutaja peab vastavale süsteemikäsklusele ligi pääsemiseks esmalt vahetama õigusastme ja sisestama selle juurde kuuluva parooli. Siis saab ta kõiki sellele astmele määratud käsklusi käivitada. Kasutajakontodele õiguste jagamine toimub seeläbi, et kasutajale määratakse õigusaste. Peaks kehtima põhimõte, et kasutajale jagatakse töö sooritamiseks minimaalselt vajalikud õigused. Nii on võimalik määratleda erinevaid rolle:

- Kirjutuskaitsega konto, mis võimaldab vaadata seadme seadistusi. Konfiguratsiooni muutmine ei ole võimalik.
- Lugemis-kirjutamiskonto võimaldab enamiku seadmete seadistuste muutmist ja vaatamist. Turva- ja parooliseadistused siia hulka ei kuulu.
- Kõikehõlmav lugemis-kirjutamiskonto on ette nähtud laialdaseks kontrolliks, mis hõlmab turvaseadeid, ligipääsuparoole ja veebil põhinevat haldusligipääsu.
- Lisaks on võimalikud spetsiaalsed kontod teise ja kolmanda kihi (*Layer-2* ja *Layer-3*) funktsioonide haldamiseks.

Kasutaja on pärast seadmele sisselogimist paigutatud automaatselt ühte õigusastmesse, alternatiivse võimalusena peab kasutaja pärast sisselogimist eraldi sisestama nii kasutatava õigusastme kui ka parooli. Turvakriitiliste rollide jaoks tuleks sisse seada ligipääsu kaitse keskse autentimisserveri kaudu.

Kasutajate ja rollide õiguste määramise võimalused lähevad isegi nii kaugele, et igale üksikule käsklusele on võimalik jagada õigused, mida iga kord enne täitmist autentimisserveri poolt kontrollitakse. Aktiivsete võrguosade haldamise õiguskavandite loomisel tuleb arvestada süsteemi eri osade võimalustega. Millisel määral erinevad õigusastmed üksteisest erinevad, peaks sõltuma kasutusalast ja turbevajadusest. Rusikareegliks võiks olla „Nii keerukas kui vajalik, nii lihtne kui võimalik“. Liiga lihtne jaotus ei paku piisavat turvalisust, samas liiga keerukas jaotus võib mõjutada töö efektiivsust ja tuua kaasa vigade tekkimise.

Parooli krüpteerimine

Marsruuterid ja kommutaatorid peaksid toetama võimalust paigutada krüpteeritud paroole konfiguratsioonifaili (vt M 2.280 Sobivate marsruuterite ja kommutaatorite ostmis- ja valimiskriteeriumid). *Cisco* seadmete puhul võimaldab selle käsk *enable secret.* Paroolide krüpteerimine on oluline konfiguratsioonifaili saatmisel võrgu kaudu või kesksele serverile salvestamisel. Kui seade võimaldab parooli krüpteerimist, siis tuleks seda ka kindlasti kasutada. Siinkohal tuleks arvestada ka krüpteerimismeetodiga, kuna mõningad seadmed kasutavad erinevaid meetodeid. Eriti vanemate operatsioonisüsteemide korral kasutatakse veel nõrku krüpteerimismeetodeid, mida uuemad versioonid võivad veel toetada. Siinkohal tuleks uuemale seadmele või operatsioonisüsteemile üleminekul kontrollida,

kas uus versioon võimaldab tugevamat krüpteerimist. Lisaks esineb kõigi seadmete jaoks protseduure, mis ei võimalda küll krüpteeritud paroolide dekrüpteerimist, aga võimaldavad paroolide lähtestamist. Mõningaid teenuseid ei ole võimalik parooli krüpteerimise kaudu kaitsta. Siia hulka kuuluvad *SNMPv1*, *SNMPv2*, *RADIUS* ja *TACACS+*. Viimatinimetatud teenuste paroolid peaksid seega olema alati ainulaadsed, ei tohiks olla kasutatavad mitte ühegi teise teenuse korral ja paroole tuleks kindla aja tagant muuta. Kui üldse, siis tuleks *SNMPv1* ja *SNMPv2* kasutada koos *Out-of-Band-Management* 'iga (vaata üleval: haldusvõrk) ja võimalusel asendada *SNMPv3* -ga.

Seanssi aegumine

Kõiki ligipääsuvõimalusi on võimalik paroolidega kaitsta. See meetod võib osutuda aga kasutuks, kui seansid jäävad järelvalveta, näiteks kui sisselogitud administraator lahkub oma arvuti tagant ja unustab seansi lõpetada või ekraanikaitse aktiveerida. Sellest lähtuvalt on soovitatav sisse seada seansi aegumisajad, mis pärast määratud aega, kui kasutaja ei ole arvutit kasutanud, kasutajakonto välja logib või lukustab. Seejuures ei tohiks seansi aegumise aeg olla seadistatud rohkem kui kümnele minutile.

Täiendavad kontrollküsimused:

- Kuidas hallatakse aktiivseid võrguosi?
- Kas süsteemihaldus toimub vastavalt turvajuhendile?
- Kas süsteemihalduse juures arvestatakse ülalnimetatud punktidega?

M 4.205 Marsruuterite ja kommutaatorite töö logimine

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: Administraator

Marsruuterid ja kommutaatorid pakuvad reeglina logimise võimalust. Nende informatsioonide analüüs aitab hinnata seadme õiget töötamist ja tuvastada rünnakukatsed. Logiinformatsiooni abiga saab ka rünnaku viisi välja selgitada ja sellest lähtuvalt konfiguratsiooni kohandada. Seetõttu tuleks logimine hoolikalt sisse seada ja seda kasutada. Hoolikas konfigureerimine on eriti oluline, kuna ainult mõtteka filtreerimise korral saab suure informatsioonihulga seest kätte vajaliku informatsiooni. Siiahulka kuuluvad eelkõige tagasilükatud ligipääsukatsed ja konfiguratsiooni muudatused. Kuna logiandmed sisaldavad isikuspetsiifilisi andmeid, tuleb kindlustada, et neid andmeid kasutatakse ainult andmekaitsekontrolliks, andmete varunduseks või nõuetekohase käitlemise kontrolliks (M 2.110 Andmeprivaatsuse suunised logimisprotseduurides). Logi maht ja analüüsi kriteeriumid tuleb dokumenteerida ja ettevõtte siseselt paika panna. Vajadusel tuleks kaasotsustusorganid juba varakult kaasata. Logida tuleks järgmised andmed:

- Konfiguratsioonimuudatused
- Taaskäivitused
- Süsteemivead
- Olekumuutused liidese, süsteemi ja võrguosa kaupa
- Sisselogimisvead (vähemalt siis, kui nad esinevad korduvalt)
- *ACL* -i reeglite vastu eksimine (tagasilükatud ligipääsukatsed)

Eriti viimane punkt peaks olema igas *ACL* -is aktiveeritud, et kõiki luhtunud katseid käsitleda ja valesid või valesti konfigureeritud reegleid ära tunda. Sõltuvalt tootjast ei ole mõningaid aspekte võimalik logimise kaudu tuvastada. Näiteks:

- Õiguste muutmine
- Paroolimuudatused
- *SNMP* kaudu tehtud muudatused
- Uue konfiguratsiooni salvestamine *NVRAM* -i

Sellisel juhul tuleks kaalutleda teiste võimaluste kasutamist, et vähemalt selgeks teha, kas on toimunud muudatusi. Tavaliselt on logitavad andmed erinevatest klassidest. See võimaldab logi filtreerimist vastavalt konfiguratsioonis määratud logiklassidele. Sobivate andmete salvestamise kõrval on väga oluline ka võimalikult kohene andmete analüüs. Selle tarvis esineb mitmeid väljundivõimalusi, mida vastavalt isiklikele vajadustele häälestades ka üksteisega koos kasutada saab.

Kasutajasessioon
Logiinformatsiooni saab näidata käimas olevas kasutajasessioonis. Selleks tuleb logimine ja seanss vastavalt konfigureerida.

Mälu
Logiinformatsiooni on võimalik salvestada süsteemi enda *RAM* -is. Selleks ettenähtud mälu maht sõltub tugevasti seadme kasutusalast ja tüübist, nii et siinkohal ei ole võimalik teha konkreetseid ettepanekuid. Logiinformatsiooni salvestamist kesksele serverile (*syslog*) tuleks eelistada *RAM* -ile salvestamisele.

SNMP
Sõltuvalt tootjast on marsruuteritel ja kommutaatoritel võimalik paljudele olukordadele luua *SNPM* -teated, mis olemasoleva võrguhaldussüsteemi poolt ära tuntakse, kuvatakse ja töödeldakse. See võimaldab automaatset analüüsimist.

Kuvamine konsoolis
Logi kuvamine konsoolis ei luba pikaajalist salvestamist ja on seega ainult täiendav meetod teistele meetoditele.

Keskne autentimisserver
Keskse autentimisserveri abiga (näiteks *TACACS+* või *RADIUS*) saab sinna paigutatud logi (*Accounting*) kasutada kasutajaaktiivsuse dokumenteerimiseks.

Syslog
Logiinformatsiooni saab võrgu kaudu kanda eraldi *syslog*- serverile (näiteks *Unix* 'i arvutil). Seda kasutatakse logiinformatsiooni keskseks kogumiseks ja arhiveerimiseks, kuna võrguosadel ei ole tihtipeale vajalikke osi selle teostamiseks. Sellest tulenevalt saab olulise informatsiooni keskses kohas kokku koguda ja analüüsida. Eeliseks on ka asjaolu, et seadme kompromiteerimisel ei ole ründajal juba üle kantud logiinformatsiooni võimalik muuta ega kustutada. Ülekanne *syslog*- serverile toimub enamasti krüpteerimata kas *TCP* või *UDP* kaudu, mistõttu on võimalik ülekande pealtkuulamine. Seetõttu on informatsiooni saatmine sisevõrgust ohtlik andmete konfidentsiaalsusele. Tuleks mõelda andmete ülekandmisele eraldi võrgu (haldusvõrk) kaudu.

NTP
Kogu logiinformatsioon tuleb märgistada korrektse ajatempliga. Ainult nii on võimalik kindlustada andmete efektiivne analüüs eriti üritatud või teostatud rünnakute korral. Sellest tulenevalt peaks sisevõrku olema sisse seatud server, mis varustab kõiki süsteeme õige süsteemiajaga. See võib toimuda näiteks *NTP* -teenusel põhjal. Peale selle tuleks kaalutleda sisevõrku eraldi ajaserveri paigutamist, mis asetseb näiteks eraldi arvutis, mis on varustatud raadiokellaga. Alternatiivina saab sobivat arvutit kasutada *NTP* -proksina ja ajainformatsiooni omakorda hankida *NTP* kaudu mõnelt Internetis paiknevalt ajaserverilt (näiteks metroloogiainstituu-

dist PTB). Kahtluse korral tuleks ja eriti suure turbevajadusega võrkudes kasutada esimest varianti (võrgusisene ajaserver, mis on varustatud raadiokellaga). Mitte mingil juhul ei tohiks kõik seadmed ise *NTP* kaudu esitada päringuid Internetis olevale ajaserverile.

Täiendavad kontrollküsimused:

- Kas turvajuhendis on kirjeldatud marsruuterite ja kommutaatorite logimise maht?
- Kuidas toimub marsruuterite ja kommutaatorite logimine?
- Kuidas toimub analüüs?
- Kas analüüsi juures arvestatakse ka andmekaitse aspektidega?
- Kuidas kindlustatakse kõigi seadmete õige süsteemiaeg?

M 4.206 Kommutaatori portide turvamine

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: Administraator

Sõltuvalt võrgu kaitsevajadusest soovitakse mõnikord, et ainult kindlad usaldusväärsed kliendid saaksid ligipääsu võrgule. Selleks pakuvad paljud kommutaatorid rea võimalusi, et isegi kui ründaja on saanud ligipääsu võrgupistikule, on võimalik ligipääs võrgule takistada.

MAC -aadressi teade
Paljud kommutaatorid võimaldavad pordi MAC-aadressi muutust protokollida. See suvand ei paku küll ligipääsukontrolli, aga võib samas olla abiks ründaja avastamisel. Näiteks saab administraatorile saata sõnumi, kui MAC-aadress peaks muutuma.

MAC - Locking
Kõige levinum viis kommutaatorite portide kaitseks on niinimetatud *MAC - Locking.* Seejuures määratakse kommutaatoris, et kindla füüsilise pordi puhul on lubatud ainult kindlad *MAC* -aadressid (erijuhtudel ainult üks *MAC* -aadress). Kui kommutaator saab *MAC* -aadressiga *Ethernet*- freimi, siis ei saadeta seda edasi võrku, vaid tühistatakse. Sedasi on „staatilistes“ võrkudes võimalik saavutada üpriski hea kaitse. Samas on vastavate tabelite hooldamine mahukas ja *MAC - Locking* ei paku kaitset ründaja eest, kes esmalt on välja uurinud lubatud MAC-aadressi ja oma seadme ühendamisel seda aadressi ka kasutab (vt G 5.113 MAC-aadresside võltsimine).

IEEE 802.1x

IEEE 802.1x standard (*EAPoL EAP over LAN*) määrab võimaluse seadmete autentimiseks autentimisserveri abiga (näiteks *RADIUS*). Autentimine toimub *EAP* (*xtensible Authentication Protocol*, *RFC 2284*) kaudu, mis pakub mitmeid erinevaid eritugevusega autentimisprotokolle (*EAP types*). Kasutamaks kliendi autentimist 802.1x kaudu, peab lõppseadmetel olema installeeritud vastav klientprogramm. Klientprogrammid erinevad üksteisest operatsioonisüsteemi toetuse ja autentimisprotokollide poolest. Ainuke autentimisprotokoll, mida kõik klientprogrammid toetama peavad, on *MD5 - Challange.* Kuna see protokoll ei paku väga tugevat kaitset, tuleks võimalusel kasutada teisi *EAP* tüüpe. Ligipääsukontroll 802.1x pakub kaitset *MAC* -aadresside võltsimise eest.

Teised meetodid
Sõltuvalt tootjast esineb teisi võimalusi, kuidas kommutaatori portide ligipääsukontrolli realiseerida. Näiteks on võimalus, et kasutaja registreerib ennast veebiliidese kaudu. Selle teostamiseks töötab kommutaatoril veebiserver, mis saadab sisestatud autentimisandmed edasi autentimisserverile. Siinkohal tuleb aga ka jälgida, et kommutaatoril paikneva veebiserveri tõttu võivad tekkida uued ohud. Seadmete puhul, mis toetavad *IEEE 802.1x* või teisi meetodeid ligipääsu

kontrolliks, on oluline ennetada vaikeolekut, milles port tavaliselt viibib. Olulised on järgmised võimalused:

Authentication off / Port on	Port on aktiveeritud ja autentimist ei toimu.
Authentication on / Port off	Port on nii kaua deaktiveeritud, kuni teostatakse edukas autentimine.
Authentication on / Port on with default policy	Port on aktiveeritud, aga niikaua, kui ei ole toimunud edukat autentimist, on lubatud ainult piiratud ligipääs. Piiranguteta ligipääs avatakse alles pärast edukat autentimist.

Tabel: Vaikeolek

Võrkudes, kus konfidentsiaalsusest lähtuvalt vajatakse kõrget turbeastet, on soovitatav pordil põhineva ligipääsukontrolli sisseseadmine.

Kui seatakse sisse pordil põhinev ligipääsukontroll, tuleb kommutaatori kasutust planeerides uurida, kas kommutaator ise ja ette nähtud klientprogrammid toetavad vastavaid protokolle ja autentimismeetodeid. Peale selle tuleks juba enne katsetada, kas klientprogrammide, kommutaatorite ja autentimisserverite koostöö sujub vigadeta. Aktiivsete võrguosade turvajuhendis ja kasutusjuhendites peaksid olema dokumenteeritud nii kasutatud toimingud kui ka vaikeseadistus.

Täiendavad kontrollküsimused:

- Kas kasutatakse portidel põhinevat ligipääsukontrolli?
- Kui kasutatakse 802.1x: Millist autentimisprotokolli kasutatakse?
- Milline on kommutaatori pordi vaikeolek?
- Kas turvajuhendis ja kasutusjuhendites on dokumenteeritud tähtis informatsioon?

M 4.207 z/OS-süsteemiterminalide kasutamine ja kaitse

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: IT-juht, Administraator

z/OS-operatsioonisüsteemi juhtimine ja kontroll toimub *HMC*- konsooli (*Hardware Management Console)*, erinevate *MCS* -konsoolide (*Multiple Console Support*) kaudu; võimalik on ka *Extended MCS* konsoolide kasutamine ja kui vajalik, siis ka monitorkonsoolide kasutamine.

HMC -konsool

HMC- konsoolid on kohtvõrgu (*LAN*) kaudu *zSeries* -süsteemi *Support Elements'* idega ühendatud. Nad lubavad turvakriitiliste toimingute teostamist riistvaras, mikrokoodis ja kogu z/OS-süsteemi konfiguratsioonis. Arvestada tuleks järgnevate nõuannetega:

Eelseadistatud *IBM* -i kasutajanimed
Eelseadistatud *IBM* -i kasutajanimede paroolid tuleb uute vastu vahetada (see kehtib ka kõigi teiste tootjate kasutajanimede kohta). Siinkohal tuleb järgida punkti M 2.11 Paroolide kasutamise reeglid .

HMC -konsooli kaitse
HMC -konsooli peaks käitama ruumis, mis on kaitstud volitamata sisenemise eest. Ligipääsu *HMC* -konsoolile tuleb loogiliselt kaitsta. Loogilise kaitse jaoks tuleks sisselogimine kindlustada inimesest lähtuvalt kasutajanime ja parooliga. Ligipääs *IBM Product Engineering'* ule tuleb tavalise tootmise ajaks deaktiveerida.
Support Elements' idega ühendamine
HMC -konsool tuleks *Support Elements* 'idega ühendada spetsiaalse kohtvõrgu (*LAN*) kaudu. Kui kasutatakse ka mõnda teist kohtvõrku (*LAN*), tuleks *Support Elements* 'ide ja *HTM* -konsooli vahel määratleda kindel seos, näiteks vastavate seadistustega domeeni turvafunktsioonis (*Domain-Security*).

Kaugühendus
HMC -konsooli käitlemisel kaugühenduse kaudu tuleb kasutusele võtta kaugpöörduse ligipääsuks vajalikud turvanõuded (vt B 4.4 Virtuaalne privaatvõrk (VPN) .

Volitusastmed
Personal tuleks jagada erinevatesse volitusastmetesse Neid astmeid tuleks

kasutada järgnevalt:

- *Access Administrator* - See aste on ainult *HMC* -konsooli haldajatele. Seda ei tohi anda tavakasutajale. Vastav aste peaks olema antud ainult vähestele töötajatele.
- *Operator* - Seda astet kasutavad tavakasutajad, kes peavad näiteks *zSeries* -operatsioonisüsteemi käivitama või peatama (*Initial Microcode Load* või *Initial Program Load*).
- *Advanced Operator* - Kuna enamik käitamisfunktsioonidest on olemas astmes *Operator* ja teised funktsioonid, nagu näiteks *Customization* on paigutatud *System Programmer* alla, siis seda astet tavaliselt ei vajata.
- *System Programmer* - Seda astet tuleks jagada ainult töötajatele, kes tegutsevad süsteemi programmeerijatena ja sellest lähtuvalt võtavad ette *HMC* -konsooli kohandamisi.
- *Service Representative* - See aste on ette nähtud ainult remonditehnikule ja ei tohi olla muudmoodi kasutatav.

Veebiserver

HMC- konsool omab eraldi veebiserverit, mis aktiveerib *HMC* -konsooli piiratud funktsionaalsuse ligipääsuks veebibrauseri kaudu. Võrgu tasandil tuleks kõik mittevolitatud ligipääsud *HMC* -konsooli veebiserverile blokeerida. *HMC* -konsooli veebiserver tuleks veebiliidese mittekasutamise korral deaktiveerida.

Vaikeseadistused

Tootja poolt kaasa antud *HMC* -konsooli vaikeseadistust tuleks muuta nii, et kasutajatele saadetakse ainult need andmed, mida nad oma tööks vajavad (*Customize User Control Process HMC* konsoolis).

Hooldustööd

Hooldustööde teostamisel *HMC* -konsooli ja tugielementide kasutamiseks tehnikute poolt tuleb sisse seada toimimisviis. Tuleb kindlustada, et pärast hooldustööde lõppu aktiveeritaks *eHMC* konsool tootmiskasutajaga, mitte ei käitata enam kõrgelt autoriseeritud tehnikute kasutajaga.

Koolitus

HMC -konsooli jaoks kasutatav personal tuleb konsooli kasutamiseks koolitada, lähtuvalt ka komplekssetest funktsioonidest. See peaks ära hoidma väärkäitamise. Tuleks kaalutleda, kas taoline praktika tõstab *HMC*- konsooli turvalisust, kuna töös vajatakse konsooli harva.

Support Elements (tugielemendid) (SE)

Tugielemendid (*Support Elements*) (kaks *IBM* -i sülearvutit) asetsevad *zSeries* -i riistvarakapis ja on ühendatud riistvararessurssidega. Tugielementidest saab anda samu käsklusi nagu *HMC* -konsooli kaudu.

Ligipääs

Ligipääsu tugielementidele tuleb füüsiliselt kaitsta. Enamasti on see tagatud seeläbi, et zSeries-süsteemi käideldakse andmekeskuses, mis on mittevolitatud ligipääsu eest kaitstud. zSeries'e riistvara riistvaralukk ei paku küllaldast kaitset.

Hooldus

Tugielemente kasutatakse tootja riistvaratehnikute poolt ka hoolduse teostamiseks. Pärast hooldustööde lõppu tuleks *zSeries* -i riistvara taas lukustada ja ülejäänud olemasolevad turvamehhanismid taas sisse lülitada.

MCS -konsool (Multiple Console Support)

MCS- konsool (nimetatakse ka *MVS* -konsooliks) võimaldab otsest ligipääsu operatsioonisüsteemile (*MCS* -i oma sisend-/väljund- protokoll, alates z/OS *V1R1 SMCS VTAM* -i kaudu) *MCS*- ja *SMCS* -konsoolide puhul tuleks eelistada järgnevaid turvamehhanisme:

Sisselogimine

Tuleb kontrollida, et kas liikme *CONSOL00 AUTH* määratluse kaitse on piisav või tuleb *MCS* -konsool niimoodi määratleda, et enne kasutamist on vajalik kasutajanime ja parooliga sisselogimine. *SMCS* -konsoolid, mida kasutatakse ka kaugjuhtimisega, vajavad kindlasti sisselogimist.

Füüsiline kaitse

Kui *MCS* -konsoolile ei ole kasutajanime ja parooliga sisselogimist sisse seatud, peab see asetsema ruumis, mis on mittevolitatud ligipääsu eest kaitstud. Siia ei kuulu konsoolid, mis võimaldavad ainult ebakriitilisi kuvafunktsioone. Kuna *MCS*-ülemkonsooli ei ole võimalik kasutajanime ja parooliga kaitsta, tuleb ta asetada ruumi, mis on mittevolitatud ligipääsu eest kaitstud. Juhul kui ei ole muid määratlusi, muudab operatsioonisüsteem z/OS esimese kättesaadava konsooli ülemkonsooliks. Ülemkonsooli paigutus liikmes *CONSOL00* tuleb teostada nii, et ülemkonsooliks saaks füüsiliselt kaitstud konsool. Teist *MCS*- konsooli, millest pärast primaarse *MCS* -ülemkonsooli äralangemist ja automaatset ümberlülitust saab ülemkonsool, tuleb kaitsta sama moodi.

Loogiline kaitse

Vastavate määratlustega tuleb kindlustada, et *MCS*- konsoolid, mida käideldakse mitteligipääsukindlates ruumides, oleksid kasutatavad ainult volitatud kasutajate poolt. Seda saab teostada liikmes *CONSOL00* paiknevate konfiguratsiooniparameetrite kaudu *AUTH=xxx* või *LOGON=REQUIRED.*

Kui *MCS* -konsoolid on teiste vahenditega piisavalt kaitstud ja kui operaatorite auditeerimist ei nõuta, võib liikmes CONSOL00 kasutada *LOGON=REQUIRED* asemel ka *LOGON=OPTIONAL* määratlust.

Individuaalne autentimine

Sisselogimisprotsessiga *MCS* -konsoolidele tuleks igale kasutajanimele omistada individuaalne autoriseerimine. See võimaldab jaotust erinevatesse operaatorgruppidesse (vt M 4.211 z/OS turvasüsteemi RACF kasutamine), mis ilma autoriseerimiseta ei oleks võimalik. Vastasel juhul on konsooli funktsioonid kättesaadavad kõigile, kes omavad füüsilist ligipääsu.

Laiendatud (*Extended*) *MCS*- konsool

Laiendatud *MCS* -konsooli abil on kasutatavad (*JES2* jaoks) *MCS*- konsooli *System Display* ja *Search Facility* kaudu TSO (*Time Sharing Option*) ja *Flasher* (*JES3* jaoks). Konsoolide jaoks tuleks järgida järgnevaid nõuandeid:

- *RACF* -määratlused - *MVS* -konsooli kaitseks tuleb kasutada vastavaid *RACF* -määratlusi (klass *OPERCMDS*). Kas laiendatud *MCS* -konsooli tohib kasutada, milliseid kasutajanimesid tohib laiendatud *MCS* -konsool kasutada ja millised käsklused on kasutusel, tuleb *RACF* -is eraldi määratleda (vaata M 4.211 z/OS turvasüsteemi RACF kasutamine). Tuleb kindlustada, et konsooli teenuseid ja sealjuures kasutatavaid z/OS käsklusi kasutaksid ainult kasutajad, kes on RACF-is vastavalt volitatud. See kehtib kõigile rakendsutele, mis töötavad laiendatud *MCS* -konsooliga.
- RSF-konsool (Remote Support Facility) - *RSF* õimaldab *zSeries* -süsteemidel automaatselt tootjaga ühendust võtta ja sealsetele tehnikutele teatada jooksva süsteemi vigu (riist- ja tarkvara). *RSF* -funktsioon lubab tootjal põhimõtteliselt ka mikrokoodi modifikatsioone süsteemi laadida. *RSF* on *HMC* -konsooli (*Host Management Console*) lisafunktsioon ja telefoniühenduse kaudu telefonivõrguga ühendatud. *RSF* -funktsiooni jaoks tuleb järgida järgnevaid nõuandeid:
- Põhilised mõtted *RSF* -i kohta - Tuleks mõelda, kas *RSF* -i taolist funktsiooni on üldse vaja ja milliseid osafunktsioone sellest vajatakse. Funktsiooni kasutamist tuleb hooldusleping kaudu kooskõlastada süsteemi eest vastutava riistvaratoega. RSF-i (ja teisi sarnaseid kõvakettafunktsioone teistelt tootjatelt) kasutatakse tavaliselt riistvara ja põhivara vigade avastamiseks ja kiirendatakse oluliselt vigadele reageerimise kiirust. Kas kaughaldus RSF-i kaudu aktiveeritakse, on andmekeskuse töötajate otsustada.
- Telefoniühenduse loomine tootjaga - Veateated luuakse *HMC* poolt, mille käigus luuakse ka telefoniühendus tootjaga. *HMC* määratlemise raames tuleb kindlustada, et sisse kantud telefoninumber oleks õige ja ainult volitatud isikutel on õigus seda muuta.
- Mikrokoodi kohandamine - Kui tootja taotleb mikrokoodi kohandamist (või teisi põhivara muudatusi), tuleb *IBM Product Engineering* 'u ligipääs vastavaks ajahetkeks aktiveerida. Ühendus luuakse *Dial-in* 'i kaudu. Vähendamaks kuritarvitamist, tuleb see pärast hooldustöid jälle deaktiveerida.
- Dokumentatsioon - *RSF* -i installatsioon ja selle kasutamine tuleb mõistetavalt dokumenteerida.

Täiendavad kontrollküsimused:

- Kas *MCS* -ülemkonsool on füüsiliselt kaitstud?
- Kas muudeti eelseadistatud paroole?
- Kas esineb menetlusjuhend, milles on reguleeritud tootjapoolne hooldus?
- Kas *HMC* -s on *IBM Product Engineering* 'u ligipääs mikrokoodi kohandamiseks välja lülitatud?
- Kas on olemas *RSF* -i dokumentatsioon?

M 4.208 z/OS-süsteemide käivitusprotsessi kaitse

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: Administraator

z/OS-süsteemi käivitamine algab *IML* -i protseduuriga (*Initial Microcode Load*), edasi toimub z/OS-operatsioonisüsteemi *IPL* -protseduur (*Initial Program Load*) ja lõpuks käivitatakse süsteemitegumid. Käivitusprotsessi juures tuleks järgida järgnevaid nõuandeid:

- *IML* -i ja *IPL* -i parameetrid - *IML* -i ja *IPL* -i parameetrid peavad olema töötajatele teada. Olemas peab olema ka aktuaalne dokumentatsioon.
- *Fallback*- konfiguratsioon - Olemas peab olema *Fallback*- konfiguratsioon. Selle konfiguratsiooniga peab süsteem olema enne viimast muudatust edukalt käivitatud.
- *IOCDS* -fail - *HMC* -dialoogis (*Host Management Console*) peab kättesaadav olema kehtiv *IOCDS* -fail (*Input/Output Configuration DataSet*), millega on võimalik süsteem käivitada.
- LPAR - Käivitatav süsteem peab olema *LPAR* -ina (*Logical Partition*) *zSeries* 'i riistvaral sisse seatud ja vastavalt konfigureeritud.
- MVS-ülemkonsool - NIP faasi (*Nucleus Initialization Program*) ajal teadete kontrollimiseks peab kasutuses olema ka *MVS* -ülemkonsool (*Multiple Virtual Systems*). Lisaks peab olema määratletud ka varukonsool, millele saab automaatselt ligi pääseda, kui tavaline ülemkonsool tehnilistel põhjustel kättesaadav ei ole (vt M 4.207 z/OS-süsteemiterminalide kasutamine ja kaitse).
- Automatiseerimine - Automatiseerimismeetodite kasutamisel tuleb dokumenteerida, millised süsteemitegumid missuguses järjekorras käivitatakse. Dokumenteerida tuleb ka vajalikud käsklused, et automatiseerimise vigu (või selle täieliku äralangemist) mingilgi määral kompenseerida.
- Käivitusprotsessi lõpp - Käivitusprotsessi lõppu tuleks paigaldada teade, mis näitab, et käivitus on lõpetatud.
- Kontroll-loend - Kasutuses peaks olema aktuaalne kontroll-loend, mida pärast käivitusprotsessi saab kasutada süsteemiolukorra kontrollimiseks. Kontrollimine kindlustab, et z/OS-süsteem ilma vigadeta käivitus (peab/on võrdlus). Kui on olemas automatiseerumismeetodid, võib kasutada ka funktsioone nendest meetoditest.

Täiendavad kontrollküsimused:

- Kas *ILM* -i ja *IPL* -i parameetrid on teada ja dokumenteeritud?
- Kas *LPAR* -id on konfigureeritud ja *HMC* -dialoogis kättesaadavad?
- Kas on olemas kõigi süsteemitegumite (*Sysem Tasks*) dokumentatsioon ja juhised, kuidas nad tuleb aktiveerida?

M 4.209 z/OS-süsteemide turvaline aluskonfiguratsioon

Algatamise eest vastutavad: IT-juht, Infoturbe osakond
Rakendamise eest vastutavad: Administraator

z/OS-operatsioonisüsteem haldab ja kasutab mitmeid autentimismehhanisme. Nende mehhanismide vale kasutuse või kuritarvitamise korral võib see mõjuda kogu süsteemi terviklust. Nendega tuleb seega aluskonfiguratsioonis arvestada. Tegemist on järgmiste funktsioonidega:

- *APF* -i (*Authorized Program Facility*) poolt autoriseeritud failid,
- *SVC* -d (*SuperVisor Calls*),
- Ressursside kaitse,
- *Pramlib'* i määratlused,
- Süsteemi protseduurid (*Started Tasks*),
- JES2 määratlused.

RACF -turvasüsteemi soovitused on kirjeldatud punktis M 4.211 z/OS turvasüsteemi RACF kasutamine . Aluskonfiguratsiooniks tuleb järgida ka M 4.220 Unixi süsteemiteenuste (USS) kaitse z/OS-süsteemides . z/OS-operatsioonisüsteemi tervikluse kaitsmiseks tuleks järgida järgnevaid alltoodud soovitusi:

APF -autoriseering

APF -autoriseeringute kaudu on võimalik saada ligipääsu privilegeeritud operatsioonidele (näiteks *MODESET SVC*). Seeläbi saab kasutada funktsioone, milleks kasutajal tavaliselt õigused puuduvad. Nii on võimalik *Supervisor* -režiimis saada ligipääs põhimälu alasse, et seal oma kasutajanimele kõrgelt privilegeeritud atribuute (näiteks *SPECIAL ACEE's - Accessor Environment Element*) omistada. *APF* -failide puhul tuleb jälgida:

- Kõiki *APF* -faile tuleb kaitsta täielikult kvalifitseeritud üldiste RACF-profiilide (nagu on kirjeldatud punktis M 4.211 z/OS turvasüsteemi RACF kasutamine) kaudu, vaatamata üldiste profiilide kasutamisele peaks profiilinimena kasutama kogu failinime.
- Kõik *APF*- failid määratletakse *Parmlib* 'i liikmes *PROGnn,* köite (*Volume*) andmetega (andmed *SMS*). Ei tohiks olla mitte ühtegi sissekannet, mille juurde ei kuulu ükski fail, vastasel juhul võib olla oht, et sinna paigutatakse mõni teine fail.
- *APF* -failidele võivad ligipääsu omada ainult töötajad, kelle ülesandeks on süsteemi hooldamine. Nende töötajate arv tuleb viia miinimumini. Ette peab olema nähtud esindajate korraldamine.

- Kuritarvitamise või kuritarvitamiskatse varakult avastamiseks tuleb pidevalt *APF*- failide muudatusi kontrollida. Muudatused nendes failides tohivad tootmistingimustes toimuda ainult teatatud hooldusajavahemikes.
- Tuleks kaalutleda, et kas *Real-Time-Monitor* aitab kuritarvitamist kiiremini avastada ja viib sellega turvalisuse tõstmiseni. Igal juhul tuleks teha vähemalt manuaalseid kontrolle *APF* -failide ligipääsudele, näiteks *SMF* -kirjete (*System Management Facility*) analüüsi kaudu.
- *APF* -failid tuleks salvestada ilma laienditeta (*Extents*).
- Tuleks arvestada, et kõiki *LINKLIST'* is määratletud faile, kasutades liikme *IEASYSxx* 'i *LNKAUTH=LNKLST* parameetrit, vaadeldakse süsteemi poolt standardjuhul *APF* -failina. Ka nendele failide puhul tuleb ülalnimetatud turvamehhanismid aktiveerida.

User SVC (*SuperVisor Calls*)
User SVC -d (kõik *SVC* -numbrid alates 200) saavad kontrolli *SuperVisor* staatuse üle *Key 0* kaudu (see vastab kernel-režiimile mõnes teises operatsioonisüsteemis), mis tähendab, et *User SVC* -l on ligipääs kõigile z/OS-operatsioonisüsteemi operatsioonidele/toimingutele. Seetõttu peavad *SVC* kasutajad järgima:

- Kõik *SVC*- programmide poolt teie käsutusse antud failid tuleb üldiste, täielikult kvalifitseeritud *RACF* -profiilide kaudu kaitsta (vaata M 4.211 z/OS turvasüsteemi RACF kasutamine).
- Kõik *SVC* -d määratletakse *Parmlib* liikmes *IEASVCxxx.* Kuna *SVC* ei saa vajalike siseste turvamehhanismide tõttu eriti väike olla, viitab väikese suurusega *User SVC* -moodul võimalikule turvaprobleemile. Turvakriitiliste aukude olemasolu vältimiseks tuleb sellised *User SVC*-d süsteemiprogrammeerijate poolt üle vaadata. Varem kasutati *SVC* -d tihti ebapiisavate turvamehhanismidega, näiteks niinimetatud autoriseerimis-SVCd, et teostada autoriseeritud toiminguid autoriseerimata keskkonnas. Kui sellised *SVC* -d on veel olemas, tuleks nad võimalusel eemaldada või asendada.
- Kui toodetega pannakse kaasa *User SVC* -d, tuleks tootjalt uurida nende turvamehhanismide kohta. Eriti tähtis on see juhul, kui kaasapandud *SVC* -moodul on väga väike, kuna see on märk puudulikust sisekontrollist.
- *SVC* -failidele peaksid ligipääsu omama ainult töötajad, kelle ülesandeks on süsteemi hooldamine. Nende töötajate arvu tuleb vähendada. Tuleb aga kindlustada, et vähemalt üks esindaja omaks ligipääsu.

Ressursid
z/OS-operatsioonisüsteemi ressursse (failid, programmid, funktsioonid jne.) tuleb *RACF* -i kaudu kaitsta (vaata M 4.211 z/OS turvasüsteemi RACF kasutamine). Tuleks järgida järgnevaid soovitusi:

- *Class Descriptor Table* (CDT) jaoks tohiks installatsioonispetsiifilisi muudatusi teha ainult moodulis *ICHRRCDE*. Tähtsaimate parameetritena tuleb

jälgida *DFTUACC* (siin soovitatakse *NONE*) ja *OPER* (siin soovitatakse *NO*). *DSNT (Dataset Name Table)* peab sisaldama *RACF* -andmepankade failinimesid.

- *IBM* 'i soovitusel peaks *Authorized Caller Table* (*AUT*) tühi olema. Antud juhul on tegemist vana funktsiooniga, mis tänapäeval on asendatud klassiga *Program,* aga on ikka veel olemas. Erandeid tuleb põhjendada.
- *TSO Authorized command and program table Parmlib* 'is (*IKJTSOxx*) võib sisaldada ainult neid käskluste ja programmide nimesid, mis on vajalikud TSO (*Time Sharing Option*) all teostamiseks.
- *Started Procedure Table* (*ICHRIN03*) peaks sisaldama ainult väheseid sissekandeid hädaolukordade jaoks, muidu tuleks autoriseeritud *Started Task* 'ide määratlemiseks kasutada *RACF* -i klassi *STARTED*. *PRIVILEGED* atribuuti tuleks vältida, *TRUSTED* kasutada ainult vajaduse korral (näiteks JES2 korral). Tabel peaks sisaldama mõningaid üldisi sissekandeid nende *Started Task* 'ide jaoks, mis ei ole määratletud, et kindlustada nende tegumite mittetäidetavus.
- *RACF Router Table'* it tuleb hallata sünkroonselt *CDT* ga.
- *RACF* pakub paroolide krüpteerimiseks kahte algoritmi, *Masking*- algoritmi ja *DES*- krüpteerimist (*Data Encryption Standard*). *RACF* -paroolid tuleks *DES* -iga krüpteerida, kuna see pakub paremat kaitset kui *Masking.* Seda juhitakse *RACF-Exit ICHDEX01'i* kaudu. *RACF* -i spetsiifilised soovitused on punktis M 4.211 z/OS turvasüsteemi RACF kasutamine .

IPL'i parameetrite fail

Alglaaduri (*IPL - Initial Program Load*) parameetrite failis paikneb olulisim informatsioon z/OS-operatsioonisüsteemi installeerimiseks. Seda faili tuleb RACFi kaudu kaitsta ning faili kasutamiseks volitatud töötajate arv peab jääma väikeseks. Tuleb jälgida, et sisse oleks viidud esindajate korraldus.

Parmlib 'i määratlused

z/OS-operatsioonisüsteemi parameetri failidesse (*SYSn, PARMLIB* , võib olla mitu faili) paigutatakse operatsioonisüsteemi põhilised määratlused. Kõiki *Parmlib* 'i faile tuleb *RACF* -iga kaitsta. Ligipääs võib olla lubatud ainult töötajatele, kes neid faile oma töö käigus töötlevad. Tuleks mõelda, et kas erinevatel parameetrite failidel ei peaks kasutama erinevat *RACF* -kaitset, kuna *Parmlib* 'is on erineva kaitsevajadusega määratlusi. *Parmlib* 'i turvakriitilised liikmed on näiteks (sorteerimata):

- *BPXPRMxx*
- CLOCKxx
- COMMNDxx
- CSVLLA00
- IEASYSxx
- IEFSSNxx
- IKJTSOxx

- MSTJCLxx
- PROGxx
- SCHEDxx
- SMFPRMxx

Ligipääs nendele määratlustele tuleb piirata vajalike töötajateni. Esindajate korraldus peab olema jõus.

Süsteemiprotseduurid
Kõik tähtsad *Started Task* protseduurid on spetsiaalsetes teekides, mis antakse süsteemile teada kas *MSTJCLxx* või *JES2/3* määratluse kaudu. Neid faile, näiteks *SYS1.PROCLIB,* tuleb kaitsta *RACF* -profiilide kaudu, mis lubavad määratlustele ligipääsu ainult autoriseeritud töötajatel. Eriti tähtis on üldkasutatavate sisselogimisprotseduuride turvalisus, kuna siin on kuritarvitamise oht suur (vt M 4.213 Logimisprotsessi kaitse z/OS all). Lugemis- ja kirjutamispääsu peaks piirama ainult süsteemihaldajale, ning peale selle vajab ainult *JES2/3* lugemisligipääsu. Need kaitsemeetmed kehtivad ka kõigile üldkasutatavatele sisselogimisprotseduuridel kasutatavatele skripti failidele (TSO CLISTs oder REXX EXECs), kuna ka siin on kuritarvitamise oht suur.

JESx määratlus (Job Entry Subsystem)

Job Entry Subsysteme JES2 ja JES3 kaitseks tuleb RACF-i kaudu põhiliselt kindlustada järgmised ressursid:

- JES enda failid,
- Sisend ja teised allikad (näiteks sõlmed),
- Tööde nimed,
- Süsteemi sisend ja väljund *JES* spuulil ja
- Väljund teistele sõlmedele kaugjuhitavatele tööjaamadele.

Järgnevaid *RACF* -funktsioone tuleks kasutada *JES2/3* turvalisuse tõstmiseks:

- *BATCHALLRACF* (Kasutajanime sundimine pakketööde korral)
- *EARLYVERIFY* (ainult *Early Verify* korral võimalik)
- *XBMALLRACF* (*Execution Batch Monitor'* i toetamine)
- *NJEUSERID* (*Network Job Entry* funktsiooni vaikimisi kasutajate määramine)
- *UNDEFINEDUSER* (*Network Job Entry* funktsiooni *Undefined User* määramine)

Peale selle võimaldab RACF JES2/3 rea *General Resource* klasside kasutamist, mida kasutatakse JES funktsioonide kaitseks:

- *OPERCMDS*
- JESSPOOL
- SURROGAT
- NODES
- WRITER

Täiendavad kontrollküsimused:

- Kas *APF* -failid on kaitstud täielikult kvalifitseeritud üldiste *RACF* -profiilide kaudu?
- Kas *APF* -faile jälgitakse?
- Kas *SVC* sid kontrollitakse regulaarselt?
- Kas *Parmlib* ja *Proclib* on kaitstud selliselt, et neile omavad ligipääsu ainult vähesed volitatud töötajad ja nende asendajad?
- Kas *JES2/3 RACF Resource* klassid on aktiveeritud?

M 4.210 Operatsioonisüsteemi z/OS turvaline käitus

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: Administraator

z/OS-operatsioonisüsteem töötab enamjaolt autonoomselt, st ilma halduspersonali sekkumiseta. Tagamaks, et z/OS-operatsioonisüsteemi funktsionaalsus oleks ilma probleemideta kättesaadav, tuleb käitlemise kindlustamiseks rakendada mõningaid alltoodud lisameetmeid:

Kontroll/jälgimine

HMC kontroll

HMCd (Host Management Console) tuleks pidevalt uurida, et avastada uued veateated (riistavara, mikrokood, tarkvara). Vead, millest on tootjale RFS-funktsiooni (Remote Support Facility) kaudu teatatud, peavad käitusorganisatsioonile enne tootja helistamist teada olema.

WTOR kontroll

Uutele operatsioonisüsteemi kaudu tulnud päringutele reageerimiseks tuleb jälgida z/OSoperatsioonisüsteemi WTOR-teateid (Write To Operator with Reply), et vajadusel neile ka kohe vastata. Sama kehtib ka operatsioonisüsteemi või tema osade WTO-teadete (Write To Operator) korral, mis nõuavad teatud juhtudel kohest reageerimist.

Süsteemitegum

Tuleb kindlustada, et kõik planeeritud süsteemitegumid töötaksid. Seda on tavaliselt võimalik kindlaks teha stardi ajal kuvatavate teadete järgi või viisist, kuidas

süsteemitegumid reageerivad päringutele. Enamasti ei piisa nende olemasolu kontrollimiseks ainult kuvari käsklustest, vaid tuleks kontrollida ka süsteemitegumite reaktsiooni.

Võimsuse kontroll

Tuleb kindlustada, et süsteemi võimsust ei ületataks. See tähendab, et vastavas plaanis kehtestatud nõuetest tuleb kinni pidada ja neid pidevalt kontrollida.

Turberikkumiste kontroll

Tuleb kontrollida kehtestatud turvanõuetest kinnipidamist. Turberikkumistest tuleb teatada määratletud mehhanismide kaudu (vt M 2.292 z/ OS-süsteemide seire).

Süsteemi täiskoormus

Süsteemi töövõime kasutamist tuleb sobivate vahenditega jälgida ning ülekoormuse korral tuleb kasutusele võtta korrigeerivad meetmed, näiteks *JES2/3* algataja (*Job Entry Subsystem*) vähendamine. Süsteemi tõhusamaks järelvalveks tuleks kaaluda, kas olemasolevatele standardfunktsioonidele (*RMF - Resource Measurement Facility*) oleks vaja lisada ka

spetsiaalseid monitore.

Automatiseerimissüsteem

Triviaalsete kontrollide regulaarseks läbiviimiseks tuleks mõelda automatiseerimisfunktsiooni kasutusele võtmisele (kas siis ise loodud programmina või

valmistootena). Siia juurde kuuluvad aktiivsete tegumite ja NJE ühenduse peab/on võrdlus, nagu ka avatud vastused (*Replies*), süsteemi jõudlus, JES2/3 ootejärjekord, jne. See võimaldab paljude struktureerimata teadete asemel kasutada ühtset *System Alive* teadet, mis omakorda teeb kontrollimise oluliselt lihtsamaks. Kui mitu z/OS-süsteemi on ühe funktsiooni järelvalve all, tuleks kogu informatsioon (*Events*) näidata ühel konsoolil (*Alert Management*). Erinevad tootjad pakkuvad oma automatiseerimispakettide raames vastavaid programme.

Automatiseeritud pakktööde *(Batch Job)*

Kaaluda tuleks automatiseerimisfunktsiooni kasutamist pakktööde kontrollimiseks. Alates kindlast pakketööde arvust on see vältimatu, kuna vastasel juhul ei ole võimalik tagada veatut järelvalvet. Mitmed tootjad pakkuvad tööde planeerijaid (*Job Scheduler*), mis suudavad kontrollida tuhandeid pakketöid.

Süsteemiteadete vähendamine

Süsteemiteateid tuleks vähendada sellisel määral, et kuvataks ainult tähtsad teated. Automatiseerimisfunktsioonide raames on soovitatav kasutada teadete filtrit (*MPF -Message Processing Facility*).

Fookuspunkti kontseptsioon (Focal Point Concept)

Paljude z/OS-operatsioonisüsteemide kasutamisel tuleks mõelda keskse kontrollpunkti sisseseadmisele (*Focal Point*).

Kasutusfunktsioonide kindlustamine

IT-turvalisuse tagamine ei ole ühekordne tegevus, töö käigus tuleb seda pidevalt kontrollida ja vastavalt olukordadele kohandada. Sellised jooksva töö käigus tehtavad kohandamised nõuavad turvalisuse seisukohalt olulisi aktsioone, mida tuleb vastavalt kaitsta. z/OS-süsteemi turvaliseks käitlemiseks tuleb seega järgida järgnevaid soovitusi:

Kontrollitud hooldustööd

Käival z/OS-süsteemil ei tohi teha tootmist mõjutavaid hooldustöid väljaspool hooldusajavahemikku. Kõik plaanitud või mitteplaanitud muudatused tuleb *Change Management* süsteemi kaudu kõigi kaasatud spetsialistidega kooskõlastada. Muudatuste plaan (*Change Plan*) tuleb järelduste tegemiseks arhiveerida.

Tarkvara installeerimine SMP/E kaudu

Tarkvara võib installeerida võib alles pärast registreerimist IT-infrastruktuuri teegi (*ITIL-Information Technology Infrastructure Library*) kaudu. Et vältida vigu tarkvara installeerimisel, tuleks kasutada SMP/E meetodit (*System Management Process Enhanced*).

Dünaamilised muudatused

Paljud turvalisuse jaoks olulised muudatused saab tänapäeval teostada dünaamiliselt, see tähendab käitlemise ajal, ilma et oleks vaja alglaadurit (*IPL - Initial Program Load*). Süsteemis võib teha dünaamilisi muudatusi ainult plaanitud hooldustööde käigus või vastava taotluse esitamisel. Turvalisuse seisukohalt väga olulisi käsklusi, näiteks *SETAPF, REFRESH, LLA, MODIFY, CONFIG, FORCE* või *SET*, tuleb *RACF*-profiilidega kaitsta. Neid tohib kasutada ainult koolitatud personal.

SDSF

SDSFi (*System Display and Search Facility*) tuleb kaitsta nii, et mittevolitatud isikud ei saaks süsteemikäsklusi kuritarvitada. Näiteks ei tohi olla võimalik suvaliselt paljude algatajate aktiveerimine. Kaitsta tuleb ka süsteemi tööde prioriteetide juhtimist *SDSF*is (liigitamine *WLM-Service* klassidesse). Rakendustel ei tohiks olla lubatud, näiteks parema jõudluse saavutamiseks, muuta oma pakketööde prioriteete.

See soovitus kehtib analoogselt ka *Flascher*'ile, mis on *JES3* toetus ja vastab *SDSF* funktsionaalsusele.

Konsooli kaitse

Konsoolide kaitse on kirjeldatud punktis M 4.207 z/OS-süsteemiterminalide kasutamine ja kaitse . Vastavate RACF-määratlustega tuleb takistada töötajate volitamata ligipääsu *EMCS*ile (*Exte*nded *Multiple Console Support*).

MVS-konsooli kaitse

z/OS-süsteemikäsklusi võivad kasutada ainult volitatud isikud. Käsklusi tuleb kaitsta vastavate *RACF*-profiilidega. Tuleb kindlaks teha, millised töötajad milliseid õigusi teatud süsteemikäsklustele vajavad ja neid teostada tohivad. Tuleks

mõelda, kas tegumite käivitamine ja peatamine ei peaks toimuma ainult *Operating* kaudu.

HCD

Mõningaid riistvara seadistusi on võimalik muuta ka tagantjärele z/OS-süsteemi käitlemise ajal. See toimub HCD-protsessi kaudu (*Hardware Configuration Definition*). Uue IOCDS (*Input/Output Configuration Dataset*) aktiveerimine tuleks aga läbi viia ainult *Change Management*'i raames.

Riistvara määratlemisel tuleb jälgida, et ressursse ei määratleta mitme üksiksüsteemi *Shared* kaudu. Näiteks ei tohiks olla võimalik kahest erinevast üksiksüsteemist ühele kõvakettale ligi pääseda. *Sysplex*-rööpklastri korral kuulub ressursside jagamine (*Resource-Sharing*) süsteemi arhitektuuri hulka ja ei ole õige konfiguratsiooni korral probleemiks.

*Operating (*Käitlus*)*

Käitlemise jaoks tuleks luua kaks *RACF*-gruppi, üks grupp pikaajalise kogemusega operaatoritele ja teine uutele (veel kogenematutele) töötajatele. Kõik töötajad peaksid saama ainult neile vajalikud õigused. Töötajad peavad olema oma tööülesannete täitmiseks piisavalt koolitatud. Eriti turvakriitilised ülesanded tuleks jätta kogenud töötajatele.

Täiendavad kontrollküsimused:

- Kas *HMC*-l kontrollitakse vigade teket?
- Kas süsteemitegumite käideldavust kontrollitakse?
- Kas kontrollitakse süsteemi maksimaalse võimsuse ärakasutamist?
- Kas süsteemi olukorra järelvalveks on paigaldatud automaatfunktsioon?
- Kas pakketööde käitlemiseks ja kontrollimiseks on olemas automaatfunktsioon?
- Kas muudatusi aktiveeritakse ainult *Change Management*'i kaudu?
- Kas hooldustööd, näiteks riistvara määratlemine, toimuvad ainult selleks ette nähtud ajavahemikus?
- Kas *EMCS*-konsool on volitamata ligipääsu eest kaitstud?

M 4.211 z/OS turvasüsteemi RACF kasutamine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: Administraator

z/OS -süsteemi turvaline konfigureerimine toimub operatsioonisüsteemi osade määratlemise ja turvasüsteemi RACF (*Resource Access Control Facility*) kaudu. Selles punktis kirjeldatakse soovitusi *RACF* i kasutamiseks. Informatsiooni *z/OS* i määratluste turbe kohta leiate punktist M 4.209 z/OS-süsteemide turvaline alus-konfiguratsioon . *RACF* is hallatakse kasutajate andmeid ja ligipääsuvõimalusi erinevatele ressurssidele profiilide vormis. Profiilid on jagatud *Dataset* profiiliks, *General Resource* profiiliks, *Group* profiiliks, *User* profiiliks ja nende ühendusteks. *RACF* i haldamiseks tuleb järgida järgnevaid reegleid:

Põhilised *RACF* i seadistused

SETROPTS määratlused

*RACF*i keskne konfiguratsioon toimub *SETROPS* seadistustes. Siin teostatakse *RACF*i üldised seadistused kogu süsteemile. Kuna siin on väga paljud muudetavad parameetrid, mis üksteist osaliselt ka mõjutavad, tuleb seadistused hästi läbi mõelda. Järgnevalt on loendatud tähtsamad parameetrid, mida on võimalik käsklusega *SETROPS* seadistada.

CLASSACT	*Access Authorization Checking*
AUDIT	Lülitab klassi protokollimisfunktsiooni sisse
RACLIST	Määrab, millised profiilid mällu laaditakse
GENERIC	Käivitab *Generic Profile Checking* funktsiooni
NOADSP	Takistab diskreetsed profiilid
PROTECTALL	Kindlustab *RACF* -profiilide loomise
WHEN	Võimaldab programmidele konditsionaalset kaitset
CMDVIOL	Protokollib kõik *RACF* rikkumised
OPERAUDIT	Kasutajaandmete kontroll atribuudiga *OPERATIONS*
ERASE	Pärast faili kustutamist kustutab failisisu

Tabel: *Resource Access Policies* üldistele ressurssiklassidele

INTERVAL	Aktiivse parooli kehtivusaeg
REVOKE	Ebaõnnestunud sisselogimiskatsete arv, enne blokeerimist
RULE	Määratleb paroolireeglid

Tabel: *Password Policies* paroolide töötlemiseks

RACF -i suhteliselt keerukas alusseadistus on *z/OS*- operatsioonisüsteemi turvalisuse seisukohalt ülimalt oluline. Teatud juhtudel tuleb siin määratleda või aktiveerida üle 30 parameetri, mistõttu on vajalik põhjalik planeerimine. See kindlustab parameetrite õige asetuse ja hoiab seeläbi ära võimalikud turvaaugud. Planeerimise abistamiseks pakub tootja RACF turvalisuse planeerijat (*Security Planner*) (olemas ka internetis). Antud planeerija annab soovitusi ka *RACF* i alusseadistuseks.

Eelseadistatud RVARY parool

RVARY -käskluse, näiteks *RACF* andmepanga *SWITCH* i, parool ei tohi jääda eelseadistuse tasemele ja seda tuleb muuta.

RACF-Exits' i *kasutamine*

Tuleks välja selgitada vajadus RACF- *Exits'* i järele. Erinevate *Exits* 'itega saavutatakse, et RACF väldiks turvakontrolle või vastupidi teostaks täiendavaid turvakontrolle. Muudetud ja enda *Exits* 'id tuleb dokumenteerida. Sealjuures tuleb märkida ka funktsioon ja põhjus. *Exits'* ite kasutamisel tuleb neid ka jälgida.

RACF i kasutajanimed

Sisselogimiskatsete piiramine

RACF i paigutatud kasutajanimed võimaldavad kasutajal ennast *z/OS* -süsteemi jaoks autentida. Kaitseks jõhkrate rünnete (*brute force attack*) vastu tuleb sisselogimiskatsete arv piirata, et kasutaja vajaduse korral automaatselt suletaks (maksimaalselt 3-5 katset).

Kasutajanimede määramine

Kasutajanimede määramiseks peab olema kindel meetod. Meetod peab kindlustama, et kasutajanimed saavad ainult isikud ja nende asendajad, kes vajavad oma töö teostamiseks vastavale süsteemile ligipääsu. Meetod võib toimida näiteks teatud formulari kaudu või automaatselt. Igal juhul peab süsteemi eest vastutaja asjakohase taotluse kinnitama.

Kasutajanime segmendid

RACF is tuleb aktiveerida ainult need kasutajanimede segmendid, mida kasutaja igapäevase töö jaoks vajab (näiteks *TSO*, *Netview, DCE* või *OMVS*).

Kasutajanimede vabastamine

Lukustatud kasutajatunnuste vabastamiseks tuleb luua meetod. Kasutaja peab vabastaja, näiteks kõnekeskuse või kasutaja konsultatsioonipunkti jaoks oma isiku tõestama ja oma taotluse kinnitama. Alles pärast seda tohib kasutajatunnused vabastada.

TSO-segmendi andmed

TSO- segmendi (*Time Sharing Option*) andmeid nagu sisselogimisprotseduuri nimi, kontonumber või mälukoht, peaksid olema *RACF* -profiilide kaudu kasutajapoolse ülekirjutamise eest kaitstud. Sellest tulenevalt saab kasutaja töötada ainult etteantud keskkonnas. Erandjuhud tuleb põhjendada ja dokumenteerida.

Lukustamine inaktiivsuse tõttu

Kasutaja tuleks turvalisusest lähtuvalt pärast kindlat ajaperioodi (näiteks 90 päeva) inaktiivsuse tõttu lukustada. Sellest reeglist tuleb aga välja arvata meetodite kasutajanimed, näiteks hädakasutajad ja *STC* kasutajanimed. Pärast veel pikema ajaperioodi, näiteks 180 päeva möödumist tuleks kaaluda kasutajanime kustutamist. Kasutajanime kustutamisel tuleb tulemused kindlasti protokollida ja edastada *RACF* haldusele. Protokollid tuleb turvaliselt salvestada ja *RACF* -haldajad kasutavad neid järelduste tegemiseks.

Kasutajanimede kustutamine

Kasutajate tunnused kustutatakse kas päringu või võrgusisese kontrolli tulemusena. Kasutajanime kustutamisel tuleb jälgida, et peale *RACF* is asuva kasutajanime kustutataks ka ülemkataloogis paiknevad määratlused ja *ALIAS* -e sissekanded. Kasutaja failid tuleb samuti kustutada või mõnele teisele kasutajale lisada.

Kitsendavate kasutajanimede limiteerimine

Suurte õigustega kasutajanimesid tuleks väljastada ainult juhul, kui töötajad neid õigusi ka tegelikult oma töös vajavad.

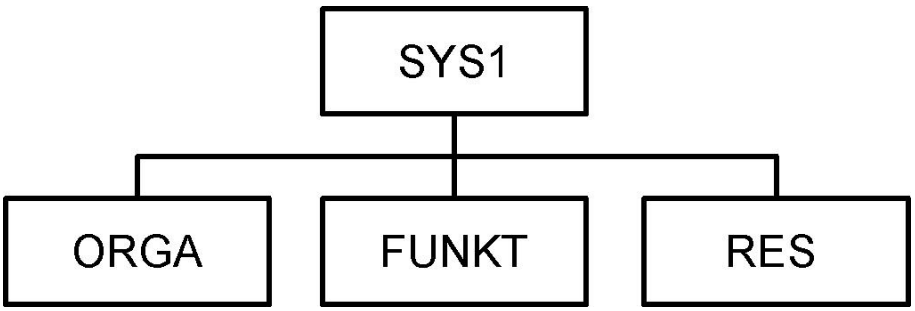
RACF-grupid ja gruppide struktuur

Õigusi ei tohiks jagada otse kasutajanimedele. Samade kohustustega kasutajad peaksid olema paigutatud gruppidesse, ning nende gruppide kaudu jagatakse vastavad õigused. Soovitatav on grupistruktuuri lahutamine, näiteks järgneva skeemi järgi:

Organisatsioonigrupid	Kasutajanimede liigitamine ametiasutuse või ettevõtte organisatsiooniüksustesse, näiteks ORGA.
Funktsioonigrupid	Selle grupi kaudu saavad kasutajad oma õigused vastavalt nende ülesannetele (funktsioonile) süsteemis, näiteks FUNKT.
Ressursigrupid	Failiressursside haldamiseks. Iga loodud failiprofiili jaoks peab *RACF* is olemas olema kas grupp või kasutajanimi. Grupid on soovitatavad, kuna neid ei saa kuritarvitada süsteemi sisenemiseks, näiteks *RES*.

Tabel: Grupistruktuuri lahutamine

Järgnevalt grupistruktuuri piltlik näide



Joonis: Soovitatud grupistruktuuri põhimõtteline ülesehitus *RACF* is

SYS1 grupi nimi on kindlalt etteantud. See on alati kõige ülemine grupp. Selles grupis paikneb ainult *IBMUSERR* , keda vajatakse süsteemi uuesti installeerimisel. *IMBUSER* 'i kasutamiseks. *RACF* -i grupi omanik (*Owner*) struktuur tuleb läbivalt sisse seada. Selles näites on ORGA, FUNKT ja RES grupi omanikuks (*Owner*) SYS1. Järgnevatele alagruppidele tuleks omanikuks märkida vastava ülalpool asuva grupi nimi. Hierarhiline ülesehitus lihtsustab ülevaadet *Group-Special*, *Group-Operations* ja *Group-Auditor* õiguste kasutamisel.

Kaitse *RACF* -määratluste kaudu

Kaitse Started Tasks eest

Started Tasks tuleb *RACF* is märgistada atribuudiga *PROTECTED*. Atribuut *PROTECTED* takistab kasutajanime kuritarvitamist tavapärase sisselogimise teel. *Started Tasks* 'e tuleb määratleda ja kaitsta *RACF* -klassis *STARTED.* Lisainformatsiooni *Started Tasks* kohta leiate meetmest M 4.209 z/OS-süsteemide turvaline aluskonfiguratsioon .

Kaitse turvakriitiliste programmide eest

Turvakriitilisi programme tuleb kaitsta *RACF* klassiga *PROGRAM.* Ligipääsu nendele programmidele tohib anda ainult kasutajatele või nende asendajatele, kes neid programme oma töös vajavad. Rohkem informatsiooni turvakriitiliste programmide kasutamise kohta leiate meetmest M 4.215 Turvakriitiliste z/OS-utiliitide kaitse .

Failide kaitse

Faile kaitstakse *RACF*is failiprofiili kaudu. See hõlmab kõiki süsteemifaile ja kõigi tootmisrakenduste faile. Failide kaitseks tuleks järgida järgnevaid reegleid:

- Faile tuleb kaitsta RACFi üldiste failiprofiilide kaudu. Tuleb vältida diskreetseid failiprofiile.
- Ükski failiprofiil ei tohiks Universal Access' iga (UACC) olla paigaldatud suuremana kui NONE. Organisatoorsete ja tehniliste mehhanismidega tuleb takistada, et kasutajad saaksid muuta oma failiprofiili UACC väärtust.
- General Resource profiilid tuleks UACC ga paigaldada suuremana kui NONE ainult juhul, kui see on ilmtingimata vajalik. See tuleks arusaadavalt dokumenteerida.
- Tootmissüsteemis ei tohi failiprofiilid ja General Resource profiilid olla Warning- režiimis, kuna vastasel juhul ei ole garanteeritud nendele profiilidele omistatud ressursside kaitse. Warning- režiimi kasutamisel testsüsteemis tuleb jälgida, et süsteemi jõudlust ei vähendataks liigselt (MVS teadete loomise ja SMF - Records tõttu).
- RACF hoolduskulude vähendamiseks on vajalikud failinimede loomise ja kasutamise ning RACF- General Resources standardid.
- Kõrgautoriseeritud faile, näiteks APF, SVC failid, Parmlibs ja Proclibs tohib kaitsta ainult täielikult kvalifitseeritud üldiste failiprofiilide kaudu. Rohkem informatsiooni nende failide kaitse kohta leiate M 4.209 z/OS-süsteemide turvaline aluskonfiguratsioon .
- RACF andmepanka, RACF varundusandmepanka ja turvakoopiaid tuleb kaitsta UACC (NONE) kaudu. Vältimaks jõhkraid rünnakuid (Brute Force Attack) andmepangas salvestatud paroolidele, tuleb ligipääs nendele failidele (isegi lugemine) piirata miinimumini.

HFS failid

Unix' i süsteemiteenuste (*USS*) alamsüsteemi (*Unix System Services*) *HFS* -faile (hierarhiline failisüsteem) tuleb *z/OS* is nagu tavalisi MVS faile kaitsta *RACF* i kaudu. Informatsiooni *Unix* 'i failisüsteemi failide kaitse kohta leiate meetmest M 4.220 Unixi süsteemiteenuste (USS) kaitse z/OS-süsteemides .

Multi-Client Capability z/OS -i all

Paljudes installatsioonides on tavaline, et üks *z/OS* -süsteem on jagatud mitme kliendi vahel. Kuna nad töötavad seega ühes süsteemis, peab z/OS-süsteem olema *Multi-Client* võimeline. Tähendab see aga seda, et kliendid ei pääse teise kliendi andmetele ligi ja ei saa seega ka ohustada konfidentsiaalsust, andmete puutumatust ja kättesaadavust.

Multi-Client Capability korral tuleb järgida järgnevaid nõuandeid:

Eraldamine RACF profiilidega

Klientide andmed ja rakendused tuleb *RACF* -profiilidega üksteisest eraldada. Tuleb luua kontseptsioon klientide eraldamiseks *RACF* iga.

Operatsioonisüsteemi kindlustamine

Ükski klient ei tohi omada kirjutuspääsu *z/OS* -operatsioonisüsteemide failidele. Muudatusi tohib teha ainult *z/OS* -süsteemi käitaja.

Suurte õigustega kasutajanimed

RACF is võivad suuri õigusi (*SPECIAL, OPERATIONS, AUDITOR*) kasutada ainult süsteemihalduse töötajad. Soovi korral võib kliendi käsutusse anda *Group-Special*, *Group-Operations* ja *Group-Auditor* õigused. Selle tarvis tuleb igal kliendile luua spetsiaalne grupikontseptsioon (*Owner* kontseptsioon).

RACF-Security-Labels kasutamine

Klientide täpsemaks eraldamiseks tuleks mõelda RACF- *Security-Labels* kasutamisele.

Hooldusaegade kooskõlastamine

Hooldusajad, mille kestel ei saa *z/OS* -süsteemi kasutada, tuleb kõikide vastava süsteemi klientidega kooskõlastada.

Täiendavad kontrollküsimused:

- Kas tähtsaimad *SETROPTS* väärtused on määratud sobivalt?
- Kas *RVARY* parool on muudetud?
- Kas tagasilükatud/nurjunud sisselogimiskatsete arv on piiratud?
- Kas on olemas meetodid lukustatud kasutajatunnuste vabastamiseks?
- Kas kasutajanimed lukustatakse, kui kasutaja on olnud eelnevalt määratud aja jooksul inaktiivne?
- Kas paigaldatud *RACF - Exits* 'id on dokumenteeritud?
- Kas hooldusajad on kõigi klientidega kooskõlastatud?
- Kas erinevate klientide andmed on piisavalt *RACF* i kaudu kaitstud?

M 4.212z zSeries -süsteemi Linux 'i kaitse

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: Asjatundja, administraator

zSeries -süsteemidel võib kasutada ka *Linux*'i operatsioonisüsteemi. Operatsioonisüsteemi kindlustamiseks tuleb siinkohal järgida ka soovitusi moodulis B 3.102 Server Unixi all . Lisaks on järgnevalt kirjeldatud mõningaid *zSeries* spetsiifilisi eripärasid, millega tuleks arvestada.

Linux' i käivitamine *zSeries* all

Linux 'i käitlemiseks *zSeries* 'i all on kolm erinevat võimalust.

Linux Native zSeries riistvaral

zSeries riistvaral toimib ainult üks *Linux* 'i operatsioonisüsteem. See tähendab, et kogu *zSeries* 'e riistvara on *Linux* 'i poolt kasutuses.

Linuz zSeries'e LPAR-is

Selle variandi korral toimub *Linux*'i käitus *zSeries* masinal asuvas eraldi *LPAR*is (*Locical Partition*). *LPAR*-režiim võimaldab mitme sõltumatu operatsioonisüsttemi käitamist samal zSereis riistvaral. Iga partitsioon käitub kui eraldi riistvara. Nendele *LPAR* idele võib muuhulgas installeerida nii *z/OS* -i kui ka *Linux*'i.

Linux z/VM-süsteemi all

Ühel zSeries arvutil või ühes z/VM LPAR-is võib olla installeeritud mitu Linuxi süsteemi. z/VM võimaldab luua niinimetatud virtuaalmasinaid, millel on võimalik Linuxi operatsioonisüsteeme üksteisest sõltumatult käidelda.

Terminali kindlustamine

SE (*Support Elements*) ja *HMC* (*Hardware Management Console*) tuleb turvata nii, nagu on soovitatud meetmes M 4.207 z/OS-süsteemiterminalide kasutamine ja kaitse .

Linux 'i kindlustamine *z/VM* i all

Linux 'i käitlemiseks *z/VM* i all tuleks lisaks arvestada järgnevate soovitustega:

- *z/VM* i jaoks tuleb kinni pidada aktuaalsetest paikade (*Patch*) olukordadest. Tuleb jälgida, et ei töötataks vananenud süsteemidega.
- *z/VM* -süsteemihaldaja õigused on väga suured. Ta võib z/VM-i all luua või kustutada virtuaalmasinaid. See on usaldusväärsust nõudev positsioon, milles süsteemihaldajale peab olema selge, et ta on süsteemi turvalisuse eest kaasvastutav.
- Pärast *z/VM* i installeerimist tuleb sisselogimisparooli ja minidiski parooli kohe muuta.
- *z/VM* i all määratletud virtuaalmasinad peaksid sisaldama ainult neid ressursse, mis on vastava ülesande jaoks vajalikud, näiteks minidiski, aadressi jne. Ligipääse kontrollitakse *z/VM* i kaudu. Virtuaalmasinad peavad üksteisest kindlalt eraldatud olema.
- *z/VM* i all tohib käivitada ainult vajalikud teenused. Mittevajalikud teenused tuleb desaktiveerida.
- *z/VM* i turvahaldus peab toimuma *z/VM* ile mõeldud *RACF* i kaudu. *z/VM* i *RACF* i saab kasutada ainult *z/VM* i kasutajate õiguste haldamiseks. Peale selle saab *RACF Resource Profile* kaudu kaitsta ka virtuaalmasinaid, minidiske ja soovi korral ka terminale. Nendele ressurssidele võivad ligipääsu omada ainult need kasutajad, kes vajavad oma tegevuse käigus vastavaid õigusi. *RACF* iga ei saa aga hallata *Linux* 'i kasutajate õigusi ning nende ligipääsu *Linux*'i operatsioonisüsteemi ressurssidele. *Linux*'i kasutajaid kontrollitakse pärast virtuaalse *Linux*'i süsteemi aktiveerimist, tavapäraste *Linux*'i turvamehhanismidega. *z/VM* i turvakriitilisi süsteemikäsklusi (näiteks *CP DIAL*) tuleks *RACF* iga kaitsta.
- *z/VM* failide ja kataloogide haldamiseks tuleks mõelda *DIRMAINT* utiliidi kasutamisele. Vastav utiliit võimaldab kasutajakataloogide ülevaatlikku haldust ja aitab seeläbi vähendada haldusvigu. *DIRMAINT* 'si turvamehhanismid peaksid baseeruma *z/VM-i RACF*il. *DIRMAINTiga* halduse raames olevad käsklused ja teated peaksid olema paigutatud auditeerimiskontrolli alla.
- *z/VM* i päeviku pidamise funktsiooni (*Journaling*) ja *RACF* i revisjoni funktsiooni (*Audit*) tuleks kasutada revisjoni teostamiseks (vaata M 2.291 *z/OS aruandlus ja auditid*).
- *TCP/IP* ühenduste turvalisuse tagamiseks tuleks kasutada *Unix* 'is ja *Linux* 'is tavalisi turvamehhanisme. Peale selle tuleks mõelda *Linux* 'i poolt pakutava autentimisteenuse *KERBEROS* ja turvasoklite kihi (*Secure Socket Layer (SSL)*) kasutamisele.
- *Linux* 'i määratlused peaksid olema seadistatud nii, et rekursiivsete funktsioonide üleskutse ei viiks operatsioonisüsteemi ülekoormamiseni (vaata G 3.69 Unixi süsteemiteenuste (USS) väär konfigureerimine z/OS-is).

Linux 'i autentimine z/OS RACF kaudu

Tuleks mõelda *Linux* 'i kasutajate autentimisele keskse z/OS RACF-i kaudu, kasutades selleks lihtsustatud kataloogisirvimise protokolli (*LDAP - Lightweight Directory Access Protocol*) ja *Linux* 'ile lisatavat autentimismoodulit (PAM-*Pluggable Authentication Module*). Eriti suure hulga hallatavate Linuxi süsteemide korral toob see kaasa kulude vähenemise.

zSeries masinate *Linux* 'i ja *Krypto* riistvara

zSeries -süsteemi saab varustada krüptograafiliste protsessorkaartidega PCICA (*Peripheral Component Interconnect Cryptographic Accelerator*) või PCICC (*eripheral Component Interconnect Cryptographic Coprocessor*). Need kaardid aitavad parandada *Krypto* funktsioonide jõudlust ja neid kasutatakse digitaalsete võtmete turvalisemaks hoidmiseks. Mõlemaid kaarte toetab ka *Linux*. Kuna *Linux* ei toeta *CCF* i (*Cryptographic Coprocessor Feature*), tuleks mõelda *Krypto* kaartide kasutamisele. Seda saab teostada kõigi ülalnimetatud installeerimismeetodite korral. *z/VM* i all saavad *Linux* 'i süsteemid üheaegselt ja üksteisest sõltumata *Krypto* kaarte kasutada.

Linux 'i ja *zSeries* riistvara kommunikatsioon

Ühele *zSeries* riistvarale, kas siis LPAR-režiimi või z/VM-i alla installeeritud *z/OS* või *Linux*'i operatsioonisüsteemide kommunikatsioon peaks toimuma võrgusiseste kanalite kaudu, näiteks *HiperSockets* 'i või virtuaalse *CTC* ühenduse (*Chanel-to-Chanel*) kaudu. See võimaldab luua operatsioonisüsteemide vahel kiire *TCP/IP* -ühenduse. Võrreldes kommunikatsiooniga lokaalvõrgus vähendatakse seeläbi vigu ja rünnakuvõimalusi, kuna informatsioon liigub ühest süsteemist teise riistvarasiseselt.

Täiendavad kontrollküsimused:

- Kas riistvara on volitamata ligipääsu eest piisavalt kaitstud?
- Kas *RACF* i kasutatakse *z/VM* i turvasüsteemina?
- Kas operatsioonisüsteemide kommunikatsioon, mis on installeeritud samal *zSeries* riistvaral, toimub sisemiste ühenduste kaudu (*HiperSockets,* virtuaalne CTC)?

M 4.213 Logimisprotsessi kaitse z/OS all

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: Administraator

Tuleb kaitsta ligipääsu z/OS-süsteemile ja eelkõige sisselogimisprotsessi. Siinkohal tuleb järgida järgnevaid soovitusi:

- Kõik ligipääsuks mittevajalikud teenused ja pordid tuleks sulgeda. RACF-profiiliga tuleks vajalikele teenustele ja portidele ligipääs piirata. Lubada tohib ligipääsu ainult volitatud isikutele.
- Paroolide kasutamist tuleks piirata, nagu on kirjeldatud meetmes M 2.11 Paroolide kasutamise reeglid . Ligipääsu z/OS-süsteemile avalike võrkude kaudu (Internet) tuleb piirat, kuna kõik kasutajakontod lukustuvad valede paroolisisestuste tõttu. Seda saab hetkel lahendada ainult digitaalsete sertifikaatide abil. Tuleks arvestada sellega, et *RACF Reply* automatiseerimist ei kasutataks turvalisusest lähtuvalt kasutajakontodel, millel on atribuut *SPECIAL.* See takistab selle, et *SPECIAL* atribuudiga kasutajakontod automaatselt lukustuvad.
- *SYS1.UADS* hoolitseb selle eest, et RACF-i rikke korral oleks endiselt võimalik süsteemile ligi pääseda. Sellesse faili võib sisse kanda ainult *IBMUSER* 'i või ühe (ka mitu) hädakasutajat.

Peale selle kehtivad soovitused, mis on toodud meetmes M 4.15 Turvaline sisselogimine .

Täiendavad kontrollküsimused:

- Kas *SYS1.UADS*- is on ohutunnuseid?
- Kas mittevajalikud TCP/IP teenused on sisselogimiseks suletud?

M 4.214 Salvestuskandjate haldus z/OS-süsteemides

Algatamise eest vastutavad: Infoturbe osakond, IT-juht
Rakendamise eest vastutavad: Administraator

Kõvaketaste ja lintide kaitseks Z/OS -süsteemides tuleks järgida järgnevaid nõuandeid.

Kõvakettad

- Kõvakettaid tuleb kaitsta vastavate PACF -profiilidega (Resource Access Control Facility)ja RACF -klassidega. RACF -is tuleb sisse seada profiil kõvaketta VTOC (Volume Table of Content) kaitseks. Tuleks mõelda töötamisele eelnevalt seadistatud profiilidega, näiteks VTOC**.
- Ülemkataloog tuleb RACF-profiiliga kaitsta ja töötajatele tuleb anda ainult lugemisõigused (READ). Kirjutamisõigustega ligipääs on lubatud ainult töötajatele, kes seda oma töös vajavad (näiteks ALIAS 'e tekitamiseks).
- Kõvaketaste haldamiseks ja ülevaate säilitamiseks kõvakettakapis olevate kõvaketaste üle on vajalik kõvaketta hõivatuse plaan. See plaan peab sisaldama vähemalt kõvaketta aadressi, kõvaketta nime, SMS kõvaketta pooli nime, mille juurde kõvaketas kuulub (SMS) ja kõvakettakapi nime, kuhu konkreetne kõvaketas on paigutatud. See informatsioon tuleb kirjalikult dokumenteerida.
- Kõvaketaste haldamiseks vajalikke programme tuleb kaitsta (näiteks lähtestamine, andmete kopeerimine). Programmid võivad olla kasutatavad ainult töötajatele, kes neid oma tööks vajavad. Programmidel ei tohiks olla võimalik kasutada atribuuti OPERATIONS.
- ISMF i (Interactive Storage Management Facility) haldusfunktsioon peab RACF -profiili kaudu kaitstud olema. Seda funktsiooni võivad kasutada ainult volitatud kasutajad.
- z/OS-käsklusi, mille abiga on võimalik lisada süsteemi kõvakettaid ja linte ning neid süsteemist eemaldada, tuleb vastava RACF profiili kaudu kaitsta. Neid käsklusi tohivad teostada ainult volitatud kasutajad (vaata M 4.210 Operatsioonisüsteemi z/OS turvaline käitus .
- SMS-i (System Managed Storage) ACS -standardprogrammid (Automatic Class Selection) peavad olema kaitstud ja neid tohivad kohandada ainult volitatud kasutajad. Kasutatavad peaksid olema ACS -failide varunduskoopiad, mida oleks võimalik hädaolukorras taastada.

Magnetribad

- Magnetribasid tuleb kaitsta vastavate RACF-profiilide ja RACF-klasside kaudu.
- Magnetribade korral haldusprogrammide kasutamisel tuleb arvestada nende programmide iseärasustega (näiteks TAPEVOL ja TAPEDSN klasside kasutamine).
- Vastavate abinõude ja reeglite kaudu tuleb kindlustada, et kasutuses oleks piisav hulk lindijaamu ja et need ei oleks asjatult kaua paigutustega blokeeritud.
- Et kaitsta magnetribal asuvaid andmeid, tuleb z/OS -süsteemides sulgeda funktsioon Bypass Label Processing. Selle tarvis tuleb General Ressource klassis FACILITY luua profiil nimega ICHBLP. Seda profiili tuleb kaitsta UACC=NONE-ga. Pidevat ligipääsu sellele funktsioonile võib lubada ainult põhjendatud erandjuhtudel.

HSM (Hierarchical Storage Manager)

- HSM i konfigureerimine toimub ühes liikmes (ARCCMDxx). Siia tuleb sisestada ka HSM i haldajate kasutajanimed ja paroolid. Eespool mainitud liiget sisaldav fail peab olema RACF -profiiliga kaitstud, et sellele pääseksid ligi vaid vastutavad töötajad.
- Magnetlintidel paiknevad failid, mis kuuluvad migratsiooniastmesse 2. Neid linte tuleb kaitsta ja neid võib töödelda ainult HSMiga.
- Vältimaks tootmise takistamist ENQUEUES ja RESERVES kaudu, tuleks HSM i varunduseks valida sobiv ajahetk. Hilisemal ajahetkel tuleb kindlaks määrata, millised plaadid salvestatakse ja kuidas peaks plaatide salvestus toimuma (Full Volume või Incremental salvestamine).

Täiendavad kontrollküsimused:

- Kas Bypass Label Processing on desaktiveeritud?
- Kas plaadipaigutusplaan on olemas?
- Kas magnetriba kaitse on aktiveeritud?
- Kas HSM on piisavalt kaitstud?

M 4.215 Turvakriitiliste z/OS-utiliitide kaitse

Algatamise eest vastutavad: IT-juht, infoturbe osakond

Rakendamise eest vastutavad: Administraator

z/OS -süsteemis on süsteemiprogrammeerijate käsutuses RACF-haldamisja mäluhaldusutiliidid, mille kaudu on vastava volituse korral võimalik teha z/OSsüsteemis põhjalikke muudatusi. Nende programmide turvaliseks rakendamiseks tuleb järgida järgnevaid nõuandeid:

Turvakriitiliste programmide kaitse

Turvakriitilisi utiliite tuleb RACF -turvasüsteemi (Resource Access Control Facility) kaudu vastavalt kaitsta. Utiliite tohivad kasutada ainult selleks ettenähtud töötajad. Samuti tuleb kaitsta programmide Alias- nimesid.

Loend turvakriitilisi utiliite:

- AMASZAP, AMASPZAP, IMASZAP
- ADRDSSU
- SYSIEH
- SMFDUMP
- ICKDSF
- IEHATLAS
- IEHINITT
- PGTFPF00
- IRRDBU00
- ICHDSM00
- IRRUT100, IRRUT200, IRRUT300, IRRUT400
- RESOLVE

Kaitse kriitiliste TSO -käskluste eest

TSO -käsklusi (Time Sharing Option), mille taga peituvad turvakriitilised utiliidid, tuleb TSOKEY00 (z/OS Parmlib 'is) kaudu kaitsta nii, et neid saaksid kasutada ainult volitatud töötajad.

Turvakriitiliste programmide volitamata installeerimine

Tuleb kindlustada, et võõrprogramme ei saaks volitamata installeerida. Internetis leidub programme, mis võivad pääseda väga sügavale z/OS-süsteemi. Paljudel süsteemiprogrammeerijatel on isekirjutatud programme, mis nende tööd lihtsustavad, aga kuid võivad teatud juhtudel põhjustada z/OS -süsteemis ka väga põhjalikke muudatusi. Selliste programmide kontrollimatut installeerimist ja käitamist tuleb vastavate turvameetmetega takistada (vt M 4.209 z/OS-süsteemide turvaline aluskonfiguratsioon ja M 4.211 z/OS turvasüsteemi RACF kasutamine). Kui selliseid programme aga vajatakse, tuleb nad süsteemi lisada ametliku installeerimisprotsessi teel.

Kontrollküsimus:

- Kas on kindlustatud, et turvakriitilisi utiliite ja TSO -käsklusi saavad kasutada ainult vastavalt volitatud töötajad?

M 4.216 z/OS-süsteemipiirangute kehtestamine

Algatamise eest vastutavad: IT-juht
Rakendamise eest vastutavad: Administraator

z/OS -süsteemi käitamiseks on tähtis teada süsteemi piiranguid, et määrata ressursside maksimaalne koormus. Järgida tuleb järgnevaid nõuandeid:

- Süsteemipiirangute kommunikatsioon - Süsteemipiirangud peavad administraatorile ja tarkvaraomanikule teada olema. Süsteemipiirangute hulka kuuluvad andmed, nagu faili maksimaalne suurus, maksimaalselt kasutatav põhimälu, FTP-ülekannete maksimaalne failisuurus (*File Tranfer Program*), *LPAR* ide arv (*Logical Partitions* zSeries suurarvutil), süsteemide arv *Sysplex* -rööpklastris ja muud taolised määratlused. Süsteemipiirangud peavad olema teada, et vältida rakenduste teostamisel vigu.
- Magnetlintjaam - Kasutuses olevate magnetlintjaamade arv peaks olema kooskõlas tarkvaraomaniku vajadustega. Vältimaks magnetlintjaama korraga kasutamist kõigi rakenduste poolt, peavad rakenduste arendajad ja rakenduste eest vastutavad isikud kokku leppima, millal ja mis rakendused magnetlintjaamale ligi pääsevad.
- Kõvakettad - Rakenduste omanikud peavad kindlaks määrama ja planeerima, milline peaks olema kõvaketaste maht. Ruumihaldus (*Space Management*) peab jälgima, et kõvaketastel olev vaba ruum oleks piisav. Vastasel korral tuleb sellest teatada rakenduse omanikule.
- Algatajad - Algatajad, mis on *JES2* -s (*Job Entery Subsystem*) aktiveeritud, juhivad pakketööde paralleelset töötlemist. Töötlemiste arv peab olema kohandatud riistvara eeldustega. Töötlemiste arv ja sellest tulenevad piirangud peavad rakenduse omanikule teada olema.
- *TSO* -rakendus ja aadressiruumid - *TSO* maksimaalne kasutajate arv ja maksimaalne aadressiruumide arv peab olema kohandatud riistvara eeldustega.
- Kokkuhoiuvõimalused - Süsteemiressursside kokkuhoidmiseks võib näiteks kasutaja pärast 30- minutilist inaktiivsust süsteemist automaatselt välja logida. Siinjuures on tarvis kontrollida, kas see tekitab käideldavate rakendustega seotud probleeme. Kasutajaid tuleb vastavast regulatsioonist teavitada.

Täiendavad kontrollküsimused:

- Kas süsteemipiirangud on administraatoritele ja rakenduste omanikele teada?
- Kas kõvaketa vaba ruumi kontrollitakse kindla aja tagant?

M 4.217 z/OS-süsteemide koormuse haldus

Algatamise eest vastutavad: IT-juht
Rakendamise eest vastutavad: Spetsialist, administraator

Ressursside haldamine *Sysplex* -rööpklastris (aga ka üksiksüsteemis) toimub *z/OS* -operatsioonisüsteemi *WLM* (*Work Load Manager*) komponendi kaudu. *WLM*- kasutuse turvalisuse tagamiseks tuleb järgida järgnevaid nõuandeid:

- *Couple-Datasets'* i kaitse - *WLM* i jaoks vajalikke *Couple-Datasets'* e tuleb kaitsta vastavate *PACF* -profiilidega (*Resource Access Control Facility*). *WLM* -tööfailidele, milleks on üks või mitu PDS-faili (*Partitioned Datasets*), kehtivad samad reeglid. Failide paigutamise programmi tuleb kaitsta *RACF Facility* -profiili *MVSADMIN.WLM.POLICY kaudu.*
- *Modify* käskluse kaitse - *WLM* -suvandeid on võimalik *Modify* -käskluse kaudu muuta. See käsklus võib olla ainult koolitatud operaatorite või süsteemiprogrammeerijate käsutuses.
- *Reset*- käskluse kaitse - *Reset* -käsklust tuleb kaitsta nii, et ainult volitatud töötajad võivad käimasolevate tööde *WLM* -reegleid muuta.
- *WLM* -rakenduste kaitse - *WLM* i definitsioone hooldatakse *ISPF* il baseeruva *WLM* -dialoogiga (*Interactive System Productivity Facility*). Ligipääs *WLM* -rakendusele peaks olema *RACF Facility* -Profil *MVSADMIN.WLM.POLICY* kaudu kaitstud ja ainult volitatud töötajatele kasutatav olema (teeninduse ja mahu haldus).
- Kooskõlas olev autoriseerimine - Kindlaksmääratud *WLM* -standardeid (näiteks *Service Class*) saab muuta nii *MVS* -käskluste kui ka *SDSF* -liidese (*System Display and Search Facility*) kaudu. Tuleb kindlustada, et *WLM* i muutmise õigused oleksid samad nii *MVS* - käskluste kaudu kui ka *SDSF* kaudu muudatusi tehes.

Täiendavad kontrollküsimused:

- Kas *Couple-Datasets'* id on *RACF* -profiilidega kaitstud?
- Kas *WLM* rakendus on kaitstud nii, et sellele omavad ligipääsu ainult volitatud töötajad?
- Kas käsklused, mis võivad *WLM* i mõjutada, on piisavalt kaitstud?

M 4.218 Teave märgistike teisenduse kohta z/OS -süsteemides

Algatamise eest vastutavad: IT-juht
Rakendamise eest vastutavad: Tarkvaraarendajad, administraator

z/OS -süsteem töötab tavaliselt EBCDIC -koodiga (Extended Binary Coded Decimal Interchange Code) (laiendatud kahend-kümnend-infovahetuskood). See kehtib nii MSV -failide (Multible Virtual Storage) kohta kui ka HFS -failide (hierarhilise failisüsteemi) (Hierarchical File System) kohta. Erandid on võimalikud ainult zFS -failisüsteemis. Windows 'i ja Unix 'i süsteemid töötavad tavaliselt ASCII -koodiga (American Standard Code for Information Interchange) (Ameerika Informatsioonivahetuse Standardkood). Erinevate süsteemide vahelise kommunikatsiooni juures tuleb järgida järgnevaid reegleid:

- Tekstifailide edastamisel tuleb kasutada teisendustabelit, mis teisendab koodid. z/OS-operatsioonisüsteemis on need tabelid juba olemas. Tuleb aga jälgida, et kasutataks õiget tabelit.
- Binaarandmete edastamisel tuleb teisendusfunktsioon välja lülitada, sest vastasel juhul muutuvad andmed kasutuks.
- Failide edastamisel Unix 'i või Windows 'i süsteemist z/OS -süsteemi HFS 'i ja vastupidi, FTP (File Transfer Program) kaudu, tuleb jälgida, et edastamisel oleks valitud õige teisendussuvand.
- Eriti programmi lähtekoodi edastamisel tuleb kontrollida, kas kõik märgid tõlgiti õigesti (siinkohal eriti mõned erimärgid), et teisendamisel ei tekiks märkamatuid programmivigu. Näiteks mõningatel juhtudel ei põhjusta valed märgid konstantsetes definitsioonides kompileerimisvigu, vaid ilmnevad alles hiljem programmi kasutamise käigus.

Täiendavad kontrollküsimused:

- Kas märkide teisendamiseks kasutatakse õigeid tabeleid?
- Kas FTP -tööd on varustatud õigete edastussuvanditega?

M 4.219 z/OS-tarkvara litsentsivõtmete haldus

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: Administraator, üksikute IT-rakenduste eest vastutavad

Mõningad tootjad kasutavad oma programmide haldamiseks niinimetatud *Activation-Keys* -id (litsentsivõtmed). Need litsentsivõtmed aeguvad mingi aja tagant ja süsteemihaldaja peab neid uuendama. Arvestada tuleks järgnevate nõuannetega:

Litsentsivõtmete uuendamine

Tuleb luua meetod litsentsivõtmete õigeaegseks uuendamiseks. Vastasel korral võib juhtuda, et aegunud litsentsivõtmete tõttu puudub tarkvarafunktsioonide kättesaadavus. Litsentsivõtmete kehtivused tuleb dokumenteerida. Dokumentatsioon peab kõigile süsteemihaldajatele kättesaadav olema. Litsentsivõtmete kehtivust tuleks kindla aja tagant kontrollida.

Hoiatus enne litsentsi lõppemist

Kui kasutuses on tarkvara, mis lõpetab litsentsi lõppedes ilma hoiatuseta töö, tuleks tootjaga läbi rääkida, et antud olukorda parandada. Tarkvara peaks näiteks enne litsentsivõtmete aegumist andma hoiatuse või lubama hädavõtmete kasutamist.

Täiendavad kontrollküsimused:

- Kas on sisse seatud litsentsivõtmete haldus?
- Kas litsentsivõtmete kehtivust kontrollitakse kindla aja tagant?

M 4.220 Unixi süsteemiteenuste (USS) kaitse z/OS-süsteemides

Algatamise eest vastutavad: Infoturbe osakond, IT-juht
Rakendamise eest vastutavad: Asjatundja, administraator

Unixi süsteemiteenused (USS) on Unixi porditava operatsioonisüsteemiliidesega (*Posix*) ühilduv alamsüsteem, mis töötab z/OS-operatsioonisüsteemis. Unixi süsteemiteenuste kaitseks tuleb rakendada meetmeid, mis on kirjeldatud moodulis B 3.102 Server Unixi all . Lisaks tuleb järgida veel mõningaid turvaaspekte:

- Kahekordne UID (kasutajaident, ID-kood) väljastamine - Tuleb tagada, et ühte UID ei esineks kaks korda, kuna vastasel juhul puudub võimalus määratelda täpne MVS-i kasutaja ID.
- HFS failid - HFS-faile (hierarhiline failisüsteem), mis sisaldavad Unixi failisüsteemi, tuleb RACF-failiprofiiliga kaitsta. RACF-profiilile peaks ligipääsu omama ainult *Unix Started Task*. HFS-failide varundus peaks toimuma HSM-funktsioonide (*Hierarchical Storage Manage*) kaudu. HSF-faile ei tohiks aga HSM-i kaudu teisaldada. See soovitus kehtib ka zFS-failidele. *Root*-failisüsteemi peab paigaldama faili suvandiga *READ-ONLY* (kirjutuskaitse). Kasutajate HFS-faile tuleks kaitsta RACF-profiiliga vastava kasutajakonto kaudu. Et kasutajad, kelle on HFS-faile ei peaks käsklusi *mount* ja *unmount* ise läbi viima, tuleks mõelda *Automount*- funktsiooni kasutamisele.
- BPXPRMxx liige - Põhilised USS-parameetrid defineeritakse *Parmlib* -is kasutaja BPXPRMxx-is. Eraldi parameetrid kirjeldavad vabasid ressursse (näiteks *MAXPROCSYS* või *MAXPROCUSER*). Vältimaks süsteemi ülekoormust, tuleb need parameetrid määrata vastavalt *zSeries* riistvara ja LPAR-i jõudlusele.
- Selle liikme määratlemiseks tuleks kasutada sümboolseid muutujaid.
- APF-volitamine - USS-failisüsteemis ei tohiks olla *File Security Pacet* (FSP) kaudu APF volitamist (*Authorized Program Facility*). Selle asemel tuleks laadida z/OS-operatsioonisüsteemi APF failid.
- Superkasutaja (*Superuser*) UID (0) ja UNIXPRIV - Mitmed käsklused, mis teistes Unixi süsteemides vajavad *Superuser'i* (ülikasutaja) (UID 0) õigusi, saab USS-i korral kaitsta RACF-profiilidega RACF-klassis *UNIXPRIV*. See tähendab, et süsteemihaldajate õigusi saab hallata RACF kaudu ja *Superuser'i* õigusi läheb veel vaja ainult väheste erandjuhtude tarvis.
- FACILITY klassi BPX.xxx RACF-profiilid - Paljude USS-funktsioonide kindlustamiseks tuleks lisaks *UNIXPRIV* klassi profiilidele kasutada ka *FACILITY* klassi *BPX.xxx* RACF-profiile. Paljudel juhtudel saab sellega vältida kõrgema volitamise (näiteks UID 0).
- Auditeerimine ja seire - USS-i auditeerimiseks ja seireks tuleks kasutada samasid mehhanisme, mida kasutatakse z/OS-süsteemide korral. USS-i protsessid kirjutavad SMF-lauseid. Ligipääsurikkumised tõlgitakse RACF-teadeteks ja tekitavad teated *Syslog* 'is. Mõlemaid allikaid tuleks analüüsida nagu on kirjeldatud punktis M2.291 *z/OS turvaaruanne ja -revisjonid.* Mõnin-

gad Unixi tegumid, nagu näiteks veebiserverid, kirjutavad logiinformatsiooni omaenda failidesse. Kui vastavad programmid on aktiveeritud, siis tuleks ka neid analüüsida.

Märgistike teisendamine

USS-süsteemi kasutamisel tuleks järgida nõuandeid, mis on antud punktis M 4.218 Teave märgistike teisenduse kohta z/OS -süsteemides .

Täiendavad kontrollküsimused:

- Kas USS-failisüsteemis loobutakse APF volitusega failidest?
- Kas *root*- failisüsteem on paigaldatud suvandiga *READ-ONLY* (kirjutuskaitse)?
- Kas kõik HFS-failid on RACF-profiilidega kaitstud?
- Kas USS-alamsüsteemi auditeeritakse?

M 4.221 Sysplex -rööpklastrid operatsioonisüsteemis z/OS

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: Vastutav spetsialist, administraator

Sysplex -rööpklaster on mitme *z/OS* süsteemi kooslus, mis paistavad väliselt ühena. *z/OS* -süsteemid võivad seejuures töötada nii ühel kui ka mitmel *LPAR* il *(Logical Partitions).* Süsteemi sünkroniseerimiseks on nad kõik ühendatud *Coupling Facility*- ga. Mitme *LPAR* i kasutamisel tuleb süsteemiaja *(Clock)* sünkroniseerimiseks kasutada niinimetatud *Timer Facility'* t. *Sysplex* -rööpklastrit kasutatakse siis, kui nõudmised käitlemisele ja jõudlusele on kõrged. Kõik *Sysplex* -rööpklastri z/OS süsteemid laetakse samalt kõvakettalt. Üksikuid *z/OS* - operatsioonisüsteeme eristatakse individuaalsete süsteemimääratluste kaudu. Sysplex-rööpklastri kasutamisel tuleks järgida järgnevaid soovitusi:

- *Coupling Facility* kasutamine -*Coupling Facility* (*CF*) ühendab omavahel kõik *LPAR* id. Kasutusse antakse ka ühiselt kasutatav mälu, mis on jagatud erinevateks objektideks nn *Coupling Facility Structures*. Ligipääs *CF* ile toimub *XES* i *(Cross-System Extended Services)* kaudu. *CF* is võib eristada kolme erinevat mälutüüpi:
- *Cache Structures* - See struktuur annab suure jõudlusega mälud mitme kasutaja ühisesse käsutusse. Kui kõvakettalt loetakse andmeid, kirjutatakse selle koopia lokaalsesse puhvermällu. Peale selle on valikuliselt võimalik üks koopia paigutada ka *Coupling Facility Cache Structure'* sse.
- *List Structures* - See struktuur lubab info jagamist mitme kasutaja vahel, mis on loendites *(Message passing)* või ootejärjekorras *(Queues of work).*
- *Lock Structures* - Selle struktuuri abil saab kõigist LPAR-idest juhtida ressursside kasutamist kas *Shared*- või *Exclusive*- režiimis.
- *Kasutamine* - *Sysplex*- rööpklastri kasutuselevõtu plaanides, näiteks käideldavuse põhjustel, peaks *Coupling Facility'* t võimalusel kasutama koos *Data Sharing'* uga. See kehtib *JES2/3* (*Job Entry Subsystem*), *RACF* (*Resource Access Control Facility*), *VTAM* (*Virtual Telecommunication Access Method*), *System Logger*, *CICS*, *IMS* ja *DB2* kohta. Kindlaks tuleb teha maht, milles *Coupling Facility* paigaldada, et tagada kogu süsteemi nõudlus.

Coupling Facilities määratletakse ja installeeritakse HMC *(Host Managment Consol)* kaudu. Soovitusi selle konsooli kasutamise kohta leiate meetmest M 4.207 z/OS-süsteemiterminalide kasutamine ja kaitse .

Couple Datasets

Couple Datasets'e kasutatakse *XCF* (*Cross-System Coupling Facility*) poolt, et *LPAR* ide kaudu gruppide või liikmete informatsiooni kontrollida. Kõik *Sysplex* -rööpklastri LPARid peavad nendele andmetele ligi pääsema. Soovituslik on kasutada *Alternate Couple Datasets* 'e. Operatsioonisüsteemis *z/OS* peavad *Couple*

Datasets' id *RACF* i poolt kaitstud olema. Ainult töötajad ja nende asendajad, kes oma töö käigus vastavaid andmeid töötlevad, peaksid saama õiguse neid andmeid muuta (vt M 4.211 z/OS turvasüsteemi RACF kasutamine *). Couple Datasets'* i vormindamiseks saab kasutada utiliiti *IXCLIDSU*. Seda programmi peaks RACF-iga kaitsma (Class *PROGRAM*). Administraator utiliit *XCMIAPU* abil saab määratleda *CFRM-Policy* (*Coupling Facility Resource Management*). See peaks olema kaitstud RACF-is läbi vastava *Facility*- Profiili, et ainult autoriseeritud isikud omaksid sellele ligipääsu. Soovitusi kriitiliste programmide kaitseks leiate meetmest M 4.215 Turvakriitiliste z/OS-utiliitide kaitse .

Sysplex käsklused

Operatsioonisüsteem *z/OS* pakub haldamiseks ja kontrolliks süsteemikäsklust *SETXCF.* See toetab järgmisi tegevusi:

- *Couple Dataset'* i määratlemine
- Vahetamine *Primary* ja *Backup-Couple Dataset* vahel
- Uue *CFRM-Policy* aktiveerimine
- *PATHIN*- või *PATHOUT*- ühenduse käivitamine
- Struktuurimahu muutmine *(Structure Size)*
- Struktuuri taastamine pärast struktuuririket

Selle käskluse kaitseks (ka kõigi teiste käskluste, mida *Sysplex* -rööpklaster toetab) tuleb määratleda vastavad RACF-profiilid (vaata M 4.210 Operatsioonisüsteemi z/OS turvaline käitus *).*

XCF kontroll

RMF (*Resource Measurement Facility*) loob nii nimetatud *XCF Activity Report'*i. Vastavat raportit saaks kasutada z/OS operatsioonisüsteemide vahelise infovahetuse jälgimiseks, et avastada kommunikatsioonisulgusid ja *Deadlock*-situatsioone ning võtta kasutusele ennetavaid meetmeid.

Ühtne *RACF* -andmebaas

Kogu *Sysplex* -rööpklastri *LPAR* ide jaoks peaks kasutama ühtsete *RACF* -määratlustega *RACF*- andmebaasi.

Standardid

Ülevaatlikkuse ja hooldatavuse parandamiseks peaks järgmistel aladel kehtestama standardid:

- PARMLIB liikmete parameetrid tuleb standardiseerida. Kõik nimed Sysplex-rööpklastris peavad olema üheselt mõistetavad. Siia kuuluvad: andmekogumite nimed, alamsüsteemide nimed, protsesside nimed, VTAM-rakenduste ID-d (vaata M 2.285 z/OS süsteemimääratluste normide määramine)
- Lokaalsete määratluste süsteemiseaded nii *PARMLIB* is kui ka *PROCLIB* is peaksid olema ühtsed. Soovitatav on kõigi määratletud liikmete struktuuride identne ülesehitus.
- *SMS* struktuur (*System Managed Storage*) peab olema ühtne terves *Sysplex* -rööpklastris.
- Kõigil *LPAR* idel peaks olema võimalikult sarnane süsteemitarkvara (teatud juhtudel on seetõttu vajalik tarkvaralitsentside kohaldamine).

Dimensioneerimine

Oluline on jälgida kõvaketta juhtimisüksuse puhvermälu, tööplaatide, *Coupling Facility* ja *SPOOL* -plaatide õiget dimensioneerimist. Kõigi nende osade suurus sõltub eelkõige *Sysplex*- rööpklastril paiknevate rakenduste tüübist ja nõuetest. Paljudel juhtudel leiab selle kohta informatsiooni ka tarkvaratootjate kasutusjuhenditest.

Serialiseerimine

Süsteemi toimingute serialiseerimiseks tuleb luua *GRS* -ühend (*Global Resource Serialization*). *GRS* -režiim peab olema liikme *IEASYS*- is või *PARMLIB*- is määratletud (*RING*- või *STAR*- režiim). Võimalusel tuleks kasutada uuemat *STAR*-režiimi, kuna see tagab *Couple Datasets'* il salvestatud *RNL* de (*Resource Name Lists*) kiirema töötlemise. Reeglina on *STAR*- režiim ka käideldavuse osas parem. *STAR*- režiim on võimalik ainult *Coupling Facility'* ga

Kõrge käideldavus tänu liiasusele

Kõrgete või väga kõrgete käideldavusnõuete korral tuleks kontrollida, kas järgnevad liiasusmehhanismid on otstarbekohased:

- *RACF* primaarse ja varundus-andmebaasiga
- Teine *Coupling Facility*
- Alternatiivne *Couple Datasets*
- Teine taimer (ühendatud kõrgkäideldavusseadega *FC 4048,* millel on eraldi vooluringe)
- Varundussüsteemid, et rikke esinemisel oleks võimalik süsteem koheselt taaskäivitada

- CTC-GRS ring (*ESCON* kanaliühendus / *General Resource Seriali-zation*)
- MCS-peakonsooli varundus (*Multiple Console Support*)
- Tähtsate kontrollfailide andmete kaitse. Võimalusel realiseerida *Concurrent Copy'* ga (utiliit *ADRDSSU*)

Lisainformatsiooni leiate punktist M 6.93 z/OS süsteemide hädaolukorraks valmisoleku plaan .

Ligipääs kõvaketastele

Kõvaketta ligipääsudel tuleks arvestada järgnevate soovitustega:

- *Sysplex* -rööpklaster ei tohiks omada ühtegi süsteemivälist kõvaketast. Kõvakettaid, mis ei kuulu süsteemi, peaks kasutama ainult andmete taastamiseks.
- Teiste *Sysplex* -rööpklastritesse mitte kuuluvate süsteemide ligipääs kõvaketastele peaks tootmistingimustes olema keelatud.
- Kui on vajadus suure jõudluse järele, tuleks kaaluda *Enhanced Catalog Sharing'* u kasutamist.
- Võimalusel ei tohiks samas *Sysplex* -rööpklastris koos käitada katsetus-/arendussüsteeme ja tootmissüsteeme.
- Kõigi *Sysplex* -rööpklastris paiknevatele z/OS süsteemidele tuleks operatsioonisüsteem laadida samalt süsteemiplaadilt.

Sümboolsed muutujad

PARMLIB i määratlemisel tuleks võimalikult paljudes kohtades kasutada sümboolseid muutujaid. See aitab vältida vigu süsteemi hooldamisel ja kergendab *System-Cloning'* ut.

System Logger

System Logger' it tuleks kasutada *Staging Dataset'* iga. (Rikke korral pääsevad teised süsteemid võrgus sellele andmekogule ligi).

Konsooliteadete vähendamine

Konsooliteadete vähendamiseks ja ülevaatlikkuse säilitamiseks on soovitatav aktiveerida *Message*- filter (vt M 4.210 Operatsioonisüsteemi z/OS turvaline käitus). See on oluline, kuna *Sysplex* -rööpklastri kõikide z/OS operatsioonisüsteemide teated kuvatakse MVS-konsoolis.

Täiendavad kontrollküsimused:

- Kas kasutatakse *Coupling Facility'* t?
- Kas *Sysplex* -rööpklastri tähtsamad osad on paigaldatud liiasusega?
- Kas *STAR* -režiimis esineb GRS-võrk?
- Kas konsooliteateid filtreeritakse?

M 4.222 Turvaprokside õige konfigureerimine

Algatamise eest vastutavad: IT-juht, IT-turvaspetsialist

Rakendamise eest vastutavad: Administraator

Selles peatükis võetakse kokku soovitused turvaprokside vaikeseadistuseks.

Need seadistused võivad aga mõjutada vastavate sisude funktsionaalsust ja tuleb seega seadistada vastavalt oma vajadustele (näiteks puuduva JavaScript 'i tõttu ei ole enam võimalik veebilehtede käitamine).

HTTP

Kliendi turvalisusest lähtuvalt on aktiivsisu filtreerimine kesksel kohal (vt M 4.100 Tulemüür ja aktiivsisu). Klientide puhul, kellel on kõrge turvavajadus, tuleks konfidentsiaalsusest lähtuvalt kõik veebilehel paiknevad aktiivsisud filtreerida. Teatud juhtudel võib usaldusväärsete lehekülgede korral aktiivsisusid lubada (White List strateegia). Vastav White List ei tohiks aga muutuda liiga mahukaks ning seda tuleks kindla aja tagant hallata.

HTTP -proksidele soovitatavad seaded:

- HTTPS -ühenduse sulgemine, kui ei kasutata HTTP -proksit
- Küpsiste keelamine (mõningate üksikute lubamine)
- Brauseri tuvastamise asendamine või filtreerimine
- Järgnevate informatsioonide filtreerimine Request-HTTP-Header 'ist:

1. Referer (kui lahkutakse mõnest domeenist)
2. Vi,
3. From

- Järgneva informatsiooni filtreerimine Response-HTTP-Header 'ist:

1. server

- Kõigi URL -ide vabastamine. Vajadusel üksikute kahtlaste URL -ide blokeerimine.
- Piiramine ainult vajalikele MIME-tüüpidele.

Tähelepanu: White List strateegiat „Keelata kõik, mis ei ole kategooriliselt lubatud" saab MIME-tüüpide keelamisel või lubamisel ainult tinglikult kasutada. Kuna veebileheküljed kasutavad suurel hulga erinevaid MIME-tüüpe, siis on relevantsete tüüpide keelustamine ja samas WWW -funktsionaalsuse säilitamine keerukas. Pragmaatiline toimimisviis oleks eriti kahtlaste MIME-tüüpide keelustamine. Kõrge kaitsetaseme tagamiseks peab administraator sellist keelunimekirja pidevalt uuendama.

HTTPS

Kahjurvara filtreerimisel tuleks kasutada samu meetodeid nagu HTTP -proksi korral. HTTPS -proksi on keskne otsustusinstants, mis võtab kasutajalt enamjaolt kogu kontrolli sertifikaatide üle. Sellest tulenevalt on HTTPS -proksi seadistus problemaatiliste sertifikaatide korral erilise tähtsusega. Järgnev tabel annab ülevaate soovitatavatest seadistustest:

Otsus	Ettepanek seadistuseks
Sertifikaatide lubamine, mis on väljastatud sertifitseerimiskeskuste poolt	Enimlevinud brauserites kasutatavaid sertifitseerimiskeskuseid võib usaldada. Lähtutakse sellest, et sertifitseerimiskeskuste usaldusväärsus on brauserite tootjate poolt kontrollitud. Sertifikaadikeskuste usaldatavust tuleks regulaarselt kontrollida. Vajadusel on võimalik sertifikaadikeskuseid lisada. Seda tohib aga teha alles siis, kui on kindlustatud sertifikaadikeskuse usaldusväärsus.
Sertifikaatide aktsepteerimine, mis ei ole väljastatud sertifikaadikeskuse poolt („ *self signed certificates“*)	Ise loodud sertifikaate kasutatakse ainult krüpteerimiseks ja see ei paku võimalust veebilehe autentsuse määratlemiseks. Selliseid sertifikaate tohiks aktsepteerida ainult erandjuhtudel ning ka siis alles pärast põhjalikku kontrolli.
Veebileheni jõudmine tunneli kaudu	Tunneli kasutamisel minnakse pahavara filtrist mööda. Sellest lähtuvalt võiks tunneli kasutamist lubada ainult erandjuhtudel, kus vastavat vastaspoolt usaldatakse.
Sertifikaatide aktsepteerimine, mille *Common Name* ei ühildu *URL* -i omaga	Kui sertifikaadi *Common Name* ei ühildu *URL* -i omaga, siis on see põhimõtteliselt viide manipulatsioonile. Selliseid sertifikaate ei tohiks aktsepteerida.
Sertifikaatide aktsepteerimine, vaatamata nende aegumisele	Usaldusväärsed veebilehed on alati hooldatud ning omavad kehtivat sertifikaati. Aegunud sertifikaate ei tohiks aktsepteerida.

Tabel: Soovitusi seadistamiseks

SMTP

Seoses SMTP -ga (e-maili teenus) peaks järgima meedet M 4.100 Tulemüür ja aktiivsisu . Erinevates turvaproksides on integreeritud spämmifiltrid. Nende filtrite omadused ei ole aga võrreldavad spetsiaalsete spämmifiltritega. Spetsiaalse spämmifiltri integreerimine turvalüüsi võimaldab seega e-mailide efektiivsema filtreerimise. Hetkeseisuga ei ole ühtegi meetodit, mis aitaks tavalisi e-maile spämmidest eristada. Spämmifiltri kasutamine on seega soovitatav ainult siis, kui üks töötaja peab iga päev kustutatud e-mailide nimekirja sorteerima.

Soovitusi spämmifiltri konfiguratsiooniks ja käitamiseks:

- Spämmifilter ei tohiks blokeeritud e-maili saatjale tagasi saata või ei tohiks saatjat informeerida keelu põhjusest, kuna sel juhul saab spämmi saatja informatsiooni adressaadi olemasolust.
- E-mailide automaatne kustutamine võib osutuda problemaatiliseks (nt õiguslikel põhjustel). Spämmifilter ei tohiks seega e-maile automaatselt kustutada, vaid peaks lisama märke, et tegemist võib olla spämmiga. Selle märke alusel saab programm või kasutaja ise kirjad erinevatesse kaustadesse sorteerida.
- Spämmifiltrit peaksid hooldama firma töötajad ise. Kui e-mailide filtreerimine on mõne muu firma poolt pakutav teenus, võivad tekkida andmekaitset puudutavad probleemid.
- Enne spämmifiltrite kasutuselevõttu tuleks uurida õiguslikku tausta. Üleüldine õigusalane olukord, mis puudutab spämmifiltrite kasutamist, on hetkel veel ebaselge. Spämmifiltrite kasutamine tuleks läbi rääkida ka ettevõtte juhtkonnaga.
- Programmid spämmide filtreerimiseks muudavad paigaldamise lihtsamaks. Need tooted pakuvad tihtipeale laiaulatuslikke täiendusvõimalusi, et parandada spämmide tuvastamist.
- Sissetulevate e-kirjade korral tuleks kontrollida, ega serverit ei ole kasutatud Mail-Relay'na. Seejuures kontrollitakse sissetulevate e-mailide korral, kas saaja domeen kuulub usaldatud võrku. Väljuvate e-mailide korral peaks saatja domeen kuuluma usaldatud võrgu hulka.

Samuti tuleks kontrollida väljuvaid e-maile. Seda tehes on võimalik kahjut piiritleda, kui vaatamata kõigile turvameetmetele mõni sisevõrgus olev e-maili programm ussiga (E-Mail Worm) nakatunud on. Sellisel viisil on nakkus ka koheselt tuvastatav.

Kahtlased e-maili aadressid tuleks keelata.
Kui spämmifiltrit turvalüüsi ei integreerita, tuleks töötajaid koolitada spämmikirju turvaliselt käsitlema. Juhised töötajatele võiksid olla:

- Kustutage spämmid ilma lugemata
- Ärge kasutage spämmide funktsiooni Unsubscribe
- Kui saatja on teada, tuleks enne kirja avamist temaga ühendust võtta
- Mõned teenusepakkujad soovivad, et eriti ohtlikud spämmid neile saadetakse.

Erandkorras võib olla mõttekas ka teenusepakkuja teavitamine

Manuste filtreerimine
Järgnevaid manuseid ei ole enamikes töökeskkondades vaja ning võidakse seetõttu filtreerida (järjestatud ohu liigi järgi):

Ligipääs kogu süsteemile:

- *.bat (DOS-Batch fail)

- *.vbx (Visual-Basic fail)
- *.com (Windows-i rakendus)
- *.hta (HTML -rakendused)
- *.inf (Installatsiooniskript)
- *.js (Jscript fail)
- *.jse (Krüpteeritud Jscript fail)
- *.wsh (Windows-Scripting-Host-Skript)
- *.vbs (Visual-Basic fail)
- *.vbe (Krüpteeritud Visual-Basic fail)

Mistahes rakenduse käitlemine :

- *.lnk (Link fail)
- *.chm (Muudetud HTML -fail)
- *.pif (Programmi infofail)
- *.rm (RealMedia fail)

Probleemid:

- *.mdb (Access andmebaas. Võivad sisaldada makroviiruseid.)
- *.reg (Registrifail. Võib registrit muuta.)

See nimekiri ei ole täielik. On palju teisi failitüüpe, millega lõppseadet kompromiteerida.

Paljudel juhtudel on need failid, mida töötamisel kindlalt vaja läheb (html, xls, pdf). Failide filtreerimine ainult faililaiendite põhjal või MIME -tüüpide põhjal ei taga veel piisavat kaitset, kuna failid, mis sisaldavad kahjurvara on tihtipeale ohututе faililaienditega ja toimivad ikkagi tavapäraselt.

Telnet

Telnet 'i tuleks kasutada ainult erandjuhtudel ja võimalusel asendada mõne teise protokolliga, näiteks SSH. Kui Telnet'i on ilmtingimata vaja kasutada, siis tuleb ALG või paketifiltriga lubatud ühenduste arv vähendada miinimumini.

FTP

Nagu Telnet 'i tuleks ka FTP-d kasutada ainult erandjuhtudel ja lubatud ühenduste arv peaks olema filtri või pääsuloendi (ACL- Acess Control List) abil viidud miinimumini. Järgnevad protokollikäsud tuleks filtreerida:

- PORT (filtreerimine takistab aktiivse FTP)

POP3

POP3 -e puhul tuleks järgida meedet M 4.100 Tulemüür ja aktiivsisu .

Kontrollküsimused:

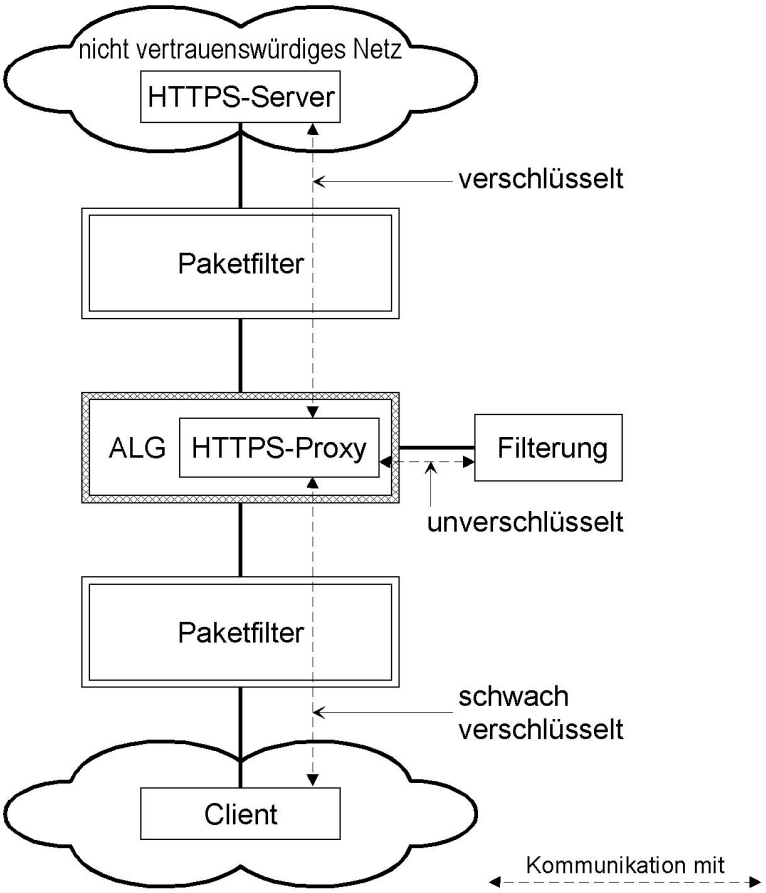
- Milliste protokollide puhul kasutatakse proksit?
- Kui kasutatakse Telnet 'i või FTP-d, siis kas lubatud ühenduste arv on vastavate filtritega viidud miinimumini?

M 4.223 Proksiserverite integreerimine turvalüüsi koostisesse

Algatamise eest vastutavad: IT-juht, IT-turvaspetsialist
Rakendamise ees vastutavad: Administraator

HTTPS -turvaproksid

HTTPS -proksi peaks sissetuleva andmevoolu dekrüpteerima, saatma filtreerimiseks edasi ja andmevoolu taas krüpteerima. Ajutiselt dekrüpteeritud andmevoolust saab otsida ebasoovitavaid sisusid. Parimal juhul toetab HTTPS-proksit juurdesoetatud ALG. Sellisel juhul on võimalik kasutada küllaltki lihtsat ülesehitust, mis on näidatud joonisel. Näitlikustamiseks on siinkohal vaadeldud olukorda, kus filtreerimine toimub eraldi seadmes. Paljudel juhtudel integreeritakse filtreerimine juba tootja poolt ALG-sse.



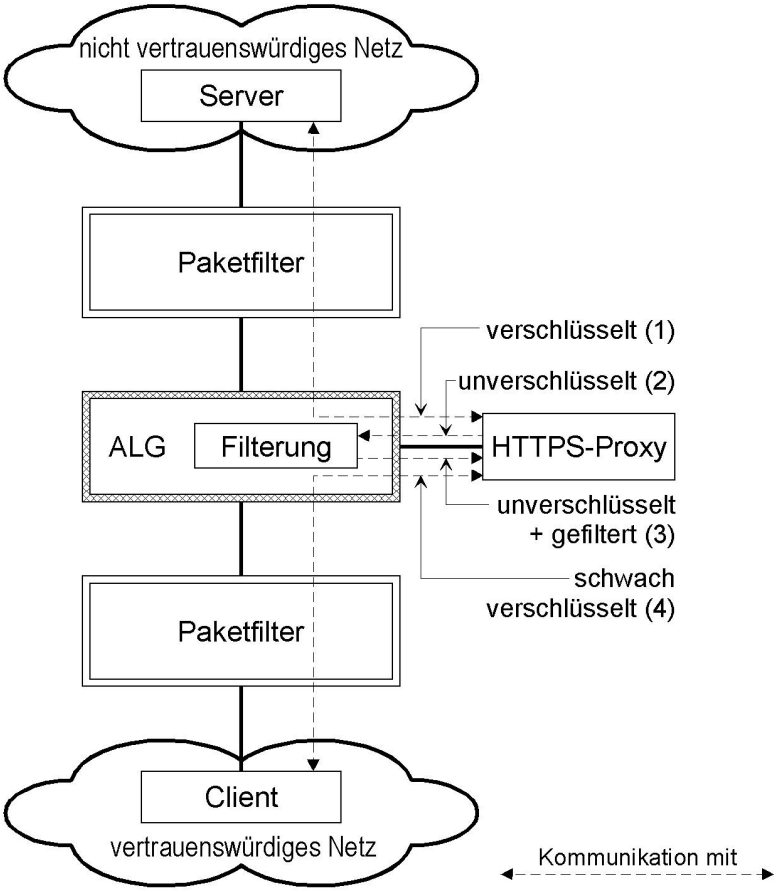
Joonis: Süsteemisisese HTTPS -proksi integreerimine (ebausaldusväärne võrk; HTTPS -server; krüpteeritud; paketifilter; ALG HTTPS -proksi; filtreerimine; dekrüpteeritud; paketifilter; nõrgalt krüpteeritud; klient, andmevoolu liikumine)

HTTPS -proksi eelised koos *ALG* -ga kasutades	*HTTPS* -proksi puudused koos *ALG* -ga kasutades

- Lihtsam seadistamine, kuna reeglina on kasutusel seadistusmenüü.
- Välise *HTTPS* -proksiga võrreldes on kommunikatsiooni hulk *SSL* -dekrüpteerimismoodulite ja sisu filtreerimismoodulite vahel väiksem (kuna andmeid ei pea ALG-st välja saatma)
- *SSL* -i keerukus soodustab vigade teket proksi tarkvara arendamisel, mis omakorda võib viia nõrkade kohtadeni. Vigade tõttu *SSL* -spetsifikatsioonis on võimalik kogu ALG üle võtta.
- Andmetöötluskiirus väheneb, kuna ressursse nõudev krüpteerimine aeglustab *ALG* -d

Tabel: HTTPS -proksi eelised ja puudused koos ALG -ga kasutades

Joonisel näidatud protseduur tuleneb juhtumist, kus ALG ei võimalda HTTPS-proksit. HTTPS -proksi paikneb eraldi demilitariseeritud tsoonis. Vastupidiselt eelmisele joonisele on siin näidatud juhtum, kus kahjurvara filtreeritakse ALG poolt.



Joonis: Süsteemivälise HTTPS -proksi integreerimine (ebausaldusväärne võrk; server; paketifilter; ALG; filtreerimine; krüpteeritud (1); dekrüpteeritud (2); HTTPS-

proksi; dekrüpteeritud + filtreeritud (3); nõrgalt krüpteeritud (4); paketifilter; klient; usaldusväärne võrk, andmevoolu liikumine)

Demilitariseeritud tsoonis paikneva *HTTPS* -proksi eelised	Demilitariseeritud tsoonis paikneva *HTTPS* -proksi puudused
• Tootevalik on *ALG* -st sõltumatu. • ALG koormuse vähendamine, kuna mahukas ja ressursikulukas krüpteerimine toimub eraldi arvutis.	• *ALG* -l tuleb seadistada mitu proksit. • Keerukate kommunikatsiooniühenduste tõttu on soodustatud vigade teke. • Võrreldes ALG -sse integreeritud HTTPS -proksiga pikeneb reaktsiooniaeg, kuna andmete laadimisel tuleb erinevate moodulite vahel luua mitu TCP - või UDP -ühendust.

Tabel: Demilitariseeritud tsoonis paikneva HTTPS -proksi eelised ja puudused

Krüpteerimise astet usaldusväärses võrgus on võimalik eelnevalt tutvustatud mudelite puhul sobitada vastavalt kaitsevajadusele. Jõudluse suurendamiseks on usaldusväärses võrgus võimalik krüpteerimisest täielikult loobuda või kasutada vähem jõudlust nõudvat krüpteerimismeetodit.

Caching -proksi

Teenuste kasutamisel on võimalik ligipääsu mitteusaldusväärsetele võrkudele piirata ainult teatud proksidele (näiteks caching- proksi HTTP jaoks). Programmide ligipääs välistele andmetele ei ole enam (sund-) proksit vältimata võimalik, kuna tulemüür ei aktsepteeri vastavat IP -aadressi (ainult caching- proksi IP-aadress aktsepteeritakse).

(Sund-) *caching* -proksi eelised	(Sund-) *caching*- proksi puudused

- Rohkelt võimalusi *HTTP*-andmeside protokollimiseks, seda juhul, kui kasutatakse üheastmelist tulemüüri (koosneb ühest paketifiltrist).
- Täiendatavad filtreerimisvõimalused, kui esineb ainult üheastmeline ülesehitus, mis koosneb ainult ühest paketifiltrist. *Caching*-proksiga on võimalik filtreerida näiteks:
  - Küpsised
  - URL-id
  - HTTP-viitajad
  - HTTP-Via
  - HTTP-server
- Edastavate andmemahtude vähenemine, tulenevalt *caching* 'u funktsionaalsusest.

Tähelepanu: Reeglina ei arendata *caching* -proksit lähtuvalt turvaaspektidest. Tuleks eelistada spetsiaalseid turvaproksisid.

- Proksi rikke korral langevad *HTTP/HTTPS* rivist välja. Ajutine kasutuselevõtt proksit kasutamata nõuab laialdast seadistustööd (Paketifiltril paiknevat keelunimistut tuleb muuta ja kui *caching*- proksi ei toimi läbipaistvalt, tuleb kliendi proksiseadistusi antud olukorraga sobitada. Reeglina on selle tõttu vajalik projekteerida ülemääraseid proksisid.

Tabel: (Sund-) caching- proksi eelised ja puudused

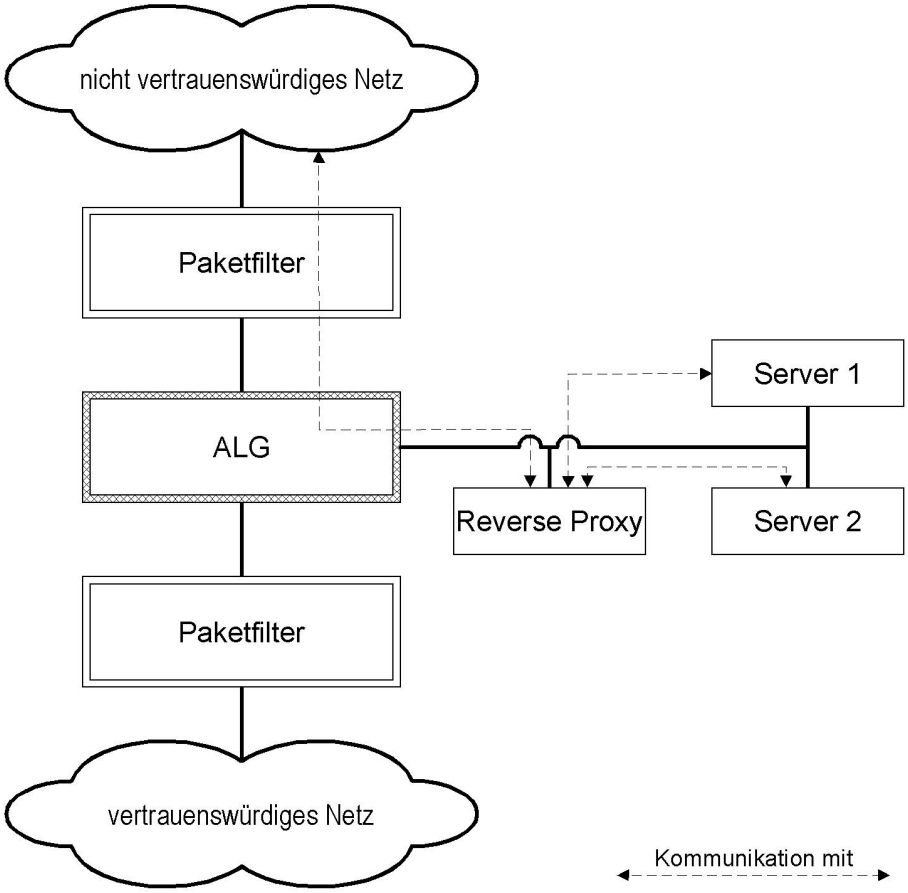
Reverse -proksi

Reverse- proksit kasutatakse peale (veebi-) serverite kasutusele andmise ka järgnevate turvanõuete saavutamiseks:

1. Ebausaldusväärsest võrgust tulevate kommunikatsiooniühenduste piiramine ja nende juhtimine läbi turvaproksi. Sellest tulenevalt lihtsustub turvalüüsi haldus ja vähenevad väärseadistused.
2. Veebiserveri identiteedi varjamine (mitu veebiserverit, mida kasutatakse andmemahu jaotamiseks, paistavad ebausaldusväärsest võrgust vaadatuna ühe IP -aadressina).
3. Veebiserveri veateadete kinnipidamine, mis võivad ründajale anda informatsiooni süsteemi pääsemise kohta (tegelikult peaks veebiserver need teated ise kinni püüdma).
4. Veebiserveri täiendav kaitse. Ründaja saab informatsiooni jälgida, kuid ei saa ligipääsu veebiserverile.
5. Ebausaldusväärse võrgu IP -pinust lahtiühendamine.

6. Veebiserverile ebausaldusväärsest võrgust esitatud soovimatute päringute filtreerimine.
7. Käideldavuse suurenemine, mis tuleneb andmejaotusest ja andmete vähendamisest tänu caching 'ule.

Järgneval joonisel on kujutatud olukord, kus kaks serverit on antud ebausaldusväärse võrgu kasutusse. Antud olukorras tuleb luua kaks kommunikatsiooniühendust, mis läbivad ALG ja süsteemivälise paketifiltri.

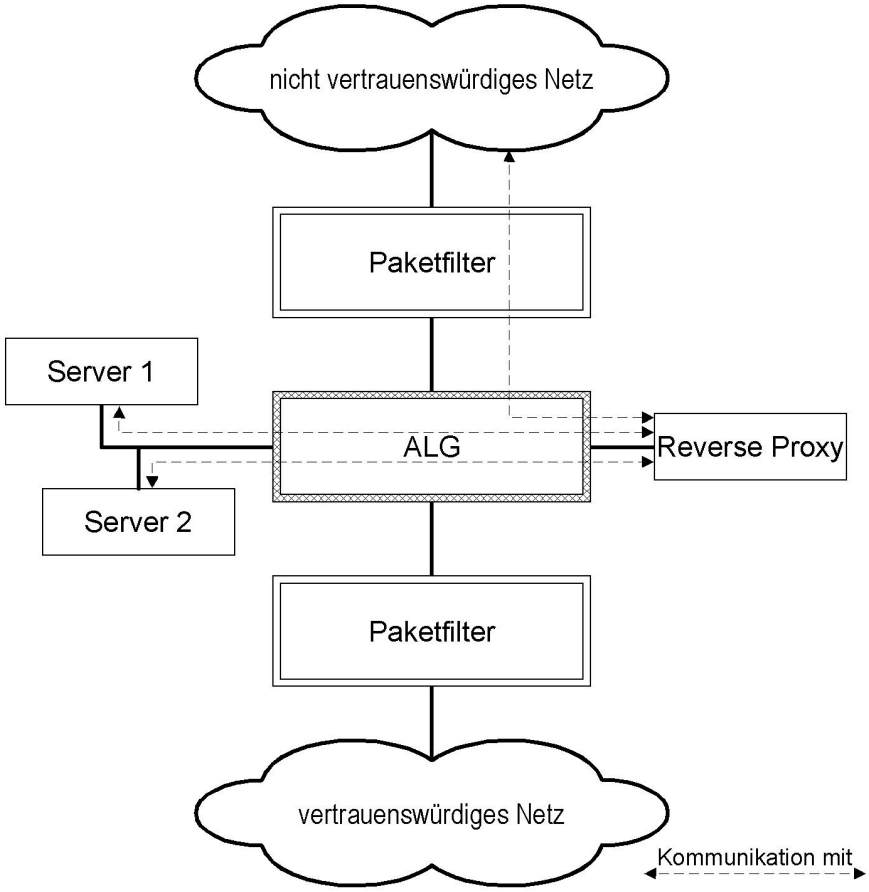


Joonis: Reverse -proksi kasutamine, et vältida suurt hulka kommunikatsiooniühendusi

ALG-s. Reverse -proksi ja serverid asetsevad ühes demilitariseeritud

tsoonis. (ebausaldusväärne võrk; paketifilter; ALG ; Reverse- proksi; server 1; server 2; paketifilter; usaldusväärne võrk)

Eelneval joonisel näidatud kommunikatsiooniühenduste hulka saab reverse -proksi abiga vähendada. Joonisel on näidatud, et ebausaldusväärsest võrgust on ligipääs lubatud ainult reverse -proksile. Server ühele ja kahele on ligipääs keelatud. Serveritele omab ligipääsu ainult reverse -proksi.



Joonis: Reverse -proksi kasutamine, et vältida suurt hulka kommunikatsiooniühendusi ALG-s. Reverse -proksi ja serverid paiknevad eraldi demilitariseeritud tsoonides. (ebausaldusväärne võrk; paketifilter; server 1; server 2; ALG; reverse-proksi; paketifilter; usaldusväärne võrk).

Turvalisuse suurendamiseks võib servereid käitada ka eraldi demilitariseeritud tsoonis (või ka usaldatud võrgus), kus nad on turvaproksi kaudu reverse -proksist eraldatud. Sellest tulenevalt raskeneb ka serveri ülevõtmine, samuti suureneb ka kommunikatsiooniühenduste arv, mis ALG -d läbib.

Kontrollküsimus:

- Milliseid proksisid kasutatakse?

M 4.224z Virtuaalsete privaatvõrkude integreerimine turvalüüsidesse

Algatamise eest vastutav: IT-juht, IT-turvaspetsialist
Rakendamise eest vastutav: Administraator

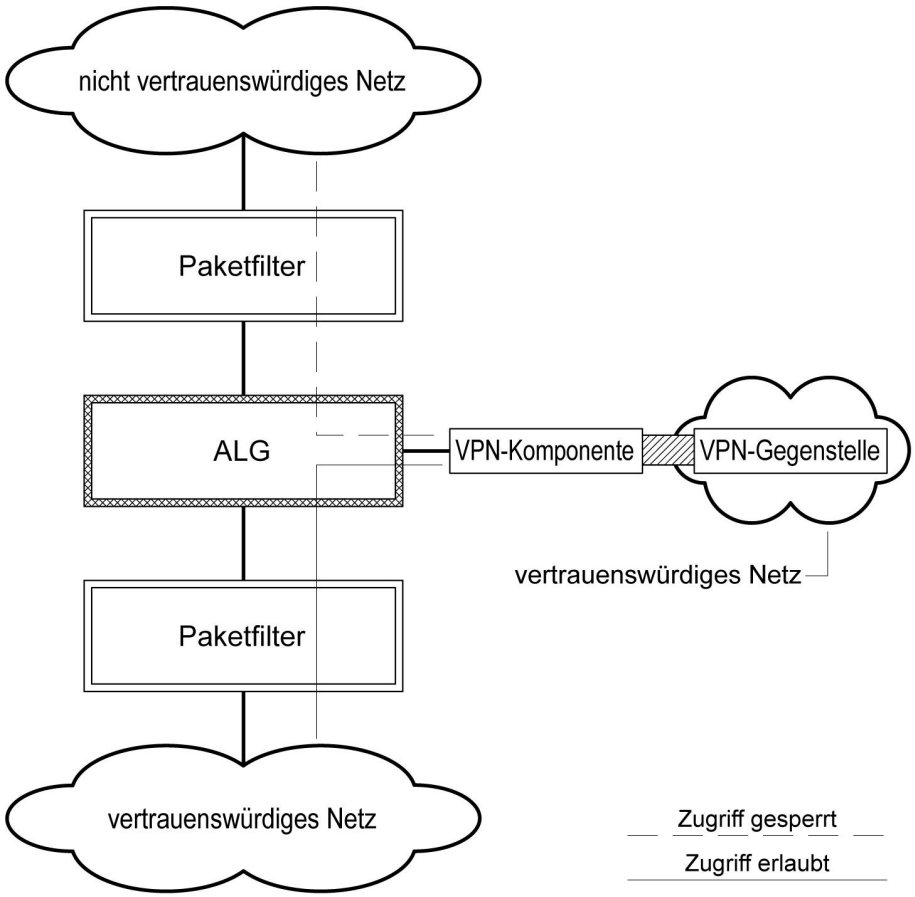
Virtuaalse personaalvõrgu (*VPN*) turvalisuseks on oluline turvalüüsi integreerida *VPN* -i lõpp-punktid. *VPN* -i osade optimaalne paigutamine sõltub seejuures mitmetest asjaoludest:

- VPN-lüüsi kaitsevajadus ebausaldusväärsest võrgust pärinevate rünnakute eest
- Ebausaldusväärsest võrgust pärit andmeedastuste ja usaldusväärses võrgus asuvate süsteemide ja teenuste ligipääsude kontrollimine
- Edastatavate andmete kaitsevajadus

Tuntuimad protokollid *VPN* -i ülesehitamiseks on *IPSSec*, *TLS/SSL*, *PPTP* ja *L2TP*. Järgnevalt vaadeldaksegi selliseid *VPN*-e. Siintoodud soovitusi on võimalik üle kanda ka enamikule teistest meetoditest. Teatud meetodi kasuks otsustamine sõltub kasutusest või kasutusalast. Asutusel võib olla otstarbekam kasutada mitut *VPN* -i erinevate *VPN* -protokollidega ja erinevate krüpteerimismeetoditega. Dokumenteerida tuleks nii *VPN* -komponentide paigutus kui ka meetodid, mida kasutatakse.

VPN kasutades *IPSec* -i või *TLS/SSL* -i
VPN -lüüsi asukoht sõltub (sarnaselt paketifiltri asukohale turvalüüsis) sellest, mitu liidest on *VPN* -lüüsi kasutuses.

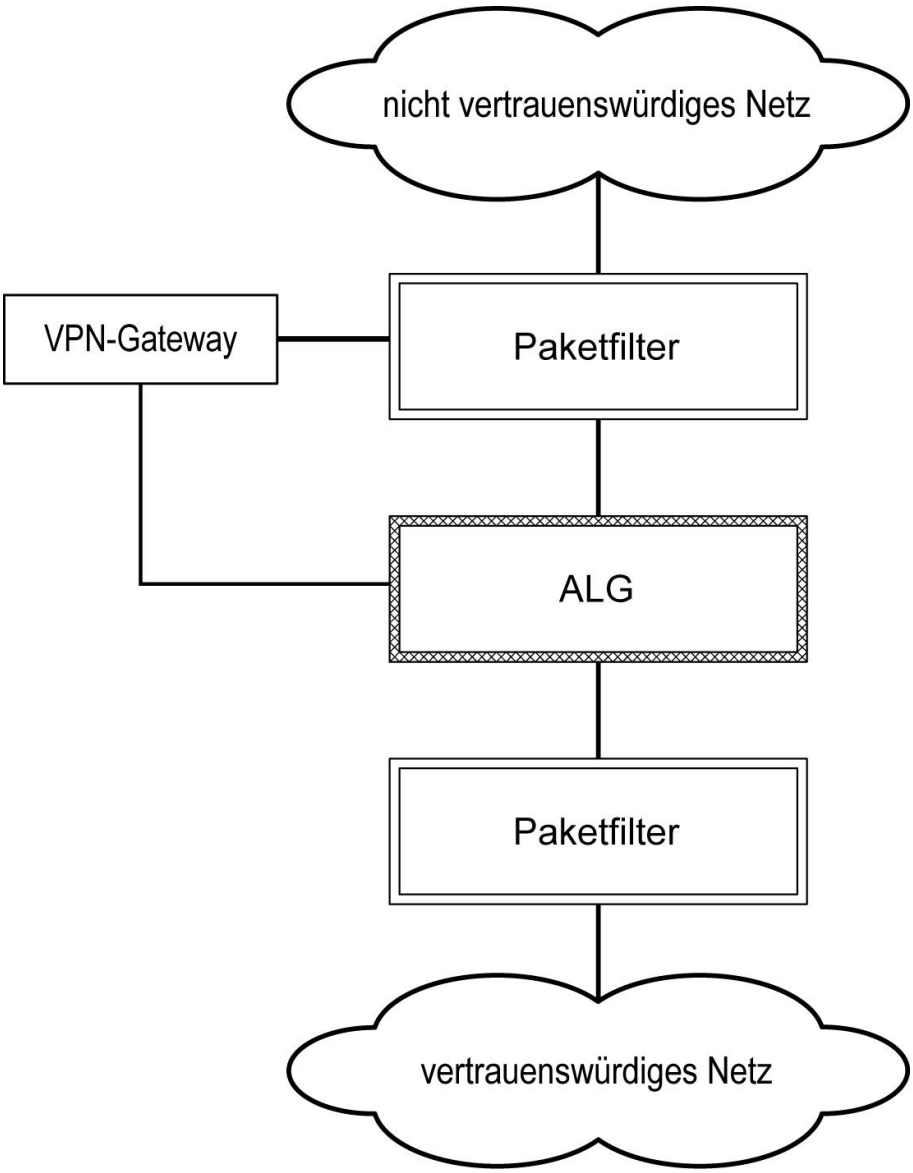
- Ühe liidesega *VPN* -lüüs: Kõrge rünnakupotentsiaali korral peaks VPN-lüüs olema ühendatud läbi paketifiltri *Application-Level-Gateway* (ALG) külge. Väline paketifilter kaitseb IP-aadressi võltsimise eest, kuna ebausaldusväärsest võrgust sissetulevaid pakette, mille saatja *IP* -aadressiks on *VPN* -lüüs, ei saadeta välise paketifiltri poolt edasi. Teel usaldusväärsesse võrku peab dekrüpteeritud andmevool läbima *ALG* ning sisenema paketifiltrisse. Eelnevate mudelitega võrreldes on volitamata ühenduse loomine ebausaldusväärse võrgu poolt märgatavalt raskendatud, kuna dekrüpteeritud ühendused on lubatud ainult *ALG* demilitariseeritud tsooni liideses ja mitte *ALG* -liideses, mis on ühenduses ebausaldusväärse võrguga.



Joonis 1: Ühe liidesega VPN-komponendi paigaldamine

(ebausaldusväärne võrk; paketifilter; ALG; VPN-komponent; VPN-sihtsüsteem; paketifilter; usaldusväärne võrk; _ _ _ _ _ ligipääs keelatud; _____ ligipääs lubatud)

- Kahe liidesega VPN-lüüs - Kahe liidesega VPN-lüüsi puhul tuleb üks liides ühendada välise paketifiltriga ning teine ALG-ga. VPN-lüüsi paigaldamine välise paketifiltri külge tagab selle kaitstuse rünnakute eest, mis tulevad ebausaldusväärsest võrgust. Ebausaldusväärsest võrgust lastakse läbi ainult ühendusi, mis on *VPN* -kommunikatsiooni seisukohast olulised. Ühendus läbib *ALG* , mistõttu on dekrüpteeritud andmevoolu võimalik rakenduse baasil kontrollida ja piirata. Lisaks on võimalik dekrüpteeritud andmevoolu sisemise paketifiltri kaudu kontrollida ja piirata.



Joonis 2: Kahe liidesega VPN-komponendi paigutamine

(ebausaldusväärne võrk; paketifilter; VPN-lüüs; ALG; paketifilter; usaldusväärne võrk)

VPN kasutades Layer-2 protokolli

Layer-2-VPN on teostatav näiteks *PPTP* (*Piont to Point Tunneling Protocol*) ja *L2TP* (*Layer 2 Tunneling Protocol*) abiga. Neid kasutatakse tihtipeale *VPN* -i ülesehitamiseks telekommunikatsioonivõrkude kaudu, näiteks *GSM* ja *ISDN*. Võrkude eraldamiseks tuleks *Layer-2-VPN* -i korral *LAN* 'i ja VPN-ühenduse vahele paigutada ALG. Erinevate õigustega kasutajagruppide sidumisel võrguga tuleks igale kasutajagrupile jagada oma võti, et tagada gruppide vahel edastatud andmete konfidentsiaalsus.

Täiendavad kontrollküsimused:

- Kas *VPN* -komponendid on turvalüüsi integreeritud sellisel kujul, et on võimalik andmevoolu efektiivne kontrollimine ja filtreerimine?
- Kas *VPN* -komponentide integratsioon turvalüüsi on dokumenteeritud?

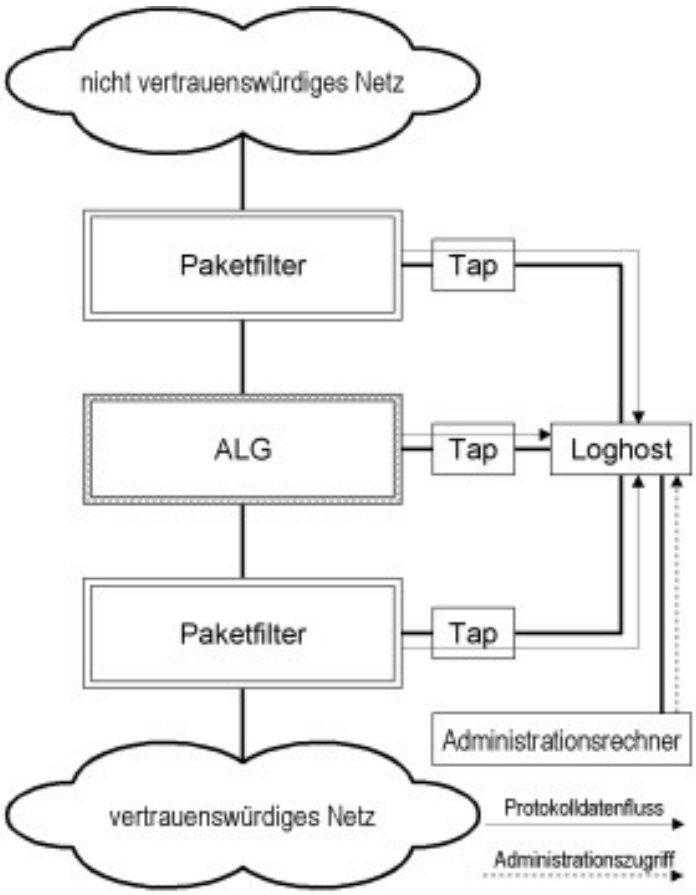
M 4.225z Logiserveri kasutamine turvalüüsis

Algatamise eest vastutav: IT-juht, IT-turvaspetsialist
Rakendamise eest vastutav: Administraator

Keerukate turvalüüside puhul tekib tihtipeale suurtes kogustes erinevate komponentide logiinformatsiooni. Logide analüüsimise lihtsustamiseks on soovitatav kesksetes kohtades kasutada logiserverit (Loghost), mis sisaldab turvalüüsi külge ühendatud komponentide logiandmed. Andmeid on võimalik seeläbi lihtsamini omavahel seostada ja see võimaldab olukorrast sõltumatut andmete analüüsimist ning vea tekke korral on võimalik leida selle põhjustaja (vt M 4.47 Turvalüüsi operatsioonide logimine). Keskse logiserveri paigaldamine on problemaatiline, kuna ühest küljest peab ta olema ligipääsetav turvalüüsi kõikidest osadest, teisest küljest ei tohi võimaldada endale autoriseerimata ligipääsu ebausaldusväärsest võrgust.
Logiserveri kompromiteerimisel lihtsustab tema keskne positsioon turvalüüsis oluliselt teiste komponentide kompromiteerimist. Turvalüüsi keskne logiserver ei tohi seega täita veel teisi ülesandeid. Logiandmetega seoses peaks järgima:

- Keskne logiserver peaks andmed salvestama liiasusega.
- Logimine peaks võimalusel toimuma ka turvalüüsi üksikutes komponentides. Komponentide jõudlus ei lange seeläbi märgatavalt, seetõttu tuleks seda salvestamist kasutada lisakaitsena rikke korral.

Üks logi tähtsaid elemente on teavitamine defineeritud või kriitiliste olukordade puhul. Tuleks jälgida, et teateid oleks võimalik edastada kesksele üksusele. Logiserveri paigaldamise tähtsaim kriteerium on, et ei tohi lisanduda nõrku kohti, näiteks võimalust turvakomponentidest mööda pääseda. Arvestada tuleks ka asjaoluga, et logiandmetel oleks keskse logiserverini turvalüüsis võimalikult lühike tee. Logi saatmisel proksi kaudu näitavad need logifailides proksi IP -aadressi, nii et tegelik saatja ei ole enam tuvastatav. Mõningatel juhtudel võimaldavad logi seaded üksikute komponentide andmete vastavat märgistamist. Logiserver paigutatakse eraldi administratsioonivõrku. Logiserverile pääsetakse seeläbi ligi administratsioonivõrgu kaudu.



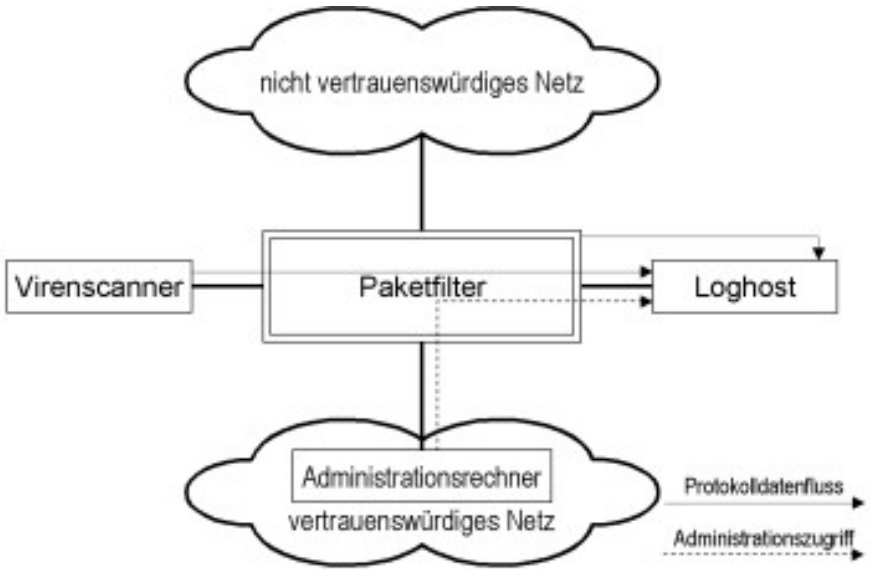
Joonis 1: Logiserveri paigutamine administratsioonivõrku.

(ebausaldusväärne võrk; paketifilter; andmevoolu kontrollseade, ALG; logiserver; paketifilter; usaldusväärne võrk; administraatori arvuti; logiandmete vool; administraatori ligipääs)

Administratsioonivõrgu puudumisel tuleb logiserver paigaldada tootmisvõrku. Sõltuvalt turvalüüsi ülesehitusest on keskse logiserveri paigutamiseks kaks kohta:

Paigutamine lihtsa turvalüüsi korral

Lihtsa turvalüüsi puhul, mis on varustatud ainult ühe paketifiltriga, sobib logiserveri paigutamiseks eraldi demilitariseeritud tsoon. Paketifiltrid omavad reeglina piisaval hulgal võrguliideseid või on kergesti laiendatavad, mis võimaldab logiserveri paigalduse spetsiaalsesse demilitariseeritud tsooni.

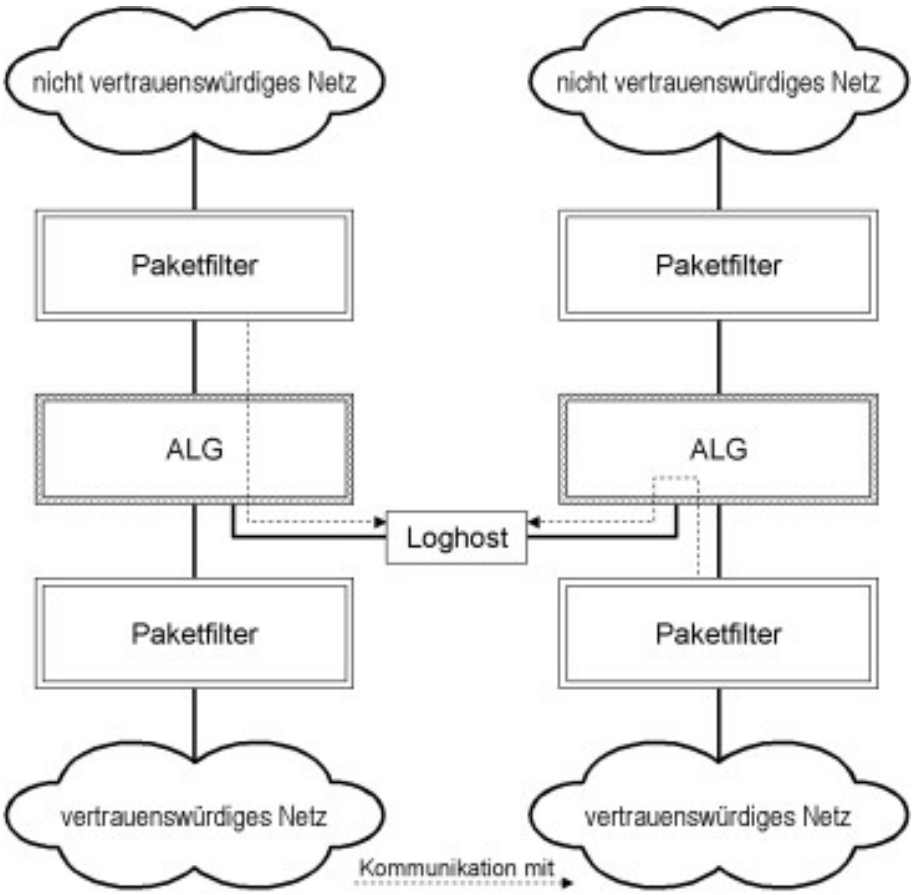


Joonis 2: Logiserveri paigutamine turvalüüsi lihtsa ülesehituse korral

(ebausaldusväärne võrk; viiruse skanner; paketifilter; logiserver; administraatori arvuti; usaldusväärne võrk; logiandmete vool; administraatori ligipääs)

Paigutamine keerukate turvalüüside korral
Keeruka turvalüüsi ülesehituse korral on vajalik saata logiandmed logiserverisse, tehes seda üle proksi. Logiserveri paigaldamist eraldi demilitariseeritud tsooni tuleb eristada logiserveri paigaldamisest ühisesse demilitariseeritud tsooni koos turvalüüsi teiste moodulitega.

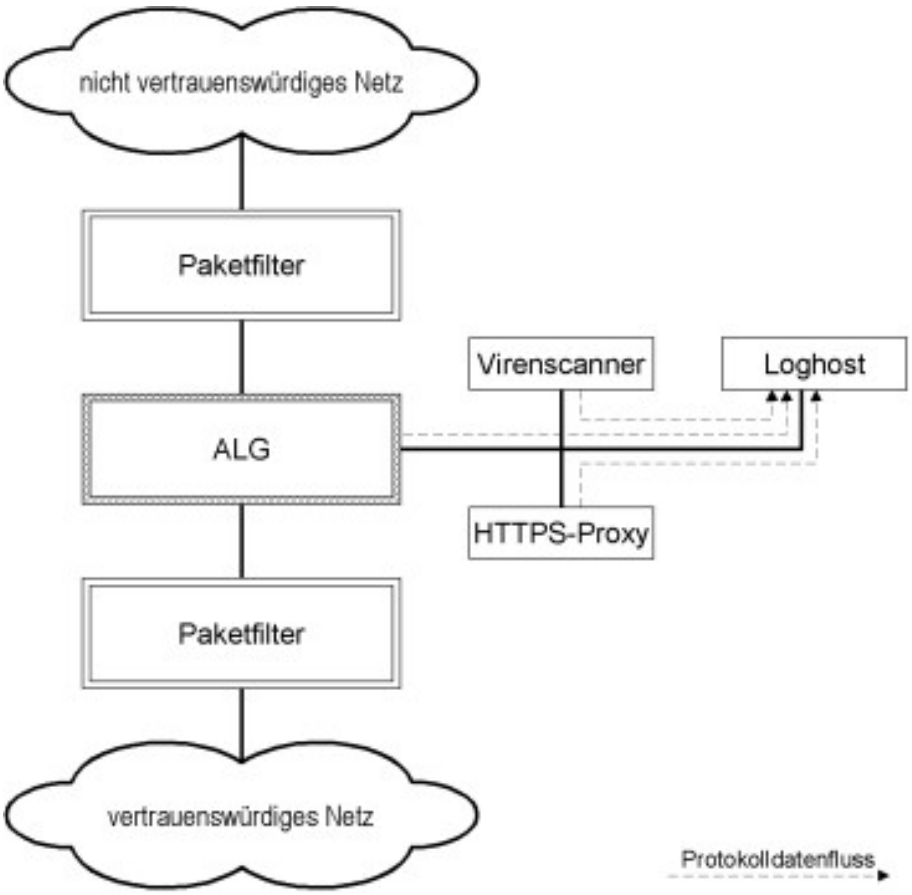
Joonisel on toodud lahendus, mille puhul on keskne logiserver paigutatud eraldi demilitariseeritud tsooni ja mida kasutab kaks turvalüüsi.



Joonis 3: Logiserveri paigutamine spetsiaalsesse demilitariseeritud tsooni (ebausaldusväärne võrk; paketifilter; ALG; logiserver; paketifilter; usaldusväärne võrk; andmevoolu liikumine)

Joonisel toodud paigutuse eeliseks kompromiteerimise korral on asjaolu, et ründajale jääb vähe ründevõimalusi, kuna ainsad otse ligipääsetavad moodulid on ALG -d ning need on rünnakute eest eriti kaitstud. Joonisel oleva lahenduse puhul tekib logiserveri integreerimisel ühendus kahe usaldusväärse võrgu vahel, mis ilma logiserveri integreerimiseta ei oleks võimalik olnud. Näidatud paigutuse korral vajatakse eraldi riskianalüüsi. Teatud juhtudel tuleb ühendamisest loobuda, mille tulemusena paigutatakse kaks eraldi logiserverit, mille logiandmed tuleb analüüsimiseks kokku liita.

Järgneval joonisel kujutatud lahenduse puhul on demilitariseeritud tsoonis peale logiserveri ka teised turvalüüsi moodulid. Need osad võivad olla järgmised rünnakusihid pärast logiserveri ülevõtmist, kuna tegemist ei pruugi olla spetsiaalsete turvatoodetega. Võimalik, et seetõttu on nende moodulite ülevõtt lihtsustatud.



Joonis 4: Logiserveri paigutamine demilitariseeritud tsooni koos teiste turvalüüsi osadega (ebausaldusväärne võrk; paketifilter; ALG ; viiruse skanner; HTTPS-proksi; logiserver; paketifilter; usaldusväärne võrk; logiandmete vool)

Tuleks eelistada lahendust, mille korral logiserver on eraldi demilitariseeritud tsoonis.

Logiserveri paigutamine demilitariseeritud tsooni koos teiste komponentidega on soovitatav ainult sel juhul, kui ALG -l ei ole piisavalt võrguliideseid.

Kokkuvõtlik tabel:

Turvalüüsi struktuur	Kaitsevajadus	Logiserveri paigutamine
Ainult paketifilter	Tavaline	Logiserver asub paketifiltris eraldi demilitariseeritud tsoonis

Keeruline turvalüüs (P-A-P)	Tavaline kõrge	Logiserveri paiknemine ühises demilitariseeritud tsoonis koos teiste komponentidega on aktsepteeritav Soovituslik eraldi demilitariseeritud tsoon Logiserveril oma demilitariseeritud tsoon
Logiserveri kasutamine mitme turvalüüsi poolt	-	Logiserveril oma demilitariseeritud tsoon

M 4.226z Viirusskannerite integreerimine turvalüüsi koostisse

Algatamise eest vastutavad: IT-juht, IT-turvaspetsialist

Rakendamise eest vastutavad: Administraator

Kahjurvara nagu viiruseid, ussviiruseid ja trooja hobuseid (lihtsustamise mõttes „viiruseid“) saab filtreerida nii turvalüüsi abiga kui ka filtrite jaotamisega töökoha arvutitele ja serveritele (st kommunikatsioonisidemete lõppsüsteemidele teisel pool turvalüüsi). Keskne viirusetõrje turvalüüsis ei suuda jaotatud viirusekaitset täielikul asendada, kuna teatud juhtudel pääseb kahjurvara süsteemi ka teisel moel (näiteks väliste andmekandjatega). Keskne filtreerimine on võimalik, kasutades Application-Level-Gateway' d (ALG).

ALG kaudu otsefiltreerimine

Kui vastav seadistus on ALG-l lubatud, on mõttekas kahjurvara kontrollida otse ALG-s.

Turvalüüsis filtreerimine ALG -ga

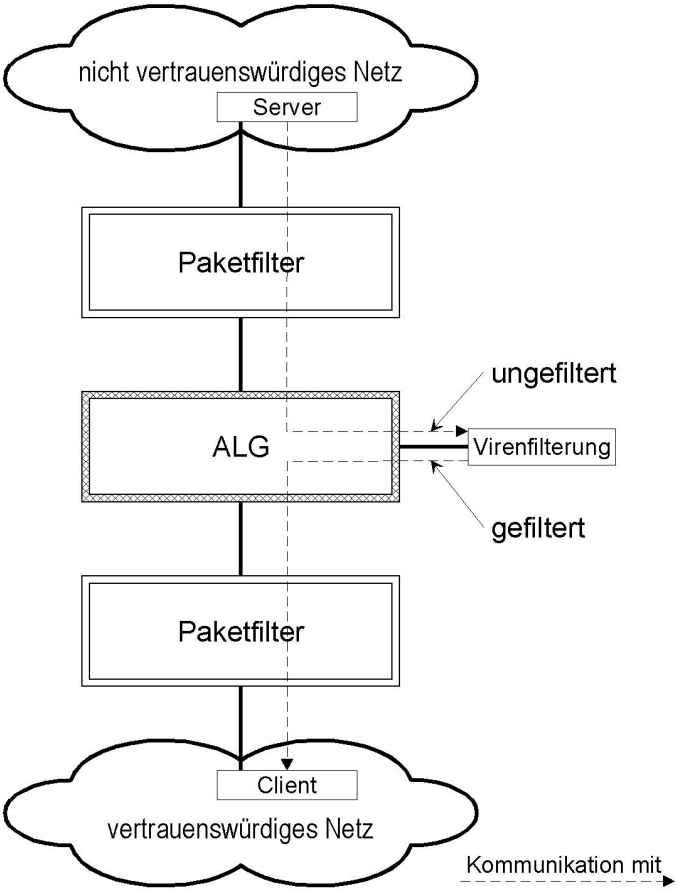
ALG -d omavad enamasti liidest, mille kaudu on võimalik ühendada mõne kolmanda firma poolt toodetud viirusetõrjeprogramm. Programm võtab andmed vastu ja saadab ALG -le teate filtreerimise tulemustest. ALG töötleb andmeid sõltuvalt kontrolli tulemustest.

Viiruseskanneri paigutamiseks sobib järgneval joonisel näidatud positsioon, kus see paikneb turvalüüsi demilitariseeritud tsoonis, mis omakorda asetseb ALG läheduses. Joonisel toodud ülesehituse puhul tuleks jälgida mõningaid punkte, kuna sellise ülesehituse korral on viirusetõrjega arvuti eriti ohustatud:

- Arvuti, millesse on paigaldatud viirusetõrje, tuleb konfigureerida eriti turvaliselt, näiteks operatsioonisüsteemi piiratud konfiguratsiooni kaudu (tugevdamine).

Turvanõuded on (vähemalt) sama kõrged, kui teistele turvalüüsi osadele.

- Arvuti tuleb vastavate paketifiltrite abil ülejäänud võrgust eraldada. Paketifiltrid ei tohiks lubada väljuvaid ühendusi, ei Internetti ega välisesse võrku. Ideaaljuhul vahetab arvuti andmeid otse ALG -ga, millelt ta saab kontrollitava andmevoolu ja millele ta filtreeritud andmed tagasi saadab. Ühendused arvutisse on lubatud ainult eraldi haldusvõrgu kaudu.
- Süsteemi kontroll peaks toimuma lühikeste intervallide tagant.
- Kompromiteerimise kohese tuvastamise võimaldamiseks tuleks arvuti varustada host 'il baseeruva IDS -iga (Intrusion-Detection-System).
- Arvutite haldamine peab toimuma turvalise ühenduse kaudu.



Joonis: Viirusfiltri integreerimine

(ebausaldusväärne võrk, server, paketifilter, ALG , filtreerimata, viirusfilter, filtreeritud, paketifilter, klient, usaldusväärne võrk)

Lõppseadmetel filtreerimine (paketifiltri kasutamine)

Üheastmeliste turvalüüside puhul, mis koosnevad ainult ühest paketifiltrist, ei ole keskne filtreerimine turvalüüsi kaudu tavaliselt võimalik, kuna paketifiltrid ei oma liidest viirusfiltriga ühendamiseks. Antud juhul tuleb viirusfilter paigaldada tööarvutitele või usaldusväärse võrgu serveritele (e-maili server, uudiste server).

Järgida tuleb ka moodulit B 1.6 Viirusetõrje kontseptsioon.

M 4.227 Lokaalse NTP -serveri kasutamine aja sünkroniseerimiseks

Algatamise eest vastutavad: IT-juht, IT-turvaspetsialist
Rakendamise eest vastutavad: Administraator

Ühendatud süsteemide puhul on paljudes olukordades vajalik, et kõik protsessiga seotud arvutid omaksid õiget süsteemiaega. Kesksel kohal on see logi informatsiooni analüüsimisel, et kontrollida veateateid, mis viitavad rünnakule võrgust, või kui mitme arvuti peale jaotatud rakendustega tekivad probleemid sünkroniseerimisel. Samuti sõltuvad hajutatud andmesüsteemid ja kesksed autentimisteenused aja sünkroniseerimisest. Süsteemiaja õigeks seadistamiseks võimaldavad enamus operatsioonisüsteeme välistele ajaserveritele ligipääsu *NTP* (*Network Time Protocol Version 3, RFC 1305*) või *SNTP* (*Simple Network Time Protocol Version 4, RFC 2030*) protokolli kaudu. *Windows* 'i arvutid, mis paiknevad *Active Directory* infrastruktuuris, sünkroniseerivad aega ka domeeni kontrolleriga. Internetis on avalikest *NTP* -ajaserveritest koosnev infrastruktuur.

NTP on avatekstprotokoll ilma krüptograafilise kaitseta, mistõttu tuleks seda kasutada ainult oma võrgu piires. Kasutades Internetis olevat ajaserveri infrastruktuuri, tuleks *NTP* -informatsiooni saamiseks ajaserverilt kasutada üht ainsat arvutit. Lokaalses võrgus paiknevad arvutid sünkroniseerivad oma süsteemikella siis lokaalse *NTP* -proksiga. Turvalüüsis tuleks sel juhul *NTP* vabastada ainult *NTP* -proksi serverile. Suure kaitsevajadusega võrkudes tuleks seadmetel keelata *NTP* -otsepäringute saatmine Internetti. Ühe variandina saab ühe sisevõrgu arvutitest varustada raadiokellaga ja anda talle lokaalse ajaserveri funktsioonid. Kahtluse korral tuleks eelistada antud varianti.

Ajasünkronisatsiooni tegemisel väliste vahenditega (raadiokellad, avalikud NTP ajaserverid jne) tuleb kindlustada, et seda informatsiooni ei kasutata ilma seda eelnevalt kontrollimata. Ajaserveri/*NTP*-proksi tarkvara peab teostama andmete usutavuse kontrolli enne kui ta andmed üle võtab ja võrgus olevatele arvutitele laiali saadab. Näide usutavuse kontrollist: andmeid ei võeta süsteemi üle, kui ajaandmete vahe on suurem kui eelnevalt määratud vahe.

Täiendav kontrollküsimus:

- Kust hangitakse ajainformatsioon?

M 4.228 Nutitelefonide, tahvel- ja pihuarvutite turvamehhanismide kasutamine

Algatamise eest vastutavad: infoturbeametnik, IT-juht

Rakendamise eest vastutavad: kasutaja, administraator

Nutitelefone, tahvel- või pihuarvuteid ja sinna juurde kuuluvaid rakendusi saab kaitsta mitmesugustes kohtades PIN-koodide või paroolidega. Kõik kasutajad peaksid teadma, kui tõhusad on nende poolt kasutatavad turvamehhanismid ning millised on nende piirid.

Nutitelefonide, tahvel- või pihuarvutite kaitse juurdepääsu eest

Tänapäeval on kõikidel kaasaskantavatel seadmetel juurdepääsukaitse, mis on tavaliselt teostatud paroolipäringuga. Isegi siis, kui kõik tootja pakutud turbemehhanismid ei ole nii kindlad, kui soovitakse, tuleks neid kasutada, kuni ei ole välja pakutud midagi paremat.

Seadmete tarneolekus on paroolipäring enamasti inaktiveeritud ja sageli on eelseadistatud triviaalne parool. Seetõttu tuleb esimesel kasutamisel parool ära muuta ja aktiveerida, nii et vähemalt seadme sisselülitamisel oleks parooli sisestamine vajalik. Nende paroolide ja PIN-koodide jaoks kehtivad samad reeglid nagu muude IT-süsteemide paroolidele (vt M 2.11 Paroolide kasutamise reeglid). Mitte mingil juhul ei tohi parool olla liiga lühike või liiga lihtne. Mitte mingil juhul ei tohi hoida nutitelefoni, tahvel- või pihuarvutit ja selle parooli ühes ja samas kohas.

Paljusid nutitelefone, tahvel- või pihuarvuteid saab väga lihtsalt hallata arvuti USB-liidese kaudu ja need pakuvad USB- või isegi õhuliidese kaudu ulatuslikke süsteemifunktsioone (nn debugging-funktsioonid). See liides tuleb inaktiveerida, kui seda ei kasutata, sest muidu võidakse ilma kasutaja teadmata lugeda andmeid või installeerida või eemaldada mis tahes rakendusi.

Automaatne lukustus / pimenduspilt

Nutitelefonidel, tahvel- või pihuarvutitel on üldiselt ette nähtud ka automaatse lukustamise võimalus, mis töö katkestamisel mõne aja pärast ise aktiveerub. Seadme edasine kasutamine on võimalik alles pärast vastava parooli sisestamist. Kui on olemas pimenduspilt, tuleks seda tingimata kasutada. Juurdepääsukaitse tuleks sisse lülitada juba varsti pärast seda, kui seadet ei ole kasutatud, soovitatavalt maksimaalselt 5 minuti pärast.

Kasutajainfo

Selleks, et nutitelefoni, tahvel- või pihuarvuti aus leidja teaks, kelle poole pöörduda, peaks seade olema seadistatud nii, et pärast selle sisselülitamist ilmub ekraanile sellekohane teave. Isiklike nutitelefonide, tahvel- või pihuarvutite korral ei tohiks olla antud täielik isiklik aadress, et varas ei saaks seda teavet kasutada sissemurdmiseks omaniku oletatava äraoleku ajal. Tavaliselt piisab nimest ja e-posti aadressist. Kui see funktsioon ei ole süsteemi poolt kasutatav, tuleks vastav rakendus installeerida või kasutada selleks ise kujundatud lukustuskuva.

Täiendavad turbemehhanismid

Nutitelefonidele, tahvel- ja pihuarvutitele on palju erinevaid turvamehhanisme nagu krüpteerimine või aegjuhtimisega inaktiveerimine. Millised nendest on saadaval või kuidas neid aktiveerida, sõltub kasutatavast seadmest. Seetõttu tuleks kasutusjuhendist selle kohta hoolikalt lugeda. Kui nutitelefonis, tahvel- või pihuarvutis on salvestatud konfidentsiaalsed ja erilist kaitset vajavad andmed, tuleks need krüpteerida. Kui seade ei paku sisseehitatud krüpteerimisfunktsiooni, tuleks installeerida täiendav krüpteerimistoode.

Nutitelefonide, tahvel- või pihuarvutite kasutamisel ametiasutustes või ettevõtetes on soovitatav kõige olulisemad turbemehhanismid nii eelnevalt konfigureerida kui ka ülevaatlikkusse andmelehte kasutajate jaoks arusaadavalt kirja panna. Kui võimalik, tuleks sellised andmelehed teha kättesaadavaks ka elektroonilisel kujul seadmel hõlpsalt leitavas kohas.

Kontrollküsimused

- Kas kasutatavatel nutitelefonidel, tahvel- või pihuarvutitel on sisselülitamise paroolid? Kas need on aktiveeritud?

M 4.229 Nutitelefonide, tahvel- ja pihuarvutite turvaline kasutamine

Algatamise eest vastutavad: infoturbeametnik, IT-juht

Rakendamise eest vastutavad: administraator, kasutaja

Nutitelefonide, tahvel- või pihuarvutite sihipärane kasutamine vajab ühendamist muude IT-süsteemidega, näiteks töökoha arvuti, seadmehalduse või -juhtimise serveriteenistuse või pilvteenusega. Selleks vajaliku riist- ja tarkvara installeerimine ja konfigureerimine peaks olema reguleeritud ja teostatud tsentraalselt. Installeerimist ei tohi läbi viia ilma vastavate testide ja kasutuslubadeta. Paljude nutitelefonide ja tahvelarvutite korral on sünkroonimine pilvteenustega eelseadistatud ja toimub peaaegu automaatselt. Tuleb takistada, et andmed ei voolaks tahtmatult üle nendele teenustele. Seda tuleb eriti kontrollida iga uue installeeritud rakenduse puhul. Vajaduse korral tuleb kasutada kohaseid vastumeetmeid.

Kaasaskantavate seadmete turbemehhanismid ja -seadistused tuleb kindlaks määrata ja kasutajate jaoks arusaadavalt kirja panna, et nad oskaksid seadet õigesti kasutada. Seepärast tuleb selgesõnaliselt keelata konfiguratsioonide muutmine.

Lisaks sellele peab kasutajaid teavitama valitud seadistuste aluspõhimõtetest.

Kui see on tehniliselt võimalik, peaksid turbemehhanismid olema valitud ja konfigureeritud nii, et kasutajatel oleks võimalikult vähe võimalusi neid mõjutada.

Seda on kõige lihtsam teostada keskse mobile-device-management-(MDM)-lahenduse kaudu. MDM-lahendused võivad avaldada paroolisuuniseid, kontrollida konfiguratsioone, hallata installeeritud rakendusi ja operatsioonisüsteemi turvapaiku ning kontrollida viirusetõrje tarkvara. Soovitatakse kasutada MDM-lahendust või vähemalt kontrollida, kas sellega saavutatakse nutitelefonide, tahvel- ja pihuarvutite kõige tõhusam turvaline kasutamine (vt ka M 4.230z Nutitelefonide, tahvel- ja pihuarvutite tsentraalne haldamine).

Nutitelefonide, tahvel- ja pihuarvutitega on tavaliselt võimalik kasutada erinevaid kasutajakontosid. Seetõttu ei ole üldiselt olemas väljatöötatud mehhanisme rollide eraldamiseks. See tähendab, et harva leidub valdkondi, mis ei ole administraatoritele juurdepääsetavad. Kasutajaid ei saa seega mingil juhul takistada, et muuta turvalisusega seotud konfiguratsioone. Seda võib saavutada üksnes vastavate eeskirjade ja kasutajate teavitamisega. Lisaks aitab see seadistusi korrapäraselt kontrollida või taastada haldustööriistadega sünkroniseerimisel uuesti endised väärtused.

Kõikide nutitelefonide, tahvel- või pihuarvutitega sünkroniseerimiseks kasutatud seadmete turvalisus on oluline vastava kaasaskantava seadme turvalisuse jaoks.

Kui statsionaarsetel seadmetel on manipuleeritud andmeid või programme, võivad need selle edastada nutitelefonile, tahvel- või pihuarvutile, ilma et seda märgataks.

Sünkroniseerimistarkvara peab olema konfigureeritud nii, et enne programmide installeerimist küsitakse kasutajalt luba. Sünkroniseerimine ei tohi toimuda ilma järelevalveta.

Tuleb protokollida, milliseid programme ja andmeid üle kanti või uuendati ning neid protokolle tuleks vähemalt pisteliselt kontrollida ebaharilike kirjete osas.

Rakenduste valikuks ja installeerimiseks tuleb rakendada nõuetekohast testimis- ja väljastamismeetodit (vt M 4.467 Nutitelefonide, tahvel- ja pihuarvutite rakenduste valimine). Kui ametiasutuses või ettevõttes kasutatakse isiklikke nutitelefone, tahvel- või pihuarvuteid ametialaselt, on selliseid meetodeid võimatu või raskem rakendada.

Turvasuunises tuleks kindlaks määrata, milliseid andmeid ja programme tohib nutitelefonidesse, tahvel- või pihuarvutitesse salvestada. Sellest sõltuvad ka edasised turvameetmed. Näiteks on tahvelarvutil, millesse salvestatakse üksnes kaitset vajavaid andmeid, muu kaitsevajadus kui seadmel, millele on installeeritud krüptograafilised võtmed või juurdepääsuparameetrid IT-süsteemide ja võrkude jaoks.

Olemas on kahjurvaraprogrammid, mis on välja töötatud just nutitelefonide ja tahvel- või pihuarvutite jaoks. Need loevad isiklikke andmeid, helistavad tasulistele teenusenumbritele või saadavad laiali SMS-rämpsposti. Mõned kahjurvaraprogrammid on spetsialiseerunud sellele, et suunata kurjategijatele edasi autentimisteavet, näiteks mobiilset TAN-i online-panganduse jaoks. Suuremal osal viirusetõrjeprogrammide tootjatest on seetõttu võetud tootepaketti viiruseskannerid nutitelefonide ja tahvel- või pihuarvutite jaoks. Sellega seoses ei tohi unustada ka viirusetõrjet sünkroniseerimiseks kasutatavatel seadmetel või teenuseosutajate juures. Ka need peavad olema varustatud ajakohaste viirusetõrjeprogrammidega.

See kehtib eriti ka isiklike PC-de või sülearvutite kohta, millega sünkroniseeritakse mõnikord ka ametialast seadet.

Kui internetiteenuseid kasutatakse nutitelefonide, tahvel- või pihuarvutitega, peavad kõik andmeühendused asutusse olema krüpteeritud nt VPN-i kaudu. Lisaks sellele peavad e-posti klient ja veebibrauser haldama SSL-i või TSL-i ja

nende kaudu ka krüpteeritult suhtlema, et pääseda näiteks juurde ettevõtte- või asutusesisesele serverile. Mõned kaasaskantavate seadmete jaoks mõeldud brauserid toetavad ka aktiivsisusid, seega Java't, ActiveX-i ja/või JavaScript'i. Samuti kui muude IT-süsteemide puhul tuleb ka siin tähele panna, et vastavalt nende programmide tüübile on nende kasutamisega seotud mõnikord ka turvarisk. Seetõttu peaksid aktiivsisud olema veebibrauseris reeglina välja lülitatud ning need aktiveeritakse ainult siis, kui need pärinevad usaldusväärsetest allikatest, st nt tuntud teenuseosutaja WWW-lehekülgedelt.

Seoses sellega, et väikeseid ja kaasaskantavaid seadmeid kaotatakse tihti, tuleb asutuses koostada inventarinimestikud. Need peavad sisaldama vähemalt järgmist teavet: identifitseerimistunnused nagu seadmenumbrid või inventarinumbrid, seadme liik, operatsioonisüsteem, installeerimise kuupäev ja konfigureerimise eripärad, paigalduskoht (kui on statsionaarne), kasutajad ja administraatorid.

Kontrollküsimused:

- Kas pihuarvutite ühendamiseks mõeldud riist- ja tarkvara installeerimine ja konfigureerimine IT-süsteemidega viiakse läbi tsentraalselt ja reguleeritult?
- Kas kasutaja jaoks on olemas arusaadav pihuarvuti juhend?
- Kas pihuarvuti rakenduste jaoks toimuvad testimis- ja väljastamisprotseduurid?
- Kas pihuarvutite sünkroniseerimist logitakse ja kas teostatakse pistelisi kontrollimisi?
- Kas pihuarvutid ja sünkroniseerimiseks kasutatavad PC-d on varustatud viirusetõrjeprogrammidega?
- Kas on olemas pihuarvutite inventariloend?

M 4.230z Nutitelefonide, tahvel- ja pihuarvutite tsentraalne haldamine

Algatamise eest vastutavad: infoturbeametnik, IT-juht

Rakendamise eest vastutab: administraator

Kaasaskantavate seadmete haldus ei ole lihtne ülesanne, eelkõige suurtes asutustes ja kasutajate korral, kes sageli ja igal pool maailmas ringi liiguvad. On olemas vahendid, mis kergendavad turbesuuniste tsentraalset haldust ja rakendamist. Selliste vahenditega saab näiteks rakendada keskseid nõudeid parooli loomisele või parandada juurdepääsukaitset sünkroniseerimisprotseduuril. Seetõttu tuleks kasutada Mobile Device Management (MDM)-lahendust.

Põhimõtteliselt on vaja hästi läbimõeldud ühendust olemasoleva IT-keskkonnaga, et takistada kasutajatel MDM-lahenduse mugava kasutamisega ühendada kontrollimata ja seetõttu võimaliku, et mitteturvalisi nutitelefone, tahvel- või pihuarvuteid ettevõtte IT-süsteemidega. Tsentraalse haldusega ei saa mitte ainult tarkvara ja teavet jaotada, vaid teostada ka organisatsioonile omaseid turvasuuniseid, nt autentimiseks, juurdepääsuks või andmevarunduseks.

MDM-lahendusega ei sünkroniseerita nutitelefone, tahvel- või pihuarvuteid tavaliselt enam kohaliku seadmega, vaid serveriga. Seetõttu ei ole andmeid võimalik enam üksnes ühest jaamast võrrelda, vaid kõikidest serveriga ühendatud seadmetest. See sünkroniseerimine peab olema krüptograafiliselt kaitstud. Paljudel juhtudel ei ole andmed ühendatud kaabliga, vaid sünkroniseeritakse traadita tehnoloogia, nt WLAN-i kaudu. Seetõttu tuleks jälgida, et selleks kasutataks ainult krüptograafiliselt kaitstud WLAN-i. Kui liin on siiski kaitstud krüpteeritud VPN-ühendusega, võib sünkroniseerida ka mitteturvatud WLAN-i kaudu (nt (kohvikutes või hotellides).

Serveri kaudu sünkroniseerimisel on võimalik turvanõudeid tehniliselt forsseerida, mis seisneb selles, et turvalisusega seotud seadistused lähtestatakse nende etteantud väärtustele. Selliste vahendite funktsioonid tsentraalseks Mobile Device Management'iks on muu hulgas järgmised:

- Personal Information Manager'i (PIM) kaudu saab hallata päevaplaane ja aadressiraamatuid, ja seda mitte üksnes üksikute kasutajate, vaid töörühmade jaoks. PIM-andmete, muu teabe ja rakenduste haldust, mis on olemas erinevatel rakendustel, saab tsentraalselt juhtida. Tänu sellele võib nt installeerida ja konfigureerida rakendusi kaugpöörduse korras;
- võimalik on aga ka aadressikogusid ja muid andmeid tsentraalselt hooldada ja edastada. See hõlbustab eriti olukordi, kui on palju liikuvaid töötajaid, kes saavad teel olles imporditud andmeid kiiresti ja mugavalt teiste töötajate kasutusse anda;
- andmed tuleb varundada tsentraalselt, ilma et kasutajad selle pärast muretsema peaksid. Samuti võib olla määratud, millal või kui sageli tuleb andmeid varundada või sünkroniseerida ja millistest raamtingimustest tuleb seejuures kinni pidada;

- võimalik on tagasiside ka nutitelefonide, tahvel- või pihuarvutite oleku kohta, nii et diagnoosimist saab läbi viia ka eemalt;
- saab luua kasutajaprofillid, et hõlbustada kasutajate haldust;
- kehtestada võib organisatsioonile omaselt kasutatavaid paroolireegleid ja muid turvaeeskirju;
- kui MDM-lahendus on loodud erinevate kasutajakontekstide jaoks, nagu nt isiklikud ja ametialased (vt M 4.468 Isikliku ja tööalase kasutamise lahutamine nutitelefonides ning tahvel- ja pihuarvutites), võib see mõlemad valdkonnad eraldada. See toimub suures osas container-lahenduse kaudu, kusjuures container'is on võimalik isiklike PIM-andmete haldus või saab installeerida isegi rakendusi;
- paljud MDM-lahendused pakuvad ka spetsiaalseid meetmeid juhuks, kui seade ära kaob. Nii võib nutitelefone ja tahvelarvuteid selliste programmidega eemalt kustutada, lukustada ja lokaliseerida. Neid funktsioone tuleks teostada tsentraalsest asutusest, keda teavitatakse seadme kadumisest, kokkuleppel kasutajaga ja pärast eelnevalt täpselt määratletud reegleid (vt M 2.306 Kahjudest teatamine ja M 6.159 Nutitelefonide ning tahvel- ja pihuarvutite kaotuste ja varguste ennetamine).

Neid funktsioone saab üldiselt pakkuda mitte ainult vanemate seadmete puhul sageli kasutatavate dokkimisjaamade, vaid ka muude liideste nagu WLAN või Bluetooth kaudu.

Nutitelefonide, tahvel- ja pihuarvutite tsentraalse haldamise vahendit tuleks kasutada võimalikult kõikide asutuses kasutatavate kaasaskantavate seadmete operatsioonisüsteemide toeks, et mitte kasutada mitmeid selliseid vahendeid paralleelselt. Sama kehtib loomulikult ka kasutatava rühmatarkvara ja e-posti platvormi kohta.

Kontrollküsimused

- Kas kasutatakse vahendeid tsentraalseks pihuarvutite halduseks?

M 4.231 Nutitelefonide, tahvel- ja pihuarvutite täiendavate turbelahenduste kasutamine

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: kasutajad, administraator

On olemas mitmesuguseid lisavahendeid pihuarvutite kasutamise turvalisuse tõstmiseks. Need pakuvad laiendatud turvafunktsioone, nagu näiteks:

- failisüsteemi ja salvestuskaartide sisu või üksikute failide või andmebaaside krüpteerimine;
- autentimise parandamine, näiteks lihtsamate või turvalisemate autentimisprotseduuride kasutamise abil;
- kaitse teiste komponentidega ühendamiseks, näiteks kommunikatsiooni krüpteerimise või ühekordsete paroolide loomise abil sisselogimiseks väliste IT-süsteemide kaudu;
- viirusetõrje;
- volitamata isikute seadmele juurdepääsu takistamine.

Nende abil saab pihuarvutite kasutamise turvalisust teatud määral tõsta. Selleks peavad aga kasutajad täiendatud turvamehhanisme täpselt tundma. Ühelt poolt peaksid kasutajad olema informeeritud nende tugevatest ja nõrkadest külgedest ja teiselt poolt oskama neid õigesti käsitseda. Üldiselt peaks aga kõigile kasutajatele selge olema, et nõrkade turvamehhanismidega ebakindlal platvormil on peaaegu võimatu juurutada usaldusväärse turvalisusega rakendust. Paljudele pihuarvutite turvatoodetele on juba välja antud hoiatusteated turvaaukude kohta. Ka olemasoleva pihuarvutite lisa-turvatarkvara abil on võimalik kõrvaldada vaid mõningaid, sugugi mitte aga kõiki pihuarvutite kasutamisega kaasnevaid turvaprobleeme.

Vaatamata sellele tuleks kontrollida, kuivõrd selliseid tööriistasid on mõttekas mingiks otstarbeks kasutada, kuna need aitavad võimalikke ohtusid vähendada. Selliste tööriistade kasutamine on soovitatav juhul, kui pihuarvuteid kasutatakse lubamarkerina või konfidentsiaalsete andmete salvestamiseks. Nii näiteks on olemas tööriistad juurdepääsukaitse parandamiseks, üksikute andmete või kogu süsteemi krüpteerimiseks ja tsentraalseks halduseks.

Kontrollküsimused:

- Kas kasutajaid koolitatakse täiendavate turvavahenditega ümber käima?
- Kas PIN-koodide ja krüptograafiliste võtmete loomine täiendavate turvavahendite kasutamiseks toimub turvaliselt ja suure hoolikusega?

M 4.232z Mälulaienduskaartide turvaline kasutamine

Algatamise eest vastutavad: infoturbeametnik, IT-juht

Rakendamise eest vastutavad: kasutajad

Seoses sellega, et kaasaskantavate seadmete nagu pihuarvutite olemasolev salvestiruum on piiratud, on enamikul mudelitel seda võimalik laiendada väliste andmekandjatega. Selle jaoks on levinud mälukaardid, nt SD-, MMC või ka Compact Flash Card'id, mille eelis on see, et neid saab kiiresti vahetada. Need kaardid ei vaja patareid, mistõttu puudub oht, et salvestatud andmed kaovad voolupuudusel. Need sobivad ka teel olles andmete varundamiseks, mis on eriti kasulik siis, kui pihuarvuti kasutaja on sageli pikalt ära. Nagu üldiselt andmevarunduse puhul, kehtib ka siin, et neid tuleb säilitada turvaliselt. Kui mälukaardid jäetakse pihuarvutis või mujal järelevalveta, võivad neid kasutada volitamata isikud, et lugeda sinna salvestatud andmeid. See toimub sülearvuti ja selleks sobiva adapteriga ühe käeliigutusega. Kui hiljem mälukaart tagasi pannakse, ei ole sellest tegevusest ühtegi jälge.

Selleks, et kaitsta väliste mälukaartide andmeid, on soovitatav krüpteerida neid vastavate täiendavate vahenditega. Seni, kui seda ei ole tehtud, peavad mälukaardid ka teel olles alati järelevalve all olema.

Kontrollküsimused

- Kas mälulaienduskaarte hoitakse turvaliselt?

M 4.234 IT-süsteemide ja andmekandjate väljavahetamise kord

Algatamise eest vastutavad: infoturbe spetsialist, IT-juht
Rakendamise eest vastutavad: administraator, vastutav spetsialist, töötajad

IT-süsteemid ja andmekandjad peavad pideva tehnika arenguga sammu pidama. Seetõttu vahetatakse neid tihedamini välja kui teisi töövahendeid. Enne kui IT-süsteemid või andmekandjad kasutusest kõrvaldatakse, tuleb selgeks teha, kuidas see peab toimuma ning kuidas nendele salvestatud teabega ümber käia. Eelkõige tuleb tagada, et nendele salvestatud tähtsad andmed ei läheks kaotsi ning et andmekandjatele ei jääks konfidentsiaalseid andmeid. Enne IT-süsteemide ja andmekandjate likvideerimist tuleb kontrollida, kas nendel ei paikne veel vajalikke andmeid. Need tuleb siis teistele andmekandjatele varundada või arhiveerida. Tuleb üle kontrollida, kas tõepoolest kõik andmed said korrektselt varundatud. Täiendavat informatsiooni antud teema kohta leiab moodulitest B 1.4 Andmevarunduspoliitika ja B 1.12 Arhiveerimine .

IT-süsteemi kasutusest kõrvaldamisel tuleks lisaks kontrollida, kas on veel olemas varundusandmekandjaid, mida selle käitamise ajal kasutati. Ka need tuleb kustutada ja kasutuskõlbmatuks muuta, kui nendele salvestatud andmeid enam ei vajata. Seejärel tuleb välja selgitada, kas IT-süsteemid või andmekandjad antakse edasi kolmandatele isikutele või hävitatakse. Tihti kasutatakse IT-süsteeme pärast kasutusest kõrvaldamist edasi, näiteks antakse välja praagitud IT-süsteemid edasi teistele osakondadele, kingitakse töötajatele või müüakse maha. Sel juhul tuleb kehtestada reeglid, kuidas edasisel kasutamisel nendele salvestatud informatsiooni kaitsta või usaldusväärselt eemaldada. Kui andmekandjad antakse edasi võõrastele, tuleb need turvaliselt üle kirjutada. Kui ka esimesel pilgul tundub, et andmekandjatel ei ole enam konfidentsiaalset informatsiooni, võivad need siiski olla ebapiisavalt kustutatud, ning võivad sisaldada jääkinformatsiooni. Peab olema tagatud, et kõik andmed ja rakendused on eelnevalt hoolikalt kustutatud (vt M 2.433 Ülevaade meetoditest andmete kustutamiseks ja hävitamiseks). Kui andmekandjale on salvestatud kõrge kaitsevajadusega andmed, on nende andmete turvaliseks kustutamiseks tihti vajalik andmekandjate füüsiline hävitamine.

IT-süsteemide ja andmekandjate kasutusest kõrvaldamise reguleerimisel ei tohi unustada ka seadmeid, mida ei peeta just IT-süsteemideks, aga mis võivad sisaldada suurel hulgal konfidentsiaalseid andmeid, näiteks mobiiltelefonid, printerid, koopiamasinad või faksiaparaadid. Faksiaparaatide edasiandmisel ja müümisel tuleb tähelepanu pöörata asjaolule, et faksi ühendusandmete ja sisu sisemised salvestid saavad turvaliselt kustutatud. Lisaks sellele tuleb seadmetelt ja andmekandjatelt eemaldada kõik märgistused ja etiketid, mis viitavad nende endisele kasutusotstarbele, näiteks etiketid IP-aadresside ja arvutite nimedega. Samuti tuleb turvaliselt kustutada ja hävitada ka IT-süsteemid ja andmekandjad, mille käitus ja/või hooldus likvideeriti. Nende turvaline kasutusest kõrvaldamine koos jäätmekäitluse või tagastamisega tuleb reguleerida vastavate lepingutega. IT-süsteemide ja andmekandjate kasutusest kõrvaldamiseks kasutatud protseduurid peavad olema asutuses arusaadavalt dokumenteeritud. Ülaltoodud informatsiooni alusel on

soovitatav koostada nimekiri süsteemi kasutusest kõrvaldamiseks tehtavatest tegevustest. Sel moel on võimalik vältida, et midagi vajalikku ununeb. Soovitatav on ka, et üksikud sammud on kirjalikult tõendatud volitatud isikute poolt.

Täiendavad kontrollküsimused:

- Kas on olemas selgelt defineeritud protseduurid IT-süsteemide ja andmekandjate kasutusest kõrvaldamiseks?
- Kas enne igat liiki IT-süsteemide ja andmekandjate kasutusest kõrvaldamist kustutatakse hoolikalt kõik andmed?
- Kas IT-süsteemide ja andmekandjate korrakohane kasutusest kõrvaldamine asutuses dokumenteeritakse arusaadavalt?

M 4.235 Andmete seisu võrdsustamine sülearvutites

Algatamise eest vastutavad: Infoturbe osakond, IT-juht
Rakendamise eest vastutavad: kasutajad, administraator

Kui sülearvutit kasutatakse ringi liikudes, on tähtis, et oleks võimalik kasutada kõiki vajalikke andmeid ja rakendusi kõige uuemas versioonis. Samuti peaksid ringi liikudes töödeldud andmed olema kiiresti salvestatud asutuse või ettevõtte IT-koosluse ITsüsteemidele, et andmebaasis ei esineks ebapüsivusi. Kõige lihtsam viis selleks on sülearvutite andmebaaside regulaarne kontroll, näiteks kasutades tööriistu, mis võimaldavad failide ja kataloogide ning sülearvutite ja töökohaarvutite või serverite vahelist sünkroniseerimist. Selleks tuleb mõelda, milline info on millistesse kohtadesse salvestatud, s.t millistele serveritele ja millistesse kataloogidesse. Esmasel vaatlusel selgub tavaliselt, kui paljudes IT-koosluse erinevates kohtades töökoha jaoks olulised andmed paiknevad. Et sünkroniseerimisprotseduurid liiga kaua ei kestaks, tuleb välja valida tööriistad:

- mille abil oleks võimalik eelnevalt kindlaks määratud kriteeriumide järgi automaatselt võrrelda ja värskendada faile ja katalooge;
- mis pakuvad filtreerimisvõimalust, et terveid katalooge või üksikuid faile kopeerimisprotseduurist välja arvata;
- mis võivad lahendada sünkroniseerimiskonflikte.

Sünkroniseerimiskonfliktid võivad ette tulla, kui alates viimasest sünkroniseerimisest muudeti ühte faili erinevates kataloogides. Sünkroniseerimisvahendid peavad peale selle olema võimalikult kasutajasõbralikud ning vaatamata sellele tagama tõhusa kaitse vale kasutamise eest. Sünkroniseerimisprotseduurid peaksid olema kaitstud juurdepääsu eest, sülearvutitel võib see toimuda juba olemasolevate juurdepääsukaitse meetodite abil. Selleks et sünkroniseerimise kaudu ei oleks võimalik andmetega manipuleerida, peavad kasutajad regulaarselt kontrollima olulise tähtsusega katalooge, kas nendes ei leidu neile tundmatuid faile. Sünkroniseerimistarkvara peaks olema selliselt konfigureeritud, et enne programmide installeerimist küsitakse kasutaja käest luba.

Sünkroniseerimisprotsess ei tohi kulgeda märkamatult, ka info selle kohta, millised failid millal üle kantakse, võib sisaldada olulisi viiteid. Sünkroniseerimine tuleb protokollida. Sünkroniseerimisprotokollid tuleb regulaarselt vähemalt üle vaadata, et kindlaks teha, kas pole toimunud volitamata sünkroniseerimisprotsesse.

Täiendav kontrollküsimus:

- Kas on olemas vahendid või meetodid andmekogude sünkroniseerimiseks sülearvutite ja statsionaarsete IT-süsteemide vahel?

M 4.236z Sülearvutite tsentraalne haldus

Algatamise eest vastutavad: infoturbe osakond, IT-juht
Rakendamise eest vastutavad: administraator

Mobiilsete lõppseadmete haldamine ei ole lihtne ülesanne, eriti suurtes asutustes ning kasutajate korral, kes rändavad maailmas palju. On olemas tööriistad, mis kergendavad turvasuuniste rakendamist ja tsentraalset haldust. Tsentraalse halduse abil saab jaotada mitte ainult tarkvara ja teavet, vaid viia ellu ka organisatsioonisiseseid turvasuuniseid, näiteks autentimise, juurdepääsu või andmevarunduse turvaliseks teostamiseks. Tarkvara kasutamisel sülearvutite tsentraalseks halduseks ei toimu sülearvutite sünkroniseerimine tavaliselt enam kohaliku lõppseadme, vaid serveriga. Seetõttu ei saa andmete võrdlemine toimuda enam mitte ainult ühest jaamast, vaid kõigist serveriga seotud jaamadest. Serveri kaudu sünkroniseerimisel on võimalik ka turvanõuetest tehniliselt mööda hiilida, kusjuures turvalisuse seisukohalt olulise tähtsusega seaded viiakse nende esialgsetele väärtustele tagasi. Selliste tööriistade tüüpilised funktsioonid sülearvutite haldusel on muu hulgas:

- Andmete varundamise võib teostada tsentraalselt, ilma et kasutajad selle pärast muretsema peaksid. Samuti võib kindlaks määrata nõuded, millal või kui tihti tuleb andmed varundada või sünkroniseerida ning milliseid raamtingimusi seejuures tuleb järgida.
- Võimalik on saada tagasisidet sülearvutite olukorra kohta ning diagnoosida kaugpöörduse kaudu.
- Kasutajahalduse lihtsustamiseks võib luua kasutajaprofiilid.
- Võimalik on ette anda organisatsioonisiseselt seadistatavad reeglid paroolide kasutamiseks ja teised turvareeglid.

Sülearvutite tsentraalseks halduseks kasutatav tööriist peaks võimalusel toetama kõiki organisatsioonis kasutatavaid sülearvutite operatsioonisüsteeme, et ei oleks vaja kasutada paralleelselt mitmeid selliseid tööriistu. Sama kehtib ka loomulikult kasutatava grupitarkvara ja meiliplatvormi kohta.

M 4.237 IT-süsteemi turvaline aluskonfiguratsioon

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutab: administraator

Operatsioonisüsteemi tootja või levitaja poolsed algsätted ei ole enamasti optimaalselt turvalised, tähtsamaks on peetud lihtsat installeerimist ja kasutuselevõttu ning seda, et iga kasutaja saaks võimalikult lihtsalt võimalikult paljusid operatsioonisüsteemi funktsioone kasutada. IT-süsteemide kasutamisel (ükskõik, kas kliendi või serverina) asutustes või ettevõtetes ei ole see tihti soovitav. Esimene samm aluskonfiguratsiooni juures peab seetõttu olema algsätete kontrollimine ja vajadusel nende vastavusse viimine turvapoliitika nõuetega. Aluskonfiguratsioon on tavaliselt suhteliselt tugevasti sõltuv kasutatavast operatsioonisüsteemist. Seetõttu on vastavad detailsed meetmed kirjas operatsioonisüsteeme kajastavates moodulites. Turvalise aluskonfiguratsiooniga tuleks saavutada, et:

- süsteem on kaitstud võrgust tulevate „lihtsate" rünnakute eest,
- lihtkasutaja ei saa uudishimust või kogemata juurdepääsu andmetele, mis pole talle määratud,
- lihtkasutaja ei saa eksituse või kergemeelsuse tõttu („Mis õige juhtub, kui ma selle faili kustutan?") oma töö käigus raskelt kahjustada süsteemi ega teiste kasutajate andmeid, ning
- süsteemiadministraatori väikeste eksituste toime oleks võimalikult piiratud.

Sätted, mis tuleks aluskonfiguratsiooni raames üle kontrollida ja vastavusse viia, puudutavad eriti järgmisi valdkondi:

Süsteemiadministraatori sätted
Süsteemiadministraatori konto jaoks tuleb valida eriti turvalised sätted. See puudutab kasutajakeskkonna sätteid, nagu näiteks:

- programmi- ja failipöördusteed,
- keskkonnamuutujad ja
- mõnede programmide konfiguratsioon.

Nimetatud sätted tuleks üle kontrollida ja vajadusel nõuetega vastavusse viia. Peale selle tuleks süsteemiadministraatori kasutajakataloogi sätted valida nii, et välistatud oleks lihtkasutajate juurdepääs.

Süsteemikataloogide ja -failide sätted

Aluskonfigureerimisel peaks kontrollima, kas õigused süsteemikataloogidele ja -failidele vastavad turvapoliitika nõuetele. Serveril peavad need süsteemikataloogide ja -failide õigused olema tugevalt kitsendatud.

Kasutajakontode sätted

Aluskonfiguratsiooni raames tuleb kontrollida, millised standardsätted kasutajakontodele kehtivad. Sätted tuleb vajadusel vastavusse viia turvapoliitika nõuetega. See puudutab peamiselt neidsamu parameetreid nagu süsteemiadministraatori kontogi, lihtkasutajale võivad aga teatud juhtudel olla mõttekamad teised sätted.

Kasutajate andmebaasi puhastamine

Tihti seatakse operatsioonisüsteemi standardinstallimise raames sisse suurem arv kasutajakontosid, mis ei ole kasutamiseks ilmtingimata vajalikud. Seetõttu tuleks aluskonfiguratsiooni raames kontrollida, millised kasutajakontod on tõepoolest vajalikud. Mittevajalikud kasutajakontod tuleb kas kustutada või vähemalt deaktiveerida, et vastava konto all ei oleks võimalik pääseda süsteemi.

Võrguteenuste kontroll

Operatsioonisüsteemi standardinstallatsioon sisaldab tihti terve rea võrguteenuseid, mida tavaliselt ei vajata ning mis just seetõttu võivad olla turvaaukude allikaks. Seepärast tuleb pärast installeerimist kontrollida, millised võrguteenused on süsteemile installeeritud ja aktiveeritud. Tarbetud võrguteenused tuleb deaktiveerida või deinstalleerida. Kasutuses olevate teenuste kontroll võib ühelt poolt toimuda lokaalselt installeeritud operatsioonisüsteemi vahendite abil ning teiselt poolt portscanner 'i kaudu väljast teiselt süsteemilt. Mõlemate meetodite kombineerimisel saab välistada võimaluse, et süsteem pakub veel tarbetuid võrguteenuseid.

Sätted pääsuks võrku

Aluskonfiguratsiooni raames tuleks kindlaks määrata ja dokumenteerida ka sätted võrkupääsuks ning olulise tähtsusega välisteenuste juurde. See puudutab näiteks (kui see pole juba installimise käigus toimunud):

- IP-aadresside jagamist ja põhjapanevate võrguparameetrite konfigureerimist või juurdepääsu konfigureerimist serverile, mis jagab automaatselt DHCP-protokolli (Dynamic Host Configuration Protocol) kaudu võrgusätteid. Serveri korral ei ole igatahes soovitatav DHCP-protokolli kasutada.
- DNS-serverile juurdepääsu konfigureerimist ja teisi nimeteenuseid, ning
- juurdepääsu konfigureerimist jagatud failisüsteemidele, andmebaasidele või teistele välisteenustele.

Lisakaitse lokaalse paketifiltriga

Kõrgete turvanõuetega serverid ja kliendid tuleb kindlustada lisaks üleorganisatsioonilistele turvalüüsidele või paketifiltritele, mis segmenteerivad sisevõrku,

ka lokaalse paketifiltriga. Vastavad funktsioonid on praktiliselt kõikides moodsates operatsioonisüsteemides olemas. Aluskonfiguratsiooni raames tuleb vähemalt kõrgete turvanõuetega serverile luua kaitse lokaalse paketifiltri kaudu. Ka tavapäraste turvanõuetega serverite kaitseks soovitatakse kasutada lokaalset paketifiltrit. Sel juhul võib valida „liberaalsema" konfiguratsiooni. Klientide jaoks soovitatakse lokaalset paketifiltrit vähemalt juhul, kui nende konfidentsiaalsusele ja terviklusele esitatakse kõrgeid või väga kõrgeid turvanõudeid. Täpsemat infot lokaalse paketifiltri kasutamiseks annab meede M 4.238 Lokaalse paketifiltri rakendamine .

Terviklusandmestiku loomine

Pärast aluskonfiguratsiooni lõpuleviimist on soovitatav luua vastava tööriista abil terviklusandmestik. Mõnedel operatsioonisüsteemidel kuuluvad vastavad programmid juba standardinstallatsiooni hulka. Terviklusandmestik ei tohi olla salvestatud süsteemile endale, vaid mõnele kirjutuskaitstud andmekandjale (näiteks CD-R) või mõnele teisele hästi kaitstud süsteemile. Süsteemi kompromiteerimise kahtluse korral on võimalik loodud kontrollsummade abil identifitseerida faile, mis on ründaja poolt modifitseeritud. Süsteemi tervikluse regulaarse kontrolli korral (vt M 5.8 Võrgu regulaarne turvakontroll) kujutab see andmebaas endast vajalikku teavet süsteemi defineeritud kindla seisundi jaoks.

Dokumenteerida tuleb, millised sätteid tuleb aluskonfiguratsiooni raames kontrollida, ja kas neid on vaja muuta, ning kuidas on neid vaja muuta. Dokumentatsioon peab olema selliselt loodud, et hädaolukorras ka keegi teine peale tegeliku administraatori saaks ilma eelnevate teadmisteta dokumentatsiooni abil süsteemis teostatud toimingute kohta teavet. Ideaaljuhul peaks olema võimalik taastada süsteem ainult dokumentatsiooni abil.

Täiendavad kontrollküsimused:

- Millised on süsteemiadministraatori kasutajakeskkonna sätted?
- Kas ebatarvilikud kasutajakontod on deaktiveeritud või kustutatud?
- Kas mittetarvilikud võrguteenused on deaktiveeritud või deinstalleeritud? Kas on tehtud *portscan* ?
- Kas on loodud terviklusandmestik? Millist tööriista kasutati?

M 4.238 Lokaalse paketifiltri rakendamine

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutab: administraator

Organisatsiooni kogu võrk peab olema kaitstud vastava turvalüüsi abil. Serverid, mis pakuvad teenuseid väljapoole, peaksid olema paigaldatud demilitariseeritud tsooni (DMZ). Vaatamata sellele on soovitatav seada juurdepääsupiirangud rakendus- või võrgutasandil sisse igal arvutil. See kehtib ka serverite kohta, mida kasutatakse ainult sisevõrgus, ning klientidele. Lokaalse paketifiltri abil on võimalik kaitsta arvutit rünnakute eest, mis käivitatakse samast alamvõrgust. Lisaks sellele saab sellist paketifiltrit kasutada detailsemaks juurdepääsukontrolliks üksikutele teenustele, nagu see on näiteks võimalik vaid paketifiltritega võrgu ülekäigukohtades. Lokaalset paketifiltrit võib kasutada ka väljuvate võrguühenduste piiramiseks ning nii süsteemi kompromiteerimise tagajärgede ärahoidmiseks. On võimalik, et selline kaitse deaktiveeritakse ründaja poolt arvuti eduka kompromiteerimise järel, teiselt poolt aga on ründajat sel moel vähemalt võimalik takistada. Sel moel saab võita küllaldaselt aega ründe avastamiseks ja võimalikeks vastureaktsioonideks. Lõpuks võimaldab lokaalse paketifiltri protokollifunktsioon teatud rünnakuid üleüldse avastada.

Praktiliselt kõik kaasaegsed operatsioonisüsteemid pakuvad võimalust filtrite defineerimiseks, mis uurivad ja töötlevad kõiki vastu võetud või saadetavaid pakette kindlate reeglite järgi. Üksikute operatsioonisüsteemide filtri võimalused erinevad seejuures tunduvalt. Siiski on praktiliselt alati võimalik defineerida paketi saatja ja vastuvõtja aadressil ja kasutatud protokollitüübil (TCP/IP, UDP/IP, ICMP jne) ning teatud juhtudel lähte- ja sihtkoha pordil baseeruvaid reegleid. Paketifiltrite reeglite abil saab näiteks pakette, mis pärinevad teatud arvutitelt või kindlatest alamvõrkudest, sihilikult tagasi lükata. Mõnedel serverirakendustel on oma mehhanismid, mis lubavad või keelavad üksikute IPaadresside või aadressipiirkondade juurdepääsu teenusele. Nende mehhanismide kõrval on lokaalsel paketifiltril operatsioonisüsteemi tasandil eelis, sest see kaitseb teenust ise võimalike rünnete eest, mis võivad viia süsteemi kuritarvitamiseni enne kui integreeritud juurdepääsupiirang üldse aktiveeruda suudab. Põhimõtteliselt peaksid kõik kõrgete turvanõuetega serverid olema kaitstud lokaalse paketifiltriga.

Paketifiltrite reeglite juurutamiseks on kaks üldist strateegiat. Musta nimekirja strateegia lubab igat liiki ühendusi, mis ei täida välistamiseks vajalikke kriteeriume (vabameelne strateegia: „Kõik on lubatud, mis ei ole selgesõnaliselt keelatud”). Eelis seisneb väiksemates kulutustes administreerimisel ja vigade otsimisel. Suureks puuduseks on siiski, et unustatud reeglid, mis võimaldavad juurdepääsu kaitseta võrguteenustele, võivad saada aluseks ründele. Vastupidiselt sellele blokeeritakse valge nimekirja strateegia korral kõik ühendused, mis ei kuulu lubatud teenuste nimekirja (piirangutega strateegia: „Kõik on keelatud, mis ei ole selgesõnaliselt lubatud”). Valge nimekirja strateegia pakub suuremat turvalisust ning seetõttu tuleks seda põhimõtteliselt kasutada, kui teatud põhjused seda ei välista. Puuduseks on kalduvus suurematele administreerimiskuludele, kuna igakordse nõuete muutmise korral tuleb defineerida uued reeglid. Erandjuhtudel, kui protokoll ei tööta kindlalt defineeritud portidel, võib kasutada musta nimekirja strateegiat.

Soovitatav on kõikidel serveritel aluskonfiguratsiooni raames sisse seada baasreeglistikuga lokaalne paketifilter, mille puhul lükatakse väljastpoolt põhimõtteliselt tagasi kõik ühenduspäringud. See reeglistik peaks olema aktiveeritud, kui süsteem võrguga ühendatakse. Vastavalt sellele, milliseid teenuseid süsteem peaks pakkuma, võib nende konfigureerimise järel vajaminevad protokollid ja pordid kasutusse anda. Ka klientide puhul peaks selle protseduuriga arvestama vähemalt juhul, kui need esitavad kõrgendatud nõudeid turvalisusele. Paketifiltrid võimaldavad enamasti võrguliikluse detailset protokollimist. Lokaalse paketifiltri paigaldamine on seetõttu kasulik ka turvalistes võrkudes, mis on turvalüüsi abil ebaturvalisest võrgust, näiteks internetist, eraldatud, sest saadud infost võib rünnete ärahoidmisel abi olla. Igatahes tuleb tähelepanu pöörata asjaolule, et ei rikutaks andmekaitseseadust. Vajadusel peaks koostööd tegema vastavate ametiisikutega (andmekaitse eest vastutav töötaja, töökollektiivi esindaja).

Interneti kontrollsõnumiprotokolliga (ICMP) seotud probleemid

Interneti kontrollsõnumiprotokolli (ICMP) kasutatakse veateadete edastamiseks IPpakettide ülekandmisel. Näiteks on olemas sõnumid, mis teatavad paketi saatjale, et sihtvõrk ei ole kättesaadav või et pakett on sihtvõrku edasisaatmiseks liiga suur. Ka tööriistade ping ja traceroute funktsiooni aluseks on ICMP-protokoll. Lisaks paljudele kasulikele omadustele on olemas ka mõned ICMP-sõnumitüübid, mille kaudu ründajad saavad võrgust tähtsat teavet ning võivad seda kasutada otseselt ründe teostamiseks. Kahjuks ei kujuta radikaalne meetod, ICMP põhimõtteliselt turvalüüsi juures blokeerida, endast samuti rahuldavat lahendust, kuna teatud kindlaid funktsioone ei ole siis enam võimalik kasutada. Tavaliselt võib ping ja traceroute tööriistadest tavalisel töökohaarvutil ja serveritel loobuda, ICMP laialdane blokeerimine võib aga esile kutsuda kahjustusi, mida on raske diagnoosida. Seetõttu tuleks kaaluda, niivõrd kui see on võimalik, selektiivset ICMP-filtreerimist nii turvalüüsis kui ka lokaalses paketifiltris. See peaks toimuma alati arvestades arvuti kasutusotstarvet (server või töökohaarvuti), selle turvanõudeid ning turvalüüsis rakendatud meetmeid. Näiteks võib sisevõrgule lubada suuremal hulgal sõnumitüüpe kui välisvõrgule. Rohkem informatsiooni ICMP filtreerimise kohta leiab moodulis B 3.301 Turvalüüs (tulemüür) ning meetmes M 5.120 ICMP-protokolli käsitlus turvalüüsis .

Rakendamine ja kontroll

Millised filtreerimise ja protokollimise võimalusi saab kasutada, oleneb operatsioonisüsteemist. Enne lokaalse paketifiltri paigaldamist tuleb läbi vaadata olemasolev dokumentatsioon. Paketifiltrite paigaldamine peaks toimuma suure hoolikusega, kuna viga võib esile kutsuda olukorra, et administraator, kes võrgu kaudu arvutil töötab, sel viisil „ukse taha jääb” ning peab tegema korrektuure süsteemikonsoolilt. Pärast lokaalse paketifiltri aktiveerimist tuleks ühelt poolt kontrollida, kas vajalikud teenused on veel kättesaadavad, teiselt poolt tuleks portscanner'iga üle kontrollida, kas kõik ülejäänud pordid on blokeeritud.

Näide

Lokaalsed paketifiltri reeglid veebiserverile

Järgnevas näites tehakse ettepanekud lokaalsete paketifiltri reeglite kehtestamiseks arvutile, mis on paigaldatud veebiserverina demilitariseeritud tsooni (DMZ). Seejuures lähtutakse sellest, et serveri administreerimine töökohaarvutilt

toimub ssh-ühenduse kaudu ning failid veebisaidi jaoks kantakse samuti arvutile ssh-ühenduse kaudu. Veebiserveri jaoks lülitati nimede teisendamine DNS-i kaudu välja, seetõttu ei ole vajalik juurdepääs DNS-serverile. Sideprotokolli UDP võib seetõttu täielikult blokeerida. Veebiserverilt ei vajata tavaliselt ping ega traceroute tööriistasid, need on lubatud vaid ICMP sõnumitüübile 3 (Destination unreachable). Kergema diagnoosi jaoks võib sisevõrgus teatud juhtudel lubada ka teisi ICMP sõnumitüüpe (näiteks tüüp 8 ja tüüp 0: echo request ja echo replay). Näites on sisevõrgu jaoks lubatud sisenev echo request ja väljuv echo replies. See võimaldab ühendada veebiserverit sisevõrgust. Lisaks sellele on tähtis, et ssh-ühendused toimuvad vaid veebiserveri suunas, kuid ei välju sellelt. Sama kehtib ka TCP port 80 ühenduste kohta, mis kuulub veebiserveri protsessi hulka: sellele pordile on lubatud sisenevad ühendused, kuid pole lubatud väljuvad ühendused. See tähendab, et põhimõtteliselt ei ole vaja väljuvaid ühenduspäringuid (ainult TCP SYN lipp on seatud), vaid lubatud on ainult väljuvad TCP-paketid, mis kuuluvad olemasoleva ühenduse juurde (TCP ACK lipp on seatud). Väljuvate ühenduspäringute blokeerimise eesmärgiks on, nagu eespool selgitatud, ründaja, kes on turvaaugu kaudu veebiteenuses loonud endale juurdepääsu arvutile, vähemalt kinni pidada. Ründaja saab selle tõkendi küll deaktiveerida, see pakub aga eriti juhul lisa turvalisust, kui seda kombineerida vastavate protokollimis- ja alarmifunktsioonidega.

Lähteaadress: Port	Sihtaadress: Port	Protokoll	TCP-lipud või ICMP-tüüp	Otsus
sisemine:*	Veebiserver:22(ssh)	TCP	SYN või ACK	Aktsepteering
väline:	Veebiserver:22	TCP	kõik	Blokeering
Veebiserver:22	sisemine:*	TCP	ACK	Aktsepteering
kõik:*	Veebiserver:80(http)	TCP	SYN või ACK	Aktsepteering
Veebiserver:80	kõik:*	TCP	ACK	Aktsepteering
kõik	Veebiserver, mitte 22 või 80	TCP	kõik	Blokeering
Veebiserver:*	kõik:*	TCP	ilma ACK-ta	Blokeering
kõik	kõik	UDP	-	Blokeering
kõik	Veebiserver	ICMP	Tüüp 3	Aktsepteering
Veebiserver	kõik	ICMP	Tüüp 3	Aktsepteering
sisemine	Veebiserver	ICMP	Tüüp 8	Aktsepteering
Veebiserver	sisemine	ICMP	Tüüp 0	Aktsepteering
Veebiserver	kõik	ICMP	teised	Blokeering
kõik	Veebiserver	ICMP	teised	Blokeering

Tabel: Paketifiltri näidiskonfiguratsioon
* tähistab tabelis suvalist porti.

Veel suuremat turvalisust on selle näite puhul võimalik saavutada, kui siseaadressidele, millelt on lubatud juurdepääs ssh kaudu, kehtestatakse edasisi piiranguid. Kui ainult kaks administraatorit oma mõlemalt töökohaarvutilt juurdepääsu omavad, peaks olema piiratud juurdepääs nende mõlema arvuti aadressidele.

Detailsemat informatsiooni paketifiltrite kohta leiab moodulist B 3.301 Turvalüüs (tulemüür) .

Täiendavad kontrollküsimused:

- Kas standardsättena lükatakse kõik ühenduspäringud välissüsteemidest tagasi?
- Kas kõik vastuvõetud ja saadetud paketid protokollitakse või on otstarbekas nende selekteerimine?

- Kuidas on võrguteenuste käsutusse andmise korral võimalik sihtgrupi piiramine IPaadresside või võrgumaskide alusel ning kuidas see on juurutatud?
- Kas on võimalik vastu võtta pakette, mis saadeti vastusena lokaalse süsteemi poolt algatatud päringule suhtluspartneri poolt?
- Kas pärast reeglistiku sõnastamist on need portscanner'iga välissüsteemist üle kontrollitud?

M 4.239 Serveri turvaline käitus

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator

Serveri turvaline käitus sõltub tervest reast faktoritest. Eriti tähtis on, et serveri administreerimine toimuks erilise hoolega turvalise juurdepääsu tingimustes. Järgnevalt on juttu üldistest põhimõtetest, millega tuleb serveri turvalise käituse tagamisel arvestada. Asjaomaste moodulite vastavates meetmetes antakse üksikutele operatsioonisüsteemidele nõuandeid olenevalt nende spetsiifikast.

Administreerimispääsud
Serveri administreerimiseks on olemas erinevaid juurdepääsuvõimalusi. Sõltuvalt kasutatud juurdepääsu laadist, tuleb rakendada terve rida turvameetmeid. Suuremate võrkude korral on soovitatav ühendada ka serverid tsentraalsesse võrguhaldussüsteemi, kuna vastasel juhul ei ole turvaline ja efektiivne administreerimine võimalik. Administreerimiseks kasutatavad meetodid tuleb turvasuunistes kindlaks määrata ning administreerimine peaks toimuma vaid vastavalt turvasuunistele. Tähtis on saada ülevaade, missugune osa serveri administreerimisest tavaliselt peab toimuma:

- lokaalselt konsooli kaudu
- kaugpöörduse teel võrgu kaudu, kuid operatsioonisüsteemi standardmehhanisme kasutades, või
- tsentraalsel võrgul baseeruva administreerimistööriista kaudu.

Soovitatav on luua ülevaade erinevate kasutuslaadide jaoks, milliseid administreerimistegevusi mingil viisil saab korraldada. Kindlasti tuleb fikseerida, kas teatud tegevusi ei tohi tavaliselt teatud viisil teha.

- Lokaalne administreerimine - Server peaks olema põhimõtteliselt paigutatud serveriruumi või vähemalt suletavasse serverikappi. Administreerimise selle osa kohta, mis peab osaliselt siiski toimuma konsooli kaudu, tuleb kindlaks määrata nõuded selles osas, kes saab konsoolile juurdepääsu, millist liiki autentimist tohib lokaalseks juurdepääsuks kasutada ning milliseid teisi nõudeid tuleb täita.
- Kaugadministreerimine - Turvamata kaugadministratsiooni (ebaturvaliste) välisvõrkude kaudu ei tohi mitte mingil juhul toimuda. Sellega tuleks arvestada juba turvasuuniste kindlaksmääramisel. Ka sisevõrgus ei tohiks, niivõrd kui see on võimalik, kasutada ebaturvalisi protokolle.Enamasti ei toimu serveri administreerimine mitte lokaalselt konsooli kaudu vaid töökohaarvutilt võrgu kaudu. Takistamaks, et seejuures administraatorite autentimisteave ja serverite konfiguratsiooniandmed volitamata isikuteni jõuavad või et isegi

ründaja nendega manipuleeriks, peaks administreerimine toimuma vaid turvaliste protokollide kaudu (näiteks mitte Telneti, vaid SSH, mitte HTTP, vaid HTTPS-i kaudu). Alternatiivina võib sisse seada oma administreerimisvõrgu, mis on ülejäänud võrgust eraldatud.
- Administreerimine tsentraalse haldussüsteemi kaudu - Kui serveri administreerimiseks tuleb kasutada tsentraalset haldussüsteemi, tuleks juurdepääsuteele esitada samasuguseid nõudeid, kui kaugadministreerimisele. Lisaks sellele on tähtis, et tsentraalse haldussüsteemi enda konfigureerimine ja administreerimine toimuks turvaliselt (vt B 4.2 Võrgu- ja süsteemihaldus).

Rutiinsed tegevused administreerimisel

Soovitatav on koostada nõuanded administraatorite tavapäraste rutiinsete tegevuste korraldamiseks administreerimise käigus vastavalt serveri turvasuunistele. See hõlmab järgmisi tegevusi:

- kasutajate sisseseadmine ja kustutamine;
- programmide installeerimine ja deinstalleerimine;
- turvatäiendite ja paikade paigaldamine (vt M 2.273 Turvalisust mõjutavate paikade ja värskenduste kiire paigaldamine);
- teiste täiendite ja paikade paigaldamine;
- süsteemi tööseisukorra regulaarne kontroll (näiteks süsteemi täiskoormatus, ketta järelejäänud vaba salvestusruum);
- ebatavaliste sissekannete logiandmete kontroll (vt M 5.9 Serveri logi);
- regulaarne tervikluse kontroll vastavate tööriistadega (vt M 4.93 Regulaarne tervikluse kontroll ja M 5.8 Võrgu regulaarne turvakontroll).

Konfiguratsioonimuutuste testimine

Mitmesugused serveriprogrammid võimaldavad enne konfiguratsioonimuutuste jõustumist neid kontrollida, vähemalt nende tehnilist korrektsust. Selle abil on võimalik takistada, et serveriprogramm pärast vigast konfiguratsioonimuutust enam ei käivitu ning viib nii vastava teenuse väljalangemiseni. Niivõrd kui sellised võimalused on olemas, peavad administraatorid nende kasutamist tundma ning neid ka tõepoolest kasutama.

Süsteemis teostatud tööde dokumentatsioon

Süsteemi ja serveriprogrammide konfiguratsiooni muutused tuleb dokumenteerida. Dokumentatsioon peab olema selliselt koostatud, et probleemide tekkimisel on näha, mis oli viimane muudatus ning millal ja kelle poolt see tehti. Seejuures on tähtis, et dokumentatsioon on koostatud selliselt, et nendest saavad aru mitte ainult administraatorid, vaid ka spetsialistidest kolmandad isikud, kellel ei ole kõnesoleva süsteemiga igapäevaselt mingeid kokkupuuteid. Lisaks sellele peaks dokumentatsiooni abil olema võimalik taastada varasem konfiguratsioon.

Tekstil baseeruvate konfiguratsioonifailide muutmiseks on olemas revisjonihalduse süsteemid. Konfiguratsioonifailides peaks olema lühikeste kommentaaride abil selgitatud ka uute konfiguratsioonisätete mõju ja funktsioon. Teiste konfiguratsioonimehhanismide jaoks on osaliselt olemas sarnased tööriistad või pakub kõnesolev tarkvara juba standardikohaselt vastavaid funktsionaalsusi. Kui kasutatakse tsentraalset administreerimissüsteemi, peavad vastavad funktsioonid olemas olema ning neid tuleks ka kasutada.

Täiendavad kontrollküsimused:

- Mil moel toimub juurdepääs süsteemi administreerimiseks?
- Kuidas testitakse konfiguratsioonimuutusi?
- Kuidas dokumenteeritakse muutusi?

M 4.240z Serveri testimiskeskkonna rajamine

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutab: administraator

Kõrgete turvanõuetega serveritele tuleb luua testimiskeskkond, milles on võimalik testida konfiguratsioonimuutusi, täiendeid ja paiku enne nende tootmissüsteemile paigaldamist. See puudutab nii turvapaikasid ja –täiendeid, kui ka tavapäraseid täiendeid, mida antakse välja tootja poolt. Testimiskeskkond peab olema loodud selliselt, et see lubab „funktsionaal-ekvivalentset" riist- ja tarkvara installeerimist. See ei tähenda ilmtingimata, et lisaks kallile serverarvutile tuleb muretseda teine, identselt konfigureeritud süsteem. Rakendusprogrammide konfiguratsioonimuutuste, täiendite ja paikade ning serveritarkvara testimiseks piisab enamasti tehniliselt oluliselt kokkuhoidlikumalt varustatud süsteemist.

Igatahes peab olema ka võimalus uute seadmeajamite testimiseks enne nende paigaldamist. Seepärast võib teatud juhtudel olla kasulik kasutada erinevat liiki testide tegemiseks erinevaid testimissüsteeme, näiteks üht süsteemi süsteemilähedaste programmide või operatsioonisüsteemi paikade testimiseks ja teist testide korraldamiseks, mis on seotud tegeliku serveritarkvaraga. Sellisel juhul on siiski vajalik endale teadvustada, et sel viisil ei ole võimalik katta teatud liiki operatsioonisüsteemi keskkonna ja serveritarkvara vahelisi vastastikuseid mõjusid. Seetõttu võib serverile esitatavate kõrgete nõuete korral turvalisuse ja usaldusväärsuse suhtes osutuda testimiskeskkonnana tõepoolest vajalikuks teine, identselt konfigureeritud süsteem.

Erinevate tüüpiliste ja sagedamini korduvate testimisjuhtude jaoks tuleks luua kontrollnimekirjad, mida on testimisel võimalik täita ning mis võivad lisaks puhtale testimise dokumenteerimisele kaasa aidata ka efektiivsuse tõstmisele ja vigade vältimisele.

Täiendavad kontrollküsimused:

- Kas konfiguratsioonimuutusi ja täiendeid ning paiku testitakse eelnevalt?
- Kuidas toimub testimiste dokumenteerimine?

M 4.241 Klientide turvaline käitus

Algatuse eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutab: administraator

Klientide turvaline käitus sõltub tervest reast faktoritest. Eriti tähtis on ka klientide korral, et administreerimine toimuks erilise hoolikuse ja turvalise juurdepääsu tingimustes. Järgnevalt kirjeldatakse mõningaid üldisi punkte, millele tuleks turvalise käituse tagamiseks tähelepanu pöörata. Asjaomaste moodulite vastavates meetmetes antakse üksikutele operatsioonisüsteemidele nõuandeid olenevalt nende spetsiifikast.

Administreerimispääsud

Klientide administreerimiseks on olemas erinevaid juurdepääsuvõimalusi. Sõltuvalt kasutatud juurdepääsu laadist, tuleb rakendada terve rida turvameetmeid. Suuremate võrkude korral on soovitatav, ja tihti ka vältimatu, et kliendid ühendatakse tsentraalsesse võrguhaldussüsteemi, kuna vastasel juhul ei ole turvaline ja efektiivne administreerimine võimalik. Administreerimiseks kasutatavad meetodid tuleks turvasuunistes kindlaks määrata ning administreerimine peaks toimuma vaid vastavalt turvasuunistele. Soovitatav on koostada ülevaade erinevate administreerimistegevuste jaoks, milliseid töid millisel viisil on võimalik teostada. Kindlasti tuleb fikseerida, juhul kui teatud tegevusi ei tohi tavapärasel viisil teha:

- Lokaalne administreerimine - Klientide administreerimine otse juurdepääsu kaudu üle konsooli on teostatav vaid vähestel arvutitel ning on suurema arvu klientidega keskkonnas enamasti erandiks. Kui administraator peab erandkorras siiski töötama kliendiarvutil, on näiteks tähtis, et administraator pöörab parooli sisestamisel tähelepanu sellele, et seda ei ole võimalik välja luurata. Teatud juhtudel tuleks mõelda, kas mitte kasutada selliste tööde teostamiseks ühekordseid paroole või midagi taolist.
- Administreerimine buutimismeediumi abil - Paljude administreerimistööde jaoks, mida on vaja teostada lokaalselt kliendiarvutil, võib olla kasulik kasutada välist buutimismeediumi, millelt toimub arvuti käivitamine (vt M 6.24 Rikkejärgse buutimismeedia olemasolu). See pakub administraatorile kindlust, et süsteemikeskkond on puhas. Sellel meetodil on aga ka terve rida puudusi, näiteks kaasnevad sellega suuremad kulutused. Lisaks ei ole sel viisil alati võimalik tuvastada kõiki kasutamisel ette tulevaid veateateid.
- Kaugadministreerimine - Ka klientide administreerimine toimub tihti administreerimisarvutilt võrgu kaudu. Takistamaks administraatorite autentimisteave väljaluuramist või ründajate poolt manipuleerimist, peab administreerimine toimuma vaid turvaliste protokollide kaudu (näiteks mitte Telneti vaid SSF-i, mitte HTTP vaid HTTPS-i kaudu).

Turvamata kaugadministreerimist (ebaturvaliste) välisvõrkude kaudu ei tohi mitte mingil juhul toimuda. Sellega tuleb arvestada juba turvasuuniste kindlaksmääramisel. Ka sisevõrgus ei tohi, niivõrd kui see on võimalik, kasutada ebaturvalisi protokolle.

Administreerimine tsentraalse haldussüsteemi kaudu

Juhul kui administreerimiseks kasutatakse tsentraalset haldussüsteemi, tuleks sellele juurdepääsuks kehtestada analoogsed nõuded, nagu kaugadministreerimisel. Lisaks sellele on tähtis, et tsentraalse haldussüsteemi enda konfigureerimine ja administreerimine toimuks turvaliselt (vt B 4.2 Võrgu- ja süsteemihaldus).

Rutiintegevused administreerimisel

Soovitatav on koostada nõuanded administraatorite tavapäraste rutiinsete tegevuste korraldamiseks administreerimise käigus vastavalt turvasuunistele. See hõlmab järgmisi tegevusi:

- kasutajate sisseseadmine ja kustutamine;
- programmide installimine ja deinstalleerimine;
- turvatäiendite ja paikade paigaldamine (vt M 2.273 Turvalisust mõjutavate paikade ja värskenduste kiire paigaldamine);
- teiste täiendite ja paikade paigaldamine või
- regulaarne tervikluse kontroll vastavate tööriistadega (vt M 4.93 Regulaarne tervikluse kontroll ja M 5.8 Võrgu regulaarne turvakontroll).

Konfiguratsioonimuutuste testimine

Klientide konfiguratsioonimuutusi tuleks enne üksikutele arvutitele jaotamist võimaluse korral testida etalonsüsteemil (vt M 4.242 Kliendi etaloninstalleeringu loomine). Kui üksikutel klientidel tehakse muutusi (näiteks vea otsimise käigus), tuleks igal juhul kontrollida, kas muutuste sisseviimine ei kahjusta kliendi teisi funktsioone.

Süsteemides teostatavate tööde dokumentatsioon

Klientide süsteemikonfiguratsiooni või rakenduste konfiguratsiooni muutused tuleb dokumenteerida. Dokumentatsioon peab olema ka klientide korral selliselt koostatud, et probleemide tekkimisel on tuvastatav, mis oli viimane muudatus ning millal ja kelle poolt see tehti.

Kõrgete turvanõueteta klientide korral võib piisata ka üksikute funktsioneerivate konfiguratsiooni seisude dokumenteerimisest (näiteks kindlatel aegadel), ilma et oleks tingimata vajalik igat üksikut sammu tuvastada. Vaatamata sellele on soovitatav kujundada dokumentatsioon selliselt, et kõik muutused oleks tuvastatavad.

Täiendavad kontrollküsimused:

- Mil viisil toimub juurdepääs süsteemi administreerimiseks?

- Kuidas testitakse konfiguratsioonimuutusi?
- Kuidas dokumenteeritakse muutusi?

M 4.242z Kliendi etaloninstalleeringu loomine

Algatuse eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutab: administraator

Soovitatav on luua klientidele etaloninstallatsioon, kus on võimalik testida aluskonfiguratsiooni ja kõiki konfiguratsioonimuutusi, täiendeid ja paikasid enne kasutajate klientidele paigaldamist. See puudutab süsteemi alussätteid, turvapaikasid ja -täiendeid, ning ka tavapäraseid täiendeid, mida antakse välja tootja poolt. Lisaks sellele võib sellist etaloninstallatsiooni kasutada ka uute klientide installeerimise lihtsustamiseks, mille käigus kantakse vastavalt eelkonfigureeritud installatsioon sobival viisil installeeritavale arvutile üle („kloonimine"). Ideaaljuhul on järgnevalt vaja vaid väheseid sätteid kohandada. Etaloninstallatsiooni, mida kasutatakse klientide kloonimiseks, tuleb konfigureerida ja testida erilise hoolega.

Etaloninstallatsioon peab olema selliselt loodud, et olulise tähtsusega riist- ja tarkvaraplatvormi parameetrid oleks ühesugused kõigile süsteemidele, mis tuletatakse sellest etaloninstallatsioonist. See ei tähenda just kindlasti, et kõikidel klientidel olema identne riist- ja tarkvara konfiguratsioon. Erinevate klientide konfiguratsioon peab olema aga piisavalt sarnane, selleks et säilitada installatsiooni vastavus etalonile. Rakendusprogrammide ja sätete testimisel, mida kasutajad klientidel eest leiavad, on lisaks väga tähtis, et administraatorid ei teeks seda administraatoriõigusi kasutades, vaid kasutaja tunnusega, kellel on needsamad volitused ja kelle jaoks valiti needsamad sätted kasutajakeskkonna jaoks, nagu süsteemiga töötavate kasutajate jaoks. Seepärast võib teatud juhtudel olla kasulik kasutada erinevat liiki testide tegemiseks erinevaid testimissüsteeme, näiteks üht süsteemi süsteemilähedaste programmide või operatsioonisüsteemi paikade testimiseks ja teist testide korraldamiseks, mis on seotud rakendusprogrammidega. Sellisel juhul on siiski vajalik teadvustada, et sel viisil ei ole võimalik katta teatud liiki operatsioonisüsteemi keskkonna ja rakendusprogrammide vahelisi vastastikuseid mõjusid. Klientidele esitatavate kõrgete turvanõuete korral võib seetõttu olla vajalik kasutada teatud kindlate kasutusmudelite korral tõepoolest vaid identselt varustatud ja konfigureeritud süsteeme. Erinevate tüüpiliste ja sagedamini korduvate testimisjuhtude jaoks tuleks luua kontrollnimekirjad, mida on testimisel võimalik täita ning mis võivad lisaks puhtale testimise dokumenteerimisele kaasa aidata ka efektiivsuse tõstmisele ja vigade vältimisele.

Kõik testimised tuleks dokumenteerida nii, et neist oleks hiljem võimalik aru saada. See on eriti vajalik turvapaikade ja uute seadme ajamite testimisel, mille korral võib vigane konfiguratsioon või installatsiooni äpardumine endaga kaasa tuua olukorra, kus kõnesolevad kliendid ei saa enam võrgule juurdepääsu või enam üldse ei käivitu. Just sellistel juhtudel võib väljendusrikas dokumentatsioon oluliselt lühendada vigade otsimiseks ja kõrvaldamiseks vajaminevat aega.

Täiendavad kontrollküsimused:

- Kas konfiguratsioonimuutusi ja täiendeid ning paiku testitakse eelnevalt?
- Kuidas toimub testimiste dokumenteerimine?

M 4.243z Windowsi klientoperatsioonisüsteemide haldustööriistad

Algatamise eest vastutavad: administraator

Rakendamise eest vastutavad: administraator

Käsuviibal põhinev tööriist secedit on kõigile tuttav juba alates versioonist Windows 2000. See tarkvaratööriist võimaldab automatiseerida turvaseadistuste konfigureerimisülesannete täitmist. Muuhulgas on selle abil võimalik automaatselt koostada, rakendada ja analüüsida malle. Üheks kõige tähelepanuväärsemaks omaduseks on võimalus võrrelda kehtivate grupipoliitikate seadistusi vastava näitekomplektiga. Kui soovite secedit tööriista Windows Vista ja Windows 7 keskkonnas käsuviibalt käivitada, peab käsuviip olema avatud konkreetsete administraatoriõigustega („*Run as Administrator*“). Hetkel kehtivaid seadistusi saab analüüsida lisaks ka veel *MMC Snap-in* -iga *Security configuration and analysis*. Vastupidiselt secedit -ile võimaldab nimetud lahendus analüüsitulemusi koostada ja kuvada ka graafiliselt. Tuleks arvestada, et ei tarkvaratööriist secedit ega ka MMC Snap-in Security configuration and analysis ei võimalda administratiivsete mallide jaoks defineeritud parameetreid konfigureerida ega analüüsida.

Turvamallide töötlemiseks tuleb Windows Vista ja Windows 7 keskkonnas kasutada *MMC Snap-in -i Security templates*. Kuna turvamallid kujutavad endast tavalisi tekstifaile, saab neid töödelda ka üldlevinud tekstiredaktoritega. Viimane võib alla muuhulgas vajalik täiendavate registrivõtmete täpsemal määratlemisel. Grupipoliitika seadistusse sisse viidud muudatused hakkavad toimima alati viivitusega, mille pikkuse määrab kindlaks grupipoliitikate töötlemisele kehtiv seadistus. Olukorras, kus muudatusi on tarvis kas mõne kasutaja või arvuti jaoks viivitamatult tööle rakendada, saab kasutada käsuviiba tööriista *gpupdate*. Nimetatud tarkvaratööriist asendab alates versioonist Windows 2000 tuttavat käsku *secedit /refreshpolicy*.

Windows Vista puhul saab käsuviiba tööriista *gpresult* rakendada Windowsi kliendi all ka selleks, et koostada kõikide seadistatud grupipoliitikate loetelu. Muuhulgas on see veel kasulik ka selleks, et selgitada välja, millised sündmused leiavad aset teatud kindla kasutaja sisselogimisel teatud kindlasse arvutisse (*gpresult /s:computername /u:username*). Antud tööriista saab ennekõike kasutada vigade otsimiseks ning kehtivate seadistuste dokumenteerimiseks Sarnaseid funktsioone nagu gpresult pakub ka MMC *Snap-in Policy* resultant set (*rsop.msc*). Lisaks hetkel kehtivate seadistuste dokumenteerimisele (logimisrežiim) saab seda tööriista kasutada veel ka kõikvõimalike teistsuguste stsenaariumite läbimängimiseks (planeerimisrežiim). Sellega on võimalik simuleerida poliitikate juurutamist, mis on nende väljatöötamise faasis ülimalt oluline, kuna aitab ära hoida paljusid juurutamisel tehtavaid vigu ja eriti neil juhtudel, kus grupipoliitikate struktuurid ja hierarhiad on väga keerulise ülesehitusega.

Group Policy Management Console (*GPMC*) kuulub *Windows Vista* standardinstallatsiooni hulka. Selle tarkvaratööriistaga kaasnevad laialdased funktsioonid, mis on *Active Directory* grupipoliitikate haldamiseks väga olulised. GPO'de loomine, linkimine ja kustutamine, varundatud grupipoliitikaobjektide seadistuste importimine, GPO-aruannete koostamine (saab muuhulgas kasutada ka dokumenteerimise eesmärgil) ning GPO'de varukoopiate loomine ning taastamine. Peale kõige muu

võimaldab GPMC kasutada ka *scripting* -liidest, mille rakendamine osutub mõttekaks eelkõige juhul, kui administreerimistööde hulk on suur. Seetõttu on GPMC kasutamine *Active Directory* keskkonnas tungivalt soovitav. Alates Windows 7-st asendati *GPMC* tööriistaga *RSAT* (*Remote Server Administration Tool*). Olukorras, kus Windows Vista kliente käitatakse domeeni all ning domeenikontrollerid ei tööta veel Windows Server 2008 all, toetab grupipoliitikate konfigureerimist tarkvaratööriist *GPOAccelerator-Tool*. Sellisel juhul tuleb grupipoliitikate konfigureerimine ette võtta mõnes Windows Vista klientsüsteemis. *GPOAccelerator-Tool* -i abil on domeeniadministraatoril võimalik klientsüsteemis luua grupipoliitikate jaoks vajalikud konfiguratsioonid. Seejärel tuleb need ümber paigutada domeenikontrolleri sysvol -kausta. Varasem *GPO Accelerator Tool* on alates Windows 7-st asendatud tööriistaga M*icrosoft Security Compliance Manager Suite.*

Üheks täiendavaks tööriistaks on migratsioonitabelite redaktor *mtedit*, mis kuulub GPMC paketti. Selle tööriistaga on mugav koostada migratsioonitabeleid, mida saab kasutada turvapoliitika domeeniülese kopeerimise või importimise puhul. Migratsioonitabeleid kasutades on võimalik muuta domeenide spetsiifilist infot (nt grupinimesid võid SID'sid). Seirepoliitikate konfigureerimiseks saab Windows Vista ja Windows 7 keskkonnas kasutada tööriista *Auditpol*. Tarkvaratööriistaga *Microsoft Baseline Security Analyzer* (*MBSA*) annab Microsoft meie käsutusse vahendi, mis analüüsib automaatselt installeeritud paikasid (*patches*). Selle tööriista kasutamine aitab administraatoritel luua värskeid ülevaateid süsteemidesse paigaldatud turvapaikadest ning seetõttu aitab see olulisel määral tõsta üldist turvalisust (vt M 4.249 Windowsi klientsüsteemide ajakohastamine).

Microsofti probleemisammude salvesti (*Problem Steps Recorder – PSR*) aitab kasutajatel nende töös tekkinud probleeme administraatorite jaoks mõistlikul ja arusaadaval moel dokumenteerida. Seda tarkvaratööriista pakutakse alates versioonist Windows 7 ning kui see on sisse lülitatud, dokumenteerib see kõik kasutaja sisestused. Lisaks salvestab see tarkvaratööriist asjassepuutuva IT-süsteemi ekraanipilte (*screenshot*) ning märgistab ja kirjeldab kasutaja sisestusi.

Probleemi täpsemaks kirjeldamiseks saab kasutaja salvestatud ekraanipiltidele lisada ka enda kommentaare. PSR koostab ZIP-faili, mis sisaldab probleemi kirjeldavat MHT-faili. Üldjuhul tuleks kehtestada töötajatele kohustus, et nad valiksid genereeritud ZIP/MHT-faili edasisaatmiseks faili sisuga arvestava turvalise sidekanali.

Administraatorid peaksid kõiki neid tarkvaratööriistu ilmtingimata kasutama vigade otsimise ja loome- ning testimisfaaside käigus. Nende tööriistade kasutamine aitab tuvastada ja ennetada konfiguratsioonide kitsaskohti.

Täiendav kontrollküsimus:

- Kas tarkvaratööriistu rakendatakse planeerimisel ja käitamisel nõuetekohaselt?

M 4.244 Windowsi klientoperatsioonisüsteemide turvaline süsteemikonfiguratsioon

Algatamise eest vastutavad: IT-juht, IT-turbespetsialist
Rakendamise eest vastutavad: administraator

Töökohal kasutatava arvuti turvalisus sõltub suurel määral sellest, kas kasutajal on võimalik mõjutada administraatoriülesannetes seda, millistele funktsioonidele on kasutajale antud ligipääs ning sellest, kas kasutajad rakendavad nende käsutusse antud turvamehhanisme või mitte. Windows Vista ja Windows 7 konfigureerimisel tuleb turvalisuse vaatevinklist lähtudes arvestada järgnevate aspektidega:

- Välja peavad olema töötatud vastavad seiresuunised (vt M 4.344 Windows Vista, Windows 7 ja Windows Server 2008 süsteemi seire). Kogutud logifaile tuleb lisaks kogumisele ka regulaarselt analüüsida.
- Active Directory keskkonnas tuleks piirata volitusi, mis lubavad tööjaamu domeeni alla juurde lisada. Sellised õigused tohivad olla vaid volitatud, administraatoriõigustega kasutajatel. Volituste piiramiseks tuleb domeenikontrollerites rakendada poliitikat Assigning user rights | Adding workstations to the domain.
- Windows Vista ja Windows 7 käitamisel kaasaskantavates arvutites tekivad täiendavad turvariskid, mille võimalikke tagajärgi tuleb pehmendada spetsiaalsete ennetavate meetmetega (vt M 2.442 Windows Vista ja Windows 7 kasutamine kaasaskantavates arvutites ja moodulit B 3.203 Sülearvuti). Windows Vista ja Windows 7 puhul saab konfidentsiaalsete andmete kaitseks kasutada kõvaketta krüpteerimislahendust BitLocker Drive Encryption (BDE) (vt M 4.337 BitLockeri Drive Encryption kasutamine).

Andmete talletamine ja töötlemine

Võrku ühendatud klientide puhul on soovitav loobuda andmete lokaalsest talletamisest. See muudab tsentraalse haldamise, turbealaste ettekirjutuste juhtimise ning andmetest varukoopiate tegemise hõlpsamaks. Lisaks kaasneb sellega ka turbealane eelis, kuna lokaalse süsteemi kompromiteerimise tagajärjel ei teki automaatset juurdepääsu tundlikele andmetele, kuna viimaseid hoitakse serveril, mis on reeglina klientarvutitega võrreldes paremini kaitstud. Mõningatel juhtudel võib andmete salvestamine lokaalselt olla turvanõuete täitmiseks siiski mõõdapääsmatu, näiteks olukodades, kus vastavale infole tohib juurde pääseda ainult üks konkreetne töökohaarvuti kasutaja ja/või kus soovitakse vältida andmete edastamist läbi võrgu. Sellistel juhtudel ei tule töökohta vaadelda aga mitte kui standardset töökohta, vaid kui töökohta, mille jaoks tuleb välja töötada ja rakendada eritingimusi. Näited asjakohaste meetmete kohta oleksid klientide tugev, nii lokaalne kui ka võrgupõhine kaitse, kõvaketaste krüpteerimine ning klientide kaasamine tsentraalselt toimivasse varunduskontseptsiooni.

Konfidentsiaalsete andmete töötlemine peab toimuma turvaliselt. Volituste kontseptsiooni aluseks võttes tuleb piirata mitte ainult otsest ligipääsu andmetele, vaid hoolitseda ka selle eest, et välistada volitusteta juurdepääsu ajutist liiki andmetele. Paljud tarkvararakendusel loovad andmetöötluse käigus ajutisi faile, mis jäetakse vastupidiselt originaalfailidele võib-olla piisava kaitseta. Seetõttu on tungivalt soovitav ajutisi faile sisaldavaid katalooge (nt Temp, Tmp ja printeri

Spool -kataloogi) andmetest puhastada. Puhastamiseks on muuhulgas võimalik kasutada skripte, mis käivitatakse süsteemi väljalülitamisel (vt M 2.326 Windows Vista ja Windows 7 grupeerimissuuniste planeerimine). Süsteemi väljalülitamisel aset leidvat saalimisfaili kustutamist saab sisse lülitada grupipoliitika objektide all poliitikaga Delete page file for virtual memory on shutting down the system ning Windows Vista või Windows 7 puhul seadistusega Shutdown: Clear virtual memory pagefile, mille asukohaks on Computer settings | Windows settings | Security settings | Local policies | Security options.

Tarkvarapiirangud

Süsteemi sihipärase konfigureerimise eesmärgiks on luua olukord, kus tavakasutaja ei saaks ette võtta administreerimistegevusi. Selle kehtestamiseks saab reguleerida juurdepääsuõiguseid failidele ja registrile ning piirata konfigureerimistööriistade nagu Microsoft Management Console'i käivitamisõigust. Vastavaid seadistusi hallatakse grupipoliitikatena ning nendega tuleks arvestada juba grupipoliitikate planeerimisfaasis. Üheks täiendavaks, turvalisust tõstvaks meetmeks võib olla tarkvarapiiranguid kehtestavate poliitikate (ing. k. Software Restriction Policies, SRP) rakendamine ja Windows 7 AppLoecker saab anda täiendavat kindlust selles osas. Tarkavara installeerimisega tohivad tegeleda vaid selleks volitatud administraatorid. Tavakasutajate installeerimisvõimalustele tuleb kehtestada võimalikult suured piirangud (vt M 2.9 Aktsepteerimata riist- ja tarkvara kasutuse keeld). Installeerimistöid, mille puhul kasutatakse Windows-Installer'it, saab piirata vastavate grupipoliitikate defineerimisega asukohas Computer Configuration | Administrative Templates | Windows-Components | Windows Installer. Kas ja millises mahus tuleks installeerimisvolitusi piirata, sõltub konkreetse ettevõtte või ametiasutuse tarkvara installeerimise juhistest. Arvestage, et need seadistused käsitlevad ainult Windows-Installer 'it ning ei suuda välistada installeerimisi või värskendusi, mille puhul kasutajad rakendavad hoopis muid lahendusi.

Tarkvarapiiranguid kehtestavate poliitikate defineerimisega arvuti GPO valdkonnas (Computer Configuration | Windows Settings | Security Settings | Software Restriction Policies) määratakse kindlaks kas lubatud programmide koguarv (positiivne loetelu) või keelatud programmide koguarv (negatiivne loetelu). Positiivset loetelu defineerides tuleks lubada mitte ainult rakendusi, vaid ka kõiki tavatööks vajalikke süsteemiprogramme. Windows Vista keskkonnas on üheks täiendavaks võimaluseks, mille abil rakenduste kasutamist piirata, funktsioon Parental controls (vt M 2.32 Piiratud kasutajakeskkonna loomine). Parental Controls ei ole aga loodud professionaalseks kasutamiseks. Parental Controls 'i piiravad funktsioonid tuleks professionaalses töökeskkonnas asendada asjakohaste alternatiivsete meetmetega.

Programme saab reeglina identifitseerida täielikult või osaliselt kvalifitseeritud andmete nime, räsiväärtuse, digitaalse allkirja ehk sertifikaadi või programmi tsooni alusel (nt internet, lokaalne arvuti). Reegleid saab lisaks tavapärastele käitusfailidele kehtestada veel ka DLL'idele, ActiveX-juhtelementidele, Windows-Installer 'i failidele ning VBScript -failidele. SRP abil käivitamisele kehtestatavate piirangute konfigureerimise võimalused on väga laialdased ning need suudavad vastata pal-

jude kasutusvaldkondade nõuetele. Pakutavate eelistega kaasneb siiski ka märkimisväärne administratiivne töökoormus, sest kindlaksmääratud reeglid võivad kiiresti muutuda väga keeruliseks ja ebaülevaatlikuks. Kui ettevõte või ametiasutus soovib kehtestada tarkvara installimist piiravaid poliitikaid, on laialdane planeerimine ja mahukas katsetamine eeltööna möödapääsmatud. Windows Vista ja Windows 7 keskkonnas saab rakenduste kasutamist piirata ka funktsiooniga Parental Controls (vt M 2.32 Piiratud kasutajakeskkonna loomine). Parental Controls ei ole aga loodud professionaalseks kasutamiseks ning domeenikeskkonnas seda rakendada ei saa. Kui institutsioonis pääsevad klientsüsteemidele juurde ka alaealised kasutajad, tuleks Parental Controlsi funktsiooniga võimaldatavad piirangud asendada alternatiivmeetmetega.

Windows 8 äppide turvaline konfigureerimine

Windows 8 äpid erinevad lisaks funktsioonidele esitatavatele nõuetele ja nende saamisele võrreldes töölaua rakendustega ka turvakonfiguratsiooni poolest. Seetõttu tuleks otsustada, kas ja milliseid Windowsi äppe asutuses kasutada lubatakse. Täiendavat materjali leiate selle kohta abivahendis mooduli Windows 8 kohta peatükis „Äppide kasutamine Windows 8 keskkonnas".

Windows 8 äppide turvaline konfiguratsioon ei toimi tavaliselt nagu töölauarakenduste korral tsentraalselt rühmasuuniste kaudu. Vajalikud on täiendavad meetmed, nt tööriista AppLocker abil, mis omakorda toetub rühmasuunistele. AppLocker'i kaudu saab konfigureerida ja juurutada järgmist: Teostatavad reeglid, Windows Installeri reeglid, Skripti reeglid ja Äppide paketi reeglid. Nende reeglite eesmärk on hoida täielikku kontrolli selle üle, milliseid Windowsi äppe kasutajad käitada saavad.

AppLocker'i konfigureerimine toimub menüüs Arvuti konfiguratsioon | Windowsi seadistused | Turvaseadistused | Rakenduste juhtimise suunised | Applocker. Täiendavat teavet leiate selle kohta meetmest M 4.419z Rakenduste juhtimine AppLockeriga alates Windows 7-st .

Teenused

Windows Vista ja Windows 7 ei ole serverioperatsioonisüsteemid ja seetõttu tuleks neid kasutada ainult klientsüsteemide käitamiseks. Windows Vista ja Windows 7 klientsüsteemid ei tohiks ise võrgukeskkonnas võimaldada ei rakenduste ega ka teenuste kasutamist. Lisaks standardsetele, administreerimisega seotud ühiskasutusõigustele ei tohiks tavapärastele töökohaarvutitele võimaldada ka mitte ühtki kataloogide ühiskasutusõigust. Kui administreerimisega seotud ühiskasutusõiguseid ei kasutata, tuleks ka need desaktiveerida näiteks sellisel moel (HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareWks =0). Juhul, kui teatud põhjustel on ühiskasutusõigused klientsüsteemides siiski vajalikud, tuleks vältida tavapärase failide ühiskasutuse lubamist, et hoiduda sellega kaasnevatest turvariskidest. Kui failide lihtne ühiskasutus on arvutis sisse lülitatud, liigitatakse kõik kasutajad, kes võrgu kaudu sellesse arvutisse oma pöördusi teevad, külalise kasutajakonto alla. Ühiskasutuse rakendamist lubavad volitused tuleb välja jagada võimalikult suurte piirangutega. Arvestage, et lihtne ühiskasutus lülitatakse standardina sisse ainult üksikarvutites, mis ei kuulu ühegi domeeni alla (arvutites, mis on installeeritud domeeni liikmena, on failide lihtne

ühiskasutus standardseadistuses desaktiveeritud). Süsteemi üldine turvalisus sõltub ka kasutatavatest süsteemiteenustest (vt M 4.246 Süsteemiteenuste konfigureerimine Windows Vista ja Windows 7 keskkondades). Alates Windows 7-st saab IT-süsteemi kasutada ka eraldi prindiserveri funktsioonides. Sellisel juhul ei tohi seda IT-süsteemi kasutada mitte ühelgi teisel otstarbel. IT-süsteemi riistvaranäitajad ja juurdepääsu turvalisus peavad vastama asjakohastele serverinõuetele (vt moodul B 3.101 Server). Kõik rakendusfunktsioonid tuleb desaktiveerida.

Kasutajakontod

Windows Vista ja Windows 7 all loodud kasutajakontosid tohivad kasutada ainult selleks volitatud isikud, st iga kasutajakonto tuleb siduda ühe konkreetse kasutajaga. Ennekõike on seda tarvis jälgitavuse tagamiseks. Ühiselt kasutatavaid kontosid tuleks võimalusel vältida. See tuleb tagada organisatoorsete meetmetega. Kui uue kasutajakonto loomine leiab aset Active Directory keskkonnas, tuleb jälgida, et konto saaks õigesti liigitatud vastava organisatsiooni allüksuse alla, kuna sellega seoses määratakse kasutajakontole ka korrektsed turvaseadistused. Kasutajale antavad volitused tulenevad lisaks grupikuuluvusele ka grupipoliitikatest, mis on seotud organisatsiooni vastava allüksusega, mille alla kasutaja on liigitatud. Juhul, kui Windows Vista või Windows 7 süsteemi haldamine leiab aset personaalsete kasutajakontode alt, võib integreeritud kasutajakonto kasutamise tõkestada. Windows Vista standardse installatsiooni puhul see reeglina nii ongi. Kõikidel juhtudel tuleks administraatorikonto ümber nimetada. Integreeritud administraatorikonto desaktiveerimine ja/või ümbernimetamine võib toimuda kas läbi kasutajate haldamise või poliitikate abil: Accounts: Administrator account status ning Accounts: Rename administrator, mille asukohaks on Computer settings | Windows settings | Security settings | Local policies | Security options. Enne administraatorikonto desaktiveerimist on soovitav läbi teha testimisfaas, mille raames toimuvad administreerimistööd eranditult personaalsete kasutajakontode alt.

Kõikidel Windowsi versioonidel on standardina olemas külaliskonto. Seda külaliskontot ei tohiks kasutada. Külalistele tuleks alati kasutada anda eraldiseisev konto. Külaliskonto tuleb desaktiveerida, kuid sellele vaatamata tuleks ka külaliskonto jaoks väljastada keeruline parool. Windows Vista või Windows 7 standardse installatsiooni puhul on külaliskonto juba desaktiveeritud, kuid parool on väljastamata. Parooli väljastamine tagab toimiva paroolkaitse ka juhul, kui keegi peaks külaliskonto kas juhuslikult või volitamata sisse lülitama. Külaliskonto ümbernimetamiseks ja desaktiveerimiseks saab kasutada kas lokaalset kasutajahaldust või poliitikaid Accounts: Guest account status ning Accounts: Rename guest account, mille asukohaks on Computer settings | Windows settings | Security settings | Local policies | Security options. Windows Vista versioonis Support User kasutajakontot ei eksisteeri. Windowsi süsteemi käitamisel domeeni keskkonnas tuleks võimalusel loobuda täiendavate lokaalsete kasutajakontode loomisest. Üldjuhul tuleks lokaaltasandi jaoks luua ainult hädavajalik arv kontosid. Lokaalseid kontosid tuleb regulaarsete ajavahemike möödudes ka kontrollida.

Vastavalt meetmele M 4.2 Ekraanilukk tuleb iga kasutaja jaoks sisse lülitada ekraaniluku paroolikaitse. Juhul, kui on võimalik kasutada ooterežiimi (Standby), peab süsteem nõudma parooli sisestamist ka siis, kui see ooterežiimilt tagasi töösse lülitatakse (System settings | Energy options | Advanced | Prompt for password after stand-by mode). Rakendada tuleb meetmeid M 2.11 Paroolide kasutamise reeglid ja M 4.15 Turvaline sisselogimine . Need on toeks ennekõike paroolide pikkuse, kvaliteedi ja muutmisintervallide küsimustes ning aitavad määratleda

kasutajakonto sulgemisreegleid ja lubatud vigaste logimiskatsete arvu.

Sisselogimise turvamine

Süsteemile tohivad ligi pääseda ainult volitatud isikud. Kasutajaõiguseid tuleb välja jagada vastavate piirangutega (vt M 4.247 Windowsi klientoperatsioonisüsteemide piiratud kasutajaõigused). Administraatorite juurdepääsusid, mis toimivad läbi võrgu, tohib anda ainult volitatud administreerimispersonalile. Lisaks tuleb ära keelata ilma paroolita lokaalsetesse kasutajakontodesse sisselogimine läbi võrgu. Selleks tuleb rakendada poliitikat Accounts: Limit local account use of blank passwords to console logon only (asukohas Computer settings | Windows settings | Security settings | Local policies | Security options). Kasutajate automaatne sisselogimine tuleb kõikides Windowsi installatsioonides välja lülitada. Automaatse sisselogimise võimalus tuleb muuhulgas välistada ka taastamiskonsooli kasutamise puhul. Administratiivseid ülesandeid täitvad kasutajad peavad endid selgelt autentima. Taastamiskonsooli kasutamisel tuleks piirata juurdepääsu väljapool süsteemikausta asuvatele andmetele. Vastasel korral võivad aset leida volitamata juurdepääsud andmetele ja pealegi veel sellised, mida ei saa logida. Selle saavutamiseks tuleb desaktiveerida järgmised taastamiskonsooli poliitikaid nagu Recovery console: Allow automatic administrative logon ja Recovery console: Allow floppy copy and access to all drives and all folders (asukohas Computer settings | Windows settings | Security settings | Local policies | Security options).

Windows Vista ja Windows 7 standardinstallatsiooni puhul on Built-In administraatorikonto juba desaktiveeritud. Kuna standardinstallatsioonis ei ole sellele kontole parooli väljastatud, tuleks Built-In administraatorikontole tagantjärele väljastada ka parool. Enne seda, kui kasutajatele võimaldatakse juurdepääs süsteemile, peavad nad endid selgelt autentima. Sisselogimisel on kohustuslik kasutada klahvikombinatsiooni Ctrl+ALT+Del (desaktiveerige poliitika Computer settings | Windows settings | Security settings | Local policies | Security options | Interactive Logon: Do not require CTRL+ALT+DEL). See tagab, et sisselogimisel kasutataks õiget sisselogimisakent, mitte mõnd „järeletehtud“ varianti. Lisaks tuleks vältida viimati sisse loginud kasutaja nime kuvamist sisselogimise aknas (poliitika Computer settings | Windows settings | Security settings | Local policies | Security options | Interactive logon: Do not display last user name). Lisaks on soovitav, et süsteem kuvaks kõikidele kasutajatele, kes püüavad end lokaalselt sisse logida, hoiatava sisuga teadet. Hoiatava teate sisu tuleks välja töötada vastavalt konkreetsetele oludele iga kasutusotstarbe jaoks eraldi. Hoiatav teade ja selle tekstiosa rakendatakse tööle poliitikatega Interactive logon: Message text for users attempting to log on ja Interactive logon: Message title for users attempting to log on asukohas Computer settings | Windows settings | Security settings | Local policies | Security options.

Domeenikontode sisselogimisinfo salvestatakse reeglina vahemällu, et kasutajal oleks võimalik end oma klientsüsteemi sisse logida ka siis, kui domeenikontroller ei ole parasjagu käideldav. Vahemällu talletatava, kontosid kajastava info hulga määrab kindlaks poliitika asukohas Computer settings | Windows settings | Security settings | Local policies | Security options | Interactive Logon: Number of previous logons to cache ning vastava info hulk tuleks hoida võimalikult väiksena. Vastavaid parameetreid tuleb seadistada iga juhtumi puhul eraldi vastavalt konkreetsetele oludele.

Süsteemi seadistused

Windowsi standardses installatsioonis on sisse lülitaud Autostart -funktsioonid, mis kujutavad endast turvariski, kuna ohtlikku sisu võidakse seeläbi käivitada ilma, et kasutajal oleks võimalik sellesse sekkuda. Sel põhjusel tuleb kõikide ajamite Autostart -funktsioonid desaktiveerida (vt lisaks meedet M 4.339 Vahetavate andmekandjate volitamata kasutamise tõkestamine Windows Vistas ja Windows 7-s). Selleks tuleb tööle lülitada poliitika asukohas Computer Configuration | Administrative templates | System | Deactivate Autoplay ning määratleda seadistuse All drives väärtus. Microsofti Windows Vista puhul leiate need seadistused asukohast Computer Configuration | Administrative templates | Windows Components | Autoplay Policies | Turn off Autoplay. Sisemised süsteemiobjektid nagu nt mutex 'id ja s emafor 'id, mis hoolitsevad erinevate harude (thread) ja protsesside sünkroniseerimise eest, on varustatud eraldi pääsuõigustega. Vastavaid pääsuõiguseid saab spetsiaalsete poliitikate defineerimisega tugevdada nõnda, et kasutajad, kes pole administreerimisega seotud, ei saaks endale volitusi nende objektide muutmiseks, mida nad ei ole ise loonud: Computer settings | Windows settings | Security settings | Local policies | Security options | System objects: Strengthen default permissions of internal system objects (e.g., Symbolic Links). Diskettidele ja CD-ROMidele võimaldab Windows reeglina ligi pääseda nii lokaalselt kui ka läbi kaugpöörduse. Juurdepääs tuleks korraga võimaldada ainult hetkel sisse logitud kasutajale.

Windowsi iseseisva internetikommunikatsiooni tõkestamine

Paljud Windowsi teenused ja rakendused loovad standardinstallatsiooni korral iseseisvalt, kasutaja jaoks märkamata, ühendusi internetis asuvate serveritega. Selliste tegevuste käigus edastatakse Microsoftile või teistele teenusepakkujatele süsteemi ja/või kasutajat käsitlevat infot. Järgnev loetelu annab ülevaate teenustest ja rakendustest, mis Microsoftile iseseisvalt andmeid edastavad. Järgnev loetelu ei pretendeeri täiuslikkusele:

- Internet Explorer
- Windows Media Player
- Windows Messenger
- Windows Time Service
- Help and Support Center
- Windows Update
- Device Manager
- Windows Activation ja Registration
- Update Root Certificates
- Event Viewer
- File Association Web Service
- Error Reporting

Enamike äsja loetletud teenuste ja rakenduste jaoks on soovitav andmeedastus välja lülitada. Selleks võib ümber konfigureerida registri ja programmide valikud ning võib muuta ka failisüsteemi. Pärast Service Pack 2 juurutamist on nende funktsioonide haldusvõimalused märgatavalt paranenud. Kasutusele võeti uus grupipoliitika kategooria asukohas Computer Configuration | Administrative templates | System | Internet Communication Management.

Riistvara turbefunktsioonide aktiveerimine ja kaasamine

Iga Windowsi süsteemi külge ühendatud ja aktiveeritud riistvara jaoks peab olema installitud ka draiver. Turbefunktsioonide (nt biomeetriaseadmete, smartcard 'ide ja kõvaketta krüpteerimise) jaoks tuleks kasutada üksnes kõige värskemaid ja Microsofti sertifitseeritud draivereid. Kui võimalik, tuleks riistvara kasutada koos Windowsiga integreeritud turva-API-dega, nt biomeetriaraamistiku ja smartcard'i autentimisega. Võimaluse korral tuleks kõikide programmide ja teenuste jaoks sisse lülitada andmekäivituse tõkestus (Opt-out).

Group Policy Object 'ide (GPOde) alusseadistused

Grupipoliitikaobjektidele tehtavaid baasseadistusi kirjeldab meede M 4.245 Windowsi Group Policy Objects alusseadistused .

Kontrollküsimused:

- Kas seirepoliitikas määratletud turvaseadistusi rakendatakse?
- Kas Active Directory keskkonnas piiratakse volitusi, mis lubavad tööjaamu domeeni alla juurde lisada?
- Kas kogutud logifaile analüüsitakse regulaarselt?
- Kas lokaalselt töödeldavate andmete turvalisus ja konfidentsiaalsus on tagatud?
- Kas Windowsi klientsüsteemide puhul on tõkestatud nende võimalused pakkuda võrgu kaudu rakenduste või teenuste kasutamist?
- Kas on tagatud, et Windowsi kasutajakontosid saavad kasutada ainult selleks volitatud isikud?
- Kas tavakasutajatele jagatakse pääsu- ja installeerimisõiguseid piirangutega?
- Kas külaliskonto on desaktiveeritud ja varustatud keerulise parooliga?
- Kas on järgitud reeglit, et kontosid peaks eksisteerima ainult hädavajalikul hulgal?
- Kas parooli ja ekraaniluku kasutamise reegleid rakendatakse?
- Kas automaatne sisselogimine ja taastamiskonsooli kasutaja automaatne sisselogimine on desaktiveeritud?
- Kas süsteemile on juurdepääs ainult volitatud isikutel?
- Kas lokaalselt sisse logivatele kasutajatele on koostatud vastav hoiatava sisuga teade?
- Kas Windowsi teenuste ja rakenduste iseseisev kommunikatsioon on tõkestatud?
- Kas Windows Vista keskkonnas on Built-In administraatori jaoks väljastatud parool?
- Kas kõikide ajamite Autostart -funktsioonid on desaktiveeritud?

M 4.245 Windowsi Group Policy Objects alusseadistused

Algatamise eest vastutavad: infoturbe spetsialist
Rakendamise eest vastutavad: administraator
IT-etalonturbe abivahendite hulgas on toodud tabel, kuhu on kokku koondatud turvaseadistusi käsitlevad nõuded. Vastavaid nõudeid saab kasutada lähtematerjalina grupipoliitika turvaseadistuste väljatöötamisel. Soovituslikud väärtused tulenevad muuhulgas meetmetes M 4.244 Windowsi klientoperatsioonisüsteemide turvaline süsteemikonfiguratsioon ja M 5.123 Võrgusuhtluse kaitse Windowsis loetletud nõuetest. Volituste jagamisele kehtivad ettekirjutused leiate meetmest M 4.247 Windowsi klientoperatsioonisüsteemide piiratud kasutajaõigused ja IT-etalonturbe abivahendite hulgast.
Näidetes kasutatud väärtused tuleb tingimata kohalikele tingimustele vastavalt ümber kohandada. Grupipoliitikate kontseptsiooni raames tuleb üksikud väärtused erinevate grupipoliitika objektide vahel ära jaotada ja vastavalt kasutusotstarbele sobivaks kohandada. Seeläbi on sissekannete puhul võimalikud ka erinevad väärtused. Juhtudel, kus loetletud baasseadistusi kohandatakse, eriti siis, kui neid muudetakse nõrgemaks, tuleb uurida, millist mõju avaldavad muudatused turvalisusele.

Kontrollküsimused:

- Kas baasseadistusi on kohandatud oma nõudmistele sobivaks?
- Kas võimalikke turvalisust puudutavaid baasseadistuste nõuete madaldamisega kaasnevaid mõjusid on piisavalt uuritud?
- Kas Windowsi Group Policy Objects'i põhiseadistused kohandati asutuse enda nõuetega?
- Kas võimalikke, turvalisust puudutavaid mõjusid, mis kaasnevad Windowsi Group Policy Objects'i põhiseadistuste nõuete vähendamisega, on piisavalt uuritud?

M 4.246 Süsteemiteenuste konfigureerimine Windows 7 keskkondades

Algatamise eest vastutavad: IT-juht, infoturbe spetsialist
Rakendamise eest vastutavad: administraator

Erinevate arvutis käitatavate süsteemiteenuste turvaline konfiguratsioon aitab palju kaasa süsteemi üldise turvalisuse tagamisele. Iga ebavajalik, kuid sisse lülitatud teenus võib osutuda ohuallikaks. Seetõttu tuleb Windows Vista, Windows 7 süsteemide konfigureerimisel arvestada, et tööle oleks lülitatud eranditult ainult vajaminevad teenused. Teenuste tsentraalse konfigureerimise võimaldamiseks on soovitav rakendada *Active Directory* keskkonnas vastavaid grupipoliitikaid. Selleks tuleb vastavaid teenuseid grupipoliitika arvutiosas *Computer Configuration* | *Windows Settings* | *Security Settings* | *System Services* kas sisse või välja lülitada. Windows Server 2003 domeenistruktuuris on võimalik Windows Vista ja Windows 7 teenuseid grupipoliitikate abil konfigureerida ainult tööriista *GPOAccelerator-Tool* abil. See kehtib järgnevatele valdkondadele:

- teenuste käivitumise liik „automaatne (viivitusega start)“ ja
- alates versioonist Windows Vista lisandunud teenused.

Täiendavat infot tarkvaratööriista *GPOAccelerator* kohta leiate meetmest M 4.243 Windowsi klientoperatsioonisüsteemide haldustööriistad .

IT-etalonturbe abivahendite all kajastuvad ka nõuanded süsteemiteenuste konfigureerimiseks, mida saab kasutada turvaseadistuste lähtematerjalina. Siinkohal olgu ära märgitud, et iga erineva süsteemiteenuse konfigureerimisel tuleb alati lähtuda kohapealsetest oludest ja nõuetest, mistõttu tuleb neid alati vaadelda nende spetsiifilises kontekstis. Mõningatel juhtudel võib vähemturvaliste konfiguratsioonide rakendamine olla kohapealsete olude sunnil lausa möödapääsmatu. Sellistel juhtudel tuleks tarvitusele võtta täiendavad kaitsemeetmed, mis suudaksid teenuse konfiguratsioonist tekkinud puudujäägid korvata. Sellekohasteks näideteks on täiendava tulemüüri kasutuselevõtt või ka töökorralduslikud meetmed.

Kontrollküsimused:

- Kas süsteemiteenuste rakendamist on analüüsitud lähtuvalt vajadustest?
- Kas kõik ebavajalikud teenused on välja lülitatud?
- Kas rakendatavate süsteemiteenuste ja nende jaoks vajaminevate GPOde defineerimisel arvestati erinevate klientsüsteemide versioonidega?
- Kui kliendil töötavate teenuste jaoks on vaja kontot, soovitatakse kasutada alates Windows 7-st saadaval olevat teenust Haldaja teenusekontod. Neid kontosid saab hallata Active Directory kaudu ja need võimaldavad hallata paroole üle domeeni, kusjuures AD viib korrapäraselt läbi automatiseeritud paroolimuutusi.
- Kas vajalike süsteemiteenuste jaoks kasutatakse eelistatult domeenide Haldaja teenusekontosid?

M 4.247 Windowsi klientoperatsioonisüsteemide piiratud kasutajaõigused

Algatamise eest vastutavad: infoturbe spetsialist
Rakendamise eest vastutavad: administraator, kasutaja

Windowsiga seotud volitusi saab välja jagada järgmistele valdkondadele:

- failisüsteem,
- sisselogimine,
- süsteemivolitused ja kasutajavolitused,
- volitused ühiskasutusse antud ressursside kasutamiseks,
- failide, skriptide ja installatsioonide käivitamise volitused;
- terviklusastmed.

Kõik volitused tuleb välja jagada võimalikult suurte piirangutega, toetudes nn *Need-to-know-* ehk *Least-Privilege-* strateegiale (vt lisaks M 4.149 Windows'i faili- ja ühiskasutusõigused). See kehtib eranditult kõikide valdkondade kohta, mille jaoks on võimalik väljastada volitusi. Rakendada tuleb Windowsi juurutamise eeltööna välja töötatud volituste kontseptsiooni (vt M 2.325 Windows Vista ja Windows 7 turvapoliitika kavandamine). Üldkehtiva soovituse kohaselt tuleks vältida volituste andmist üksikute kasutajate kaupa, kuna selle tagajärjel tekib liiga keeruline ja ebaülevaatlik volituste struktuur, mis võib osutuda vastuvõtlikuks väärkonfiguratsioonidele. Volituste väljajagamine peaks võimalusel toimuma eranditult gruppide baasil. Niimoodi tuleb enamik volitusi välja jagada ainult üks kord ja töö käigus vajalikud konfigureerimistööd tehakse grupikuuluvuse alusel. Allolevad soovitused kehtivad ülaltoodud valdkondade kohta.

Failisüsteem ja register

Turvagruppi „Everyone" ei tohiks kasutada. Süsteemiketta, enamasti C:-ketta puhul ei tohiks mitte ühegi eelinstallitud failikausta lisada turvagruppi „Authenticated users". See grupp tuleks eemaldada ka juurkataloogi turvaseadistustest. Turvagrupile „Everyone" antakse nii Windowsis kui ka teistes tarkvarades sageli süsteemiketta osa kaustade jaoks kirjutamisõigus, seda eriti kataloogis C:\ProgramData. Selline seadistus võimaldab teatud anonüümseid võrgujuurdepääse ja skriptioperatsioone, mida pole enamasti üldse tarvis, kuid mis kujutavad endast ohtu. Seetõttu tuleks selline kirjutamisõigus tagantjärele alamkaustadest eemaldada. Asjakohaste kaustade leidmiseks saab kasutada näiteks tarkvaratööriista AccessChk.

Kui tervikluse või konfidentsiaalsusega seotud turbenõuded on suured või väga suured, tuleks installida vaid selline tarkvara, mis ühildub terviklustasandite (Integrity Level), kataloogistruktuuri ning Windows Vista ja Windows 7 standardsete piiratud volitustega. Lisateavet selle kohta saab kas tootjatelt või Microsoftist. Lisaks on soovitatav erinevate rakenduste jaoks defineerida eraldiseisvad grupid. Gruppide otstarbe alusel tuleb seejärel registris ja failisüsteemis välja jagada ka tarkvara ja andmete pääsuõigused. Piirangute väljatöötamiseks on tarvis luua ülevaade

mitte ainult süsteemi, vaid ka rakenduste eripära kajastavatest kataloogidest ja failidest. Kui konfidentsiaalsus- või terviklusnõuded on väga suured, tuleks süsteemikataloogides, muudes süsteemiketta kataloogides ja registrivõtmetes desaktiveerida standardvolituste pärimisfunktsioon, et programmifailidele ja -andmetele saaks väljastada konkreetsed eraldi volitused. Turvagrupid „Authorized users" ja „Administrators" tuleb sel juhul eemaldada ning asendada eraldi kasutajakontodega. Tavapärasest suuremate turbenõuete korral tuleks eraldi kasutajakontosse ümber tõsta ka kõik kasutajasisestused, mis ei ole seotud Systemi või TrustedInstalleri nimeliste kaustade, failide ja võtmetega. Nii välistatakse teistest, juba kompromiteerimise ohvriks langenud kontodest toime pandavad ründed. Samas on suur oht, et volituste andmisel tehtud vea tõttu võib terve süsteem muutuda nii kasutuskõlbmatuks, et seda ei õnnestu enam parandada. Seega on protsessiga kaasnev suur arendus- ja katsetustööde maht õigustatud üksnes väga suurte turbenõuete korral. Et tuvastada kõrvalekaldeid kataloogistruktuurides ja registris kajastuvate volituste vahel, saab kasutada kolmandate tootjate analüüsitööriistu, nt AccessChk.

Terviklusastmed

Windows Vista ja Windows 7 ühilduvusrežiimi (Compatibility Mode), Microsofti Application Compatibility Toolkiti ning osa .NET-l põhinevate kolmandate tootjate lahenduste kasutamine võib suurendada rakendusprotsesside terviklusastet (vt M 4.341 Tervikluse kaitse alates Windows Vista). Suurte ja väga suurte turbevajaduste korral tuleks selliste rakenduste kaitsmiseks käitada neid täiesti eraldi, st isoleeritud klientides, et välistada teiste rakenduste paralleelne kasutamine. Kui see ei ole töökorralduse seisukohalt võimalik, on soovitatav süsteemifaile ja -andmeid kaitsta piirangutega, mida kirjeldatakse lõigus „Failisüsteem ja register". Suurte ja väga suurte turbenõuete puhul tuleks tõkestada selliste komponentide käivitamine, mis võiksid terviklusastmetest üle hüpata. Siia kuuluvad näiteks Windows Installer, Windowsi tarkvara ühilduvusrežiim ning kasutajaliideseid juhtivad ja salvestavad funktsioonid (Snipping-Tool, Remote Assistance, VNC, Makro Recorder). Sellised komponendid kehtestavad süsteemiomaduse UIAccess=TRUE. Lisateavet saab tarkvara tootja käest. Samas tuleb arvestada, et kui näiteks Windows Installer on desaktiveeritud, ei saa installida ei tarkvara ega ka värskendusi. Suurte ja väga suurte turbenõuete korral võib olla lisameetmena mõistlik käivitada programmide teatud osi üksnes madalas terviklusastmes. Näiteks saab käsuga *icacls java.exe / setintegritylevel low* teadmata allikast pärit java-programme käivitada üksnes madalas terviklusastmes. Samas tuleb tõdeda, et sedalaadi piirangute kehtestamine eeldab rakenduse suuremahulisi kohandamis- ja katsetustöid. Programmipõhiste volituste ja terviklusastmete kohandamist aitavad lihtsustada kolmandate tootjate tarkvaralahendused.

Süsteemi- ja kasutajavolitused

Windows Vista ja Windows 7 puhul tuleks suurte ja väga suurte turbenõuete korral aluseks võtta seadistused, mida kajastataks Microsofti dokumentatsioonis pealkirjaga „Specialized Security – Limited Functionality (SSLF)". Asjakohased dokumendid on olemas internetis ja neid pakutakse Microsoft Techneti levituskanali kaudu. Erinevalt pealkirjas sisalduvast sõnast *specialized* saab neid dokumente siiski laialdaselt kasutada, eeldusel et samal ajal ei kasutata ühtki vanemat Windowsi tarkvara ning kogu ülejäänud kasutatav tarkvara ühildub Windows Vista või Windows 7-ga probleemivabalt. Kui seadistustes kehtestatakse veelgi suuremad piirangud, tuleks neid mõnes väljavalitud klientsüsteemis esmalt mõni nädal katsetada, et kontrollida, kas koostöö süsteemi- ja võrguhalduse ning erialarakenduste

vahel toimib piisavalt hästi. Tootmisprotsesside puhul tuleks kõik süsteemivolitused tööle rakendada domeenikontrolleri ja grupipoliitikatega. Mitte ühegi süsteemivolituse seadistusväärtus ei tohi olla konfigureerimata. Vastasel korral on seda võimalik mis tahes lokaalsete administraatoriõigustega konto alt manipuleerida. Teavet mõningate oluliste seadistuste kohta, mis väljuvad SSLF-i piiridest, leiate asjakohase mooduli kasutamist selgitavate abimaterjalide hulgast.

Klient-server-võrkude ja koduvõrkude ühiskasutusse lubamise volitused

Ühiskasutusse lubamist võimaldavaid volitusi ei tohiks anda integreeritud süsteemigruppidele „Authorized users" ega ka grupile „Everyone". Samuti on soovitatav desaktiveerida klientides kõik lokaalsed kasutajakontod ja kasutada nende asemel üksnes Kerberosega autentimisel põhinevaid domeenikontosid. Kodukasutajagruppide funktsioon Homegroups ei sobi tavapärasest suuremate turbenõuete korral (vt M 4.423 Kodugrupi funktsiooni kasutamine Windows 7-s).

Programmide, skriptide ja installimise käivitamine

Suurte ja väga suurte turbenõuete korral tuleks Windows Installer tavarežiimi jaoks desaktiveerida. Selle tagajärjel ei saa installida värskendusi (*updates*) ja ka suurt osa tarkvara. Desaktiveerimiseks tuleb kasutada grupipoliitikat asukohas *Computer Configuration* | *Administrative Templates* | *Windows-Components* | *Windows Installer* | *Disable Windows Installer (Always)*.

Kontrollküsimused:

- Kas vastav, piiranguid kehtestav kasutajaõiguste kontseptsioon on välja töötatud ja on seda rakendatud?
- Kas volitusi jagatakse välja gruppide baasil?
- Kas välja jagatud volituste õigsust kontrollitakse regulaarselt, näiteks pärast igat installeerimist või värskendust?
- Kas kasutajaid on koolitatud, kuidas tuleb jagada volitusi, kui nad peavad vastutama juurdepääsude võimaldamise eest näiteks kas enda või projekti kohta käivatele andmetele?
- Kas kõik volitused on antud piirangutega nn need-to-know või least-privilege-strateegiate järgi?
- Kas Windowsi rakenduste jaoks on määratletud piirangutega volituste kontseptsioon ja kas seda rakendatakse?
- Kas turvarühmalt „Igaüks" on ära võetud kirjutamisõigus süsteemikaustades?
- Ega ei ole antud ühiskasutuse õigusi integreeritud süsteemirühmadele, nagu „Autenditud kasutajad" või „Igaüks"?
- Kas piirangutega volitused on kooskõlastatud turvapaikade halduse ning võrgu- ja süsteemihaldusega?

M 4.248 Windowsi klientoperatsioonisüsteemide turvaline installimine

Algatamise eest vastutavad: infoturbe spetsialist
Rakendamise eest vastutavad: administraator
Installeerimisfaasis ei ole Windowsi süsteem veel täielikult konfigureeritud (vt planeerimisfaasi meetmeid), mis tähendab, et soovitud turvaseadistused ei pruugi veel toimida nii nagu tarvis. Sel põhjusel peaks Windowsi installeerimine ja algne konfigureerimine aset leidma võimalikult turvalises keskkonnas. Võimalusel, näiteks töökohaarvuteid installeerides (nii lokaalselt kui ka läbi võrgu) tuleks eelistada juba eelnevalt ette valmistatud (eelkonfigureeritud) standardse konfiguratsiooni installeerimist. Enne kasutuselevõttu ning eriti enne internetiga ühendamist peaks Windowsi süsteem olema ennekõike täiesti uuendatud ning sinna peaks olema paigaldatud kõik institutsiooni jaoks heaks kiidetud värskendused. Juhtudel, kus Windowsi süsteem ei ole *Active Directory* domeenistruktuuri alla integreeritud, tuleb grupipoliitikaid, mis sisaldavad muuhulgas ka turvaseadistusi, konfigureerida lokaalsel tasandil, arvutis. Seda võib teha Microsofti operatioonisüsteemide Windows Vista ja Windows 7 nii käsitsi kui ka skriptidega. Otsus, kui detailseid seadistusi tehakse, tuleb vastu võtta juba planeerimisfaasis.
Grupipoliitikate mehhanism võimaldab luua kiire algkonfiguratsiooni, kui arvuti domeeni alla liidetakse. Pärast domeeniga liitumist tuleb arvutiobjekt liigitada *Active Directory* vastavasse organisitsiooni allüksusesse (*Organisational Unit*, OU). Juhul, kui arvuti jääb standardsesse *Active Directory* konteinerisse *Computer*, rakendatakse selle suhtes vaid asukoha ja domeeni GPOsid, aga mitte OU GPOsid, kuna sellele *Active Directory* konteinerile ei ole võimalik OU grupipoliitikaobjekte lisada. Arvestada tuleks ka sellega, et pärast arvuti ümberliigitamist uue organisatsioonilise üksuse alla tuleb arvuti taaskäivitada. Sel moel laetakse ka kõik arvutiga lingitud GPOd arvutisse ning rakendatakse ka tööle. Pärast installeerimist tuleks kontrollida, kas vastavad turvaseadistused on ka reaalselt kasutusele võetud. Kontrollida tuleks siinjuures installeeritud komponente, rakendatud poliitikaid, failisüsteemi ja registriga seotud volitusi, välja antud kasutajaõiguseid ja lubatud süsteemiteenuseid.

Windows Vista ja Windows 7 puhul kehtib täiendav nõue, et operatsioonisüsteem tuleb pärast installeerimist aktiveerida. Ainult installeeritud ja aktiveerimata Windows Vista, mille puudub *Service Pack 1* (SP1), muutub pärast kolmekümnepäevast kasutusperioodi (*Grace Period*) töökõlbmatuks. Vista *Client* taandatakse kohustuslikus korras nn piiratud režiimile, ing. k. *Reduced Functionality Mode* (RFM), mille puhul on kasutatavate funktsioonide hulk palju väiksem. Remondipaketiga *Service Pack 1* loobus Microsoft RFM-i kasutamisest. RFM-i asemel kuvab Windows Vista hoiatavaid teateid, mis sobivad muuhulgas ka selleks, et takistada või viivitada Windows Vista süsteemi jaoks kriitilise tähtsusega töid. Klientidel alates Windows 8-st (välja arvatud Enterprise) tuleb tootevõti sisestada nüüd juba installeerimise ajal. Windows 8 Enterprise'i korral kasutatakse tootevõtme asemel KMS-i (Key Management Service) ja MAK (Multi Activation Key) mehhanisme.

TPM-i kasutamine alates Windows 8-st

Meetme M 2.324 Windows Vista ja Windows 7 kasutuselevõtu planeerimine põhjal tehtud kasutusotsuse kohaselt tuleb TPM püsivara seadistuste ajal välja lülitada või vajaduse korral kasutamiseks käivitada. Täpsem protseduur ja sellele järgnevad TPM-i kasutusvõimalused operatsioonisüsteemi kaudu erinevad üksteisest püsivara versiooni, TPM-i versiooni ja operatsioonisüsteemi versiooni poo-

lest.Aktiveerimise teemat käsitlevad lähemalt meetmed M 4.336 Hulgilitsentslepinguga Windows süsteemide aktiveerimine alates Windows Vistast või Windows Server 2008-st ja M 4.343 Hulgilitsentsilepinguga Windowsi süsteemide reaktiveerimine alates Windows Vistast või Windows Server 2008-st .

Domeenikuuluvus

Arvuti lisamiseks mõne domeeni alla peab olema kas vastav arvutikonto domeenis juba ette valmistatud või luuakse arvutikonto domeeniga liitumise käigus. Selleks on vaja asjakohaseid administraatorivolitusi, millega tuleb piiravalt ümber käia. Seda, kas arvutikonto tuleks luua enne installeerimist või selle käigus, tuleks otsustada lähtuvalt ettevõtte või ametiasutuse igapäevasest praktikast. Domeeni tulevased liikmed tuleks domeeniga liita installeerimistööde käigus, st neid ei tuleks kõigepealt installeerida üksikarvutitena. Niimoodi tagatakse näiteks see, et lihtne failide ühiskasutus jääb läbivalt desaktiveerituks ja süsteemi alla ei looda juurde täiendavaid administraatori kasutajaõigusega kontosid.

Järelevalveta installeerimised

Windows võimaldab kasutada operatsioonisüsteemi paigaldamiseks järelevalveta installeerimise mehhanismi (*unattended installation*). Selle käigus toimub installeerimine eelnevalt koostatud vastusfaili baasil ning ilma administraatori sekkumiseta. Windows Vista ja Windows 7 puhul kasutatakse operatsioonisüsteemi järelevalveta installeerimiseks vastusfaili *Unattend.xml* . Seda vastusfaili saab koostada ja muuta utiliidiga *Windows System Image Manage*. Utiliit *Windows System Image Manager* on *Windows Automated Installation Kit* -i *(WAIK)* koostisosa. WAIK ei kuulu Windows Vista installeerimise andmekandjatel olevate programmide hulka, kuid seda saab hankida Microsofti internetiaadressidelt *www.microsoft.com/downloads* . Windows Vista ja Windows 7 uues ettevalmistustööriistas *Business Desktop Deployment* (BDD) on aga WAIK juba olemas. BDD funktsioonide hulka kuuluvad Windows Vista ja Windows 7 planeerimine, ülesehitamine, testimine ja ettevalmistamine (Microsoft Deployment Toolkit 2010). Juhtudel, kus Windowsi süsteeme installeeritakse järelevalveta funktsiooni abil, tuleb arvestada järgnevaga:

- Tundlikku infot nagu paroole ja vastusfaile tuleb piisavalt kaitsta, et volitamata isikud neile ligi pääseks. Vastusfaili koostamise käigus, näiteks *Setup Manager* -iga või Windows Vista ja Windows 7 puhul *Windows System Image Manager* -iga töötades tuleb kasutatud paroolid krüpteerida.
- Eelnevalt on tarvis määratleda, kuidas käiakse ümber installeerimisskripti või vastusfaili jaoks vajalike paroolidega, mis võimaldavad liituda domeeniga.
- Windows Vista ja Windows 7 puhul on võimalik järelevalveta installeerimistööde ajaks automaatset sisselogimist aktiveerida ainult eelnevalt koostatud vastusfaili vastava konfigureerimisega.
- Pärast installeerimistööde lõppu tuleb kõik tundlikku infot sisaldavad skriptid ja failid viivitamatult ning turvalisel moel kustutada (vt M 4.56 Turvaline kustutus Windows operatsioonisüsteemides).

Kohandatud installeerimisandmekandjad

Juhtudel, kus Windowsi installeerimiseks kasutatavad originaalandmekandjad võivad olla vananenud, tuleb pärast installeerimist paigaldada eraldi veel kõik paigad, remondipaketid ja värskendused. See omakorda pikendab installeerimiseks kuluvat aega ning suurendab selle arvuti jaoks rünnete õnnestumise ohtu, kuna teatud aja jooksul on arvuti kaitsemehhanismid aegunud. Ründeohu vähendamiseks ja selleks, et kõik värskendused saaksid installeeritud juba installeerimistööde käigus, võib rakendada ühte kahest:

- integreeritud installeerimist (nimetatakse ka *Slipstream* installeerimiseks) või
- kombineeritud installeerimist.

Windows Vista ja Windows 7 puhul saab värskendusi installeerimise raames paigaldada ettevalmistustööriistaga BDD. Integreeritud installeerimisfunktsiooni kasutades paigaldatakse korraga Windows ja mõni *Service Pack*. Kombineeritud installeerimine võimaldab operatsioonisüsteemi installeerida järelevalveta installeerimisrežiimis koos *hotfix* 'ide ja täiendavate rakendustega. Integreeritud installeerimisfunktsiooni kasutamiseks luuakse uus andmekandja. Selle käigus kirjutatakse originaalandmed üle *Service Pack* 'i andmetega. Võimalike andmekandjatena tulevad kõne alla optilised andmekandjad nagu CD-ROM või DVD, *Remote Installation Service* 'i (RIS) või *Windows Deployment Services* (WDS) *Network Distribution Shares* või installeerimiskaustad. Siinkohal tuleks arvestada, et remondipaketti, mis on installeeritud integreeritud režiimis, ei ole enam hiljem võimalik deinstalleerida.

Kombineeritud installeerimisrežiimi jaoks vajalik andmekandja koostatakse seeläbi, et installeerimise originaalandmekandjale lisatakse täiendavad installeerimisfailid. Järelevalveta installeerimise vastusfail (standardina kannab see nimetust kas *Unattend.txt* või Windows Vista ja Windows 7 puhul *AutoUnattend.xml*) ja *cmdlines.txt* tuleb asjakohaselt kohandada. Täpsed tegutsemisjuhised leiate Microsofti dokumentatsioonist. Enamatel juhtudel võib installeerimiseks soovitada selleks kohandatud andmekandjaid. Kumba režiimist eelistada, tuleb otsustada ettevõttes ja ametiastutuses iga juhtumi puhul eraldi. Alates Windows Vistast ja Windows 7-st eeldab jaotamine üksnes WIM Image'i kohandamist. WIM Image on operatsioonisüsteemist WIM-andmevormingus salvestatud kujutis. Neid hoitakse enamasti kas vahetatavatel andmekandjatel või võrgus. Kiirete muudatuste ja värskenduste jaoks esitatakse installimisprotsessis päring kas ühiskasutuse serverile või WSUS-serverile. See ei ole aga ilmtingimata vajalik.

Süsteemikomponendid

Süsteemi installeerimise raames tuleb tagada, et installeeritaks ainult vajaminevad süsteemikomponendid. IT-etalonturbe abivahendite hulgas leiduvates tabelites on toodud loetelud komponentidest, mida võiks kasutada Windowsi baasinstallatsiooni loomiseks (seisund: *activated*). Sõltuvalt vajadustest võib installeerida ka täiendavaid komponente, mis on IT-etalonturbe abimaterjalide tabelis ära märgitud mõistega „valikuline" (*optional*). Selliste Windowsi komponentide installeerimisest, mis on märgistatud mõistega „ *deactivated*", on turvalisuse põhjustel mõttekas loobuda.

Kontrollküsimused:

- Kas süsteemide puhul on tagatud, et need võetaks võrgukeskkonnas kasutusele alles pärast seda, kui installeerimistööd, konfigureerimine ja turvapaikade ning värskenduste paigaldamine on täielikult lõpuni viidud?
- Kas süsteemi installeerimise raames tagatakse, et installeeritaks ainult vajaminevad süsteemikomponendid?
- Kas pärast installeerimist kontrollitakse turvaseadistuste reaalset töölerakendumist (installeeritud komponente, rakendunud poliitikaid, failisüsteemi ja registri volitusi, välja jagatud kasutajaõiguseid, lubatud süsteemiteenuseid)?
- Kas Windows Vista süsteem aktiveeriti?
- Kas installeerimisskriptides ja konfigureerimisfailides sisalduvad paroolid on kaitstud ning kas need said pärast installeerimist süsteemist kustutatud?
- Juhul, kui kasutatakse järelevalveta installeerimisrežiimi, kas selleks on rakendatud asjakohaseid meetmeid?
- Kas Windows-süsteemide puhul on tagatud, et need võetakse võrgukeskkonnas kasutusele alles pärast täielikku installeerimist, konfigureerimist ja kõikide turvapaikade ning värskenduste paigaldamist?
- Kas Windows-süsteemi installeerimise raames tagatakse, et installeeritakse ainult vajaminevad süsteemikomponendid?
- Kas on tagatud, et vajalikud Windowsi turvaseadistused on pärast installeerimist ka tegelikult konfigureeritud (installeeritud komponendid, kasutatud poliitikad, volitused andmesüsteemis/registris, määratud kasutajaõigused, lubatud süsteemiteenused jne)?
- Kas installeerimisskriptides ja konfigureerimisfailides sisalduvad paroolid on kaitstud ning kas need kustutati pärast installeerimist süsteemist?
- Kas Windowsi ilma järelevalveta installeerimise korral väljastatakse administraatori parool?
- Kas on kaalutud TPM-i kasutamise eeldusi ja puudusi ning on tehtud otsus selle kasutamiseks operatsioonisüstemis?

M 4.249 Windowsi klientsüsteemide ajakohastamine

Algatamise eest vastutavad: infoturbe spetsialist, administraator
Rakendamise eest vastutavad: administraator

Kogemused on näidanud, et Microsoftilt regulaarselt ilmuvaid, turvet puudutavaid värskendusi ja paikasid tuleks installeerida nii kiiresti kui vähegi võimalik. Selle teadmise rakendamisel jõutakse aga tihti probleemideni, kuna ühelt poolt tuleb värskendused installeerida võimalikult kiiresti ja ilma viivitusteta, kuid teiselt poolt on neid enne paigaldamist tarvis põhjalikult testida. Universaalseid lahendusi selle probleemi kõrvaldamiseks ei ole. Tuleb leida sobiv kompromiss turvalisuse ja töökoormuse vahel. Planeerimisel tuleb arvestada meetmega M 2.273 Turvalisust mõjutavate paikade ja värskenduste kiire paigaldamine .

- Paikade ja värskendustega ümberkäimiseks tuleb juurutada asjakohane töökorralduslik protsess (nt muudatuste halduse raames).
- Protsess peab lisaks Windowsi süsteemide värskendustele ja paikadele käsitlema veel ka kasutuses olevaid rakendusi (nt Microsoft Internet Explorerit, Microsoft Office programme ja ka kolmandate tootjate tarkvara).
- Administraatorid peavad ennast regulaarselt kursis hoidma võimalike avastatud turvaaukudega ja nende lappimiseks saada olevate paikadega.
- Värskenduste puhul tuleb tagada, et need paigaldatakse esmalt kontrolli eesmärgil testsüsteemi.
- Süsteemide jaoks peab olema välja töötatud strateegia, kuidas võimalike probleemide korral taastada süsteemide funktsioone.

Turvapaikade versioonide kontrollimine

Windowsi süsteemide ajakohasuse tagamiseks tuleb võrrelda hetkel installeeritud turvapaikade versioone Microsofti poolt väljastatud kõige uuemate turvavärskendustega. Tarkvaratööriistaga *Microsoft Baseline Security Analyzer* (MBSA) on Microsoft loonud vahendi, mis analüüsib automaatselt süsteemi versiooni. Selle või mõne muu sarnase tööriista kasutamine aitab administraatoritel luua värskeid ülevaateid süsteemidesse paigaldatud turvapaikade versioonidest ning seetõttu aitab see olulisel määral tõsta üldist turvalisust. MBSA tarkvaratööriista saab konfigureerida selliselt, et võrdluse baasmaterjalina ei kasutata mitte mõnda internetis asuvat Microsofti serverit, vaid *Microsoft Windows Server Update Services* (WSUS) lokaalset koopiat. Sel moel on võimalik kõrvutada süsteemide hetkeseisundit ja ettevõttes eesmärgiks seatud norme. Seda protseduuri rakendatakse eelkõige testimiseks, et välja selgitada, kas kõik ettevõttes heaks kiidetud paigad ja värskendused on ka reaalselt süsteemidesse paigaldatud või mitte. Integreerides MBSA omakorda *Microsoft Systems Management Server* 'i (SMS) alla, saab testitulemusi ka otse SMSi andmebaasi salvestada. MBSA tarkvaratööriistal on graafiline kasutajaliides (*mbsa.exe*), kuid seda võib juhtida ka käsuviiba abil (*mbsacli.exe*). Käsuviibaga on võimalik seda utiliiti integreerida automaatsesse protsesside hulka nõnda, et ka tulemusi saab omakorda automaatselt (nt skriptide toel) edasi töödelda. MBSA suudab kontrollida operatsioonisüsteemi paikade versioone ja tuleb toime ka täiendavate rakendustega nagu näiteks Microsoft Office, Exchange Server, Microsoft Internet Explorer (siin ka spetsiaalselt tsoonide konfiguratsiooni kontrollimisega). Kontrolle saab teha lokaalselt ja suures osas ka kaugpöördusega.

Ajakohastamismeetodid

Windowsi süsteemi ajakohastamiseks võib kasutada Windowsi enda funktsiooni *Automatic Updates* või lahendust, mille korral installeeritakse värskendused ja paigad mõne teise (välise) tarkvara jaotamisemehhanismi toel. Strateegia valik peaks lähtuma igast juhtumist eraldi, arvestades konkreetsete asjaoludega. Juhul, kui tarkvara laialaijagamiseks kasutatakse mõnda välist mehhanismi, tuleb *Automatic Updates* funktsioon välja lülitada, et vältida paralleelkasutuse võimalikke negatiivseid tagajärgi. Olukorras, kus kasutatakse Windowsi automaatset ajakohastamisfunktsiooni, on võimalik valida järgmiste konfiguratsioonide vahel:

- Värskendused laetakse automaatselt alla ja installeeritakse vastavalt määratletud ajakavale (see funktsioon on saadaval alles pärast *Automatic Updates* tarkvara värskendamist).
- Värskendused laetakse automaatselt alla, kuid neid ei installeerita automaatselt.
- Uute värskenduste ilmumise korral saab administraator vaid sellekohase teate, värskenduste allalaadimist ei toimu.
- Windows Vista uuendused, mis on soovitatavad, aga pole määrava tähtsusega, saab automaatsest installeerimisest välja võtta (Windows Update | Change Settings| Recommended Updates).

Värskenduste käsitsi installeerimisest tuleks loobuda. Ajavahemik, mis jääb turvaaugu ilmsikstuleku ja selle lappimise vahele, peab olema võimalikult lühike ning seetõttu on heaks kiidetud paikade installeerimiseks soovitav kasutada kas *Automatic Updates* mehhanismi või mõnda välist tarkvara laialaijagamise mehhanismi. Kuna turvakaalutlustest lähtuvalt tuleb otseühendusi internetiga vältida ja enne installeerimist värskendusi testsüsteemides testida, ei ole soovitav Windowsi süsteeme ajakohastada *Automatic Updates* funktsiooniga otse läbi väliste allikate (nt Microsofti). Selle asemel tuleks Windowsi süsteemide konfiguratsioonis kindlaks määrata, et ajakohastamiseks kasutataks institutsiooni enda *Update* -servereid. Selle abil on võimalik rakendada järgmist, mõistlikku ajakohastamisprotsessi:

- administraatorid saavad informatsiooni uute värskenduste kohta,
- värskendused laetakse alla ja testitakse testsüsteemis,
- pärast edukalt lõppenud testimisfaasi antakse värskendus organisatsiooni *Update* -serveril ühiskasutusse,
- Windowsil töötavad arvutid laevad ühiskasutusse antud värskenduse *Update* -serverilt alla ja installeerivad selle.

Rakendustarkvara ja tööriistad

Rakendustarkvara ja tööriistade värskendusfunktsioonidele (*update*) ei piisa väga sageli tavapärastest kasutajavolitustest, mistõttu kuvavad need kasutajatele häirivaid ja segadust tekitavaid teateid. Administraatorid peaksid sellised teated kasutajate jaoks kõrvaldama, nt sellega, et koondavad värskenduspaketid kokku tarkvara jaotussüsteemidesse või kasutavad Task Scheduleri (alates Vistast) funktsioone.

Kasutajate teavitamine

Paljudele värskendustele järgnevad taaskäivitused ning mõningad automaatsed süsteemiprotsessid, mis röövivad töötajate tööaega. Pärast taaskäivitamisi

kuvatakse sageli teateid või protsessi edenemisribasid, mis võivad osas kasutajates segadust tekitada. Samas ei tohi pooleliolevate protsesside edukat lõpetamist tõkestada, nt käsitsi algatatud taaskäivitustega. Seetõttu tuleb kasutajaid enne suuremaid värskendusi teavitada töös tekkivatest võimalikest viivitustest. Samuti tuleks kasutajate käest pisteliselt koguda tagasisidet, kuidas värskendustsüklit paremaks muuta. Süsteemide kontrollimisel pärast värskendusi ja suuremaid süsteemimuudatusi (nt pärast uue Service Packi paigaldamist) tuleks mõne päeva vältel senisest rohkem tähelepanu pöörata Windowsi logidele ja tarkvaralogidele, et tuvastada võimalikud uut tüüpi vead. Osade klientide puhul tuleks pisteliselt kontrollida:

- kas kõik värskendused on edukalt lõpuni installitud (Windowsi süsteemilogi);
- kas rakendustepõhised volitused ja turvaseadistused on jätkuvalt korrektsed (kontrollida kas käsitsi või turvamallidega), eriti Windowsi kaustad, võrk ja tulemüür;
- kas rakendused, turbetarkvara ja -riistvara töötavad õigesti.

Täiendavad kontrollküsimused:

- Kas süsteemidesse paigaldatud turvapaikade versioone võrreldakse regulaarselt Microsofti välja antud värskenduste versioonidega?
- Kas administraatorid hoiavad ennast regulaarselt kursis võimalike avastatud turvaaukudega ja nende lappimiseks saada olevate paikadega?
- Kas ajakohastamise jaoks on välja töötaud strateegia?
- Kas välja töötatud ajakohastamise strateegia arvestab ka rakenduste värskendustega?
- Kas värskendusteks kasutatavad andmeallikad on usaldusväärsed?
- Kas on tagatud, et installeeritakse ainult testitud ja ühiskasutusse antud värskendusi?
- Kas süsteemide jaoks on välja töötatud strateegia, kuidas võimalike probleemide ja vigade korral funktsioone taastada?

M 4.250z Keskse võrgupõhise autentimisteenuse valimine

Algatamise eest vastutavad: IT-juht, infoturbe spetsialist
Rakendamise eest vastutavad: administraator

Igasugused IT-süsteemid peaksid reeglina tagama, et kasutajad, kes neid süsteeme oma töös rakendavad, läbiksid esmalt autentimise. Ainult niimoodi on võimalik ära hoida volitamata isikute juurdepääsu teenustele, mida süsteem kasutada võimaldab, või andmetele, mis on süsteemi salvestatud. Ainukeseks erandiks on siinkohal IT-süsteemid, mille puhul on ette nähtud, et need peavad sarnaselt avalikele infoteenustele olema kõigile vabalt ligipääsetavad (nt avalikud veebiserverid vms). Pärast edukat autentimisprotseduuri peab süsteem tagama, et kasutajad pääseksid ligi vaid nende volitustele vastavatele teenustele ja andmetele. Autentimist läheb tihti tarvis mitte ainult mõne üksiku teenuse või süsteemi kasutamiseks, vaid ka selleks, et tagada samade autentimisandmetega (nt kasutajatunnuse ja parooliga) juurdepääs nii erinevatele teenustele kui ka erinevatele süsteemidele. Sellistel juhtudel läheb tarvis keskset, võrgu baasil toimivat autentimisteenust, mille puhul ei oleks autentimisandmeid enam tarvis igas üksikus süsteemis eraldi hallata ega värskendada.

Ekstreemjuhtu kujutab endast siinkohal nn *Single Sign-On* , mille puhul leiab aset kogu IT-koosluse kõikide teenuste keskne autentimine. Selle lahenduse eeliseks on asjaolu, et kasutajatel tarvitseb end vaid üks kord sisse logida. Kasutajatel läheb tarvis vaid ühte parooli või *token*- it ning tänu sellele pole neil enam vaja erinevaid paroole meeles pidada ega suurt arvu erinevaid *token*- eid endaga kaasas kanda. Puuduseks on aga tõsiasi, et kui potentsiaalsel ründajal peaks õnnestuma end kasutajana süsteemi sisse logida, tekib tal korraga juurdepääs kõikidele vastava IT-koosluse teenustele.Enne keskse, võrgu baasil toimiva autentimissüsteemi juurutamist on ülimalt oluline läbi viia põhjalik planeerimistöö, kuna autentimissüsteemi funktsioonid ja turvalisus on määrava tähtsusega kogu IT-koosluse turvalisuse tagamisel. Tsentraalselt toimiva autentimise võib lahendada mõne autentimissüsteemiga nagu näiteks Kerberos. Kerberose täiendavaks eeliseks on võimalus rakendada seda lisaks Unixil töötavatele süsteemidele veel ka Windowsi operatsioonisüsteemides.

Järgnevalt toome teieni täpsema ülevaate erinevatest soovitustest, millega tuleks arvestada võrgu baasil toimiva autentimissüsteemi valikul ja rakendamisel.

Võrguprotokollide krüpteerimine Võrgu baasil toimiva autentimislahenduse jaoks vajalik kriitilise tähtsusega info edastatakse vastupidiselt lokaalsele kasutajahaldusele kas LAN'i või WAN'i kaudu. Seetõttu on ülimalt vajalik, et volitamata isikud ei saaks seda infot ei lugeda ega ka muuta. Lisaks tuleb tagada, et ründajal ei oleks võimalik ennast sisse logida lihtsalt eelnevalt salvestatud sisselogimisinfoga. Selleks tuleb sisselogimisinfo, mis liigub autentimise otstarbel serveri ja klientsüsteemi vahel, krüpteerida ja täiendavalt, näiteks *Challenge-Response* -protseduuri kasutades dünaamiliseks muuta.

Autentimisserveri turve

Reeglina hoitakse kõiki autentimiseks vajaminevaid andmeid ühes keskses serveris. Seetõttu on oluline tagada, et need kriitilise tähtsusega andmed oleksid kaitstud volitamata juurdepääsude eest. Autentimisserverit tuleb seega igal tasandil võimalikult hästi kaitsta (kaitsevajadus on võrreldav turvalüüside kaitsevajadusega). Muuhulgas tuleb tegeleda järgnevaga:

- Seade tuleks paigaldada eraldiseisvasse serveriruumi. Selleks vajalikud kohustuslikud nõuded leiate moodulist B 2.4 Serveriruum . Serveriruumi puudumisel võib autentimisserveri üles seada serverikappi (vt B 2.7 Kaitsekapid).
- Seadet tohib paigaldada ainult turvatud võrgu piiresse.
- Autentimisserveri kontseptsiooni loomiseks ja käitamiseks peavad eksisteerima sobiv personal ja piisavad ressursid. Autentimisserveri käitamisega seotud ajakulu ei tohi alahinnata. Juba ainuüksi süsteemi poolt loodavate logiandmete analüüs võtab tihti küllaltki palju aega. Administraatoritel peavad olema põhjalikud teadmised kasutatavatest IT-komponentidest ja neil peab olema läbitud asjakohane koolitus.
- Autentimisserveril tohiks käitada ainult seal vajaminevaid teenuseid ning kõikidest teistest teenustest või vähemalt madala turbevajadusega teenustest nagu näiteks veebiserver, tuleks loobuda. Lisaks tohivad sinna olla installeeritud ainult sellised programmid, mis on tööfunktsioonide tagamiseks hädavajalikud.
- Sellesse süsteemi tohivad ennast sisse logida ainult administraatorid. Administraatori kasutajaõiguste väljajagamine peab olema hoolikalt dokumenteeritud. Turvalisuse seisukohast eriti kriitilisi sekkumisi läbi viies tuleks võimalusel alati lähtuda „nelja silma“ põhimõttest. Administraatorid peaksid enda sisselogimiseks kasutama tugevaid autentimismeetodeid.
- Autentimisserveri administreerimine tohib olla võimalik vaid läbi turvalise juurdepääsu, seega näiteks kas mõne turvalise konsooli, krüpteeritud ühenduse või eraldi võrgu (administreerimisvõrgu) kaudu.
- Autentimisserveri korrektne konfiguratsioon on selle turvaliseks käitamiseks määrava tähtsusega. Konfiguratsioonis tehtud vead võivad viia turvaaukude või avariide tekkimiseni. Parim võimalik konfiguratsioon peab olema hoolikalt dokumenteeritud.
- Autentimisserveri operatsioonisüsteemidesse ja programmidesse peavad alati olema paigaldatud kõige värskemad turvapaikade versioonid.
- Rakendatava tarkvara puhul tuleb regulaarselt kontrollida selle terviklikkust (vt M 4.93 Regulaarne tervikluse kontroll). Vigade ilmnemisel tuleb autentimisserver välja lülitada.
- Logimise puhul peab olema selgelt dokumenteeritud, milliseid sündmusi logides kajastatakse (vt M 5.9 Serveri logi), kuhu need salvestatakse ja milliste ajavahemike tagant need läbi analüüsitakse.
- Autentimisserverite temaatika peab kajastuma nii organisatsiooniüleses andmevarunduse kontseptsioonis kui ka avariikontseptsioonis. Andmetest

loodud varukoopiate uuesti sisselugemisel tuleb jälgida, et kasutajate ja nende kasutajaõiguste haldamise andmed säiliksid kõige värskemas versioonis.
- Autentimisserveri turvaline käitamine eeldab regulaarset kontrollimist, kas rakendatud turvameetmed töötavad korrektselt. Käitamise turvalisuse kontrollimiseks tuleb regulaarselt läbi viia auditeid.

Lisaks tuleb keskselt toimiva halduse puhul arvesse võtta veel ka serveri ja võrgu avariisid, kuna need võivad olla põhjustatud *Denial-Of-Service* tüüpi rünnetest. Olukordades, kus kogu võrgu arvutid sõltuvad antud serveri autentimisfunktsioonide töökindlusest, laieneb *Denial-Of-Service* tüüpi rünne tervele võrgule. Seetõttu on soovitav kasutusele võtta kõrgkäideldav süsteem, mille teostuseks sobib liiasusega server (vt M 6.43 Liiasusega Windowsi serverid). Kuna usaldusväärsel autentimisel on täita keskne roll ükskõik millise võrgu turvalisuse tagamisel, on ülimalt oluline tagada autentimisserveri turvaline ja nõuetekohane käitamine. Sel põhjusel tuleb välja valitud protseduurid sisse töötada olemasolevasse organisatsiooniülesesse turvapoliitikasse.

Paroolid

Analoogselt meetmega M 2.11 Paroolide kasutamise reeglid tuleb kasutusele võtta sobivad abinõud, mis tagaksid paroolide võimalikult kõrge kvaliteedi.

Logimine

Autentimissüsteem peab suutma kajastada sündmusi, mis on loetletud meetmes M 5.9 Serveri logi . Kõik logifailid tuleb salvestada keskselt serverile. Kuna see võimaldab luua detailseid kasutajaprofiile, tuleb andmekaitsest lähtuvatel põhjustel tagada, et volitamata isikutel poleks võimalik neid andmeid endale lugemiskõlblikuks teha. Keskse logiserveri puhul tuleks tagada, et andmeid poleks võimalik andmeedastuse käigus pealt kuulata. Selle tagamiseks saab rakendada näiteks andmeedastusprotokolle, mis võimaldavad andmete krüpteerimist, VPN-ühendust või keskse autentimisserveri ja logiserveri vahelist eraldi võrku.

Täiendavad kontrollküsimused:

- Millised IT-koosluse teenused toetavad keskse autentimisserveri kasutamist?
- Kas *Single Sign-On* protseduuri kasutatakse?
- Kuidas kaitstakse autentimisinfot andmeedastuse raames?
- Kuidas kaitstakse autentimisserverit võimalike rünnet eest?

M 4.251 Töötamine võõraste IT-süsteemidega

Algatamise eest vastutavad: infoturbe osakond, kasutajad, ülemused
Rakendamise eest vastutavad: kasutajad

Tihti on tarvis ka tööülesannetes ringi liikudes ligi pääseda erinevat liiki elektroonilisele infole, näiteks vaadata kalendermärkmiku sissekandeid, saata e-maile või konkreetseid faile alla laadida. Tihti on kõige lihtsam kasutada sel otstarbel võõraid IT-süsteeme või sideühendusi, näiteks:

- avalikus traadita võrgus faile alla laadida,
- kasutada külastatava organisatsiooni büroo arvuteid või nende intranetti või
- luua firmavõrguga ühendus mõne hotelli WLAN-pääsupunkti kaudu.

Kõikidel neil juhtudel peaksid kasutajad aga kindlasti teadma, et tegu on võõraste isikute poolt hallatud IT-süsteemidega, mistõttu tuleb kasutada täiendavaid turbemeetmeid. Lähtuda tuleks alati sellest, et kuna võõra kasutuskeskkonna turvalisus ei ole teada, tuleb seda käsitleda kui madala turvalisusega keskkonda. Iga töötaja peaks olema teadlik, et võõraste arvutite ja võõraste kasutuskeskkondadega kaasnevad reeglina alati ka suuremad ohud IT-turvalisusele. Isegi neil juhtudel, kus võõra keskkonna turbeaste näib muljetavaldav, võib siiski tegu olla väära ettekujutusega. Näiteks võib võrgukeskkond olla palju kehvemini kaitstud kui oma enda sülearvuti ning selle tagajärjel võidakse endaga kaasa tuua erinevaid probleeme nagu arvutiviiruseid või trooja hobuseid. Külastatavas asutuses võib ka nt ilmneda, et sealne institutsiooniline arusaam IT-turbest on väga teistsugune, näiteks võib puududa konsensus selles osas, millised on turbe jaoks püstitatud eesmärgid, turbeaste või turbemeetmed. Mobiilsete võrkude puhul võib juhtuda, et võrgu kasutajad vahetuvad pidevalt, st teatud hulk kasutajaid lahkub pidevalt ja teatud hulk tuleb ka juurde. Sellistes olukordades on väga raske kindlaks teha, kes teatud ajahetkel antud võrgus üheskoos aktiivselt omi asju ajasid. Mobiilsed võrgud on oma eripärade tõttu väga vastuvõtlikud rünnete suhtes, mida ei pruugita võib-olla isegi tuvastada, samuti on nende puhul väga raske esile tuua kindlaid väiteid eksisteeriva turbeastme kohta.

Enne võõrasse võrku sisselogimist või sealsete teenuste kasutamist peaksid kasutajad esmalt veidi järele mõtlema, kas vastav keskkond on piisavalt usaldusväärne või mitte. Ülisoodsad pakkumised võivad olla loodud spetsiaalselt sel eesmärgil, et mobiilsetest arvutisüsteemidest andmeid välja nuhkida ja neid manipuleerida. Potentsiaalne ründaja võib näiteks pakkuda võimalust kasutada tasuta internetipääsu või WLAN-pääsupunkti, et nii lihtsal moel selle kaudu edastatavad andmed enda jaoks loetavaks teha. Kasutajad peaksid olema alati piisavalt valvsad ka suhteliselt lihtsate ja ülevaatlike teenuste kasutamisel. Töölähetustel võib olla näiteks vajalik sülearvutist teatud materjale välja printida. Selleks võidakse kasutada hotellide trükiteenuseid, internetikohvikute või koopiakeskuste teenuseid, ning ka külastatava ettevõtte kohapealseid printereid. Tuleb aga arvestada, et iga trükitellimusega (*print job*) muudetakse trükitavad materjalid kättesaadavaks ka kõrvalistele isikutele, st neile, kes vastavaid teenuseid osutavad. Väljatrükitavad materjalid tuleb printerile edastada faili kujul

ning võib juhtuda, et andmeedastuse käigus salvestatakse need IT-süsteemide vahemällu. Väljatrükke võidakse kogemata valmistada mitmes eksemplaris ning võib ka juhtuda, et väljatrükid lihtsalt unustatakse printerisse. Seetõttu peaksid kasutajad enne võõraste IT-süsteemidega tööleasumist ja enne võõraste teenuste kasutuselevõttu arvestama järgmiste soovitustega:

- viige ennast kurssi olemasolevate turvameetmetega,
- looge endale täpsed ettekujutused, st lähtuge mobiilse IT kasutusele kehtivatest reeglitest ja ettekirjutustest ning ärge kasutage võõraid IT-süsteeme ega -teenuseid kõikmõeldavate tegevuste ega andmete tarbeks.
- Mitte mingisugusel juhul ei tohiks kasutada veebilehitsejate paroolide ja kasutajanimede AutoComplete -funktsiooni, sest vastasel korral on võõra arvuti järgnevatel kasutajatel lihtne ennast teie kasutajanimega kuhugi sisse logida.
- Niipea, kui olete oma töö lõpetanud, tuleks reeglina kõik võõras arvutis selle kasutamise käigus tekkinud ajutised andmed kustutada. Tihti ei ole seda aga sugugi lihtne teha, kuna paljud operatsioonisüsteemid loovad ajutisi andmeid väga paljudesse erinevatesse kohtadesse. Lisaks võib võõraste IT-süsteemide puhul olla takistuseks asjaolu, et teile antud kasutajaõigused ei luba teil kõiki enda tekitatud andmeid kustutada. Kõige vaatamata tuleks siiski vähemalt vahemälu (Cache) ära kustutada.

Täiendav kontrollküsimus:

- Kas kõiki töötajaid informeeritakse sellest, millega tuleks võõrast IT-d kasutades arvestada?

M 4.252 Koolitusarvuti turvaline konfigureerimine

Algatamise eest vastutavad: infoturbe osakond, IT-juht
Rakendamise eest vastutavad: administraator

Turbeprobleemide vältimiseks ja koolitusarvutite volitamata kasutamise tõkestamiseks tuleb luua minimaalne konfiguratsioon ja kehtestada kasutajaõigustele piirangud (vt M 2.63 Pääsuvolituste kehtestamine ja M 4.135 Süsteemifailide pääsuõiguste andmise kitsendused). Koolitusarvutite võimaliku minimaalse konfiguratsiooni kohta leiate soovitusi meetmest M 4.95 Minimaalne operatsioonisüsteem . Enne koolitusarvutite kasutamist tuleb kindlaks teha, milliseid rakendusi ja kommunikatsiooniliideseid eelseisva koolituse jaoks vajatakse. Koolitusarvutite standardse konfiguratsiooni väljatöötamisega (vt M 2.69 Tüüpsete tööjaamade rajamine) saab vähendada installeerimisele kuluvat tööaega ja tagada minimaalse turbeastme rakendumise. Enne iga koolitust tuleb kontrollida, kas arvutite konfiguratsioon vastab koolituse vajadustele. Aeganõudvate kontrollide vältimiseks tuleks selleks otstarbeks luua eraldi tarkvarapaketid ja need lihtsalt enne iga kasutust uuesti installeerida (vt M 4.109 Tööjaamade tarkvara reinstalleerimine).

Koolitusarvutid ei tohiks võimaldada andmete (koolitusmaterjalide ja teadmiste kontrolli materjalide) lihtsat ja kontrollimatut kopeerimist ning lisaks sellele peaksid need tõkestama ka igasuguste täiendavate teenuste ja programmide (nt eksami spikrite) paigaldamist. Seetõttu tuleb nende arvutite kasutajatele anda piiratud kasutajaõigused ning tõkestada andmete võimalikku teisaldamist välistele andmekandjatele (vt lisaks M 4.4 Eemaldatavate andmekandjate draivipilude ja väliste andmekandjate nõuetele vastav kasutamine). Lisaks tuleks läbi mõelda, mil määral on andmetest, näiteks harjutusülesannetest või eksamitulemustest, tarvis luua varukoopiaid.

Juhul, kui koolitusarvutite operatsioonisüsteemis turvaprogrammid puuduvad, tuleks need täiendavalt installeerida. Eriti mõistlik oleks paigaldada tervikluse kontrollimise programm (vt M 4.93 Regulaarne tervikluse kontroll) ja tarkvarapakettide filter. Soovitav on installeerida ka viirusetõrjet ja logianalüüsi võimaldavad programmid.

Täiendav kontrollküsimus:

- Kas kõikide koolitusarvutite konfiguratsioon on turvaline?

M 4.253 Nuhkvara tõrje

- Asutuse turvapoliitikat tuleb nuhkvara ohtude osas ajakohastada.
- Töötajaid tuleb koolitada või sisevõrgu kaudu teavitada.
- Brauseris blokeerida aktiivsisu *(ActiveX, JavaApplets, JavaScript)* käivitus.
- Pidevalt ajakohastada tarkvara
- Kontrollida andmevahetust võrgus, soovimatu liikluse avastamiseks; soovitatav on kasutada IDSi.
- Kui viirusetõrjevahend ei toeta nuhkvara avastamist, installeerida lisavahend süsteemidesse või lüüsi.

M 4.254z Juhtmeta klaviatuuri ja hiire turvaline kasutuselevõtt

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator, kasutaja

Juhtmeta klaviatuurid ja hiired on perifeeriaseadmed, mis suhtlevad kas raadiolevi või infrapunaliideste kaudu vastuvõtumoodulitega, mis on omakorda kas läbi COM-pordi, PS2-liidese või USB-ühenduse arvuti külge ühendatud. Kuna neil puudub galvaaniline ühendus arvutiga, vajavad juhtmevabad seadmed eraldi toidet kas patareide või akude näol. Kuna need seadmed ei suuda korraga väga palju energiat salvestada, pole nende katkestusteta tööaeg väga pikk. Tehnika arengu hetkeseisu arvestades tarbivad infrapunal töötavad seadmed rohkem voolu kui need, mis töötavad raadioleviga. Kõikide süsteemide töösagedused jäävad litsentsivabasse vahemikku. Enamik juhtmevabu klaviatuure ja hiiri edastavad oma signaale laiusel 27 MHz ning on varustatud kahe levikanaliga, mõningad juhtmevabad seadmed töötavad ka sagedusel 2,4 GHz.

Raadiosignaalil töötavate seadmete leviala on reeglina kaks kuni viis meetrit. Vastupidiselt infrapunal toimivate süsteemidele pole raadiosignaali puhul saatja ja vastuvõtja vahel otsest „silmsidet“ tarvis. Seadmete tööraadius sõltub väga suurel määral ümbritseva kasutuskeskkonna tingimustest. Kõik teised samas sagedusalas töötavad seadmed nagu näiteks raadiotelefonid, raadioleviga mänguasjad, puldist juhitavad garaažiuksed ja 2,4 GHz sagedusel töötavad WLAN-ühendused võivad nende süsteemide tööd pärssida ja leviala vähendada. Metallist tõkked (terasarmatuurid, teraskapid jms) võivad vastava tehnika töökorrast välja viia. Raadiolevil toimivate seadmete valmistajad nimetavad tooteinfos tööraadiusena kaugust, mille piires toimib nende seadmete andmeedastus ilma tõrgeteta. Odava vastuvõtutehnoloogiaga varustatud seadmetel on nimetatud tööraadius aga reeglina palju väiksem kui vahemaa, mille sees oleks antennide ja kõrgkvaliteetse vastuvõtuelektroonika abil suunatud signaalide vastuvõtmine, salvestamine ja analüüsimine veel võimalik. Seetõttu ei ole võimalik välistada pealtkuulamise ohtu suuremas levialas kui seadme tegelik tööraadius.

Raadiosidel töötavate seadmete üheks probleemiks on ebapiisav pealtkuulamiskindlus. Seadmetest väljuvaid signaale on kolmandatel osapooltel võimalik vastu võtta ja salvestada. Juhul, kui need raadiosignaalid ei ole turvaliselt krüpteeritud, muutuvad vastavad andmed teistele kergesti ligipääsetavaks. Poodide tootevalikus leidub hulgaliselt juhtmevabu klaviatuure, mis edastavad klahvivajutusest tekkivaid signaale täiesti krüpteerimata kujul ning muudavad need seeläbi kolmandatele osapooltele täiesti pealtkuulatavaks. Vastuvõetud signaalide nähtavaks muutmiseks mõnes teises arvutis läheb tihti tarvis vaid sama tootja täiendavat vastuvõtjat.

Infrapunatehnoloogial töötavad süsteemid kasutavad enamasti Infrared Data Associationi IrDA standardit. IrDA standard ei sisalda aga mitte ühtki turvameedet, mis kaitseks andmesidet pealtkuulamise eest. Andmeid turvatakse vaid

protokolli tasandil ülekandel tekkivate vigade vastu ning selleks rakendatakse kontrollsummaprotseduure. Turvamehhanisme nagu autentimist, krüptograafilist tervikluse kaitset ja krüpteerimist nende hulgas ei eksisteeri. Vähesel määral kaitseb andmete edastamist infrapunakiirte väga piiratud tööraadius ja vajaminev „silmside“. Võimaliku hajukiirguse tõttu on aga nende süsteemide turbeaste siiski madalam kui kaabliühendusega süsteemidel. Mõningad tootjad on turule toonud ka omapoolsete turvalahendustega tooteid. Selliste lahenduste turvalisuse kohta pole võimalik andmeid esitada, kuna neis kasutatud algoritmid on reeglina tootjate poolt salastatud. Sama konstruktsiooniga seadmete paralleelseks kasutamiseks on tootjad varustanud need erinevate tunnusnumbritega. Märgistamisel rakendatakse erinevaid põhimõtteid, näiteks määratakse ID-de kogumikust ühele seadmele kindel väärtus või valib tarkvara patarei vahetamisel välja mõne uue ID. Saadaval on ka tooteid, mis toimivad läbi Bluetooth-liidese. Bluetoothi turvamehhanismide korrektsel rakendamisel ja konfigureerimisel pakuvad need reeglina suuremat kaitset kui tootjapoolse tehnikaga raadiosidel töötavad süsteemid. Lõpetuseks olgu ära märgitud, et klaviatuuride puhul eksisteerib nende klaviatuurimaatriksi ja ühenduskaabli elektromagnetilise kiirguse tõttu pealtkuulamise oht (vt HS.77 Kiirgusturve). Sama kehtib ka juhtmevabade klaviatuuride kohta. Pealtkuulamisega seotud riskid on aga juhtmeühendusega klaviatuuride puhul enamasti märgatavalt väiksemad kui juhtmevabade klaviatuuride sidekanalitest tekkivad riskid.

Paljud raadiosidel töötavad klaviatuurid ja hiired saadavad oma andmeid kas läbi raadiolainete või infapunavalguse arvutitesse ilma turvameetmeid rakendamata. Seda infot on võimalik kolmandatel osapooltel ilma suurema vaevata lugeda ja võib-olla koguni manipuleerida. IT-turbe seisukohast tuleks selliste seadmete kasutamisest seega üldjuhul loobuda. Tooteid, mis on varustatud valmistajafirma enda välja töötatud sertifitseerimata turvamehhanismidega, pole võimalik turbe väärtuse seisukohast hinnata. Kasutaja võtab siinkohal endale riski, kuna valmistajafirma enda välja töötatud ja laialdaselt hindamata toode ei pruugi pakkuda piisavalt kõrget turvet, et andmeid efektiivselt kaitsta. Juhtmevabad süsteemid, mis põhinevad standarditel nagu Bluetooth ja mille turvamehhanismid on korrektselt kasutusele võetud ja sisse lülitatud, pakuvad eelmistega võrreldes palju suuremat kaitset. Tundlikes valdkondades tuleks aga reeglina alati raadiolevil töötavatest klaviatuuridest ja hiirtest ning infrapunatoodete kasutamisest loobuda.

M 4.255 Infrapunaliidese kasutamine

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator, kasutaja

Infrared Data Association (IrDA) on avaldanud spetsifikatsioone, mis defineerivad algselt protokolli alumistes kihtides asuva infrapunaliidese, mille puhul kasutatakse infrapunakiirguse kujul olevat valgust lühidistantsidel aset leidva andmeedastuse kandjana. Tänaseks on IrDA jõudnud juba erinevate kasutusvaldkondade jaoks välja töötatud kõrgemate protokollideni. IrDA'd toetavad nüüdseks kõik levinud operatsioonisüsteemid ning pihuarvutites ja mobiiltelefonides kasutatakse seda laialdaselt nii seadmete omavaheliseks suhtlemiseks kui ka suhtlemiseks arvutitega. IrDA standard ei sisalda aga mitte ühtki turvameedet, mis kaitseks andmesidet pealtkuulamise eest. Andmeid turvatakse vaid protokolli tasandil ülekandel tekkivate vigade vastu ning selleks rakendatakse kontrollsummaprotseduure. Turvamehhanisme nagu autentimist, krüptograafilist tervikluse kaitset ja krüpteerimist nende hulgas ei eksisteeri. Vajadusel tuleb need juurutada rakenduse tasandil. Vähesel määral kaitseb andmete edastamist infrapunakiirte väga piiratud tööraadius ja vajaminev „silmside". Võimaliku hajukiirguse tõttu on aga nende süsteemide turbeaste siiski madalam kui kaabliühendusega süsteemidel.

IrDA-liidesega varustatud seadmete kasutamisel tuleb jälgida, et vastav liides käivitataks ainult vastaval vajadusel. Kuna protokollis autentimist ette ei ole nähtud, võib täiesti suvaline isik läbi IrDA-liidese andmeid seadmesse edastada. Näiteks mobiiltelefon, mille IrDA-liides on sisse lülitatud, võtab vastu SMS'e, et neid edasi saata. Pihuarvutisse ja sülearvutisse saab IrDA-liidese vahendusel saata programme, mis võivad muuhulgas sisaldada ka kahjulikke funktsioone. Lisaks kõigele koormab sisselülitatud IrDA-liides veel ka mobiilse seadme patareisid või akut. Kuna ühendamisvõimalus piirdub väga väikese alaga, on andmeside pealtkuulamine enamikel juhtudel välistatud. Allesjäävat pisikest jääkriski, mis on tingitud IrDA-komponentide hajukiirgusest, on võimalik minimeerida täiendavate turvamehhanismidega (nt rakenduse tasandi autentimise ja krüpteerimisega) või asendades IrDA-ühenduse juhtmeühendusega.

Kuna ühendamisvõimalus piirdub väga väikese alaga, on andmeside pealtkuulamine enamikel juhtudel välistatud. Olemasolevat vähest jääkriski, mis põhineb IrDA-komponentidel, saab veelgi minimeerida, kasutades täiendavaid turbemehhanisme (nt autentimine ja krüpteerimine rakenduse tasemel) või IrDA kasutamine juhtmeühenduse ülekande kaudu.

Kontrollküsimused

- Kas kõikide IT-komponentide IrDA-liidesed on sel ajal, mil neid tarvis ei lähe, välja lülitatud?

M 4.256 SAP süsteemi turvaline installeerimine

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator

SAP-süsteemi installeerimisel tuleb arvestada järgnevalt kirjeldatud aspektidega, kuna süsteemi turvalisusele pannakse alus juba installeerimisfaasis.

Rakendatava operatsioonisüsteemi turvamine

SAP-süsteemi komponendid installeeritakse IT-süsteemi programmidena ning neid käitatakse protsessidena. Seetõttu on SAP-süsteemi turvalisuse tagamiseks oluline ka rakendatava operatsioonisüsteemi turvalisus (vt M 4.257 SAP-installatsioonikaustade turvamine operatsioonisüsteemi tasandil). Modelleerimisel tuleb arvestada ja rakendada asjasse puutuvaid IT-etalonturbekataloogide mooduleid. Lisaks tuleks IT-süsteeme karastada (ing. k. *hardening*), st kõik ebavajalikud teenused ja programmid desaktiveerida või veelgi parem, eemaldada. Täiendavat infot leiate meetmest M 2.346 SAP dokumentatsiooni kasutamine .

Installeerida tuleb ainult vajalikud komponendid

SAP-süsteem koosneb reeglina paljudest erinevatest komponentidest. Kõikvõimalikud komponendid, mis kasutust ei leia, kätkevad endas aga turvariske, kuna need unustatakse tihti ära ning seetõttu jäävad nende konfiguratsioonid oludele kohandamata. SAP-süsteemi jaoks on eriti oluline vastu võtta otsus, kas reaalselt läheb tarvis ainult ühte või kahte pinu (seda muidugi juhul, kui rakendatava süsteemi versioon nende eraldi installeerimist võimaldab). Kui süsteem seda ei võimalda, tuleb ebavajalik pinuosa muuta turvaliseks nõnda, et selle funktsioonide volitusteta kasutamine oleks välistatud.

Turvaliste paroolide valimine

Olulisi autentimisandmeid tuleb süsteemi sisestada juba installeerimise käigus. Olulisteks andmeteks on näiteks tehniliste kasutajate paroolid, mida SAP-süsteemi komponendid (nt Java pinu ja ABAPi pinu vahelist kommunikatsiooni tagavad komponendid) kasutavad sisekeskkonna sideühenduste autentimisel. Tuleb jälgida, et selleks otstarbeks valitaks turvalised paroolid. Vastavad paroolid peaksid lähtuma paroolidele kehtestatud organisatsioonisisestest ettekirjutustest. Uus parool tuleb kindlasti sisestada ka neil juhtudel, kus installeerimise rutiin on parooli juba ette andnud. SAP-süsteemi jaoks riskianalüüsi tehes tuleks arvestada, et sel administraatoril, kes installeerib SAP-süsteemi ja määrab paroolid, on potentsiaalne võimalus SAP-süsteemi turvamehhanismidest mööda hiilida. Tehnilistel kasutajatel, kelle jaoks tuleb sisestada paroolid, on reeglina suured priviileegid. Seetõttu peavad usaldusväärsed administraatorid vastavad paroolid pärast installeerimistööde lõppu ära muutma. Alternatiiviks on paroolide sisestamine „nelja silma“ põhimõtet järgides, mille puhul kumbki administraator sisestab paroolist ainult talle teada oleva poole. Eriti kehtib see väljasttellimise puhul. Parooli pikkust valides tuleb arvestada, et ABAPi ja Java pinu puhul kehtivad erinevad piirangud:

ABAPi pinu paroolid võivad olla kuni kaheksakohalised. Suur- ja väiketähti siinkohal ei eristata. Java pinu kohta aga eelnimetatud piirangud ei kehti. Paroolide sisestamise valdkonna puhul tuleb seega arvestada, kas vastav tehniline kasutaja luuakse ABAPi või Java pinu alla.

Seadistusega määratud paroolid tuleb kehtivate paroolisuuniste nõuete kohaselt dokumenteerida ja hoiule panna. Viiteid paroolide koostamise kohta leiate muuhulgas ka meetmest M 2.11 Paroolide kasutamise reeglid .

Installeerimisallikate turvamine
SAP-süsteeme ei installeerita reeglina otse CD või DVD pealt. Installeerimiseks vajalike andmete kättesaadavaks tegemiseks kasutatakse enamasti kas lokaalset või võrgus asuvat kataloogistruktuuri. CD-del või DVD-del hoitavad andmed kopeeritakse nendesse kataloogidesse. Andmeid ei ole soovitav hoida lokaalse koopiana selles arvutis, kuhu on installeeritud SAP-süsteem, vaid eraldi arvutis. Andmetele saab sel juhul juurde pääseda võrgu kaudu. Suuremates ametiasutustes ja ettevõtetes võib seda kataloogi kasutada täiendavate SAP-süsteemide installeerimiseks. Juhul, kui süsteeme ei installeerita eraldiseisva ja varjestatud võrgusegmendi alla, on mõttekas installeerimisarvuti selleks ajaks, mil seda ei vajata, võrgust lahti ühendada. Installeerimiskataloogide juurdepääsud on soovitav operatsioonisüsteemide vahenditega turvalisemaks muuta nõnda, et neile pääseksid ligi ainult volitatud administraatorid. Eriti oluline on, et volitusteta administraatoritel ei oleks installeerimisallikatele kirjutamisõigusega juurdepääsu, kuna see võimaldaks neil andmeid muuta. Kui installeerimisallikaid hoitakse lokaalsete koopiatena SAP-süsteemiga arvutites, on soovitav need pärast installeerimistööde lõppemist sealt ära kustutada.

SAP-juhiste rakendamine installeerimistöödel
SAP-süsteemi installeerimisjuhend sisaldab reeglina suurt hulka viiteid SAP-juhistele, mis annavad nõu, kuidas süsteemi kõige paremini installeerida ja kuidas lahendada installeerimisel tekkivaid probleeme. Enamikel juhtudel viitavad dokumentatsioonis toodud SAP-juhised ka veel omakorda teistele SAP-juhistele, mille tagajärjel võib kokku kuhjuda päris suur hulk informatsiooni. Asjakohased juhised tuleks kokku koguda juba installeerimistööd ette valmistades. Enamikel juhtudel piisab alustuseks, kui lugeda installeerimise dokumentatsioonis viidatud juhiseid ja viia läbi täiendav iteratsioonisamm. Tihti antakse viidetes veel ka täiendavat infot selle kohta, kas info tuleb kohustuslikus korras läbi töötada või tuleb seda rakendada ainult teatud tingimustel. Soovitame tungivalt kogu olulise info ka reaalselt läbi töötada, kuna vastasel korral võivad kergesti tekkida vigased installatsioonid. Eriti neil juhtudel, kus SAP-süsteemi installeerimine on küll lõpetatud, kuid selle käigus tekkis vigu, on võimalik, et teatud SAP-süsteemi funktsioonid ei ole täielikult töökorras. Selle kõigel võib olla ka turvalisust mõjutavaid tagajärgi, mistõttu tuleks alati eesmärgiks seada ilma vigadeta lõpuni viidud installeerimine. Veateateid võib ignoreerida vaid juhul, kui SAP-süsteemi installeerimisjuhised seda konkreetselt lubavad. SAP-juhiseid vahendab SAP Service Marketplace (vt M 2.265 Digitaalallkirjade õige kasutamine arhiveerimisel). SAP-juhised on soovitav välja printida ning pärast nende läbitöötamist tuleks need lisada süsteemi dokumentatsiooni hulka.

Värskeimate SAP-turvajuhiste kaasamine
Aina rohkem ja rohkem leidub tooteid, mille kohta on väljastatud SAP-turvajuhised. Vaatamata sellele, et nende turbealaste soovituste kvaliteet võib olla väga erinev, on siiski mõttekas neid juhiseid iga installeeritava SAP-komponendi puhul kasutada. Teatud ajavahemike tagant neid turvajuhiseid uuendatakse, mis tõttu tuleks ka juba installeeritud süsteemide puhul arvestada võimalike uuemate juhistega. Turvajuhiseid väljastatakse eelisjärjekorras uuenenud süsteemi- ja tooteversioonide kohta. Selle vaatamata on ka vanemate, R/3 süsteemide käitajatel soovitav kasutada ajakohastatud tooteversioonide turvajuhiseid, kuna palju soovitusi saab kas otse üle võtta või tuleb neid ainult natukene kohandada. SAP-turvajuhistele pääseb ligi SAP Service Marketplace'i kaudu (vt M 2.346 SAP dokumentatsiooni kasutamine).

Andmebaasi turvaline installeerimine ja konfigureerimine
Andmebaas, mida SAP-süsteem oma töös pidevaks andmete säilitamiseks kasutab, on kriitiline komponent, mida tuleb ilmtingimata kaitsta volitamata juurdepääsude eest. Lisaks üldistele aspektidele, mis käsitlevad andmebaasi turvalist installatsiooni, tuleb arvestada ka spetsiifilisemate soovitustega meetmest M 4.269 SAP süsteemi andmebaasi turvaline konfiguratsioon . Andmebaaside turvalisust käsitleb ka moodul B 5.7 Andmebaasid .

SAP-süsteemimaastiku turvaline installeerimine ja konfigureerimine
Vastavalt planeeritud süsteemimaastikule (vt M 2.341 SAP kasutuselevõtu planeerimine), tuleb installeerida puudutatud SAPi ja mitte-SAPi komponendid (nt tulemüürid).

Täiendavad kontrollküsimused:

- Kas kõik installeerimise raames valitud paroolid on turvalised?
- Kas installeerimisallikaid kaitsti volitamata juurdepääsude eest?
- Kas installeerimise käigus rakendati kõiki olulisi SAP-juhiseid?
- Kas SAPi oluliste turvajuhiste soovitused on ellu rakendatud?

M 4.257 SAP-installatsioonikaustade turvamine operatsioonisüsteemi tasandil

Algatamise eest vastutavad: infoturbe osakond, IT-juht
Rakendamise eest vastutavad: administraator

SAP-süsteemi installeerimise käigus ekstraheerib installeerimisprogramm algul installeerimisallikates (nt võrgus asuvas kataloogis, CD-l, DVD-l) hoitavad andmed mõnda installeerimiskataloogi (nt /sapinst). Selles kaustas installeerimise ajal aset leidvad sündmused logitakse. Sõltuvalt installatsiooniprogrammist võivad logifailid sisaldada ka konfidentsiaalset infot. Siia alla kuuluvad näiteks valitud SAP System-ID-d (SAPSID-d), lokaalseid arvuteid kajastav info (nt IP-aadress, arvuti nimi), tehniliste kasutajate valitud nimed. Loetava teksti kujul võivad esineda aga ka installeerimise käigus sisestatud paroolid. Eriti kehtib see vanemate installeerimisprogrammide versioonide kohta. Seetõttu on pärast installeerimistööde lõpetamist soovitav toimida järgnevalt:

- Kogu installeerimiskataloogist tuleks luua varukoopia. Andmete varundamine tuleks teostada selliselt, et volitamata isikutel ei oleks võimalik nendele andmetele ligi pääseda.
- SAPi installeerimisel tekkinud probleemide korral tuleb andmete varukoopiad ja protokollid lasta üle vaadata SAPi ekspertidel. Selleks otstarbeks võib need saata kas SAP-le või pöörduda SAPi nõustajate poole. Seetõttu peab volitatud administraatoritel niisugustel juhtudel olema võimalus neile andmetele ligi pääseda. Juhtudel, kus andmed saadetakse SAP-le või kui need tehakse kättesaadavaks kolmandatele isikutele, tuleb arvestada, et seeläbi usaldatakse nende isikute kätte konfidentsiaalne info. Seetõttu tuleb eelnevalt sõlmida vastavad konfidentsiaalsuslepped.
- Seejärel võib installeerimiskataloogi installeeritud süsteemist ära kustutada.

Sõltuvalt SAP-süsteemi turbevajadustest võib olla mõttekas analüüsida logiandmeid, et selgitada, kas need sisaldavad loetaval kujul paroole, mida kolmandad osapooled võiksid enda huvides ära kasutada ning need paroolid kas kustutada või maskeerida. Nimetatud meedet rakendavad uuemad installeerimisprogrammide versioonid automaatselt juba logide koostamise käigus nõnda, et *support* -funktsioonid selle all ei kannata, juhul, kui muudetud logifaile on *support* -juhtumite raames tarvis kasutada.

Täiendav kontrollküsimus:

- Kas installeerimiskataloogist on tehtud varukoopia ja kas see on seejärel süsteemist ära kustutatud?

M 4.258 SAPi ABAP-pinu turvaline konfiguratsioon

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator

ABAP-pinu kujutab endast SAP-süsteemi traditsioonilist käitamiskeskkonda. Eelkõige kehtib see nende süsteemiversioonide suhtes, mis kannavad tähistust SAP R/3, kuna R/3 komponentide ja moodulite käitamine leiab aset ABAP-pinus. ABAP-pinu algne konfigureerimine on väga töömahukas ja koosneb paljudest üksiketappidest. Tööde maht kasvab veelgi, kui lisaks puhta SAP-baasi konfigureerimisele tuleb konfigureerida veel ka rakendusi ja mooduleid, nagu seda näiteks R/3-süsteemide puhul teha tuleb. Selleks tuleb ametiasutuse või ettevõtte kõik olulised tööprotsessid konfiguratsiooni (*Customizing*) või ABAP-koodi kohandamisega järgi ehitada. Järgnevalt kirjeldatakse turbe seiskohast olulisi tööetappe, mida tuleb järgida ABAP-pinu algse konfiguratsiooni loomisel. Näited piirduvad SAP-baasi konfiguratsiooniga ja ei kajasta seetõttu ei mooduleid ega ka rakendusi.

Käitamise mandandi määratlemine
Esmalt tuleb SAP-süsteemi käitamiseks kindlaks määrata selle mandant. Mandandi mõiste (*Client*) käsitleb SAP-süsteemi tehnilist alajaotust. Seda ei tohiks segi ajada mandandi mõistega tavapärase kliendi tähenduses. Pärast installeerimist ei tohi kasutada olemasolevaid standardseid mandante numbritega 000 (SAP referentsmandat), 001 (käitamist ettevalmistav mandant), ja 066 (*Earlywatch* -mandant). SAP-süsteemis võib eksisteerida mitmeid erinevate kasutusotstarvetega mandante. Kõik SAP mandandid on omavahel aga seotud läbi SAP-referentsmandandi, kus leiavad aset konfigureerimised, mis kehtivad globaalselt, tervele SAP-süsteemile. Turbe seiskohast tuleks seada eesmärgiks, et SAP-süsteemis ei käitataks üheskoos väga erinevate turbenõuetega mandante. Nii näiteks ei tohiks SAP-süsteemis mitte kunagi üheskoos käitada produktiivmandanti ja arendusmandanti. Üheskoos käitamisel saavad arendajad muuta ka mandantidest sõltumatuid objekte, millel on omakorda otsene mõju produktiivmandandile. Seetõttu tuleb need ilmtingimata teineteisest eraldada.

Turbe seisukohalt oluliste IMG-tegevuste läbiviimine
SAP-süsteemi konfigureerimiseks vajalikke tööetappe sisaldab SAPi Implementation Guide (IMG, SAP Reference IMG), mis on SAPi eeldefineeritud süsteemisisene loetelu. Loetelu on hierarhilise ülesehitusega ning see on viidud kooskõlla vastava süsteemiversiooni ja installeeritud komponentidega. Lisaks selle on IMG-sid võimalik koostada ka ise (Project IMG-sid), mis sisaldavad ainult süsteemi kasutamiseks hädavajalikke, SAPi Reference IMG-st võetud konfigureerimisetappe. IMG-d pakuvad veel ka võimalust fikseerida, millised konfiguratsioonid on juba tehtud, ning nii saab tehtud töödest alati ülevaate. Meetmes M 2.346 SAP dokumentatsiooni kasutamine sisaldub viide SAPi IMG dokumentatsioonile, millega tuleks arvestada. Kõik planeerimise raames kindlaks määratud IMG-tegevused (vt lisaks M 2.341 SAP kasutuselevõtu planeerimine) tuleb läbi töötada. Kõikidel juhtudel tuleb läbi viia järgnevad IMG-tegevused:

- Aktiveerige HTTP-Services või desaktiveerige, juhul, kui neid hiljem tarvis ei lähe (transaktsioon: SICF), vt lisaks M 5.127 SAP Internet Connection Framework (ICF) kaitse .
- Jagage välja IDOC-liidese volitused (transaktsioon: PFCG), vt lisaks M 5.128 SAP ALE (IDoc/BAPI) liidese kaitse .
- Jagage välja RFC liideste volitused (transaktsioon PFCG), vt lisaks M 2.342 SAP pääsuõiguste planeerimine ja M 5.126 SAP RFC liidese kaitse .
- Seadke sisse IDOC-administreerimine (transaktsioon: OYEA), vt lisaks M 5.128 SAP ALE (IDoc/BAPI) liidese kaitse .
- Content-Server Administration (transaktsioon: CSADMIN), vt lisaks M 5.129 SAP süsteemide HTTP teenuste turvaline konfiguratsioon .
- Konfigureerige Internet Connection Manageri (ICM) profiili parameetrid (transaktsioon SMICM, *Jump* , *Parameters*).
- Defineerige Proxy konfiguratsioon (transaktsioon SM30 THTTP-ga).
- Viige läbi kõik tegevused, mis kuuluvad mõiste alla „Süsteemi administreerimine“.

IMG-tegevused puudutavad muuhulgas ka järgnevalt kirjeldatud meetmeid. Kui neil meetmetel on aga turbe seisukohast vägagi oluline roll, toome need siinkohal eraldi välja.

Profiili parameetrite kohandamine
Profiili parameetritega saab konfigureerida SAP-süsteemi peamisi funktsioone. Seetõttu tuleb konfigureerimistööde käigus ka profiili parameetreid vastavalt vajadustele kohandada. Kuna profiile eksisteerib erinevates versioonides (nt *Start* -profiil, *Default* -profiil, *Instance* -profiil), peavad administraatorid ennast profiilimehhanismiga kurssi viima. Reeglina tuleb iga üksiku profiili parameetri jaoks defineerida selle poolt rakendatav seadistus. Turbe seisukohast väärivad erilist tähelepanu järgnevad parameetrid:

- kõik parameetrid eesliitega „auth/“,
- kõik parameetrid eesliitega „login/“,
- kõik parameetrid eesliitega „snc /“, juhul, kui SNC-d kasutatakse,
- kõik parameetrid eesliitega „ssf/“, juhul, kui SSF-i kasutatakse.

Profiilide haldamiseks tuleks kasutada transaktsiooni RZ10. Hoiduda tuleks failisüsteemi tasandi käsitsi muutmisest. Profiili parameetrite kuvamiseks võib kasutada raportit RSPARAM, mis käivitatakse transaktsiooniga SE38. Profiilide faile tuleb operatsioonisüsteemi tasandil kaitsta volitamata juurdepääsude eest. Täiendavat infot profiilidega ümberkäimise kohta leiate meetmest M 2.346 SAP dokumentatsiooni kasutamine .

Süsteemi muutmisvõimaluste konfigureerimine

Süsteemi muutmisvõimalused tuleb seadistada vastavalt SAP-süsteemi rollile. Seadistusega määratakse kindlaks, kas sisemisi süsteemikomponente ja rakenduste komponente üldse tohib muuta või mitte. Selles on puudutatud näiteks ABAP-System-Code, reeglina ka kõik Data Dictionary (DDIC) objektid ja objekti nimeruum. Tootmissüsteemide puhul on soovitav kehtestada süsteemi muutmisvõimalusena globaalne seadistus „mittemuudetav“. Sel juhul on võimalik muudatusi sisse viia ainult transportsüsteemi vahendusel. Tootmissüsteemidele on see lahendus vägagi sobilik, kuna muudatusi saab sel juhul teha vaid läbi defineeritud protseduuride ja tööetappide. Siinkohal on oluline, et struktureeritud muudatuste haldamise protsess oleks defineeritud ja et seda ka järgitaks, vt lisaks M 4.272 SAP transportsüsteemi turvaline kasutamine . Sama seadistus nagu tootmissüsteemidel, st globaalne seadistus „mittemuudetav“, tuleks kehtestada ka testimissüsteemidele ja kvaliteeditagamise süsteemidele. Muudatused tuleb ette võtta arendussüsteemis ning pärast kvaliteedi tagamise protsessi läbimist tuleks need salvestada esmalt kvaliteedi tagamise süsteemi ning seejärel ümber kanda tootmissüsteemi. Arendussüsteemide puhul tuleks kõikide nende komponentide seadistuseks, mida arendustegevus otseselt ei puuduta, määrata „mittemuudetav“. Seevastu need komponendid, millega arendustööd tehakse, tuleks varustada seadistusega „muudetav“. Süsteemi muutmist käsitlevate seadistusteni saab jõuda kas transaktsiooniga SE06 või SE03. Täiendavat ja täpsemat infot leiate antud teema kohta meetmest M 2.346 SAP dokumentatsiooni kasutamine .

Mandantide konfigureerimine

Lisaks SAP-süsteemiterviku kaitsmisele võimalike muudatuste vastu saab muudatuste vastu kaitsta ka mandante eraldi, tõkestades mandantidest sõltuvate omaduste muutmist. Seda seadistust tuleks kasutada kõikide produktiivmandantide puhul. Vastava seadistusega mõjutatakse veel ka seda, kas mandantide muutmine registreeritakse automaatselt nõnda, et pärast kontrollimist oleksid need kohe saadaval transportimise töökäsuna, mida oleks võimalik transportida teistesse samade seadistustega käitavatesse mandantidesse. Muudatuste haldamise kontseptsioonis peab olema kindlaks määratud, millisest skeemist lähtuvalt jagatakse mandantide vahel muudatusi laiali ja millised on mandantide kasutusotstarbed (nt produktiivmandant, testimismandant, arendusmandant). Seadistusi saab teha transaktsiooniga SCC4. Oma produktiivmandandile on soovitav teha järgnevad seadistused (teadmiseks: seadistusväärtuste nimetused leiate samas lühendatud kirjaviis eest ka SAP-süsteemis):

- Mandandi roll: „ *Productive client* “.
- Mandantidest sõltuvate objektide muutmised ja transportimised: „muudatusi mitte lubada“.
- Mandantideüleste objektide muutmised: sks. k. „ *keine Änderungen von Repository- und mand.unabh. Cust.-Obj* .“.
- Mandantide kopeerija (*client copier*) ja võrdlustööriista kaitse: „Kaitseklass nr 2: keelata ülekirjutamine, keelata väline käideldavus“.
- Piirangud CATT-i ja eCATT-i käivitamisel: „keelata eCATT ja CATT“.

Vastavad seadistused peaksid kehtima testimis- ja vastuvõtusüsteemis. Teistele mandantidele (arendus, koolitus, Demo) tuleb seadistusi vastavalt kohandada. Administraatorid peavad olema väga täpselt kursis mandantide konfigureerimise võimalike tagajärgedega. Viiteid asjakohase detailsema dokumentatsiooni kohta leiate meetmest M 2.346 SAP dokumentatsiooni kasutamine .

Operatsioonisüsteemi käivitusfunktsiooniga käskude turve
ABAP-pinus on võimalik käivitada operatsioonisüsteemi käskusid. Käsud käivitatakse operatsioonisüsteemi tehnilise kasutaja operatsioonisüsteemi volitustega, mille all SAP-süsteem töötab. Reeglina on nende puhul tegu laialdaste administraatoriõigustega. Seetõttu peab juurdepääs nendele funktsioonidele olema kaitstud. Ennekõike tuleb tõkestada käskude loomise ja muutmise võimalusi. Seetõttu tuleks rakendada järgmiseid soovitusi:

- Volitusi, mis lubavad käivitada väliseid operatsioonisüsteemikäskusid (volitus S_LOG_COM) või neid hooldada (volitus S_RZL_ADM koos ACTVT=01), tuleb välja jagada ainult vähestele.
- Juurdepääs transaktsioonile SM49 „ *Execute external OS commands* “ tohiks olla ainult volitatud administraatoritel.
- Juurdepääs transaktsioonile SM69 „ *Maintain External OS Commands* “ tohiks olla ainult volitatud administraatoritel.
- Operatsioonisüsteemi käskude jaoks on võimalik ette anda parameetrid, mida tuleb käivitamisel kasutada ja seeläbi saab vältida täiendavate parameetrite juurdelisamist. Seda võimalust tuleks kasutada. Eriti kehtib see enda defineeritud käskude kohta.

Täiendavat ja täpsemat infot operatsioonisüsteemi käskude kaitsmise kohta leiate meetmest M 2.346 SAP dokumentatsiooni kasutamine .

Paroolide kvaliteedi tagamine
SAP-süsteemi juurdepääsu võimaldavate paroolide kvaliteedi tagamiseks tuleks arvestada järgmiste nõuannetega:

Paroolide jaoks tuleb kehtestada minimaalne pikkus. Selleks saab kasutada profiili parameetrit „login/min_password_lng“. Soovitavalt võiks see olla kaheksakohaline. Kaheksakohaline kombinatsioon on samas ka ABAP-pinu parooli maksimaalne pikkus.

Paroolide jaoks tuleks välja töötada omad kriteeriumid, mis reguleerivad nende keerukust. Neid on võimalik seadistada järgnevate profiili parameetritega:

- login/min_password_diff:

minimaalne kogus numbreid ja tähti, mis peavad uues paroolis vanaga võrreldes erinema

- login/min_password_digits:
paroolis sisalduv minimaalne arv numbreid

- login/min_password_letters:
paroolis sisalduv minimaalne arv tähti

- login/min_password_specials:
paroolis sisalduv minimaalne arv viitemärke
Keerukuse jaoks kriteeriume välja töötades tuleks arvestada, et need kehtestaksid läbivalt ühtlased nõuded.

Paroolidele tuleks määrata maksimaalne kehtivusaeg, et süsteem sunniks kasutajaid regulaarselt paroole muutma. Selle konfigureerimiseks saab kasutada profiili parameetrit „login/password_expiration_time“, mis määrab kindlaks päevade arvu, mille möödumisel tuleb parooli muuta. Soovituslik väärtus peaks jääma vahemikku 60 kuni 90 päeva.

Võib defineerida ka paroolid, mida on keelatud kasutada. Neid tuleks hallata tabelis USR40 transaktsiooniga SM31. Sellega tuleks piirata triviaalsete paroolide kasutamisvõimalusi.

Seadistusväärtused tuleb valida kooskõlas kehtiva paroolisuunisega.

Paroolirünnete vastase kaitse konfigureerimine
SAP-süsteemi on soovitav kaitsta paroolirünnete vastu - pärast teatud arvu ebaõnnestunud sisselogimiskatseid ühendus lihtsalt katkestatakse. Vastavat arvu saab konfigureerida profiili parameetris „login/fails_to_session_end“. Korduvalt rünnete osaliseks saanud kasutajakontode kaitsmiseks täiendavate rünnete vastu on soovitav vastavad kasutajakontod pärast teatud arvu ebaõnnestunud sisselogimiskatsete täitumist sulgeda. Vastavat arvu saab konfigureerida profiili parameetris „login/fails_to_user_lock“. Lisaks eelnevale tuleb veel otsustada, kas suletud kasutajakontod muudetakse taas südaööl automaatselt kasutuskõlblikuks, või peab seda tegema administraator käsitsi. Vastavat süsteemi käitumist saab konfigureerida profiili parameetris „login/failed_user_auto_unlock“. Seadistusväärtused tuleb valida kooskõlas kehtiva paroolisuunisega.

Mitmekordsete sisselogimiste tõkestamine

SAP-süsteemid suudavad ära hoida kasutajakonto paralleelsed sisselogimised. Tootmissüsteemides ei ole reeglina eriti mõistlik lubada ühe isiku paralleelseid sisselogimisi ning seetõttu tuleb seda ka takistada. Süsteemi käitumist saab seadistada eraldi nii SAPGui- kui ka RFC-sessioonide jaoks, defineerides profiili parameetrid „login/disable_multi_gui_login“ ja „login/disable_multi_rfc_login“. Enne seda, kui paralleelsed sisselogimised RFC jaoks ära keelata, tuleb tagada, et ühe ja sama kasutajakonto paralleelsed sessioonid oleksid välistatud.

Single Sign-On -i turvaline konfiguratsioon

Erinevate SAP-süsteemide käitamise korral saab kasutajate sisselogimise lihtsamaks muuta funktsiooniga SAP *Single Sign-On* (SSO). Sel juhul ei ole paroole enam tarvis korduvat sisestada, kuna pärast SAP-süsteemi sisselogimist väljastatakse kasutajale Single Sign-On Ticket, mis võimaldab ka teisi SAP-süsteeme kasutada ilma korduva sisselogimiseta. Otsus, kas ja milliste SAP-süsteemide jaoks *Single Sign-On* mehhanismi kasutada, tuleb langetada planeerimisfaasis. Single Sign-On funktsiooni rakendamisel tuleb arvestada järgnevate, turbe seisukohalt oluliste aspektidega:

- Single Sign-On funktsiooni kasutusvõimalusi tuleks konfigureerida ainult usaldusväärsete süsteemide vahel. Turbe seisukohalt lähtudes tuleks Single Sign-On funktsiooni kasutamist kindlasti vältida valdkondades, mis jäävad ettevõtte või ametiasutuse piiridest väljapoole.
- Iga kasutusvaldkonna puhul on soovitav tsentraalse sisselogimise otstarbel kasutada vaid ühte SSO-Ticketeid väljastavat süsteemi. Kõik ülejäänud süsteemid peaksid SSO-Ticketeid ainult aktsepteerima.
- Kasutaja veebilehitseja ja SAP-süsteemi vaheline andmeside tuleb ilmtingimata krüpteerida. Vastasel korral esineb oht, et ründe toimepanijal õnnestub SSO-Ticketit pealt kuulata ja tekitada nii endale juurdepääs ilma SAP-süsteemi sisse logimata.

SAP-süsteemi SSO-konfiguratsiooni reguleerivad järgnevad profiili parameerid:
- login/accept_sso2_ticket:
süsteem aktsepteerib SSO-Ticketeid

- login/create_sso2_ticket:
süsteem väljastab SSO-Ticketeid

- login/ticket_expiration_time:
väljastatud SSO-Ticketite kehtivusaeg tundides

- login/ticket_only_by_https:
SSO-Ticketeid väljastatakse ainult läbi HTTPSi toimuvatele pöördustele

- login/ticket_only_to_host:
SSO-Ticketeid rakendatakse ainult pöördumistel väljastava süsteemi poole

SSO konfigureerimiseks läheb tarvis täiendavaid administratiivseid tegevusi, mille haldamiseks saab kasutada transaktsioone SSO2, SSO2_ADMIN (SSO2_ACL) ja STRUSTSSO2. SAP soovitab kasutada transaktsiooni SSO2. Viiteid täiendavale infole leiate meetmest M 2.346 SAP dokumentatsiooni kasutamine .

Lisaks SAPi SSO-mehhanismile, mis kasutab Ticketeid, saab SSO jaoks kasutada ka väliseid süsteeme. Vastavad süsteemid peavad sellisel juhul kasutama SNC-liidest (Secure Network Communication). Windowsil põhinevate keskkondade puhul (alates Windows 2000) viidatakse võimalusele rakendada *Single Sign-On* funktsiooni tarbeks Kerberost. Sellistel juhtudel leiab sisselogimine aset vaid Windowsi süsteemis. SAP-süsteemi pöördudes pole sellisel juhul enam kasutajanime ega parooli tarvis sisestada. Vajaminev Windows-Kerberos SNC-Provider on standardina juba olemas ning lisakulusid sellega ei kaasne. Selle vaatamata tuleb arvestada, et Windows Kerberos SNC-Provider ei võimalda andmesidet krüpteerida. Seetõttu saab kasutada vaid SNCi baasil autentimist. Alates versioonist Windows 2000 on siiski ka standardina olemas juba võimlaus rakendada arvutite vahel IPSec-i ja tagada nii andmeside üldine krüpteerimine. Otsus, kas selline *Single Sign-On* funktsiooni rakendus on ettevõttele või ametiasutusele vastuvõetav, tuleb langetada iga juhtumi puhul eraldi.

Täiendavaid abinõusid SNCi kohta leiate meetmetest M 5.125 SAP-süsteemi siseneva ja väljuva kommunikatsiooni kaitse , SAPi infoallikad meetmes M 2.346 SAP dokumentatsiooni kasutamine .

Täiendavad kontrollküsimused.

- Kas kõik planeeritud IMG-tegevused on ka ellu viidud?
- Kas tootmissüsteemides on süsteemi muutmise võimalused desaktiveeritud?
- Kas profiili parameetreid on kohandatud vastavalt planeeritule?
- Kas paroolide puhul on tagatud, et need on kvaliteetsed?
- Kas dialoog-kasutaja läbi on tõkestatud paralleelsed sisselogimised?
- Kas *Single Sign-On* funktsiooni kasutatakse turvaliselt ja nii, nagu planeeritud?

M 4.259 ABAP-pinu turvaline kasutajate haldus

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator

ABAP-pinu kasutajate turvaline haldamine on kogu süsteemi turvalisuse eelduseks, kuna sellega määratakse kindlaks kasutajad, kellel on õigus pääseda SAP-süsteemi. Kasutajahalduse valdkonnas tuleb arvestada vähemalt järgnevate aspektidega. Sõltuvalt kasutusvaldkonnast tuleb arvestada veel ka teiste, täiendavate teemadega, mis sõltuvad ametiasutuse või ettevõtte spetsiifikast. Lisaks tuleb arvestada veel ka ettekirjutustega, mis tulenevad seadustest. Täiendavaid viiteid SAP-süsteemide kasutajate haldamist käsitlevatele SAPdokumentidele leiate meetmest M 2.346 SAP dokumentatsiooni kasutamine .

Kasutajatele nimede andmise põhimõtted
Kasutajanimed peavad olema üheselt mõistetavad. Seetõttu tuleb määratleda nimeandmise põhimõtted, mis tagaks selguse ka neil juhtudel, kui inimeste nimed on ühesugused. Reeglina on ettevõtetes ja asutustes töötajate identifitseerimise põhimõtted, näiteks personaalsed numbrikoodid, juba välja töötatud. Kasutajad on mõttekas jaotada klassidesse (sisetöötajad, välistöötajad, partnerid, tehnilised kasutajad) ja need klassid omakorda kasutajanimede sisse kodeerida.

Kasutajate eksimatu identifitseerimine
Kasutajahalduse kontseptsiooniga tuleb tagada, et iga kasutajanimi tähistaks kõikides süsteemides ikka ja alati ainult ühte isikut.
Sobivate töökorralduslike meetmetega tuleb tagada, et üks kasutajakonto ei oleks korraga mitme inimese kasutada (tõkestada *account sharing*).

Avariiadministraatori sisseseadmine
Avariide puhuks tuleks luua eraldi SAP-konto, mida kasutataks avariiliste administreerimistööde tarbeks. Konto nimeks ei ole soovitav valida selle tavapärast tähendust, kuna otstarbele viitav nimi võib provotseerida selle kasutajakonto vastu suunatuid ründeid. Avariiliste administreerimistööde tarbeks ei tohi kasutada kontot SAP*. Avariiadministraatorile antakse reeglina laialdased volitused ning seetõttu tuleb seda kontot kaitsta turvalise parooliga. Avariiennetuse planeerimise raames tuleb välja töötada protseduurid, kuidas vastavat kontot kasutada (vt M 2.341 SAP kasutuselevõtu planeerimine ja M 6.97 SAP süsteemi valmisolek hädaolukorraks). Avariiadministraatori parooli tuleks hoida mõnes turvalises kohas, näiteks seifis. Juurdepääs paroolile peaks olema võimaldatud ainult „nelja silma“ põhimõtet järgides.

Standardsete kasutajate turve
SAP-süsteemis eksisteerib mitmeid standardseid kasutajaid, mida on tarvis kaitsta. Kaitsta tuleb järgnevaid kasutajaid:

- SAP*

- DDIC
- EARLYWATCH
- SAPCPIC
- TMSADM
- SAPSYS
- WF-BATCH (mille loob alles automaatne *Workflow-Customizing*).

Turbe alla kuuluvad järgmised tegevused:

- parooli muutmine (vt ka allpool)
- kasutajatunnuse desaktiveerimine
- teatud lühiajaliste tööde puhul (nt System Update) tuleks kasutajatunnused desaktiveerida. Protseduuride reguleeritud toimimiseks tuleb välja töötada vastavad protsessid. Viimased peavad suutma tagada, et pärast tööde lõppu saaksid kasutajatunnused uuesti tööle lülitatud - kasutajate liigitamine gruppi SUPER

Pärast kasutajatunnuste desaktiveerimist võib funktsioonide töös esineda häireid. Süsteemi kasutusotstarbest sõltub, kas desaktiveerida on tarvis lühema- või pikemaajaliselt ning vastav otsus tuleb langetada iga juhtumi puhul eraldi. Siinkohal tuleb arvestada täiendavate riskidega, mis võivad tekkida standardsete kasutajate uuesti tööle lülitamisel võib-olla teadaolevate standardsete paroolidega. Kasutajaid SAP* ja DDIC ei ole soovitav kustutada, kuna need luuakse automaatselt uuesti, näiteks uue mandandi sisseseadmisel. SAP* kasutaja tööd saab mõjutada profiili parameetriga „logon/no_automatic_user_sapstar“. See parameeter on soovitav aktiveerida. Enne SAP* kasutaja desaktiveerimist peab olema loodud ja töökorda seatud alternatiivne kasutajakonto avariiliste administreerimistööde tarbeks. Uute komponentide installeerimisel võib luua uusi täiendavaid standardseid kasutajaid. Viimased tuleb omakorda pärast installeerimist turvaliseks muuta. Täiendavaid viiteid SAP-süsteemide standardseid kasutajaid käsitlevatele SAP-dokumentidele leiate meetmest M 2.346 SAP dokumentatsiooni kasutamine
.

Standardsete paroolide muutmine
Standardsed kasutajad on varustatud standardsete paroolidega. Kasutajatunnuste volitamata kasutuse tõkestamiseks tuleb need paroolid ära muuta. Pärast paroolide muutmist võib aga tekkida olukord, kus süsteemi funktsioonid ei pruugi enam töötada, või ei tööta enam korrektselt. Niimoodi võib näiteks juhtuda kasutajatega TMSADM (vt lisaks SAP note 139854) ja SAPCPIC. Juhul, kui puudutatud süsteemifunktsiooni kasutatakse sageli, tuleb standardset kasutajat võib-olla käitada standardse parooliga. Antud asjaoluga tuleb riskide analüüsimisel arvestada. Kasutajate SAP* ja DDIC puhul tuleb arvestada, et juhul, kui need kasutajatunnused ära kustutatakse, luuakse need automaatselt uuesti, näiteks uute mandantide sisseseadmisel. Uuesti loodud kasutajatunnused varustatakse standardsete paroolidega. Kontrollimise otstarbel, et selgitada, kas kõik mandandid eksisteerivad, kas neile on kehtestatud tõkkeid, ning kas kasutajatel SAP*, DDIC, SAPCPIC

ja EARLYWATCH on standardsed või muudetud paroolid, saab transaktsiooniga SE38 kasutada raportit RSUSR003.

Haldusprotseduur
Kasutajate halduse puhul tuleb arvestada erinevate haldusprotseduuride kasutusvõimalustega. Juhtudel, kus kasutatakse tsentraalselt töötavat kasutajahaldust, tuleks vältida kasutajakontode loomist lokaalsel tasandil. Nii tsentraalselt kui lokaalselt toimiva kasutajahalduse puhul tuleb rakendada ja järgida asjakohaseid protsesse ja protseduure (vt M 2.341 SAP kasutuselevõtu planeerimine). Protsessid peaksid muuhulgas käsitlema ka erandjuhtudele rakendatavaid reegleid. Rakendatava haldusprotsessi puhul tuleb arvestada järgmiste aspektidega:

- Baashalduse jaoks tuleb välja töötada spetsiaalne töörollide kontseptsioon.
- Haldusalase kontseptsiooni planeerimistööde raames tuleb välja töötada ka töörollide ja volituste muudatuste haldamise põhimõtted. Siinkohal tuleb arvestada sellega, et töörollide muutmise ja rollidesse jaotamise kooskõlastamisprotsessi tuleb kaasata ka igapäevatöö eest vastutavaid isikud ja tööprotsessidega seotud riske, mis tulenevad rollide muutmisest või kasutajate liigitamisest uute töörollide alla, saab analüüsida kas tarkvaratööriistaga „SAP GRC Access Control“ või teiste tootjate tarkvaralahendustega.

Täiendavad kontrollküsimused:

- Kas standardsed kasutajad on kaitstud?
- Kas standardsed paroolid on muudetud?
- Kas isikud ja kasutajakontod on omavahel selgelt seotud, nõnda, et eksimused on välistatud?

M 4.260 SAP-volituste haldus

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator

SAP-süsteemis töödeldavate andmete turvalisus sõltub väga suurel määral kasutajate ja administraatorite jaoks sisse seatud volitustest. Volitustega määratakse kindlaks, millised funktsioonid (SAP-sõnavara kohaselt transaktsioonid) on erinevate kasutajate jaoks kättesaadavad ning milliseid andmeid on kasutajal nende abil võimalik näha ja muuta. Seetõttu on volituste konfigureerimine ja haldamine süsteemi üldise turvalisuse tagamiseks väga olulised ja seda ennekõike valdkonnas, mis puudutab kõikvõimalikke oma organisatsiooni töötajate poolt toimepandud pettusi. SAPi volituste süsteem on väga paindlik, kuid seetõttu on seda ka keeruline konfigureerida. Vastupidiselt operatsioonisüsteemidele, kus volitused jagatakse välja otse objektidele (nt failidele), töötavad SAP-süsteemid lubade põhimõttel: enne funktsiooni kasutamist kontrollitakse, kas kasutajal on olemas teatud tüüpi volitused. Kui kasutajal on vajalikud volitused olemas, kontrollitakse, kas tema volitustesse sisse kantud väärtused vastavad funktsiooni käivitamise eelduseks olevatele nõuetele. Kontrollitavad volituste tüübid ja väärtused määrab siinkohal kindlaks funktsiooni programmeerija ning need võivad arvesse võtta ka andmeid, mis edastati funktsioonile värske pöörduse raames. Funktsiooni programmeerija otsustab viimaks ka selle üle, kas ta rakendab kasutaja suhtes tegelikult hädavajalikku volituste kontrollimist või mitte. Volituste haldamise puhul tuleks arvestada allkirjeldatud soovitustega. Loetelu tuleb kohandada ja täiendada vastavalt kohapealsetele oludele.

Koolitus
Administraatorid, kes vastutavad kasutajatunnuste, rollide, profiilide või volituste haldamise eest, peavad ilmtingimata läbima SAP-volituste kontseptsiooni ja haldamist käsitleva koolituse (tööprotsessid, tarkvaratööriistad, õige kasutus) või tõestama, et neil on olemas asjakohased teadmised. Ainult niimoodi on võimalik tagada, et volitusi hallatakse arukal viisil.

Vastutuste lahutamine („nelja silma“ põhimõte)

Volituste kontseptsioon peab olema välja töötatud selliselt, et vastutused oleksid võimalikult hästi teineteisest eraldatud. Siinkohal tuleb arvestada järgnevaga:

- Kasutajate administreerimisega peaks tegelema vaid üks administraator. See administraator peaks oskama kasutajatunnuseid luua, muuta ja rollidega siduda. Sel administraatoril ei tohi olla volitusi, mis lubavad rolle ja profiile luua ja muuta. SAP võimaldab kasutada sel otstarbel malli SAP_ADM_US.
- Rollide jaoks peaks eksisteerima eraldi administraator, kellel on õigus rolle luua ja muuta, kuid tal ei tohi olla õigusi, mis lubaksid tegeleda kasutajate

ja profiilide loomise ja muutmisega. SAP võimaldab kasutada sel otstarbel malli SAP_ADM_AU.
- Profiilide jaoks peaks olemas olema eraldi administraator. Rolliadministraator tohib genereerida olemasolevate rollide tarbeks profiile, mis ei sisalda süsteemi suhtes kriitilisi volitusi (näiteks S_USER*), kuna viimased tooksid endaga kaasa volitused kasutajate ja rollide haldamiseks. SAP võimaldab kasutada sel otstarbel malli SAP_ADM_PR. Need administraatorid tuleb liigitada grupi alla SUPER.
- Administraatorite haldamiseks on ette nähtud üks eraldi administraator. See administraator tegeleb kasutaja-, rolli- ja profiiliadministraatorite haldamisega. Administraatorite administraator tuleks liigitada profiili S_A.SYSTEM alla, mida läheb tarvis kasutajate haldamiseks kasutajagrupis SUPER. Administraatorite administraatorit tuleks kasutada „nelja silma“ põhimõtet järgides. Näiteks kasutajate administraator võib selle sulgeda ning vastavalt vajadusele uuesti aktiivseks muuta.

Ülesannete lahutamisega (eeldusel, et see on tehniliselt õigesti lahendatud), saavutatakse olukord, kus administraatoritel ei ole võimalik endile ise volitusi välja jagada ning neil on võimalik täita ainult oma tööülesannetest tulenevaid kohustusi. Väikeettevõtetes ja väikestes ametiasutustes võib piiratud inimressursi tõttu tekkida olukord, kus vastavat tööülesannete lahutamist ei saa juurutada ning kõiki neid ülesandeid peab täitma üksainus inimene. Sellistel juhtudel on administraatoril võimalik teiste jaoks märkamatult kõiki SAP-süsteemi andmeid vaadata ja muuta. Reeglina tuleb sellist olukorda pidada turbe seisukohast kriitiliseks, mistõttu on tarvis juurutada täiendavaid kontrolle. Sama kehtib ka reeglina nende valdkondade kohta, mis puudutavad olulisi, finantside ja bilansiga seotud protsesse ning isikuandmete töötlemist, kus vastav funktsioonide lahutamine on kohustuslik. Kui seda ei ole võimalik tagada, tuleb töökorralduslike meetmetega luua sobivad kontrollimehhanismid ja hoolitseda selle eest, et neid ka rakendataks. Vastavad kontrollid, mis selgitavad kontrollimehhanismide olemasolu, leiavad aset ka näiteks Sarbanes Oxley Act kontekstis läbi viidud kontrollide raames. SAPi ette antud ja väljastatud rolle tuleb hoolikalt kontrollida ja kohandada lähtuvalt konkreetsetest vajadustest. Täiendavat infot SAP-dokumentidele, mis käsitlevad SAP-süsteemide kasutajahalduse ülesehitamist ja olulisi volitusi, leiate meetmest M 2.346 SAP dokumentatsiooni kasutamine .

Kasutajahalduse tööriistad

Volitusi, profiile ja rolle saab hallata ka käsitsi. Turvalisuse seisukohast lähtudes on aga tungivalt soovitav, et sellisest tegevusest loobutaks, kuna käsitsi haldamise korral toob hallatavate objektide arvukus endaga alati kaasa probleemid volitustega. Seepärast on ülimalt soovitav kasutada profiiligeneraatorit (transaktsioon PFCG). Sellistel juhtudel ei tohi profiile enam käsitsi muuta. Volituste korrektseks väljajagamiseks peavad administraatorid viima endid kurssi profiili generaatori kasutamisega seotud protsesside ja protseduurideega. Profiili generaator tuleb esmalt käivitada transaktsiooniga SU25. Eriti oluline on tunda kontrollmärgistuste kasutamist ja hooldamist (transaktsioon SU24). Puuduvaid volitusi saab tuvastada testimisfaasis (nt kas transaktsiooniga SU53 või volitusi kontrolliva transaktsiooniga ST01). Lisaks süsteemi sisse ehitatud tööriistadele pakuvad kasutajate ja volituste haldamiseks oma väliseid tarkvaralahendusi ka kolmandad tootjad. Vastavatel toodetel on reeglina väga mugavad kasutajaliidesed, kuna need töötavad otse

operatsioonisüsteemi keskkonnas. Lisatoodete kasutamist kui alternatiivset lahendust süsteemi enda tarkvaralahendustele tuleks kaaluda iga juhtumi puhul eraldi, võttes arvesse kaasnevaid kulutusi ja nende kasutegurit. Täiendavaid viiteid SAP-dokumentidele, mis käsitlevad kasutajate haldamist profiili generaatoriga, leiate meetmest M 2.346 SAP dokumentatsiooni kasutamine .

Rakenduste eripäradega arvestav volituste haldamine

Mõningad tooted ja rakendused kasutavad lisaks SAP standardsele volituste kontseptsioonile veel ka oma enda volituste kontseptsioone ja volituste haldustööriistu (nt SAP Customer Relationship Management, mySAP CRM või siis moodul Human Capital Management, HCM). Nendega haldamisel tuleb arvestada, et need toovad endaga kaasa lisatööd. Eriti tuleb arvestada sellega, et toodet või rakendust on võimalik turvaliselt käitada ainult siis, kui ka rakenduste spetsiifikaga seotud volitused on rakenduste eripärasid arvesse võtva haldustööriistaga turvaliselt konfigureeritud. Reeglina tuleb selleks rakendada minimaalseid volitusi ja rollide, ülesannete ning vastutuse lahutamist. CRM-süsteemis ei tohi näiteks kauba tellimise ostukorvi tellimust sisse anda see isik, kes selle ostukorvi on loonud.

Rakenduste tasandil on enamasti oluline pöörata tähelepanu äririskide haldamisele: volituste väljajagamisel on muuhulgas määravaks ka riskide haldamine, mis seab volituste väljastamisele ka omad reeglid.

Täiendavad kontrollküsimused:

- Kas volituste haldamise raames rakendatakse „nelja silma“ põhimõtet?
- Kas volituste väljastamisel kasutatakse profiili generaatorit õigesti?
- Kas rakenduste eripärasid käsitlevate volituste mehhanismidega on piisavalt arvestatud ning kas need on turvaliselt konfigureeritud?

M 4.261 Kriitiliste SAP volituste turvaline rakendamine

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator

Volitusi, mis lubavad käivitada kas õiguslikult või ettevõttemajanduslikult või turbe seisukohalt kriitilisi operatsioone, nimetab SAP kriitilisteks volitusteks (Critical Authorizations). Puudutatud on näiteks igasugused operatsioonid, mis võivad viia pettusteni või mille abil on võimalik lugeda või muuta olulisi andmeid ja konfiguratsioone. SAPi kriitiliste volituste väljastamisel tuleb olla ülimalt hoolikas. Seetõttu tuleb juba eelnevalt paika panna, kuidas SAPi kriitiliste volitustega ümber käiakse. Töökorralduslikud ja tehnilised meetmed ning protsessid peavad suutma tagada, et soovitud turbeaste oleks ka reaalselt saavutatav. Järgnevalt on täiesti teadlikult jäetud esitamata kõikvõimalikud kriitilisi SAP-volitusi koondavad loetelud, kuna need loetelud ei oleks mitte kunagi täielikud ning annaksid administraatoritele vaid väära kindlustunde. Loetelude puhul jäetakse reeglina nende kontrollimine ja täiendamine unarusse. Sellele vaatamata on iga konkreetse SAP-kasutusjuhtumi puhul jätkuvalt väga oluline välja selgitada SAPi kriitilised volitused ning seetõttu ei tohi antud tööetappi mitte mingil juhul tegemata jätta.

SAPi kriitiliste volituste, profiilide ja rollide väljaselgitamine

SAPi kriitilised volitused sõltuvad SAP-volituste kontseptsioonist tingituna muuhulgas ka volitusobjektide väljadest ja väljaväärtustest. See kehtib eriti nende volituste kohta, mida kasutatakse rakendustes või moodulites ning on seetõttu ettevõttemajanduslikust seisukohalt kriitilised. Seepärast on soovitav välja selgitada, millised on volitusobjektide kriitilise tähtsusega väljad, et seeläbi omakorda välja selgitada, millised on puudutatud volitusobjektid. Ainult niimoodi on võimalik tulevikus kontrolle läbi viia ning ainult volitusobjekte teades on võimalik vastavaid kontrolle automatiseerida. Volitusobjektide kriitiliste väljade näideteks on kulukeskus, tellimuste valdkond, tulukeskus või tehas. SAPi kriitilisteks volitusteks loetakse ka kõiki administraatorivolitusi, mida läheb tarvis SAP-süsteemi haldamiseks. Siia alla kuuluvad kõik volitused, mis on tuletatud volitusobjektidest ja algavad eesliitega „S_“. Lisaks volitustele on võimalik tuvastada ka kriitilisi profiile ja rolle, mis on olemas juba alates tarnimise hetkest. Kõik profiilid, mille lõpuosas on märge „_ALL“, kuuluvad kriitiliste profiilide hulka, kuna reeglina antakse neile kõik volitused, mis on kas süsteemi, rakenduse või mooduli teatud alamvaldkonna jaoks olulised. Kõik rollid, mille tähistuse hulgas leidub kombinatsioon „ADM“, kuuluvad kriitiliste rollide hulka, kuna need tähistavad reeglina administratiivsete ülesannetega seotud rolle.

SAPi kriitiliste volituste, profiilide ja rollide väljaselgitamisel tuleb arvestada, et SAP pakub nimede jaoks kasutamiseks kahte kontseptsiooni, mida rakenduste või omaarendustega alati ei arvestata. Seetõttu võivad tekkida ka sellised kriitilised volitused, profiilid ja rollid, mis ei mahu ette antud nimeskeemi raamidesse. SAPi kriitiliste volituste käsitsi tuvastamine on üldkokkuvõttes keeruline. Nii SAP kui ka kolmandad tootjad pakuvad aga tarkvaralahendusi, mis suudavad kriitilisi volitusi tuvastada automaatse tööprotsessina. Reeglina on kontrollitarkvara tootja nende toodete puhul ise eelnevalt defineerinud, mida loetakse SAPi kriitilisteks

volitusteks ja mida mitte. Täiendavat viiteid SAP-dokumentidele, mis käsitlevad volituste kontrollimist, leiate meetmest M 2.346 SAP dokumentatsiooni kasutamine . Kriitiliste volituste identifitseerimiseks on hädavajalik omada piisavaid teadmisi protsessi aluseks oleva volituste kontrollide kohta.

SAPi kriitiliste volituste, profiilide ja rollide kohandamine

Pärast seda, kui SAPi kriitilised volitused, profiilid ja rollid on tuvastatud, tuleks neid vastavalt volituste planeerimisele kohandada. Võimalikke kõrvalmõjusid süsteemi tööfunktsioonidele tuleb vaagida ennekõike süsteemi haldamist puudutavate profiilide ja rollide kohandamise puhul. Seetõttu tuleb pärast kohandamist kindlasti üle kontrollida, kas süsteem käitub ka reaalselt nii, nagu oli ette nähtud, või esineb selle töös vigu. Kohandamisprotsess, millega kaasnevad ette antud volituste, profiilide või rollide suuremahulised muudatused, võib olla väga keeruline ja aeganõudev ning seetõttu ei tohiks seda läbi viia igapäevaselt toimivas süsteemis.

SAPi kriitiliste süsteemivolituste kasutamise piiramine

Volituste planeerimise raames tuleb kindlaks määrata põhimõtted, kuidas käiakse ümber SAPi kriitiliste volituste, profiilide ja rollidega. Siinkohal tuleb arvestada järgmiste soovitustega:

- igapäevaselt toimivas süsteemis ei tohi kasutada profiile SAP_ALL, SAP_NEW* ja S_DEVELOP*.
- Administratiivse poolega seotud volitusi, profiile ja rolle tohib vastavalt volituste planeerimisele (vt M 2.342 SAP pääsuõiguste planeerimine) välja jagada ainult haldamisega seotud töötajatele. Lisaks tuleb hoolitseda selle eest, et rollid saaksid piisavalt lahutatud.

Täiendavat infot leiate antud teema kohta meetmest M 2.346 SAP dokumentatsiooni kasutamine .

SAPi kriitiliste volituste loetelu hooldamine

Pärast SAPi kriitiliste volituste tuvastamist on soovitav seda loetelu SAP-süsteemis alati värskena hoida. Sellisel juhul on võimalik automaatselt kontrollida, milliste kasutajatega on SAPi kriitilised volitused seotud. SAPi kriitiliste volituste loetelu eest saab hoolitseda transaktsiooniga SU96. Raportiga „RSUSR009“ on võimalik kuvada kasutajaid, kelle käsutuses on mõni SAPi kriitiline volitus. Kriitiliseks võivad osutuda ka mittekriitiliste volituste kombinatsioonid, kuna nende kasutamise tagajärjel võidakse käivitada kas üks või mitu transaktsiooni, mis võivad olla turbe seisukohast kriitilised. SAP võimaldab kontrollifunktsiooni, millega saab automaatselt otsida selliseid kasutajaid, kellel on volitused, mis lubavad käivitada teatud liiki transaktsioonide kombinatsioone. Sel otstarbel tuleb transaktsiooniga SU98 (SUKRI tabeli värskendamine) tagada, et kriitiliste kombinatsioonide loetelu oleks pidevalt värske. Raportiga „RSUSR008“ on võimalik identifitseerida kasutajaid, kelle käsutuses on SAP volituste kriitilised kombinat-

sioonid. Uuemates SAP-süsteemides (alates versioonist 6.20) tuleks kasutada raportit RSUSR008_009_new, mis on loodud asendamaks raporteid RSUSR008 ja RSUSR009.

Tarnimisseisundis SAP-süsteemi SAPi kriitiliste volituste ja kriitiliste transaktsioonikombinatsioonide loetelud on pelgalt näited ning seetõttu ei tohiks neid rakendada kontrolli eesmärgil. Need loetelud tuleb ise koostada ja neid tuleb ise ajakohastada. Neid võib hinnata ka näiteks Sarbanes Oxley Actiga seotud kontrollide raames. Selle valdkonna tarbeks pakub SAP tasulist, NetWeaver platvormi jaoks loodud täiendavat tarkvaralahendust SAP GRC Access Control, mis aitab vastavaid riske tuvastada automaatselt. Kontrollitööriistu võib leida ka teistelt tootjatelt.

Täiendavad kontrollküsimused:

- Kas SAPi kriitilised volitused, profiilid ja rollid on välja selgitatud?
- Kas SAPi kriitiliste volitustega ümberkäimiseks on koostatud vastav kontseptsioon?
- Kas SAPi kriitilisi volitusi ja transaktsioonide kriitilisi kombinatsioone kajastavaid tabeleid värskendatakse mõistlikult?

M 4.262 SAP-volituste lisakontrollide konfigureerimine

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator

SAP-süsteem võimaldab eelkonfiguratsiooniga läbi viidavaid volituste kontrollimisi muuta (vt lisaks M 2.342 SAP pääsuõiguste planeerimine). Volituste kontrollimisi on võimalik välja lülitada. Rakendada on võimalik ka täiendavaid volituste kontrolle. Selle võimalusega tuleks volituste planeerimise etapis ka arvestada. Üldjuhul tuleb volituskontrollide muutmisel arvestada järgnevate aspektidega.

Volituste kontrollide desaktiveerimine
Volituste jaoks olemas olevate kontrollifunktsioonide väljalülitamine võib kahjustada SAP-süsteemi turvalisust, kuna sellega lülitatakse välja juurdepääsude kontrollimine. Enne kontrollide väljalülitamist tuleb hoolikalt järele uurida, millised võivad olla selle tagajärjed turvalisusele. Täiendavat infot leiate meetmest M 2.346 SAP dokumentatsiooni kasutamine .

Transaktsioonide loomine programmide käivitamiseks või raportite tarbeks
Programme ja raporteid on võimalik käivitada näiteks transaktsiooniga SE38 (ABAP *Editor*). Kõikidel programmidel ja raportitel ei ole aga päris oma eraldi transaktsioonikoodi. Juhul, kui kasutajatele on tarvis anda juurdepääs teatud programmidele või raportitele, on soovitav see lahendada transaktsioonidega. Sellise lahenduse eeliseks on asjaolu, et juurdepääsu transaktsioonile ja seega ka programmile ning raportile on võimalik kaitsta S_TCODE tüüpi volitustega. Lisaks saab juurdepääsu transaktsioonile SE38 ka tõkestada, kuna sellega on põhimõtteliselt võimalik käivitada ükskõik millist koodi. Ka sellise tegevuse puhul tuleb jätkuvalt arvestada asjaoluga, et profiili generaatori poolt loodud volituste eest, mis võimaldavad käivitada programme ja raporteid, tuleb täiendavalt hoolt kanda. Selleks on tarvis volitusobjektist S_PROGRAM tuletatud rollide volitusprofiilide volitusi vastavalt volituste planeerimise nõuetele kohandada.

Parameetritransaktsioonide kasutamine
Uute loodavate parameetritransaktsioonidega on võimalik transaktsioonidele väärtuseid ning käivitamisparameetritele väärtusevahemikke ette anda. Loodavad parameetritransaktsioonid (transaktsioon SU93) saab siduda eraldi volitustega (volitusobjekt S_TCODE), mis piiravad nende juurdepääsu. Antud kontekstis on oluline arvestada, et parameetritransaktsioonide rakendamine ei sobi turbemeetmeks, mis peab piirama juurdepääsusid transaktsioonide funktsioonidele või andmetele. Juurdepääsusid programmidele, raportitele või tabelitele tuleb reeglina alati piirata läbi asjakohaste volitusobjektide (programmidele ja raportitele S_PROGRAM ning tabelitele S_TABU_DIS).

ABAP-volitusgruppide kohandamine
Programmide, raportite ja tabelite tarbeks on võimalik koostada nn volitusgruppe. Niimoodi on võimalik volitusi gruppidesse koguda ja ühisesse gruppi kuuluvate programmide, raportite ning tabelite juurdepääsusid saab juhtida ühe volitusobjekti kaudu. ABAP-volitusgruppide rakendamisel tuleb arvestada alljärgnevaga:

- Juurdepääs reguleeritakse alati kõikide ühte gruppi kuuluvate objektide tarbeks.
- Volitusgrupp kujutab endast täiendavat kontrolli. Tavapärased volituste kontrollid, mida viib läbi kas programm või raport, jäävad sellest puutumata.
- Kui otsustatakse volitusgruppe kasutama hakata, saab alustada tööd üldiste gruppide planeerimise suunas, näiteks kas rakenduste või moodulite lõikes. Üldisi gruppe saab seejärel juba vastavalt soovitud turbeastmele edasi arendada.
- Planeerijad ja haldusega tegelevad administraatorid peavad tundma volitusgruppide täpset toimimisviisi.

Täiendavat infot volitusgruppide konfigureerimise kohta leiate meetmest M 2.346 SAP dokumentatsiooni kasutamine .

Enda loodud täiendavad volitusobjektid
Juhul, kui ettevõttes või ametiasutuses arendatakse välja oma (ABAP-) programme või kui olemasolevate programmide programmikoodi modifitseeritakse, on võimalik ka uute, enda poolt defineeritud volitusobjektide tarbeks lisada volituste kontrollifunktsioone. Selleks, et profiiligeneraator nendega arvestaks, peavad kontrollmärgistused olema defineeritud transaktsiooniga SU24 ja vastavalt kohandatud. Antud tegevused tuleb lahendada muudatuste haldamist käsitlevate protsesside raames.

Muudatuste dokumenteerimine
Kõik volituste kontrollimises tehtavad muudatused tuleb dokumenteerida.

Täiendavad kontrollküsimused:

- Kas volituste kontrollid lülitatakse välja ainult pärast seda, kui neid on hoolikalt kontrollitud?
- Kas programmide ja raportite jaoks koostatakse transaktsioone ning kas juurdepääsuõiguseid jagatakse välja piirangutega?
- Kas ABAP-volitusgruppe rakendatakse mõistlikult?

M 4.263 SAP sihtpunkti kaitse

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator

Lisaks serverirollile, mille puhul võimaldab SAP-süsteem juurdepääsu erinevatele funktsioonidele, võib SAP võtta enda kanda ka kliendirolli, näiteks juhtudel, kus süsteem loob juurdepääsu funktsioonidele, mille pakkujateks on teised SAP-süsteemid. Sihtpunktid kirjeldavad siinjuures erinevaid sihtsüsteeme ning sisaldavad kogu juurdepääsuks vajalikku infot. Reeglina kuuluvad siia alla arvuti nimi või IP-aadress, kasutatav protokoll ja andmesidepordi number, kirjeldades sihtsüsteemini viivat võrguühendust. Sihtpunktide jaoks võidakse aga talletada ka autentimisinfot. Infot kasutatakse sihtpunkti pöördumisel selleks, et sihtsüsteemi sisse logida. Juhul, kui autentimisandmeid ei talletata, peab sisse logiv kasutaja need ise sisestama. Kaugpöördusel toimuv funktsioonide käivitamine leiab sellisel juhul aset sisestatud kasutaja volitustega. Sihtpunktide kontekstis, mille poole pöördutakse RFC-ga (*Remote Function Call*), kasutatakse siinkohal reeglina järgmisi mõisteid:

- RFC kasutaja: kasutaja, kes on serverisüsteemis aktiivne ja kellel on teatud volitused,
- RFC *Service* kasutaja: RFC kasutaja nimetatakse ümber *Service* - kasutajaks siis, kui sisselogimise andmed (kasutajanimi ja parool) on salvestatud klientsüsteemi.

Sihtpunkte hoitakse tabelis, mis ei sõltu mandantidest ning seetõttu on igal kasutajal juurdepääs kõikidele SAP-süsteemi sihtpunktidele. Seetõttu tuleb vastavate sihtpunktide juurdepääsusid kaitsta. Sihtpunktide puhul tuleb arvestada järgnevate soovitustega.

Autentimisandmete salvestamine

Autentimist puudutavat infot tuleks talletada vaid siis, kui see on vältimatu. Siinkohal tuleks kaaluda, kas põhitähelepanu tuleb suunata kasutatava parooli kaitsmisele või hoopis sellele, kuidas kaitsta sihtsüsteemi volitamata juurdepääsude eest. RFC-sihtpunktide puhul, milleni jõutakse läbi programmide, tuleb arvestada, et autentimisandmete talletamine on möödapääsmatu, välja arvatud juhul, kui serverisüsteem on konfigureeritud nn *Trusted-RFC-Communication* 'i jaoks, mille puhul võivad enamasti kõik usaldusväärse SAP-süsteemi RFC-pöördused toimuda ilma autentimiseta. Juhul, kui autentimisandmeid salvestatakse, tuleks selleks otstarbeks välja valida eranditult kommunikatsiooni-tüüpi kasutaja. Eriti tähtis on vältida dialoog-tüüpi kasutajate registreerimist, kuna sellisel juhul võib sihtpunkti vahendusel aset leida interaktiivne, ilma paroolita sisselogimine. Paroolide krüpteerimata kujul salvestamise võimalusest tuleks tingimata loobuda.

Sihtpunktide juurdepääs

Sihtpunktide juurdepääsusid tuleb piirata nõnda, et pöördused oleks võimalikud ainult volitatud kasutajatele.

Sihtpunktide juurdepääsusid saab juhtida volitusobjektiga S_ICF. Juurdepääsu juhtimiseks on volitusobjekti jaoks defineeritud järgmised volitusväljad:

ICF_FIELD: kaitstava objekti tüüp.
See väli võib sisaldada järgmisi väärtusi:

- SERVICE: ICF- Services 'i kasutamiseks,
- DEST: RFC-sihtpunktide kasutamiseks (alates 6.20)

ICF_VALUE: kaitstava ICF-objekti väärtus.

See väli sisaldab vastava objekti väärtust. Väärtuste eest, mida soovitakse kaitsta, hoolitsetakse ICF- *Services* 'i puhul transaktsiooniga SICF ja RFC-sihtpunkti puhul transaktsiooniga SM59. Siinkohal tuleks arvestada järgnevaga:

- Sihtpunktid tuleb kasutusvaldkondade põhjal gruppidesse jaotada. Sellisel juhul saab kasutajatele võimaldada ligipääsu kõigile, kindla kasutusvaldkonnaga seotud sihtpunktidele. Probleemid võivad aga esile kerkida siis, kui samu sihtpunkte kasutatakse korraga mitme kasutusvaldkonna raames, kuna iga sihtpunkti on võimalik korraga liigitada ainult ühe kasutusvaldkonna alla. Sellistel juhtudel tuleb luua täiendavad alajaotused.
- Erineva kahjupotentsiaaliga sihtpunktide juurdepääsusid tuleb juhtida lahutatud volitustega.

Tuleb arvestada, et sihtpunkti on võimalik kasutada mitmel erineval otstarbel. Juurdepääsu kaitse saab seetõttu toimida vaid kui sissesaamist takistav asjaolu. Sihtsüsteemide kaitse eest peavad hoolitsema lõppude lõpuks käivitatav funktsioon ise ja sihtsüsteemis rakendatavad volituste väljajagamise põhimõtted.

Eriti kehtib see sihtpunktide puhul, kuhu pöördutakse *Trusted*-RFC vahendusel (kannavad sellisel juhul ka nimetust „*Trusted Destination*“). Sellistel juhtudel kasutatakse volituste juhtimiseks volitusobjekte S_RFC ja S_RFCACL. Täiendavat infot sihtpunktide juurdepääsudega ümberkäimise kohta leiate meetmest M 2.346 SAP dokumentatsiooni kasutamine .

Kasutusest kõrvale jäävate sihtpunktide turve

Sihtpunktide puhul, mida ei kasutata, tuleb otsustada, kas need jäävad kasutusest kõrvale ainult ajutiselt või loobutakse nende kasutamisest täielikult. Esimesel juhtu tuleks sihtpunktid desaktiveerida, teisel juhul aga kustutada.

Sihtpunktide ülekandmine teistesse süsteemidesse

Juhtudel, kus ühe süsteemi sihtpunktid kantakse üle mõnda teise süsteemi, kantakse muuhulgas üle ka sihtpunktidesse salvestatud autentimisandmed.

Vastavaid sihtpunkte on sellisel juhul võimalik süsteemis, kuhu need importditi, kohe edukalt sihtpunktina määratletud sihtsüsteemi pääsemiseks kasutama hakata. Sellega tuleks arvestada sihtpunktide (nt süsteemikoopiate) ülekandmisel.

Sihtpunktide hooldamise ja sihtpunktitabeli juurdepääsu piiramine

Sihtpunktide hooldamiseks kasutatakse transaktsiooni SM59. Soovitavalt peaks juurdepääs nendele transaktsioonidele olema ainult volitatud administraatoritel (volitusobjekt S_TCODE). Tuleb arvestada asjaoluga, et RFC-sihtkohaandmed salvestatakse RFCDES-tabelisse. Paroolid on sealjuures salvestatud küll kodeeritult, kuid SAP-süsteemis on olemas kõik selle info lahtikodeerimiseks vajalikud andmed. Seetõttu tuleb piirata ka otsest juurdepääsu tabelile (vt M 4.264 SAP süsteemide tabelite otsemuudatuste piiramine).

THOST-tabeli turve

THOST-tabelis kajastuvad sümbolilised arvutinimed (SAP-nimed), mida SAP-süsteemis kasutatakse, DNS-arvutinimede (võrgunimede) kujul. Seetõttu tuleb juurdepääsu tabeli hooldusele (transaktsioonile SM55 või SE16) piirata, võimaldades seda ainult volitatud administraatoritele (volitusobjekt S_TCODE). Siinkohal tuleb hoolitseda, et SAP-nimed ja võrgunimed omavahel õigesti kokku langeksid, et pöördused viiksid alati õigete IT-süsteemideni.

Täiendavad kontrollküsimused:

- Kas sihtpunktide jaoks vajalikke kasutaja sisselogimisandmeid salvestatakse vaid neil juhtudel, kus teistsuguseid lahendusi ei ole võimalik kasutada?
- Kas sihtsüsteemis on kõik sihtpunktide tarbeks salvestatud kasutajad *Service* -kasutaja tüüpi kasutajad?
- Kas juurdepääs sihtpunktidele on võimaldatud ainult volitatud kasutajatele?
- Kas juurdepääs sihtkoha hooldusvõimalustele on piiratud?

M 4.264 SAP süsteemide tabelite otsemuudatuste piiramine

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator

Kõiki SAP-süsteemi andmeid hoitakse SAP-andmebaasi tabelites. Kasutamise tagajärjel, näiteks transaktsioonide, programmide või RFC-moodulite käivitamisel tekivad tabelitesse muudatused.

Tabelite juurdepääsutransaktsioonide volituste piiramine
SAP-süsteemis on võimalik tabelite sisule ka otse ligi pääseda ning seda lugeda ja muuta. Juurdepääs tabelitele ja tabelite sisule võib toimuda erinevate transaktsioonide vahendusel. Nendeks võivad olla nt SE16 *Data Browser*, SE80 *Workbench*, SE84 *Repository Browser*, SM30 *Maintain table views*, SM31 *Table maintenance*, SE11 *Data Dictionary*, SQVI *Quick Viewer*. Sõltuvalt rakendatava SAP-süsteemi versioonist ja sellest, millised rakendused ja moodulid on installeeritud, võib eksiteerida veel ka täiendavaid, tabelitele otsejuurdepääsu võimaldavaid transaktsioone või raporteid. Juurdepääsu ülal nimetatud transaktsioonidele tuleb piirata vähemalt nõnda, et see piirduks volitatud administraatorite või kasutajatega. Transaktsioonide loetelu, mille juurdepääsu tuleks nimetatud põhjusel piirata, tuleb täiendada, võttes aluseks kohapealse süsteemi eripärad. Juurdepääsu konfigureeritakse volitusobjektiga S_TCODE. Soovitav on regulaarselt kontrollida, millistel kasutajatel on juurdepääs selles mõttes kriitilistele transaktsioonidele. Selleks võib rakendada näiteks kasutaja infosüsteemi (transaktsioon SUIM), mis aitab koostada kasutajate loetelusid erinevate otsingukriteeriumite alusel. Transaktsiooniga S_BCE_68001398 on võimalik otse üles loetleda need kasutajad, kellel on juurdepääs teatud kindlale transaktsioonile. Seda transaktsiooni saab kasutada üksiktestide läbiviimiseks.

Tabelitele juurdepääsu võimaldavate volituste konfigureerimine

Juhul, kui tabelite otsejuurdepääsu võimaldavaid transaktsioone ei saa piirata, on võimalik tabelitele tehtavaid pöördusi juhtida tabelite otsevolitustega. Selleks kasutatavad volitusobjektid on S_TABU_DIS, S_TABU_CLI ja S_TABU_LIN. Volitusobjektiga S_TABU_DIS on võimalik väljastada volitusi mandantidega seotud tabeligruppidele. Need defineeritakse tabelis TBRG ning need koondavad üksikuid tabeleid kokku gruppidesse. Iga tabeligrupi jaoks defineeritakse TDDAT-tabeliga sinna juurde kuuluv volitusgrupp. Juurdepääsu juhtimiseks salvestatakse tabelite volitusgruppide nimed väärtustena parameetrisse DIBERCLS. Lubatud operatsioone juhitakse parameetriga ACTVT. Volitusobjektiga S_TABU_CLI on võimalik analoogselt väljastada volitusi mandantidest sõltumatutele tabeligruppidele. Juhul, kui juurdepääsu transaktsioonidele, mis võimaldavad otsejuurdepääsu tabelitele, ei saa lõplikult välistada, tuleb tabelite juurdepääsu kontrolliks ilmtingimata rakendada volitusobjekte S_TABU_DIS ja S_TABU_CLI.

Volitusobjektiga S_TABU_LIN on võimalik väljastada volitusi tabelite üksikutele ridadele. Antud mehhanism eeldab aga täiendavaid kohandamisseadistusi (c*ustomizing*). Selleks tuleb defineerida ja tööle lülitada nn organisatsioonikriteeriumid. Kuna autoriseerimise ulatuse defineerimine on suhteliselt keeruline, ka-

sutatakse seda objekti praktikas väga harva. Sagedasti kasutatav võimalus teatud tabelite juurdepääsude lubamiseks on parameetritransaktsioonide defineerimine. Sellega määratletakse transaktsioonid, mis käivitavad teisi, eelnevalt defineeritud väärtustega transaktsioone. Antud näite puhul käivitatakse transaktsioon SE16 otse koos soovitud tabeli nimega. Tabeli nimi defineeritakse parameetri „DATABROWSE-TABLENAME“ väärtusena. Parameetritransaktsioonid defineeritakse transaktsiooniga SE93. Selle protsessi puhul tuleb arvestada, et tabelite pääsuõigused tuleb ikkagi välja jagada S_TABU_DIS abil, kuna parameetritransaktsioonid ei sobi juurdepääsude juhtimiseks. Täiendavat infot SAP-dokumentatsioonide kohta leiate meetmest M 2.346 SAP dokumentatsiooni kasutamine .

Täiendav kontrollküsimus:

- Kas tabelitele otsejuurdepääsu võimaldavaid volitusi on piiratud?

M 4.265 SAP süsteemi pakktöötluse turvaline konfigureerimine

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator

Tausttöötlemise (*batch* -töötluse) raames toimuvad protseduurid ehk pakktööd (*batch-jobs*) tavaliselt automaatselt. Lisaks saab tööde läbiviimist määrata teatud aegadele. Konfigureerimisel tuleb arvestada alljärgnevaga:

- Pakktöid juhitakse transaktsiooniga SM36. Õiguseid sellele transaktsioonile tohivad omada ainult volitatud *batch* -administraatorid.
- Järgnevate volitusobjektide kaudu toimub pakktöö haldamine. Volituste määramine peab enamatel juhtudel olema reguleeritud volituste kontseptsiooniga.
- Volitusobjekti S_BTCH_ADM täiendamine väärtusega „Y“ võimaldab täielikku juurdepääsu *batch* -administreerimisele.

Tuleb arvestada, et täiendavate piirangute kehtestamine on sel juhul võimatu. Selliste volitustega kasutaja saab alati käivitada kõiki haldusoperatsioone ning seetõttu tohib neid volitusi anda vaid vähestele administraatoritele (nt *batch* -haldajale, asendustöötajale):

- Volitusobjekti S_BTCH_JOB täiendamine väärtusega „LIST“ võimaldab *batch*- haldajal näha pakktööde poolt tekitatud *spool* -ülesandeid. Kuna see sisaldab pakktöö väljundandmeid, tuleb volituste kontseptsiooni raames otsustada, millistel asjaoludel ja kes seda volitust kasutada tohib.
- Kasutajad saavad alati – ilma et neil oleks vaja erivolitusi – ise töid luua ja hallata. Alljärgnevaid volitusobjekte saab kasutada konkreetseid volitusi eeldavate spetsiaalsete operatsioonide jaoks.
- S_BTCH_JOB: võimaldab sõltuvalt väärtusest alljärgnevat:
- väärtus „DELE“: teiste kasutajate tööde kustutamine
- väärtus „LIST“: *Spool* -ülesannete kuvamine
- väärtus „PROT“: töölogide, sealhulgas ka teiste kasutajate töölogide vaatamine,
- väärtus „SHOW“: töö detailse info vaatamine
- väärtus „RELE“: teiste kasutajate tööde deblokeerimine

Kuna antud operatsioonid on kriitilise tähtsusega, eeldab nende kasutamine hoolikat planeerimist. Reeglina ei tohi neid volitusi anda tavakasutajatele.

- S_BTCH_NAM: kasutaja saab käivitada pakktöid teise kasutaja volitustega. Kasutajad, kelle all saab pakktöid käivitada, tuleb volitustes ära märkida. Selle volituse määramine on turvalisuse seisukohast oluline ja mõistlik ainult *batch* -administraatorite puhul, näiteks selleks, et käivitada pakktöid tehniliste kasutajate

all.

- Kuna pakktöötlus toimub töö taustal ja automaatselt, jääb see tavaliselt märkamatuks. Seega võib kuluda palju aega, enne kui suudetakse tuvastada pakktöötluse volitusteta muutmist. See on põhjus, miks volituste väljajagamisel tuleb tingimata rakendada piiranguid.
- Tausttöö toimub tavaliselt pakktöö loonud kasutaja volitustega. Seetõttu mõjutavad seda kasutaja konfigureeritud volitused.
- Kui pakktöid tehakse tehniliste kasutajate volitustega, siis tuleb tehniliste kasutajate volitusi piirata. Tehnilist kasutajat ei tohiks varustada profiiliga SAP_ALL.
- Juurdepääs pakktöö haldamisele peab olema ainult volitatud administraatoritel.
- Pakktöö võib SAP-süsteemi koormata. Seega tuleb otsustada, kas tavakasutajad võivad pakktöid käivitada või kas see vajab pärast kasutajapoolset töö loomist *batch*- administraatori poolt kinnitamist ja planeerimist.

Lisaviited pakktöötluse SAP-dokumentatsioonile leiate meetmest M 2.346 SAP dokumentatsiooni kasutamine .

Täiendavad kontrollküsimused:

- Kas pakktöö haldamine on võimalik ainult volitatud administraatoritel?
- Kas ainult volitatud kasutajatel on volitused teiste kasutajate pakktöödele ligi pääsemiseks?

M 4.266 SAP Java protokollistiku turvaline konfigureerimine

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator

SAP-süsteemi Java pinu võimaldab kasutada Javal põhinevaid tehnoloogiaid. Neid kasutatakse suuremalt jaolt veebipõhistes valdkondades. Erinevalt ABAP-pinust on Java pinu suhteliselt uus ja selle funktsioone ei kasutata nii sageli. Uued, Javal põhinevad tehnoloogiad täiendavad ABAPi võimalusi ning seetõttu Java pinu tähtsus aina kasvab. Kuigi paljud tööks olulised funktsioonid toimuvad jätkuvalt ABAP-pinus, kasutatakse liideskomponentide jaoks Javat. Java pinu moodustatakse aplikatsiooniserveri poolt, mis kasutab J2EE (*Java 2 Enterprise Edition*) spetsifikatsiooni. Kuna Java ja ABAP-pinud on integreeritud *NetWeaver ApplicationServer* 'iga ja suhtlevad üksteisega J*avaConnector* 'i (JCo) abil, vajab installeeritud Java pinu kaitset. Selleks kasutatakse ABAP-pinuga võrreldes täiesti erinevaid turvamehhanisme ja -kontseptsioone. Järgnevalt kirjeldatakse turbe seiskohast olulisi tööetappe, mida tuleb järgida Java pinu algse konfiguratsiooni loomisel. Näide piirdub rakendusserveri konfigureerimisega ega puuduta seetõttu teisi installeeritud rakendusi.

Java pinu installeerimine

Java pinu tuleks eraldi installeerimist võimaldavate SAP-süsteemi versioonide (versioonid kuni 6.40) hulka installeerida ainult siis, kui kasutatakse Javal põhinevaid tooteid või rakendusi. Kui Java pinu ei saa eraldi installeerida ja kui seda pole tarviski, siis peab konfiguratsioon välistama võimaluse Java pinule juurde pääseda. Selleks tuleb kõik Java pinu teenused desaktiveerida.

Java pinu koolitus

Java pinu haldavad administraatorid peavad tundma J2EE arhitektuuri ja turvalisuse kontseptsioone. See eeldab eriti häid teadmisi J2EE-vastavusega objektide staatilise konfiguratsiooni osas, mida teostab administraator administreerimistööriista abil. Siinkohal kasutatakse rollipõhist turvakontseptsiooni. Tuleb arvestada, et SAP täiendas J2EE Java autentimist- ja autoriseerimisteenust (JAAS) SAPil põhineva kasutajate haldusmootori (*User Management Engine*, UME) funktsioonidega. Seeläbi täiendati turvaseadistuste staatilist konfigureerimist dünaamilise, programmikoodiga tehtava konfigureerimisvõimalusega, mida saab juhtida UME kaudu. UMEs saab seega näiteks programmides lubatud tegevused koondada rollideks. Seejärel saab selle rolli määrata kasutajatele, kes saavad nõnda vajalikud volitused. Lisaks peavad administraatorid endale teadvustama, et Java pinul on ka veel eraldi kasutajate ja volituste haldus, mistõttu tuleb seda alati administreerida. Selleks on soovitav kasutada UMEt (vt M 2.341 SAP kasutuselevõtu planeerimine), kuna see vähendab administreerimistööd.

Ebavajalike teenuste väljalülitamine

Java pinu pakub paljusid teenuseid. Kindlasti ei lähe kõiki neid alati tarvis. Ohutuse tagamiseks tuleb seega kõik ebavajalikud teenused desaktiveerida.
Probleemiks on siinjuures teenuste võimalik omavaheline sõltuvus. Lisaks saab eristada süsteemiteenuseid ja süsteemiga mitte seotud teenuseid. Java pinu haldamine toimub eraldi tööriista, nn „ *Visual Administrator* “ abil. Sellega saab

teenuseid hallata ka ükshaaval. Teenused asuvad *Visual Administrator* 'i navigeerimisabina kasutatava objektipuu lõigus „Server“. Teenuse valimisel näidatakse kohe selle detailset infot. Soovitav on toimida alljärgnevalt:

- Esmalt tuvastatakse teenus, mis pakub vajaliku rakenduse käivitamiseks vajalikku tehnoloogiat (nt *Servlet* 'il baseeruvatele rakendustele teenus servlet_jsp).
- Seejärel tuleb tuvastada teenuse sõltuvused. Selleks tuleb selgitada, millised teenused peavad olema aktiveeritud, et vaadeldav teenus oleks käivitatav. Seda on näha teenuse omaduste registrikaardis „Sõltuvusseosed“. Tavaliselt läheb tarvis ainult tugeva sõltuvusseosega teenuseid.
- Leitud teenuste puhul tuleb tegutseda sama meetodi alusel, kuni teenuste nimekiri enam ei täiene.
- Nimekirja mitteilmuvad teenused võib desaktiveerida. Tuleb arvestada sellega, et Java pinu käitamine vajab teatud teenuseid.
- Ebavajalikud rakendused võib peatada või deinstalleerida. Seda saab teha teenusega „deploy“.
- Ebavajalikud rakenduse „pseudonüümid“, mida hallatakse teenuse „http“ kaudu, võib desaktiveerida.
- Pärast seda, kui ebavajalikud teenused või rakendused on desaktiveeritud, tuleb kontrollida, kas vajalikud teenused või rakendused veel töötavad.
- Juhul, kui rakendus või Java pinu enam ei tööta, tuleb analüüsida Java pinu logisid. Tavaliselt on seal veateated, mis viitavad vajalikule, kuid desaktiveeritud teenusele. Vastasel korral on õige kombinatsiooni leidmine võimalik ainult katse ja eksituse meetodil.
- Süsteemiteenuste jaoks tuleb muuta käivituskäitumist „ *always* “, mida tehakse XML-konfiguratsioonifaili „runtime.xml“ kaudu operatsioonisüsteemi vastavas teenuste kataloogis, või kasutades graafilise kasutajaliidesega „ *Configurations* “-tööriista (väärtus: “ *never* “ või “ *manual* “).

Kuna Java pinu muutub iga versiooniga ja põhiliseks erinevusteks on teenuste arv ja funktsioon, ei saa siinkohal kindlat nimekirja anda. Teenuste ja nende funktsioonide SAP-dokumentatsiooni täiendavad viited leiate meetmest M 2.346 SAP dokumentatsiooni kasutamine .

Standardsisu eemaldamine

Kogu standardsisu, näiteks dokumentatsioon (nt teenus *deploy* : sap.com/. . . docs.examples), näidisprogrammid (nt teenus *deploy* : sap.com/. . . htmlb.ear) või staatilised HTML-leheküljed tuleb deinstalleerida.

HTTP-teenuse kaitsmine

HTTP-teenust tuleb kaitsta ning see hõlmab muuhulgas järgnevat:

- kataloogi kuvamise keelamine
- ebavajalike pseudonüümide desaktiveerimine
- HTTP PUT (failide üleslaadimine) keelamine

Asjakohase SAP-dokumentatsiooni leiate meetmest M 2.346 SAP dokumentatsiooni kasutamine .

Krüptograafilise funktsioonteegi installeerimine

Selleks, et Java pinus saaks kasutada tugevaid krüptograafilisi meetodeid, tuleks paigaldada neid pakkuv krüptograafiline funktsiooniteek. Selleks saab kasutada ka Java keskkonna tasuta võimalusi. Krüptograafiliste funktsiooniteekide kasutamisel tuleb mõelda, kas see ühildub Java pinuga, ning millised on pakkuja litsentsitingimused. Ka Java pinu komponendid nagu süsteemiteenuste ja rakenduste turvaliseks salvestamiseks mõeldud *Secure-Storage* vajavad krüptograafilisi meetodeid. Seega on piisav turvalisus saavutatav alles pärast krüptograafilise funktsiooniteegi installeerimist.

Autentimismoodulite konfigureerimine

Java pinule juurdepääsu loovaks autentimiseks saab kasutada mitut autentimismeetodit. Nii saab lisaks kasutajanimele ja paroolimeetoditele konfigureerida autentimise jaoks näiteks sertifikaate või *Single Sign-On* pileteid. Seejuures saab määrata kasutatud meetodite järjekorra ja ka selle, kas mõni teatud meetod on ainukesena autentimise jaoks piisav. Volituste kontseptsiooni raames tuleb otsustada, milliseid meetodeid kasutada ja kuidas neid kasutada. Vajadusel saab teiste tootjate teekide abil kasutada täiendavaid meetodeid. Seejuures kasutatakse Java standardi poolt määratud JAAS-liidest.

Süsteemiressursside juurdepääsu piiramine

Volituste kontseptsioon peab määrama, millised kasutajad või grupid tohivad Java pinu süsteemiressurssidele ligi pääseda ja milliseid pääsutegevused on lubatud (nt lugemine, kirjutamine, sisu kuvamine). Konfigureeritavad operatsioonid sõltuvad siinjuures ressursi tüübist. Seega tuleks näiteks pärast installeerimist koostada detailne plaan, lähtudes konkreetsest Java pinust. Lisainfo leiate meetmest M 4.268 SAPi Java pinu pääsuõiguste turvaline konfiguratsioon .

Administreerimisliidese juurdepääsu piiramine

Java pinu administreerimiseks kasutatakse mitut liidest:

- *Visual-Administrator* - *Visual-Administrator* suhtleb Java pinuga P4-liidese kaudu. Seega peab juurdepääs P4-liidesele (instantsile 00 standardina port 50004) olema volitamata juurdepääsu eest kaitstud tulemüüriga. Kuna P4-protokolli saab ka HTTP kaudu tunneldada (instantsile 00 standardina port 50001), tuleb ka seda porti kaitsta.
- Java pinu Telnetiteenus (instantsile 00 standardina port 50008) - Kui seda käsuviibal põhinevat juurdepääsu ei kasutata, tuleb Telneti teenus desaktiveerida. Kui Telneti kasutatakse, tohivad sellele ligi pääseda ainult volitatud administraatorid. Telneti ressurss (*security* -teenus, *Resources*,

root/system/telnet) tuleb seega konfigureerida selliselt, et „GrantedUsers“ alla sisestataks ainult volitatud administraatorite grupp.
- Failisüsteem, millesse konfiguratsioonifaile salvestatakse - Installeeritud Java pinu kataloogide ja failide pääsuõigustele tuleb kehtestada piirangud. (Teadmiseks: sõltuvalt Java pinu versioonist võib esineda erinevaid failisüsteemi *layout* 'e. Arengusuunaks on Java pinu konfiguratsioonide hoidmine ainult andmebaasis).

Juurdepääs administreerimistööriistadele (*Visual Administrator*, *Configtool*) peab piirduma volitatud administraatoritega. Siiski tuleb arvestada, et tööriistad töötavad võrgu kaudu, nii et ründajad võivad kasutada enda installeeritud programme. Seega tuleks piirang konfigureerida võrgu tasemel selliseks, et juurdepääs administratiivsetele portidele (vt eespoolt) oleks võimalik ainult teatud kindlate arvutite kaudu. See ei välista küll ründeid, kuid muudab need vähemalt raskemaks.

Paroolide kvaliteedi tagamine

Java pinu kasutajate jaoks tuleb konfigureerida tugevad paroolid. Parooli kvaliteedi tagamise võimalused on erinevates Java versioonides erinevad.

Miinimumnõudeks on seada parooli vähim pikkus väärtusele, mis on kirjas paroolisuunises. Parool peab olema vähemalt kaheksakohaline (konfiguratsioon kõigile kasutajatele „*Set Filter*“ kaudu).

Ka paroolide maksimaalne vanus peab olema määratud vastavalt paroolisuuniste nõuetele. Seda konfigureeritakse kasutajate omaduste kaudu. Soovitada võib 90-päevast perioodi.

Java pinu *Single Sign-On* turvaline konfigureerimine

Selleks, et Java pinule *Single Sign-On* kaudu ligi pääseda, tuleb importida nende süsteemide, millelt *Single Sign-On* pileteid vastu võetakse, sertifikaadid. Tuleb jälgida, et *Single Sign-On* pileteid võetaks vastu ainult usaldusväärsetest süsteemidest (vt ka M 4.258 SAPi ABAP-pinu turvaline konfiguratsioon).

Täiendavad kontrollküsimused:

- Kas töös olevatest süsteemidest on eemaldatud standardsed sisud?
- Kas tugevaid meetodeid pakkuv krüptograafiline funktsiooniteek on installeeritud?
- Kas aktiveeritud on ainult vajalikud teenused?
- Kas juurdepääs administreerimisliidestele on piiratud?

M 4.267 SAP Java pinu turvaline kasutajate haldus

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator

SAPi Java pinul on eraldi kasutajahaldus, mida saab kasutada ABAP-pinust sõltumatult. Siinkohal tuleks arvestada järgnevaga:

Kasutajate mälu konfigureerimine

Java pinu haldab oma kasutajaid kasutajate mälus, mis on alates versioonist 6.30 konfigureeritav. Valida saab peamiselt Java pinu andmebaasi või *User Management Engine* (UME) vahel. UME kasutamisel saab kasutajate mälu jaoks kasutada ka LDAP-kataloogi või ABAP-pinu. Tavaliselt tuleks kasutajate mälu jaoks kasutada UEMi asemel ABAP-pinu. Sel moel saab kasutajaid hallata ABAP-pinus. Juurdepääs ABAP-pinule toimub *JavaConnector* 'i (JCo) kaudu, kasutades ABAP-pinu kasutaja SAPJSF volitusi. Kasutuse kavandamise raames tuleb otsustada, millist kasutajate mälu tuleks kasutada.

Avariiadministraatori määramine

Sarnaselt ABAP-pinule tuleb ka Java pinu jaoks määrata avariiadministraator. Tema puhul peavad kehtima samad töökorralduslikud kaitsemehhanismid nagu ABAP-pinu avariiadministraatori puhul (vt M 4.259 ABAP-pinu turvaline kasutajate haldus).

Standardkasutaja kaitsmine

Java pinu standardkasutajaid nagu administraator, süsteem ja külaline saab kaitsta järgnevalt:

- Tuleb valida turvaline parool. Sõltuvalt versioonist tehakse seda installeerimisel või käsitsi pärast installeerimist.
- Külalise konto (kasutaja *Guest*) tuleb desaktiveerida.

Kasutajate haldamise kontseptsioon

Planeerimise raames tuleb koostada kasutajate haldamise kontseptsioon, mis arvestaks ka Java pinuga. Siinkohal tuleb muuhulgas arvestada sellega, et kasutajaid hallatakse tavaliselt ainult tööriistaga *Visual-Admin*. Standardses lahenduses tuleb selleks sisse logida administraatoriõigustega (vajalik on kuulumine gruppi „Administraatorid“). See tähendab, et näiteks *Help-Desk* -töötajaid ühendavad administratiivsed volitused. Seda saab küll sisemise volituste struktuuri ümberkonfigureerimisega piirata, kuid see on töömahukas ega takista kõiki administratiivseid tegevusi. Selle asemel võib kasutajate haldamiseks kasutada ka UME veebiliidest, juhul kui UME on kasutuses. Java pinu võimaldab tundmatutel kasutajatel end ise registreerida. Kontseptsiooni raames tuleb otsustada, kas see funktsioon on vajalik. Eriti tuleb mõelda riskidele, kuna ise registreerunud kasutajad saavad

Java pinus end autentida. Muid volitusi kasutajatel küll tavaliselt pole, kuid turvapuudujääkidega rakenduste olemasolu korral (nt kui teatud URL-ide kasutamisel puudub volituste kontroll) on võimalik, et ise registreerunud kasutajad saavad neid ära kasutada. See funktsiooni vajalikkuses tuleb kahelda ennekõike just internetikasutuse puhul.

Iseregistreerimise takistamiseks tuleb UME omadus „ume.logon.selfreg“ seada väärtusele „FALSE“. Konfigureerimine toimub failisüsteemi *Properties* -failiga või Java pinu tööriistaga „*Configtool*“. Reeglina vajab ise registreerimise kasutamine hoolikat planeerimist ning selle standardsest kasutamisest tuleb hoiduda. Ise registreerimise kasutamiseks tuleks nõuda turvahalduse luba.

Juurdepääs UME-veebiliidesele

UME-veebiliides võimaldab kasutajaid hallata brauseri kaudu. Selle funktsiooni kasutamisel tuleb arvestada alljärgnevaga:

- Standardina saavad UME-veebiliidest kasutada nii kasutajad kui ka administraatorid. See võimaldab tavakasutajal hallata oma kasutajakontot (nt muuta parooli). Gruppi „Administraatorid“ kuuluvad kasutajad saavad hallata kasutajaid (nt luua uusi kasutajaid).
- Kasutajate haldamise UME-veebiliidest tohivad kasutada ainult volitatud administraatorid. Seda saab tagada juurdepääsu URL-i vastavate autentimisnõuetega.
- Kaaluda tuleks võimalust, kas lubada UME-veebiliidese kasutamist ainult volitatud administraatoritele, kes rakendaksid selleks klientarvuteid.
- Kui rakendused kasutavad kasutajapõhiste omaduste (*UME-Properties*) salvestamiseks UMEd, siis tuleb arvestada, et kui kasutajal on võimalik kasutada UME-veebiliidest, saavad ta neid ise muuta.

Seda, kas ja milliste turvalisuse raamtingimuste puhul UME-veebiliidest kasutada tuleks, tuleb otsustada planeerimisfaasis.

Täiendavad kontrollküsimused:

- Kas kasutajatele on kindlaks määratud soovitud mälu suurus?
- Kas avariiadministraator on loodud?
- Kas standardkasutajad on kaitstud?
- Kas kasutajate turvalise haldamise kontseptsioon on olemas?
- Kas UME-veebiliidese haldamine, juhul kui seda kasutatakse, on turvaline?

M 4.268 SAPi Java pinu pääsuõiguste turvaline konfiguratsioon

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator

SAPi Java pinu konfiguratsiooni planeerimisel tuleb arvestada alljärgnevaga:

- SAPi Java pinu volituste kontseptsioon erineb oluliselt ABAP-pinu volituste kontseptsioonist, kuna siin on rakendatud Java spetsifikatsiooni J2EE kontseptsioone.
- Õige ja turvalise konfiguratsiooni tagamine nõuab J2EE-turvamudeli ja J2EE-turvakontseptsioonide põhjalikku tundmist. Seega tohivad konfigureerida ainult koolitatud administraatorid.
- Ressursside juurdepääsupiirangute ja *Java Protection* -domeenide (*Code Security*) konfigureerimine toimub „*security*“-teenuse kaudu.
- Juurdepääsu piiramine JNDI-objektidele (Java objektide registreerimine ja nimeteenus) toimub „*naming*“ teenuse kaudu.
- Juurdepääsu piiramine Java *Bean* -meetoditele toimub „ejb“-teenuse kaudu vastavate *Bean* -objektide omaduste alt registrikaardis „*Security*“.
- Hetkel saadaolevad objektid sõltuvad installeeritud rakendustest.
- Grupp „*root*“, mis on saadaval 6.40-st varasemates versioonides, tähistab administraatorite grupi asemel kõiki kasutajaid. Seega vastab grupp sarnasele Windowsi grupile „*Everyone*“.
- Pärast installeerimist tuleb volituste kontseptsioonist lähtudes eelseadistatud volitusi kontrollida ja vajadusel muuta.

Reeglina tuleb volituste määramisel rakendada ka piiranguid. Volituste kavandamise raames tuleb otsustada, millisel kasutajal on õigus millistele objektidele ligi pääseda.

Täiendav kontrollküsimus:

- Kas SAPi Java pinu volituste väljajagamisel on rakendatud piiranguid?

M 4.269 SAP süsteemi andmebaasi turvaline konfiguratsioon

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator

SAP-süsteemi poolt salvestamiseks kasutatav andmebaas sisaldab kogu SAP-süsteemi infot. Juhtudel, kus andmebaas ja SAP-süsteemi komponendid pole installeeritud samasse arvutisse, toimub side SAP-süsteemi ja andmebaasi vahel SQL-päringute abil, mida edastatakse kohtvõrgus. Seega tuleb andmebaasi võimalikult hästi kaitsta. Tuleb arvestada järgmiste punktidega:

- SAP-süsteemide ja andmebaasi installeerimine ühte arvutisse on üldjuhul mõistlik ainult väiksemate ettevõtete ja ametiasutuste puhul. Suuremate institutsioonide puhul tuleb eelistada lahutatud installatsiooni, kuna sel moel saab andmebaasiarvuti optimaalselt koormus- ja jõudlusnõuetega kooskõlla viia.
- Mitte ükski andmebaasi administraator ei tohi omada juurdepääsu SAP-süsteemi tabelitele. Andmebaasivolitusi tuleb kontrollida ja vastavalt kohandada. Seejuures tuleb arvestada sellega, et tavaliselt leidub alati mõni andmebaasiadministraator, kellel on täielik juurdepääs kõikidele institutsiooni andmebaasidele ja seega ka tabelitele.
- Juurdepääsu andmebaasile tohib lubada ainult SAP-süsteemist endast. Erilist tähelepanu vajavad siinkohal järgnevad aspektid. Otseseid andmebaasiühendusi teistest süsteemidest või klientidelt tuleb takistada tulemüüriga ja andmebaasi tohib kasutada ainult läbi SAP-süsteemi. Muud rakendused ei tohi siin ise tabeleid luua. Eriti hoolikalt tuleb välistada andmebaasilingid andmebaasi ja SAP-süsteemi tabelite ning teiste andmebaaside vahel.
- SAP-süsteemi andmebaasiarvutil ei tohi kasutada ühtki teist teenust ega rakendust. Erandiks on operatsioonisüsteemi seiret puudutavad tööriistad. Nende kasutamisel tuleb tagada, et pöördumised toimuks ainult autenditult ja kindlatest arvutitest (administreerimisserver, administraatori klient).
- SAP-süsteemi poolt kasutatav andmebaasikonto peab olema kaitstud turvalise parooliga.
- Kasutatav andmebaasitoode peab olema turvaliselt konfigureeritud. Ebavajalikud funktsioonid ja teenused tuleb välja lülitada. See puudutab eriti just HTTP-l põhinevaid juurdepääsuliideseid, näiteks rakenduste serverit, mida andmebaasid pakuvad juurdepääsuks läbi veebiliidese. Tavaliselt pakutakse selleks ka administreerimisvõimalusi. Juhtudel, kus standardseid kasutajaid administreerimiseks ei vajata, tuleb need kustutada. Kõik standardsete kasutajate paroolid tuleb ära muuta, ka siis, kui nende kontod desaktiveeritakse.

Sõltuvalt kasutusvaldkonnast tuleb tarvitusele võtta ka veel täiendavaid meetmeid. Seega tuleb nimekirja vastavalt vajadusele täiendada. Soovitav on ellu viia SAPi soovitused andmebaasi kaitsmiseks. Infot selle kohta leiate meetmest M 2.346 SAP dokumentatsiooni kasutamine .

Täiendavad kontrollküsimused:

- Kas SAP-süsteemi andmebaas on otsese juurdepääsu eest kaitstud tulemüüriga?
- Kas SAPi poolt vastava andmebaasitoote jaoks avaldatud soovitused on ellu viidud?

M 4.270 SAP logimine

Algatamise eest vastutavad: IT-juht, infoturbe osakond

Rakendamise eest vastutavad: administraator

Süsteemi funktsioonide ja SAP-süsteemi turvalisuse kontrollimiseks tuleb sündmuseid logida. SAP-süsteem pakub selleks mitmeid võimalusi. Palun arvestage, et käesolev meede käsitleb logimist tähenduses „SAP-põhisüsteemi seire, lähtudes IT-turbe vaatevinklist“. Käesoleva meetme eesmärgiks ei ole ettevõttemajanduslikud kontrollid (auditid). SAP-dokumentatsiooni ja süsteemiseire funktsioonide detailse kirjelduse leiate meetmest M 2.346 SAP dokumentatsiooni kasutamine . Logimisel tuleb reeglina arvestada järgnevaga.

Logimiskontseptsioon

Tuleb luua logimiskontseptsioon. Kontseptsioon peab arvestama ABAPi ja Java pinuga. Kontseptsioonis peab olema määratletud, milliseid logiandmeid SAP-süsteemis kogutakse. Kuna logimisel võib esineda ka isikuandmete kajastamist, tuleb kavandamisse kaasata andmekaitsespetsialist ja töötajate esindus.

Logiandmete turvalisus

Logiandmed võivad sisaldada olulist süsteemiinfot ja isikuandmeid. Juurdepääs logiandmetele peab seega olema piiratud. Seetõttu võib olla vajalik teha seadistusi nii SAP-süsteemis endas kui ka väljaspool SAP-süsteemi (nt faili tasandil).

Oluliste süsteemisündmuste analüüs

Olulised süsteemisündmused logitakse süsteemilogis. Sündmuseid tuleb regulaarselt analüüsida. Selleks võib kasutada transaktsiooni SM21. Tuleb arvestada, et selle transaktsiooni kaudu on võimalik ligi pääseda ka kaugete SAP-süsteemide süsteemilogidele, eeldusel, et on olemas vastavad volitused. Juurdepääsu transaktsioonile SM21 tohivad seega omada ainult volitatud administraatorid. Mitme SAP-süsteemi käitamisel tuleb kasutada tsentraalset logimist, et analüüsimine oleks koondatud ühte süsteemi.

Traces- funktsiooni kasutuse piiramine

Traces võimaldab juurdepääsul täpselt logida süsteemi tegevusi. Seejuures võib juhtuda, et nähtavaks muutuvad ka töödeldud andmed, näiteks andmebaasi suunatud SQL-päringute logimise või ALE-liidese kaudu edastatud dokumentide logimise tagajärjel. Käitatavates süsteemides on seetõttu *Traces*- funktsiooni kasutamine keelatud. Veaanalüüsid peavad toimuma test- või arendussüsteemis. Juhul, kui *Traces*-funktsiooni kasutamine on toimivas süsteemis vältimatu, tuleb seda reguleerida vastava erandliku protseduuriga. Juurdepääs *Trace* -transaktsioonidele, mille alla käivad tavaliselt transaktsioonid eesliitega „ST“ (nende transaktsioonide nimekirja koos lühikese kirjeldusega saab näha transaktsiooni SE93 abil), peab olema piiratud (volitusobjekt S_TCODE).

Tabelite muudatuste jälgimise aktiveerimine

SAP-süsteemi andmebaasi tabelid sisaldavad kõiki süsteemi- ja äriandmeid. Logimise ja auditi kontseptsiooni raames tuleb määratleda, milliste tabelite puhul on vajalik muudatuste jälgimise aktiveerimine. Tavaliselt logivad SAP-rakendused kõiki kontrollimiseks vajalikke andmeid. SAP *Basis* puhul on muudetavad tabelid, ehk siis tabelid, mida klient saab muuta, varustatud aktiveeritud muudatuste jälgimisega. See võimaldab kontrollida tabeli muudatusi. See on oluline ka ettevõtetele, mis kuuluvad *Sarbanes Oxley Act* 'i alla, kuna sel moel saab kontrollimise raames selgitada, milline kasutaja milliseid muudatusi tegi. Siinkohal tuleb arvestada, et tabelite muudatuste jälgimist saab aktiveerida ainult siis, kui arendaja on seda võimaldanud. Aktiveerimine toimub *Data Dictionary*(DDIC) all, kuhu kus tuleb vastava tabeli jaoks määrata valik „Andmete muudatuste logimine“ (transaktsioon SE13). Lisaks tuleb logimine aktiveerida süsteemi profiilis. Selleks tuleb konfigureerida parameetrit „rec/client“, mille kaudu seadistatakse, millise mandandi jaoks tuleb muudatuste jälgimine aktiveerida (seadistamisvõimalused: OFF / mmm/ nnn,mmm,. . . / ALL). Muudatuste jälgimist soovitatakse käitamis- ja *Customizing* -mandantide jaoks. Seadistus „ALL“ ei ole mõistlik. See tekitab näiteks värskenduste puhul probleeme jõudlusega, kuna see puudutab ka mandanti 000 ja võimalikke test-mandante.

Seiretööriistadele juurdepääsu piiramine

SAP-süsteemis leiduvatele seiretööriistadele tohivad ligi pääseda ainult volitatud administraatorid. Tavaliselt saab seda teha juurdepääsu piiramisega transaktsioonidele ja volituste seadistustele. Tuleb arvestada sellega, et osad seiretööriistad pakuvad juurdepääsuks ka veebiliideseid, näiteks ABAPi pinu *Message-Server Monitor* või Java pinu seiretööriistad (nt *SQL-Trace*, *Systeminfo*).

SAP Security Audit Log -i kasutamine

SAP Security Audit Log salvestab olulisi turvalisust puudutavaid süsteemisündmuseid. Seetõttu tuleb tagada, et seda ka reaalselt kasutataks. Konfigureerimine toimub transaktsiooniga SM19. Transaktsioon SM18 on mõeldud vanade logifailide kustutamiseks, transaktsioonid SM20 ja SM20N on analüüsiks. *Security Audit Log* võimaldab rakendada nn dünaamilisi konfiguratsioone, mille seadistusi saab töö käigus muuta ja nn staatilisi konfiguratsioone, mille seadistuste muutmine vajab süsteemi taaskäivitamist. Logitavate sündmuste konfigureerimisel tuleb arvestada alljärgnevaga:

- Kõik sündmused kategoorias „kriitiline“ tuleb aktiveerida.
- Kõik sündmused kategoorias „oluline“ tuleb aktiveerida.
- Kategooria „väheoluline“ sündmuste puhul tuleb otsustada, kas need vajavad logimist. Seejuures tuleb arvestada sellega, et nende hulgas on ka sündmuseid, mis tekitavad arvukaid logisissekandeid. Olukorras, kus *Security Audit Log* saab täis, lõppeb ka sündmuste logimine.

Juurdepääs transaktsioonidele SM18, SM19, SM20 ja SM20N peab olema võimalik ainult volitatud administraatoritele. *Security Audit Log* vajab regulaarset analüüsimist.

Täiendavad kontrollküsimused:

- Kas välja on töötatud mõistlik logimise kontseptsioon?
- Kas logisid analüüsitakse regulaarselt?
- Kas administratiivsetele funktsioonidele ja logifailidele on juurdepääs ainult volitatud administraatoritel?

M 4.271 SAP süsteemi viirusetõrje

Algatamise eest vastutavad: IT-juht, infoturbe osakond, arendusosakonna juht
Rakendamise eest vastutavad: administraator, arendaja

Versiooniga SAP NetWeaver 04 loodi võimalus ühendada SAP-süsteemidega väline viirusetõrjeprogramm. Sellega võimaldatakse kõikidel ABAPi ja Java pinu rakendustel kontrollida töödeldavaid andmeid, et tuvastada võimalikke arvutiviiruseid. Selleks otstarbeks defineeriti „Viirusetõrjeprogrammi liides“, kuid vastavad viirusetõrjeprogrammid peavad pöörduma otse selle liidese poole. Oma väljatöötatud programmi või teiste firmade toodetud SAP-süsteemide lisatarkvara puhul tuleb jälgida, et neil oleks olemas viirusetõrjeprogrammi liidese tugi. See puudutab kasutamist olukordades, kus andmed laetakse SAP-süsteemi ja pakutakse teistele kasutajatele allalaadimiseks. SAP-süsteemide teiste toojate tarkvara soetamise kriteeriumitesse tuleks võtta kontroll näitamaks, kas need toetavad viirusetõrjeprogrammi liidest.

Viirusetõrjeprogrammide kasutamine SAP-keskkonnas tuleb kooskõlastada kogu ametiasutust või ettevõtet hõlmava arvutiviiruste kaitsekontseptsiooniga. Viirusetõrjeprogrammide liidese dokumentatsiooni käsitlevad täiendavad viited leiate meetmest M 2.346 SAP dokumentatsiooni kasutamine .

Täiendavad kontrollküsimused:

- Kas enda väljatöötatud lahendustes on arvestatud viirusetõrjeprogrammide liidesega?
- Kas viirusetõrjeprogrammi SAP-liidese tugi on üles loetletud SAP-süsteemi tarkvara soetamise eraldi kriteeriumina?

M 4.272 SAP transportsüsteemi turvaline kasutamine

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator

SAP-transpordisüsteemi (*Transport Management System*, TMS) kaudu toimub uute funktsioonide või muudetud objektide paigaldamine ABAP-pinusse. Kuna see kujutab endast selget riski, peavad transpordisüsteemi konfiguratsioon ja kasutus olema võimalikult turvalised. Transpordisüsteemi puhul tuleb seega arvestada, et reeglina peavad transporte loovad, kontrollivad ja teostavad isikud tundma SAP-transpordimehhanismi (*Transport Organizer, Transport Management System*) kontseptsioone ja meetodeid.

Volitused transpordisüsteemis
Transpordisüsteemide jaoks kasutatavate transaktsioonide kaitse ja volituste abil tuleb tagada, et transpordisüsteemi saaks kasutada ainult volitatud isikud. Muuhulgas puudutab see järgnevaid transaktsioone: SE01, SE03, SE06, SE09, SE10, STMS*

Transpordikataloogi kaitsmine
Transporditavad andmed salvestatakse failide kujul failisüsteemi transpordikataloogi. Juurdepääs transpordikataloogile peab olema seega operatsioonisüsteemi ja võrgu tasandil piiratud selliselt, et ligipääsu võimalus oleks vaid volitatud isikutel ja volitatud kaugematel instantsidel. Seejuures tuleb jälgida, et kõikidel ühe transpordidomeeni instantsidel peab olema juurdepääs samale transpordikataloogile. Arvestada tuleb sellega, et transpordifailide volitusteta muutmine võib põhjustada vigu importimisel või muid, turvalisusega seotud probleeme.

Transportide turvaline ülekanne
Transpordid laetakse failisüsteemist SAP-süsteemi. Selleks saab kasutada tsentraalset transpordikataloogi, millele pääseb ligi kohtvõrgu kaudu. Teise variandina on võimalik transpordifaile edastada ka käsitsi või aegjuhtimisega, kasutades andmeedastusmehhanisme (nt ftp, sfpt, scp). Kuna transpordifaile tuleb volitamata nägemise ja muutmise eest kaitsta, peab kasutatav edastamismehhanism tagama andmete turvalisuse näiteks krüpteerimise abil.

Täiendavad viited transpordisüsteemi kohta asuvad meetmes M 2.346 SAP dokumentatsiooni kasutamine .

Täiendavad kontrollküsimused:

- Kas transpordisüsteemi olulised transaktsioonid on kaitstud?
- Kas transpordiandmed on kaitstud nii operatsioonisüsteemi kui ka võrgu tasandil?

M 4.273 SAP Java protokollistiku tarkvara levitamise turvaline kasutamine

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator

Java pinu kasutab eraldi tarkvarajaotust, mis erineb ABAP-pinu transpordisüsteemist. Niinimetatud *Software Deployment Manager* (SDM) on mõeldud uue tarkvara paigaldamiseks Java pinusse. *SDM*-i ülesehitus on klient/server-põhine, see võimaldab muudatusi paigaldada ka vahemaa tagant. Lisaks üldnõuetele (vt M 2.221 Muudatuste haldus) tuleb tarkvarajaotuse (*Deployment*) turvalisuse kontekstis arvestada alljärgnevaga:

- SAP-tarkvarajaotuse jaoks peab olema kavandatud ja loodud kontseptsioon. Tarkvarajaotuse kontseptsioon peab olema kohandatud Java eripäradega sobivaks, kuna siin tuleb ABAP-pinuga võrreldes kasutada erinevaid meetodeid ja tarkvaratööriistu.
- Testimis-, kinnitamis- ja vastuvõtuprotseduuri jaoks tuleb määratleda vastutusalad.
- Tarkvaraarendajad või muud isikud ei tohi tarkvara otse arenduskeskkonnast töötavatesse süsteemidesse jaotada. Tuleb arvestada sellega, et SAP-arenduskeskkond suudab tarkvara Java pinusse laadida ka otse. See võimalus tuleb välistada tehniliste meetmetega (nt tulemüüriga).
- Tarkvarajaotuseks kasutatavat *Software Deployment Manager*'i (SDM) teenust tuleb käitada turvaliselt. Vanemad SDM-i versioonid pakuvad vaid nõrka kaitset, kuna tugi on vaid ühe kasutaja jaoks ja täiendavate volituste andmine on võimatu.
- SDM-serveri komponendid ei tohi töötada pidevalt, neid tuleb käivitada vastavalt vajadusele.

SAP-dokumentatsiooni käsitlevad allikad leiate meetmest M 2.341 SAP kasutuselevõtu planeerimine .

Täiendavad kontrollküsimused:

- Kas tarkvarajaotuse kontseptsioon on kohandatud Java eripäradega vastavaks?
- Kas on loodud protseduurid, mis muudavad tarkvara jaotamise võimalikult turvaliseks?
- Kas arendajate jaoks on välistatud võimalus tarkvara otse Java pinusse sisestada?

M 4.274 Salvestisüsteemide turvaline aluskonfiguratsioon

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator

Kõiki salvestisüsteemide konfiguratsioonitöid tuleb teha vastavalt koostatud turvapoliitikale (vt M 2.352 Kohtvõrgu salvesti (NAS-süsteemi) turvapoliitika väljatöötamine , M 2.353 SAN-salvestivõrgu turvapoliitika väljatöötamine) ning dokumenteerida ja kommenteerida lähtuvalt meetmest M 2.358 Salvestisüsteemide süsteemisätete dokumenteerimine .

Operatsioonisüsteem
SAN-süsteemidena käitatavad salvestisüsteemid on eriotstarbelised serverid, mida hallatakse sisemise operatsioonisüsteemiga. See operatsioonisüsteem on tavaliselt piiratud võimaluste, kuid suurema võimsusega versioon tavalisest operatsioonisüsteemist. Ka SAN-süsteemide puhul, mis võivad koosneda paljudest üksikkomponentidest, hallatakse mõnikord teatud komponente standardilähedaste süsteemide poolt. Eriti just selliste operatsioonisüsteemide, kuid ka tootjapõhiste „tundmatute“ süsteemide puhul peab enne kasutuselevõttu olema tagatud, et kõik tarkvara- ja püsivarakomponendid oleks värskendatud, tagamaks süsteemi parimat võimaliku stabiilsuse ja kaitse rünnete, näiteks usside eest.

Aluskonfiguratsioon
Enne salvestisüsteemi integreerimist IT-käitamisse tuleb luua turvaline aluskonfiguratsioon. Tootja tarnib mitmeid seadmeid tüüpkonfiguratsiooniga, mille esmaseks eesmärgiks on kiire kasutuselevõtt ja võimalikult laialdased funktsioonid, kuid nende turvamehhanismid on praktiliselt aktiveerimata. Seega tuleb tüüpseadistusi ja aluskonfiguratsiooni testida selleks sisseseatud, eriti turvalises *offline* -testvõrgus või administreerimisvõrgus. Konfigureerimisel tuleb arvestada, et mitte iga administreerimis- või konfigureerimistööriist (konsool, veebiliides, väline konfigureerimisprogramm) ei pruugi näidata kogu vajalikku olulist infot. Seega on oluline olemasoleva dokumentatsiooni alusel kontrollida, kas kõik vajalikud seadistused on tehtud. Oleks soovitav, et konfigureerimistööriistad dokumenteeriks kõik salvestusseadme konfigureerimissammud kontrollitaval moel vähemalt lokaalsetes logifailides, eelistatult aga tsentraalses logimissüsteemis. Aluskonfiguratsiooni saab jaotada järgnevateks sammudeks:

- Lokaalne konfiguratsioon: seadet ennast puudutavate konfiguratsiooniparameetrite kontrollimine ja kohandamine (näiteks RAID-tasandite seadistamine, kõvaketaste seostamine *Volume* 'idega, varundusseadmete seostamine salvestiseadmetega), logimise seadistused, konsooli juurdepääsu seadistused jne.
- Võrgu konfiguratsioon: seadme kohtvõrku sidumine, administreerimisvõrku ja salvestivõrku puudutavate konfiguratsiooniparameetrite kontrollimine ja kohandamine. Administreerimisteenused nagu telnet, tftp või http, mille puhul edastatakse kogu info krüpteerimata teksti vormis, tuleb asendada samaväärsete krüpteeritud variantidega nagu ssh, sftp ja https.

- SAN-süsteemide puhu tuleb võrk sisemiselt tsoonimise ja *Port-Binding* 'u abil segmenteerida. Ühendatud serveritele tuleb määrata ainult tegelikult vajaminevad SAN-ressursid.
- Salvestisüsteemide administreerimine tuleb kaasata tsentraalsesse volituste haldamisse (nt *Active Directory* , LDAP, *Radius* ,. . .).

Kasutajakontod ja paroolid

Kasutajate ja rollide sisseseadmise võimalused ning volituste määramine võib tootjate lõikes oluliselt erineda. Seega tuleks vastavatele seadmete jaoks koostada juba eksisteerival, salvestiseadmete administreerimisõiguste ja rollide kontseptsioonil põhinev detailne kontseptsioon. Sageli on üks või mitu administreerimispääsu konfigureeritud üldtuntud standardnimede ja parooliga või lausa paroolita. Vastavatelt internetilehekülgedelt saab alla laadida nimekirjad tootjapõhiste standardkontode ja paroolidega. Seadme kasutuselevõtmisel tuleb võimalusel standardsed kasutajakontod ära muuta. Kõikidel juhtudel tuleb ilmtingimata ära muuta standardkontode paroolid. Mittekasutatavad kasutajakontod tuleb desaktiveerida. Vastavalt õiguste ja rollide kontseptsioonile tuleb seejärel sisse seada ettenähtud kasutajakontod ja -rollid. Konfiguratsioonifaile tuleb eriti hoolikalt kaitsta volitusteta juurdepääsu eest. Ka siis, kui on näiteks tagatud paroolide krüpteeritud salvestamine, tuleb faile ikkagi kaitsta volitusteta lugemise eest, kuna need sisaldavad ülitähtsat infot ja isegi krüpteeritud paroolid on sobivate programmide abil suhteliselt lühikese ajaga dekrüpteeritavad. Kindlasti tuleb arvestada institutsiooni paroolimäärustega pikkuse, tugevuse ja muutmise sageduse kohta.

Sisselogimisteade

Salvestisüsteemi logimisteated tohivad olla nähtavad ainult administreerimisvõrgus. Vastavad logimisteated sisaldavad sageli infot (nt mudeli- või versiooni numbrit, tarkvara väljalaske seisundit või paiga versiooni), mida potentsiaalne ründaja võib ära kasutada. Juhul, kui institutsiooni intranetist sisselogimist ei saa vältida, tuleb tavaline logimisteade asendada kohandatud versiooniga, mis ei sisalda siseinfot. Logimisteade ei tohi mitte mingil juhul sisaldada infot seadme mudeli- ja versiooninumbri ega operatsioonisüsteemi versiooni kohta. Selle asemel tuleks seadmesse sisse logimisel kuvada järgnevat infot:

- Juurdepääs lubatud ainult volitatud personalile.
- Kõiki töid tuleb teha vastavalt turvapoliitikale.
- Seade on seotud tsentraalsete kontrollmehhanismidega, näiteks võrguhaldussüsteemiga (NMS) logimiseks ja turvapoliitika rikkumiste tuvastamiseks.
- Turvapoliitika rikkumisel on distsiplinaarsed/karistusõiguslikud tagajärjed.

Logimine

Salvestisüsteemil toimuv sisemine logimine tuleb konfigureerida selliselt, et esmajoones oleks nähtav info, mida läheb tarvis probleemide varaseks tuvastamiseks. Salvestisüsteemi ning administreerimiseks ja logimiseks kasutatava arvuti ajad tuleb NTP-serveri abil sünkroniseerida. Üldiselt tuleks kõik institutsiooni IT-süsteemid NTP abil ühele ajale sünkroniseerida.

Liidesed

Salvestisüsteemide mittekasutatavad liidesed tuleb desaktiveerida. See tähendab, et kasutamata liidesed (nt jadaliidesed terminali ühendamiseks) ei tohi olla ühendatud, ja teenused, mida ei kasutada, peavad olema selgelt desaktiveeritud.

Konfiguratsiooni testimine

Testimise lõpetamisel tuleb standardsüsteemide ja administreerimisvõrgu kaitse kontrollimiseks läbi viia turvakontroll.

Konfiguratsiooni varundamine

Aluskonfiguratsiooni konfiguratsioonifailid on edasise konfigureerimise aluseks. Varukoopiad tuleb teha nii seadmega kaasas olnud tüüpkonfiguratsioonist kui ka andmetest, mis on aluskonfiguratsiooni tulemuseks, ning neid varukoopiaid tuleb hoida kaitstud kohas. Need on taaskäivitamise aluseks pärast tõsiseid rikkeid (vt M 6.98 Salvestisüsteemide valmisolek hädaolukorraks).

Täiendavad kontrollküsimused:

- Kas häälestamisel lähtuti turvapoliitikast?
- Milline on üldise administreerimisrollide kontseptsiooni seos salvestisüsteemide administraatorikontodega?
- Kas kõik mittevajalikud standardsed kasutajakontod on desaktiveeritud ja kõik standardsed paroolid ära muudetud?
- Kuidas tagatakse, et pärast konfiguratsiooni muutmist või süsteemi reinstalleerimist ei seataks paroole tagasi standardväärtustele ning et standardsed kasutajakontod jääksid desaktiveerituks?
- Kas sisselogimisteade on tavalisele kasutajale nähtamatu?
- Kas kõik olulised konfiguratsiooniandmed on dokumenteeritud?

M 4.275 Salvestisüsteemide turvaline kasutamine

Algatamise eest vastutavad: infoturbe osakond, IT-juht
Rakendamise eest vastutavad: administraator

Salvestisüsteem töötab tavaliselt suuremalt osalt iseseisvalt, ilma et töötajad peaksid sekkuma. Tõrgeteta töö tagamiseks tuleb siiski võtta tarvitusele ka mõned meetmed, mis peaksid tagama salvestisüsteemi funktsioonide täieliku töökindluse. Käitamise seiret teostab haldussüsteem (vt M 2.359 Salvestisüsteemide seire ja haldamine).

Seire

- Rakendused, süsteemiprogrammid - Niihästi teenusprogrammid nagu automaatset andmevarundust juhtiv Scheduler kui ka viirusetõrjetarkvara peavad töötama tõrgeteta.
- Mahtuvuskontroll ja süsteemi koormus - Salvestusseadmete mahtuvuspiire ei tohi ületada ja kitsaskohad salvestisüsteemis või salvestusvõrgus tuleb tuvastada õigeaegselt, et jõutaks võtta tarvitusele vastumeetmed.
- Kriitiliste sündmuste seire - Jälgida tuleb turvalisuse seisukohast kriitiliste seadistuste terviklikkust ja turvareeglitest kinnipidamist. Sündmustest, mis rikuvad olulisi turvareegleid, tuleb teavitada selliselt, et neid teateid ei saaks ignoreerida.
- Süsteemiteadete vähendamine - Süsteemiteadete hulka tuleks vähendada, nii et kuvataks ainult olulisi teateid.

Organisatsioonilised meetmed

Turvalise käitamise raames tuleb vahet teha regulaarsetel ülesannetel ja sündmusepõhistel ülesannetel, olenevalt sellest, kuidas need esinevad seoses turvaintsidentide, paikade panemise või volituste muutmisega.
Töö katkemist põhjustavateks salvestisüsteemi muudatusteks ja hooldustöödeks tuleb määrata hooldusajad. Töötavat salvestisüsteemi ei tohi väljaspool hooldusek ette nähtud aegasid ei hooldada ega muuta juhul, kui sellega kaasneb tööprotsesside mõjutamine.
Kõik muudatused, niihästi planeeritud kui plaanivälised, tuleb muudatuste haldamise protseduuri abil kooskõlastada kõikide vastava ala spetsialistidega. Muudatuste kava tuleb kontrollimise tagamiseks arhiveerida. Eriti oluline on jälgida, et SAN-süsteemi salvestisüsteemide ja võrgukomponentide püsivara või operatsioonisüsteemi täiendamine on lubatud ainult hooldusaegade raames.
Salvestisüsteemi konfiguratsiooni või sisetarkvara olulised muudatused tuleb kindlasti dokumenteerida. Vastav dokumentatsioon peab eriti just tõrgete kõrvaldamiseks ja avariiolukordade tarbeks olema üheselt mõistetav ja kergesti kättesaadav.
Komponentide varundamise ja arhiveerimise logifaile tuleb tingimata pärast süsteemi konfiguratsiooni muutmist kontrollida. Vajalikud on ka plaanivälised kontrollid, et välja selgitada, kas varundatud andmeid on võimalik taastada.

Süsteemihalduse varundamine

Salvestisüsteemi haldussüsteem tuleb varundada selliselt, et volitusteta kasutajate juurdepääs oleks välistatud.

Kontrollküsimused:

- Kas salvestisüsteemi töö üle teostatakse järelevalvet sisemiste rakenduste kättesaadavuse, süsteemikoormuse ja kriitiliste sündmuste suhtes?
- Kas süsteemi koormust kontrollitakse?
- Kas muudatusi aktiveeritakse ainult muudatuste haldussüsteemi kaudu?
- Kas hooldustöid, näiteks täiendite paigaldamist, tehakse ainult selleks ette nähtud ajal?

M 4.276 Windows Server 2003 kasutamise plaanimine

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: IT-juht, administraator

Enne Windows Server 2003 juurutamist tuleb teha põhjalik planeerimistöö, et kasutuselevõtmine saaks toimuda reguleeritult ja turvaliselt, ning et oleks tagatud ka selle edasine turvaline käitamine. Seejuures tuleb tagada, et turvapoliitikast (vt M 2.316 Serveri turvapoliitika kehtestamine) peetaks kinni ja et kogu teostus oleks poliitikatega kooskõlas. Siinkohal tuleb arvestada sellega, et Windows Server 2003 standardne installatsioon on ebavajalike komponentide kasutamise vältimiseks ilma eelinstalleeritud tarkvarakomponentideta. Sõltuvalt kasutusvaldkonnast tuleb kindlaks määrata, millise serverirolli jaoks Windows Server 2003 planeeritakse ja milliseid tarkvarakomponente tuleb vajadusel täiendavalt paigaldada. *Active Directory* kasutuselevõtu või käitamisega seonduvaid küsimusi/planeerimistöid puudutatakse siin ainult osaliselt.

Üldkontseptsioon

Windows Server 2003 planeerimine toimub mitme sammuna. Defineeritud nõuete kataloog, mis lähtub meetmest M 2.80 Tüüptarkvara nõuete kataloogi koostamine , lihtsustab planeerimist oluliselt ja seda tuleks kasutada. Planeerimine võib toimuda *Top-Down* -visandi põhimõtte alusel. Terviksüsteemi kontseptsiooni visandi alusel määratakse kindlaks spetsiifiliste osakontseptsioonide konkreetne planeerimistöö. Kontseptsiooni visandis käsitletakse näiteks järgnevaid tüüpilisi küsimusi:

- Kas üles ehitatakse uus võrk või on tegu olemasoleva võrgu migratsiooniga?
- Kas olemasolev Windowsi võrk (nt Windows 2000 Server võrk) migreeritakse täielikult või ainult osaliselt Windows Server 2003 peale ümber?
- Kas tegu on täiendavalt kasutusele võetava serveriga või olemasoleva serveri täiendusega (vt M 4.283 Windows NT 4 Serveri ja Windows 2000 Serveri turvaline migratsioon Windows Server 2003-ks)?
- Millised komponendid (nt failiserver, printimisserver, DNS-server) asendatakse ning millised jäävad alles?
- Kas olemasolevad protseduurid või komponendid, näiteks olemasolev Kerberose süsteem või olemasolev PKI, tuleb integreerida Windows Server 2003 süsteemi? Siinkohal tuleb muuhulgas arvestada ka võimega teiste IT-süsteemidega koos talitleda, ja samuti pakutavate funktsioonidega.
- Kas serveri planeeritud konfiguratsioon sobib eeldatava andmekoguse ja tippkoormusega?
- Kas litsentseerimismudel on piisav ja sobiv ettevalmistamise kontseptsiooni ja avariikontseptsiooni jaoks?
- Kas Windows Server 2003 ja teiste operatsioonisüsteemide nagu Windows 2000, Windows 95, Novell või Unix segarežiim on vajalik? Kui see on nii, siis mõjutab see süsteemis kasutatavaid autentimismeetodeid, mis võivad sõltuvalt teistest kasutatavatest operatsioonisüsteemidest sisaldada ka kitsaskohti ja seega vähendada kogu Windows Server 2003 keskkon-

na turvalisust. Segakeskkonna turvastandard peaks olema määratletud IT-turvapoliitikas.

Rollide planeerimine
Serverirollid tuleks defineerida osakontseptsioonide koostamise raames. Windows Server 2003 kasutuskontseptsioon määrab erinevate konfiguratsiooniabilistega kindlaks konkreetsed rollid, mis võetakse esmalt planeerimise lähtepunktiks. Rollid tuleb planeerida vastavalt kasutusvaldkonnale ja nõuete loetelule. Üksikute rollide osakontseptsioonides tuleb arvestada erinõuetega, näiteks eeldatava andmehulga ja koormusega, sideprotokollide ja –liidestega, pääsuõiguste kontseptsiooniga, vastavate operatsioonisüsteemi komponentide konfiguratsiooniga jne.

Rollid (valik)

Serveriroll	Serveri konfiguratsiooniabiline	Manuaalne konfiguratsioon	Turvakonfiguratsiooni abiline
Failiserver	x		x
Printimisserver	x		x
Rakendusserver	x		x
Meiliserver	x		
Terminaliserver	x		x
RAS/VPN server	x		x
Domeenikontroller	x		x
DNSi server	x		x
DHCP server	x		x
Voogmeedia server	x		x
WINSi server	x		x
Veebiserver		x	x
Kauginstalleerimise server		x	x
Bastion-host		x	
Sertifikaatide server		x	x

Turvakonfiguratsiooni abiline toetab mitmeid täiendavad Microsofti toodete serverirolle, näiteks andmebaasiserveri rolli.

Serverirollide kombineerimine

Rolle saab kombineerida ja seega vähendada niihästi soetamiskulusid kui ka administreerimisele kuluvate tööde hulka. Kombineerimisvõimalusi piiravad peamiselt järgmised aspektid:

- IT-süsteemi turvalisus / kaitsevajadus
- Windows Server 2003 disainist tulenevad piirangud
- nõuded skaleeritavusele

Järgnevad rollijaotuse võimalused on soovituslikud. Planeeritud rollikombinatsioonid tuleb kõikidel juhtudel läbi testida.

- Rakendusserver, sertifitseerimisserver, veebiserver, RAS/VPN server - neid rolle tuleks peamiselt turvalisuse huvides kasutada teistest rollidest eraldi.
- Terminaliserver, printimisserver - need rollid tuleb teistest rollidest eraldada peamiselt disaini- ja skaleeritavuse põhjustel. Printimisserverile installeeritakse näiteks teiste tootjate draivereid, mis võivad mõjutada serveri käideldavust.
- *Bastion-host* - *Bastion-host* on kaitsev arvuti, mis on otse ühendatud internetiga. *Bastion-host* 'e kasutatakse tavaliselt veebiserverite, DNS-serverite, FTP-serverite, SMTP-serverite ja NNTP-serverite funktsioonides. *Bastion-host* 'i roll sobib paljastatud olekus serveritele ja seda ei tohi kombineerida teiste serverirollidega.
- Kombinatsioonid - Infrastruktuuri teenuseid saab käitada koos ühel serveril. Kui kasutatakse *Active Directory* 't, tuleks DNS integreerida domeenikontrollerite alla. Kõrgendatud turvanõuete puhul keskmistes ja suurtes keskkondades ei tohiks omavahel integreerida WINS-i ja domeenikontrollerit.
- Andmeserverile on sageli võimalik lisada täiendavaid rolle, näiteks infrastruktuuri teenuseid. Lisaks võib andmeserver võtta enda kanda voogmeediaserveri rolli. Kauginstalleerimisteenuseid (RIS) on võimalik kasutada failiserveril, näiteks *Helpdesk* -juhtude raames. Siinjuures võivad aga kauginstalleerimisteenused mõjutada serveri turvalisust. Meiliserveri rollide teenuseid saab teatud administratiivsete või infrastruktuuriliste kasutusalade jaoks kombineerida teiste rollidega. Siinkohal tuleks nõuete loetelus selgelt vahet teha *Bastion-host* 'i rolliga.
- Muud serverirakendused ja -teenused - *Internet Information Services* (IIS) sisaldab baasteenuseid erinevate serverirollide jaoks (nt veebiserveri tarbeks), kuid ei moodusta iseseisvat serverirolli. Turbe seisukohalt tuleks planeerimisel vahet teha staatiliste ja dünaamiliste IIS-i komponentide vahel. Täiendavaid serverirolle saab luua lisatarkvara abil. Kokkusobivust standardsete rollidega tuleb kaaluda lähtuvalt konkreetsest olukorrast, seejuures tuleb arvestada eespool, rollide kombinatsioonide juures kirjeldatud võimalike konfliktidega. Planeerimine peaks toimuma tarkvara valikuprotsessi tulemuste baasil (vt B 1.10 Tüüptarkvara). 16-bitised rakendused ja muu vananenud tarkvara, mis ei paku rakenduse tasandil töötavaid turvamehhanisme või mis ei toeta Windows Server 2003 mehhanisme, kujutavad endast kõrgendatud turvariski. Seega tuleb Windows Server 2003 keskkonna planeerimisel arvestada eriliste varundamisnõuetega andmete ja võrgu tasandil. See on oluline nii tehnilisest kui ka töökorralduslikust küljest.
- Rollid heterogeensetes keskkondades - Olemasolevate teenuste ja rollidega heterogeensed serverikeskkonnad mõjutavad samuti rollide planeerimist,

eriti siis, kui olemasolevad teenused tahetakse Windows Server 2003 peale migreerida või sellega konsolideerida või kui teatud rolle tahetakse kasutada paralleelselt erinevatel platvormidel (selle klassikaliseks näiteks on DNS). Lõppkokkuvõttes sõltub rollide planeerimine ka olemasolevate andmekogumite ja tootmissüsteemide formaadist ja migreerimisvõimalustest ning sellega seotud lähema ja kaugema aja strateegiatest.

Serveri konfigureerimise kavandamine

Riistvara valimisel tuleb lähtuda jõudlusest, käideldavusest ja serveri rollist.

Jõudluse osas tuleb arvestada tootja miinimumnõudmistega, samuti nõuete kataloogiga. Microsofti veebilehel saada olevad koormuse simuleerimise tarkvaratööriistad võimaldavad ennustada Windows Server 2003 komponentide koormuskäitumist. Eriti hoolikalt tuleb prognoosida samaaegsete kasutajate maksimaalset arvu. Paljude kasutajate või intensiivse kasutamise puhul tuleb kaaluda mitme serveri koondamist klastriks. Planeeritud serverirollid ja serverirakendused, eeldatav koormus ning andmehulk on riistvara konfiguratsiooni edasiste parameetrite valimisel määrava tähtsusega. Olulisteks parameetriteks on näiteks kõvakettamassiivide ja partitsioonistruktuuride jaotamine. Sõltumatute kõvakettamassiivide (RAID- *Level*) sisseseadmine on soovitav teatud serverirollide, näiteks failiserveri või andmebaasiserveri jõudluse ja käideldavuse tagamiseks. Windows Server 2003 tarkvaralised RAID-variandid võimaldavad kiirelt ja soodsalt seadistada andmeliiasust. Siiski ei sobi nad jõudluse tõstmiseks ja ei suuda töö ajal kompenseerida ketta tõrget. Planeerimisel tuleb kindlasti eelistada riistvaralisi RAID-tasandeid. Partitsiooni struktuuri planeerimine peaks lähtuma eeldatavast andmehulgast ja erinevate andmeliikide loogilisest eraldamisest. Näiteks on mõistlik kasutada üht partitsiooni, mis sisaldab ainult operatsioonisüsteemi ja programmifaile. Kasutatavad või ajutised andmed tuleks laiali jaotada eri partitsioonidele, mis asuvad võimalusel erinevatel kettamassiividel. Windows Server 2003 SP1 või varasema puhul on andmekandjate kontingendid konfigureeritavad ainult partitsiooni või *Volume* 'i tasandil.

Võrguühendus

Windows Server 2003 kasutuse planeerimise raames tuleb arvestada sobiva võrguühendusega. Vajaminevad kommunikatsiooniprotokollid saab tuletada serverirollist või -rollidest. Siinkohal tuleb kontrollida, kas kommunikatsiooniprotokollid satuvad konflikti võrgu kontseptsiooniga, kommunikatsiooniprotokollide turvapoliitikaga või sõltuvalt olukorrast ka turvalüüside kontseptsiooniga. Serveri jaks andmete läbilaskevõimet valides võib lähtuda klientide poolt tehtavate pöörduste oletatavast arvukusest. Krüpteeritud juurdepääsude puhul tuleb arvestada, et jõudlus võib langeda. Sellele vastavalt tuleks jõudlust skaleerida, näiteks kiiremate protsessorite ja võrguadapteritega või tarkvaraliselt võrgukoormuse tasakaalustamise abil klastris Windows Server 2003 all. Niihästi kommunikatsiooniprotokollid kui ka andmete läbilaskevõime on käideldavuse olulised meetmed ja vajavad hoolikat planeerimist. Planeerides serverit, mille kaudu pääseb ligi ebaturvalistele võrkudele või mis asub eriti paljastatud olekus, näiteks internetiühendusega veebiserver, tuleb arvestada kõrgendatud turvanõuetega. Avalike serverite planeerimisel võib tegutseda sarnaselt kaitstud serverite planeerimisele, kuid planeerimise kõikide aspektide puhul tuleb lähtuda kõrgendatud ohust, mis tuleneb sissemurdmiskatse-

test, *Denial-of-Service* -rünnetest või muudest kompromiteerimiskatsetest. Lisaks tuleb määrata kontseptsioon, kuidas serverit/servereid kohtvõrgust isoleerida ja kuidas saab vajadusel kaitsta andmesidet, mis leiab aset suhtes kohtvõrguga. Näitena võib nimetada turvalüüse ja demilitariseeritud tsoone. Reeglina ei soovitav käitada kaitstud *Active Directory* keskkonna liikmesservereid avalikus asukohas või demilitariseeritud tsoonis. Turvalisuse kontekstid tuleb vastavalt eraldada.

Juurdepääsuvõimalused

Kasutamise planeerimisel tuleb arvestada ka sellega, milliseid juurdepääse läheb tarvis (NetBIOS kasutusload, WebDAV, DFS jne). Kommunikatsiooni turvalisuse tagamise seisukohast tuleb arvestada ka meetmetega M 4.277 Windows Serverite SMB, LDAP ja RPC kommunikatsiooni kaitse ja M 5.132 Windows Server 2003 WebDAV turvaline kasutamine . Iga lubatud juurdepääsu vajalikkust tuleb põhjendada.

Serveri administreerimise planeerimine

Kasutuse planeerimise raames tuleks arvestada järgnevate täiendavate aspektidega. Siinkohal tuleks kasutada eraldi osakontseptsioone, olemasolevaid kontsepte tuleb täiendada:

- Administreerimise planeerimine (vt M 2.364 Halduse planeerimine alates Windows 2003-st) võib hõlmata ka administreerimiseks vajaminevat lisatarkvara.
- Seire (seire, logimine, analüüs) (vt M 2.365 Windows Server 2003 süsteemiseire planeerimine).
- Turvapaikade haldus, värskendused.
- Ettevalmistamine (vt M 4.281 Windows Server 2003 turvaline installeerimine ja ettevalmistus ja M 4.283 Windows NT 4 Serveri ja Windows 2000 Serveri turvaline migratsioon Windows Server 2003-ks *)*
- Olemasolevate andmete ülevõtmine.

Nende aspektide otsused tuleb langetada Windows Server 2003 turvapoliitikas ja nendega edasisel planeerimisel arvestada. Enne tootmises kasutamist peab poliitika siduvas vormis valmis olema.

Litsentsimudel

Sobivad litsentsimudelid sõltuvad Windowsi süsteemi kasutusaladest. Litsentsi kontrollimise jaoks tarnitakse Windows Server 2003 koos toote võtme ja aktiveerimisega. Tuleb jälgida, et vaadeldud IT-kooslus oleks piisavalt litsentseeritud ja et üksiku Windows Server 2003 süsteemi jaoks oleks saadaval aktiveeritav või aktiveerimiseta installeerimisallikas ja litsents. Vajadusel tuleb sellega arvestada ettevalmistamise kontseptsioonis ja avariikontseptsioonis.

Täiendavad kontrollküsimused:

- Kas vajalikud serverirollid on tuvastatud ja nende sobivust kontrollitud?

- Kas vajalik koostalitlusvõime teiste IT-süsteemidega on tagatud?
- Kas võrguühenduse mahtuvus ja turvalisus vastavad nõuetele?

M 4.277z Windows Serverite SMB, LDAP ja RPC side kaitse

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator

Windowsi serverite ja klientsüsteemide vahelise side peamisteks protokollideks on SMB, RPC ja LDAP. Need protokollid on tihedalt seotud Windows Serverite turvaarhitektuuriga ja kasutavad turvalise side tagamiseks integreeritud tehnoloogiaid. Loetava teksti kujul sisselogimine, mida nimetatakse Windowsi puhul ka standardseks autentimiseks, tuleb ära keelata. Sama kehtib ka mõningate teiste, nõrga krüpteeringuga sisselogimismeetodite kohta, mida on üldkasutatavate auditeerimistööriistadega kerge kompromiteerida. Sisselogimine peab olema seega piisavalt tugevalt krüpteeritud ja seda nii Windowsi keskkonnas endas kui ka Windowsi ja teiste IT-süsteemide (nt Samba või MacOS-Xi) vahelise side puhul. Planeerimisel tuleb arvestada, et mõned SMB, RPC ja LDAP standardsed seadistused on pärast tüüpinstalleerimist veel määramata. Seadistusi kajastava info leiate IT-etalonturbe abivahendite alt (vt *RPC, SMB ja LDAP Windows Server 2003 all* teemas *Windows Server 2003 abivahendid*). Turvaseadistusi tuleb kontrollida ja vajadusel kohandada. Lisaks seal mainitud seadistustele peaksid olema sisse lülitaud ka vähemalt Windows Server 2003 ja SP1 tüüpsed turvaseadistused (vt *Microsoft Security Guide* „ *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP* “ (versioon 2.0, kuupäevaga 27. detsember 2005) tabelit *Windows Default Security and Services Configuration.xls*).

Ühilduvus

Pärast tüüpinstalleerimist tehtavad turvaseadistused on seotud G 2.114 Windowsi Serveri ühtimatud SMB, RPC ja LDAP turbeseadistused all kirjeldatud ohtudega. Heterogeenses võrgus tohib neid seadistusi muudatuste haldussüsteemis kinnitada alles pärast seda, kui nende sobivust kõikide asjassepuutuvate süsteemidega on isoleeritud testsüsteemi keskkonnas edukalt testitud. Testi ajal tuleks kontrollida ka käideldavust suurtel koormustel. Süsteemide all peetakse siinkohal silmas erinevate Windowsi versioonide ja *Service Pack* -ide kliente ja servereid, samuti erinevaid operatsioonisüsteemi platvorme. Põhjalikud ühilduvusjuhised on dokumenteeritud *Microsoft Knowledge Base* artikli 823659s. Mõned peamised ühilduvusjuhised, sobivad tarkvaratööriistad ning aktiveerimisega seotud tegutsemisjuhised leiduvad ka IT-etalonturbe abivahendite hulgas (vt *RPC, SMB ja LDAP Windows Server 2003 all* teemas *Windows Server 2003 abivahendid*).

Turvamallid

Seadistusi tuleb teha serveri turvamallis, vt meedet M 2.366 Windows Server 2003 turvamallide kasutamine .

Dokumentatsioon

Minimaalne dokumentatsioon peab sisaldama iga serveri tõhusat turvamalli ja nende sisu. Kui mõningaid seadistusi ei ole üle võetud mitte kõikides, vaid ainult osades valdkondades, tuleb vastavad alad piiritleda, seda põhjendada ja viidata alternatiivsetele turvameetmetele nagu näiteks serveri tugevam isoleerimine või

IPSec protokolli aktiveerimine (vt M 5.90 Protokolli IPSec kasutamine Windowsi keskkonnas).

Täiendavad kontrollküsimused:

- Kas Windowsi keskkonnas toimuva side tüüp-turvaseadistusi on vastavalt käesoleva meetme soovitustele kohandatud ja testitud?
- Kas sideprotokollide autentimisprotseduurid on piisavalt kaitstud?
- Kas heterogeensete võrkude puhul võeti arvesse ühilduvust ja käitumist erinevate koormuste korral ning kas seda testiti isoleeritud keskkonnas?

M 4.278z EFS-i turvaline kasutamine Windows Server 2003 keskkonnas

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator, kasutaja

Windows Server 2003/XP krüpteeriv failisüsteem (*Encrypting File System*, EFS) on kasutajale lihtne käsitseda ning võimaldab töötada krüpteeritud failidega rakendustest sõltumatult. Eriti hästi sobib see üksikkasutajatele ja avalikele klient-arvutitele, mida kasutatakse teatud aja jooksul väljaspool kaitstud IT-keskkonda. Peaeesmärgiks on eraldiseisvate lokaalsete andmete konfidentsiaalsuse tagamine. Asjakohased põhitõed leiate meetmest M 4.147 EFS-i turvaline kasutamine Windows 'i keskkonnas . Samas ei sobi EFS eriti hästi kaugserverites (nt failiserverites) asuvate tsentraliseeritud kasutajaandmete läbivaks krüpteerimiseks. See on võimalik ainult võtmehalduse spetsiaalse planeerimise abil. Suurte andmehulkade ja suure hulga kasutajate võtmete kaitsmisega kaasneb paratamatult töömahu oluline suurenemine.

Erinevused juurutamisel

Planeerimise alguses tuleb selgelt eristada, kas EFS-iga tuleb tagada serverile salvestatud andmete krüpteerimine võrgus või kas on tarvis krüpteerida ainult lokaalse serveri sessioonide andmeid ja konfidentsiaalseid administratiivseid andmeid. Viimase puhul töötab arvuti nagu aktiveeritud EFS-iga klient-arvuti ja seetõttu tuleks rakendada meedet M 4.147 EFS-i turvaline kasutamine Windows 'i keskkonnas . Siiski tuleks olla ettevaatlik ja vältida liigset krüpteerimist süsteemi seisundiinfo (nt DNS-tsoonifailide, printimisserverite ootejärjekordade), logifailide (nt IIS-logi) ja ühiste ajutiste kaustade (*C:\WINDOWS\Temp*) puhul. Enne selliste kriitiliste failide krüpteerimise sisselülitamist tuleks simuleerivates tingimustes testida tegelikku koormust, vastasel korral võib G 4.54 Turbe kadu krüptofailisüsteemi (EFS) kasutamisel hävitada kogu serveri. Üheks võimaluseks, kuidas suurendada EFS-i abil administratiivsete sessioonide turvalisust serveris, on krüpteerida sessiooni andmed (nt ajutised kataloogid, töölaua kaustad, isiklikud failid, printimise ootejärjekorrad) ning konfidentsiaalsed tööandmed, näiteks dokumentatsioon. See on vähem kriitiline, kuna probleemi korral lakkab töötamast profiil, kuid tsentraalsed teenused jäävad puutumata. Rakendused loovad failidest töö ajal regulaarselt ajutisi koopiaid. Tuleb kontrollida, milliseid kaustasid rakendused ajutiste failide jaoks kasutavad. Nende kaustade jaoks võib EFS-i aktiveerida, et volitusteta kolmandad isikud ei saaks neid töötlemise ajal näha.

Kaugandmete (võrgus asuvate, serverile salvestatud failide) krüpteerimisteenusena tuleks EFS-i kasutada ainult siis, kui serveriandmete konfidentsiaalsuse tõttu on tarvis ülimalt kõrget turvalisust ja täiendavad riskid ning töömaht on õigustatud. See tuleb fikseerida IT-keskkonda käsitlevas poliitikas. EFS-i kasutusala tuleb täpselt määratleda. Seejuures tuleb arvestada ka infoga G 4.54 Turbe kadu krüptofailisüsteemi (EFS) kasutamisel. Kui EFS-i kasutatakse koos WebDAV-lubadega, ei toimu faili krüpteerimine mitte serveril, vaid hoopis klientsüsteemis. Krüpteeritud faili võib lisada WebDAV-kinnitusele HTTP-ülekande abil. EFS-i pole selleks tarvis serveril aktiveerida. Kasutaja jaoks on riskid samad nagu failide lokaalsel krüpteerimisel tema klientsüsteemis. Ülalmainitud poliitikas tuleb määratleda, kui suures ulatuses peab administraator tagama tsentraalseid vahendeid selliste andmete hooldamiseks, varundamiseks ja taastamiseks juhtudel, kui võti kaotatakse. Mida

laiaulatuslikumalt seda vajatakse, seda kõrgemad on nõuded ja tsentraalse võtmehalduse töömaht. EFS-i aktiveerimine ametiasutuse või ettevõtte keskkonnas on soovitav ainult juhul, kui samaaegselt kasutatakse ka *Public Key* infrastruktuuri (PKI) ja konfigureeritud taastamisagenti.

EFS-i desaktiveerimine
Pärast Windows Server 2003 standardset installeerimist on EFS aktiivne. Taastamisagent on konfigureerimata seisundis. EFS tuleks normaalse töö tagamiseks serveri turvapoliitikas desaktiveerida:

Start | Control Panel | Administrative Tools | Local Security Policy | Public Key Policies | Encrypting File System, desaktiveerida omadus *Allow users to encrypt files using Encrypting File System.*

Active Directory keskkonnas tuleks see seadistus kehtestada grupipoliitika abil kõikidele serveriarvutitele ja klient-arvutitele.

Kui EFS desaktiveeritakse töötavas süsteemis mõnel hilisemal ajal, tuleks süsteemist üles leida kõik krüpteeritud andmekogumid. Seda saab teha Windows Server 2003 *Support Tools* programmiga *EFSinfo.exe*. Käsurea käsu näide: efsinfo /s:c:\

DRA rollide lahutamine

Rollide õige lahutamine ei lase administraatoritel piiramatult krüpteeritud andmetele ligi pääseda. Oluline on siinkohal andmete taastamisagent (*Data Recovery Agent*, DRA), millega saab andmeid taastada tsentraalselt ja krüpteeritavatest kasutajatest sõltumatult. Andmete taastamisagendid luuakse spetsiaalsete turvasertifikaatidega. DRA puhul tuleb kinni pidada järgnevatest tingimustest:

- DRA sertifikaati ei tohi siduda eeldefineeritud administraatorikontoga,
- DRA rolli kandvatel kasutajakontodel ei tohi üldjuhul olla administraatori õiguseid,
- andmete taastamisagente tuleb luua võimalikult vähe,
- DRA kasutamiseks tuleb alati rakendada eraldi kontot.

DRA privaatvõti tuleks koos kaitstud parooliga eksportida välisele andmekandjale ja süsteemist kustutada. Privaatvõtme varundusega andmekandjat tuleb hoida piiratud juurdepääsuga kohas (seifis). Turvalisuse suurendamiseks võib paroole hoida andmekandjatest eraldi. Kaaluda tuleks riistvaralise turvamooduli (HSM, vt B 1.7 Krüptokontseptsioon) kasutamist, mis suurendaks DRA privaatvõtme turvalisust.

Andmevarundus

Andmevarunduse teenusekonto ei tohi omada EFS-i sertifikaati ega ka taastamise sertifikaati ja peab seega suutma andmeid ainult krüpteeritult lugeda ja varunduse andmekandjale kirjutada.

Aegunud DRA-sertifikaadid

Aegunud DRA-sertifikaadid mõjutavad turvalisust kriitiliselt, kuna nad:

- võimaldavad juurdepääsu kõikidele seni krüpteeritud andmetele (ohustavad konfidentsiaalsust) ja
- kujutavad endast serveril oleva, seni krüpteeritud andmekogumi ainukest taastamisvõimalust (ohustavad käideldavust).

Enne vana DRA-sertifikaadi aegumist tuleb lisada uus, kuna krüpteerimine lakkab töötamast vahetult pärast aegumist. Uue DRA jaoks tuleb rakendada samu turvameetmeid (vt eespool). Sellega tuleb planeerimisel ja käitamisel arvestada. Vanu DRA-sertifikaate on mõistlik kõrvaldada alles pärast seda, kui kogu andmekogum on dekrüpteeritud ja uue DRA-ga taas krüpteeritud. Sõltuvalt andmete hulgast ja organiseerituse astmest võib sellega kaasneda suur töömaht ning tõsine risk seoses andmete käideldavuse ja tervikluse tagamisega, seega tuleks seda teha ainult eriolukorras, näiteks kui seniste DRA-sertifikaatide võtmete tugevust ei peeta enam piisavaks.

Tsentraalne võtmehaldus

EFS nõuab defineeritud tsentraalset võtmehaldust. Lokaalse serveri või klientide ise allkirjastatud sertifikaate vältimiseks oleks äärmiselt mõistlik kasutada *Public Key* infrastruktuuri (PKI). Lisainformatsiooni selle teema kohta leiate IT-etalonturbe alt. Lisaks tuleks lubada EFS-i sertifikaatide automaatset pikendamist, kuna pärast nende aegumist võetakse kasutusele ise allkirjastatud sertifikaadid. Taastamisagendi kindlaks määramine on hädavajalik, et ennetada ohtusid nagu G 4.55 Andmekadu alates Windows Server 2003 / XP parooli taastamisel. Vastava assistendi leiate asukohast *Start* | *Control Panel* | *Administrative Tools* | *Local Security Policy* | *Public Key Policies* | *Encrypting File System* menüü *Action* | *Add Data Recovery Agent* ... Kasutajavõtme kaotamise riski saab vähendada, kui lubatakse privaatvõtmete arhiveerimist EFS-i sertifikaate väljastaval sertifitseerimisüksusel. Võtmete tsentraalne salvestamine suurendab aga kahjuks jällegi kuritarvitamise riski. Sellega suureneb oluliselt sertifitseerimisteenuste organisatoorne ja administratiivne töömaht, eriti võtmete taastamisagentide, rollide lahutamise ja sertifitseerimisüksuse kaitse osas.

Taastamisjaam

Suuremates IT-kooslustes tuleks kaaluda taastamisjaama sisseseadmist, mida hoitakse turvatud juurdepääsuga alas ja aktiveeritakse ainult vajadusel. Krüpteeritavaid faile saab kanda varundamistööriista abil (nt *ntbackup*) taastamisjaamale ja seal DRA-võtme abil taastada. DRA-võti võib jääda taastamisjaamale. Taastamisjaama kasutamise täiendavaks eeliseks on asjaolu, et ebausaldusväärne tarkvara ei saa ohustada taastamisjaamas hoitavat võtit.

Taastamisjaama jaoks saab kasutada virtualiseerimistehnoloogiat. See tähendab, et kogu operatsioonisüsteem paigaldatakse simuleeritud riistvarakeskkonda. See muudab virtuaalse keskkonna salvestamise vahetatavale andmekandjale ja selle turvalise hoiustamise hõlpsaks.

Koolitus

Kasutajaid tuleb koolitada, et nad tunneks EFS-i funktsioone ja riske. EFS-i kasutamisega saab turvalisust suurendada, kui kasutajad on koolitatud ja võtmehaldus rakendatud.

Täiendavad kontrollküsimused:

- Kas EFS-i kasutatakse ainult konfidentsiaalsusega seonduvate kõrgete kaitsevajaduste puhul?
- Kas kasutusvaldkond (nt sessiooni andmete krüpteerimine serveril) on selgelt määratletud ja kõik kasutajad piisavalt koolitatud?
- Kas andmete taastamisagentide (DRA-de) kasutamine on piiritletud?
- Kas aegunud DRA-sertifikaate hoitakse kindlas kohas?
- Kas andmete varundamise teenusekontolt on EFS-i ja taastamissertifikaadid eemaldatud?
- Kas on olemas tsentraalne võtmehaldus *Public Key* infrastruktuuri (PKI) kujul?
- Kas kasutatakse taastamisjaama?

M 4.279z Windows Server 2003 laiendatud turvaaspektid

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator

Kõrgendatud kaitsevajadusega IT-kooslustes, milles kasutatakse Windows Server 2003-e, tuleb sellise kaitsetaseme saavutamiseks võtta tarvitusele lisameetmed. Siinkohal pole silmas peetud mitte ainult süsteemi üldise käideldavuse suurendamist (liiasust, kõrge käideldavusega klastrit), vaid ka sihipäraseid meetmeid rakenduste, andmete ja võrgus toimuva andmeliikluse suurema usaldusväärsuse ja terviklikkuse tagamiseks. Need meetmed võivad piirata funktsioonide kasutamist ja koostalitlusvõimet. Seetõttu tuleks alati kasutada testkeskkonda, et tagada vajalike funktsioonide säilimine. Järgnevalt selgitatud aspektid on üldistavad ja kaugeltki mitte ammendavad. Sõltuvalt serveri rollist, kasutamisotstarbest ja vastavast ohuastmest tuleb võtta tarvitusele lisameetmed. Täiendavaid asjakohaseid pidepunkte leiate Windows Server 2003 spetsiifikat käsitlevatest meetmetest.

Toote aktiveerimine

Toote võrgu kaudu aktiveerimine vajab töötavat internetiühendust ja HTTP-protokolli. Installeerimise ajal tuleks see ühendus realiseerida ainult proksiserveriga turvalüüsi kaudu, mis tähendab, et valikut *AutoActivate* tohib kasutada ainult koos valikuga *ActivateProxy*. Selleks tuleb vastusfaili töödelda käsitsi. Aktiveerimise võib hiljem aktiveerida skriptjuhtimisega (nt installeerimisjärgse skriptis) või käsitsi.

Serveri kõrge turbevajaduse korral võib kasutada ka telefoni teel aktiveerimist.

Krüpteerimine

IPSec -i abil saab turvata kõiki klientsüsteemi sisenevaid ja sealt väljuvaid IP-del põhinevaid kommunikatsiooniühendusi. Seejuures on võimalik autentida kommunikatsiooni lõpp-punkte ja edastada andmepakette allkirjastatult ja krüpteeritult nõnda, et tagatakse kõrgendatud turbenõuetega kaasnev andmete terviklikkus ja konfidentsiaalsus. *IPSec* -infrastruktuuri osakontseptsioon peaks arvestama kasvava administreerimistööde mahuga ja see eeldab testkeskkonnas teostatavat asjaosaliste süsteemide ühilduvuse kontrolli. Kui SSL/TLS-protokolli ja *Encrypting File System* (EFS) jaoks läheb tarvis USA ametkonna NIST (*National Institute of Standards and Technolog*) FIPS (*Federal Information Processing Standard*) suunistele vastavat krüpteerimist, saab seda määrata valikus konsool *Local Security Settings* | *Local Policies* | *Security Options* | *System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing.* Aktiveerimine tähendab turvalist krüpteerimist (nt 3DES), kuid mitte ilmtingimata alati maksimaalset võtmepikkust. Näiteks ei arvestata AES-iga (EFS-i puhul). Kõikidel juhtudel tuleb kindlasti arvestada ka suureneva arvutusvõimsusega ja selle võimaliku mõjuga serveri koormuskäitumisele. Lisaks tuleks *System cryptography: Force strong key protection for user keys stored on the computer* seada vähemalt *User is prompted when the key is first used* peale. Sellega sunnitakse turvasertifikaadi privaatvõtme juurde pääsemiseks sisestama parooli.

Kõrge käideldavus

Kõrgete käideldavusnõuete puhul tuleb liiasusega varustada võib-olla mitte ainult serveri riistavara osad, vaid kogu server, ja koondada see kõrge käideldavusega klastrisse. Windows Server 2003 *Enterprise Edition* toetab klastriteenuse

abil kaheksat sõlme ühes klastris, mida saab optimeerida vastavalt kõrge käideldavuse nõuetele ja koormuse jaotusele. Kõik liiasusega serverid peavad vastama ühtsetele riistvaranõuetele. Rollide planeerimisel tuleb arvestada klastri planeerimisega, kuna teatud teenuste klasterdamisvõimalused on piiratud. Võrgu koormuse tasakaalustamist toetab mitte ainult *Enterprise Edition*, vaid ka *Web Edition* ja *Standard Edition*.

Denial-of-Service

Kaitseks DoS rünnete vastu tuleks kontrollida serveri TCP/IP-seadistusi (vt IT-etalonturbe abivahendeid, *Windows Server 2003 IP-protokollide kaitse* teemas *Windows Server 2003 abivahendid*) ja vajadusel seadistada. Registrivõtme määramiseks soovitatakse kasutada administratiivseid malle (vt M 2.368 Administratiivsete mallide kasutamine alates Windows Server 2003-st). Nimetatud meetmeid tuleks kindlasti kasutada juhtudel, kui serverit kasutatakse nähtavas keskkonnas, näiteks turvalüüsina või demilitariseeritud tsoonis (DMZ). Kaitstud IT-keskkonna piires pole nende kasutamine kohustuslik. Veebiserveri või nn bastion-host'i (ettevõtte võrgu avalikult ligipääsetava arvuti) puhul läheb tarvis täiendavaid spetsiaalseid kaitsemeetmeid, mida on kirjeldatud moodulis B 5.10 Interneti Information Server (IIS).

Plug and Play

Olukorras, kus server ei ole volitusteta juurdepääsude eest piisavalt kaitstud, kujutab endast täiendavat potentsiaalset ohtu automaatne riistvaratuvastus (*Plug and Play*). Tavaliselt piisab sellest, kui desaktiveeritakse kõik mittevajalikud ühendused (nt BIOS-is ja Windowsi seadmehalduris). Vahetatavate andmekandjate kettaseadmed tuleks eemaldada või sulgeda või teiste firmade tarkvaratööriistade abil kontrolli alla saada. Windows Server 2003 pakub vastavaid funktsioone ainult väga piiratud kujul. *Plug and Play* täielikku eiramist ei ole Windows Server 2003-s ette nähtud ja selle rakendamine mõjutaks süsteemi stabiilsust. Testimise töökulu ja risk on õigustatud ainult eriti kõrgete turvanõuete puhul.

Ressursivolitused

Süsteemikataloogide ja süsteemiobjektide standardsed ressursivolitused on piirava iseloomuga, kuid väga kõrge kaitsevajaduse puhul on tarvis neid täiendavalt tugevdada. Selleks eemaldatakse teatud standardsetelt gruppidelt mõningad volitused ja seotakse need konkreetsete kasutajakontodega. Seadistused konsoolis *Local Security Settings* | *Local Policies* | *Security Options* | *System objects: Default owner for objects created by members of the Administrators group* töötavad standardina valikul *Administrators group*. Kasutajatel on alati oma objektile erivolitused. Lisaks ei saa optimaalselt lahendada gruppide kui objektide omanike seiret. Seadistus *Administrators group* tuleks asendada seadistusega *Object creator*. See muudab serveri administreerimise siiski oluliselt keerulisemaks.

M 4.280 Turvaline põhikonfiguratsioon alates Windows Server 2003-st

Algatamise eest vastutavad: IT-juht, infoturbe spetsialist
Rakendamise eest vastutavad: administraator

Turvaline konfiguratsioon tähendab turvapoliitikast ja -reeglitest, serveri rollidest ja IT-keskkonnast tulenevate seadistuste rakendamist. Mitmed seadistused korduvad nii erinevate rollide kui ka kasutusotstarvete puhul. Turvaline põhikonfiguratsioon tuleb luua juhtudel, mis tegelevad serveri ettevalmistamisega, serveri konfiguratsiooni muutmisega ning olukordades, kus poliitikad ja ettekirjutused on muutunud. Lisaks tuleks seadistuste elluviimist regulaarselt kontrollida, et vältida igapäevastest administreerimistöödest või muudest mõjudest tulenevaid valeseadistusi. Vajalikud seadistused tuleb identifitseerida näiteks kontrollnimekirja kujul. Nimekirjas tuleks arvestada etalonturbe modelleerimisel kindlaks tehtud meetmetega.

Standardsed turvaseadistused ja turvamallid

Leitud seadistuste jaoks tuleks vajadusel koostada turvamallid ja administratiivsed mallid (M 1.1 Vastavus normidele ja eeskirjadele). See tõstab põhikonfiguratsiooni standardiseerimise ja automatiseerimise taset, samuti on seadistusi hiljem lihtne kontrollida ja auditeerida. Põhikonfiguratsiooni saab suhteliselt vähese vaevaga dokumenteerida, kui mallid eksportida ja lisada dokumentatsioonile. Sellele tuginedes saab IT-muudatuste halduses (M 2.221 Muudatuste haldus) luua põhikonfiguratsioonile kinnitamise protseduuri. Mainitud aspektid eeldavad, et Windows Server 2003 ja Server 2008 standardsete seadistustega ei manipuleerita meelevaldselt. Standardsed grupipoliitikad peaksid jääma samaks, süsteemisiseste kontode (nt *NT Authority*) baasvolitusi ei tohiks muuta. Standardvolitused alamkomponentides, näiteks WMI ja komponentide teenustes, peaksid alles jääma. Kõrvalekalded tuleb planeerida, põhjendada ja ellu viia kontrollnimekirjade abil, eriti kui kõrvalekalde tulemuseks võib olla turvastandardi langemine. Standardseadistuste etaloniks on kaasasolevad turvamallid, peamiselt *defltsv.inf* (serverile) ja *defltdc.inf* (domeenikontrollerile), mis asuvad kaustas *C:\WINDOWS\inf*. Mallis *setup security.inf* (kataloog *C:\WINDOWS\security\templates*) on kirjas kõik seadistused pärast installeerimisprogrammi lõpetamist. Versioonis Windows Server 2008 on saadaval üksnes järgmised turvamallid:

- Defltbase.inf;
- Defltsv.inf (serverile);
- Defltdc.inf (domeenikontrollerile). Need mallid salvestatakse eranditult Windowsi installikausta *%systemroot %\inf*.

Lisateavet leiate meetmest M 2.366 Windows Server 2003 turvamallide kasutamine .

Windows Server 2008 konfigureerimiseks, st mallifailide juhtimiseks ja muutmiseks, tuleks kasutada tsentraalset haldustööriista Microsoft Security Compliance Manager (vt meetmed M 2.491 Windows Server 2008 rollide ja turvamallide kasutamine ja M 4.416 Windows Server Core'i kasutamine). Etalonideks on ka turvakonfiguratsiooni abilise konfiguratsioonimallid (alates Windows Server 2003 SP1-st), tabel „Windows Default Security and Services Configuration.xls" (tootja dokumentatsioonist „Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP", versioon 2.0), IT-etalonturbe meetmed või muu tootja dokumentatsioon. Alates Windows Server 2008-st tuleb arvestada dokumendi „Windows Server 2008 Security Baseline Settingsi" seadistustega. See tabel kuulub Security Compliance Management Toolkiti hulka. Selle meetme järgmistes lõikudes loendatakse mõningaid seadistusi ja nõudeid. Neid ei kajastata ei Windows Server 2003 ega ka Windows Server 2008 teistes meetmetes, kuid need mõjutavad põhikonfiguratsiooni turvalisust. Nendega tuleks kontrollnimekirja koostamisel samuti arvestada. Etalonideks on ka turvakonfiguratsiooni abilise konfiguratsioonimallid (alates SP1), tabel *Windows Default Security and Services Configuration.xls* (tootja dokumentatsioonist „ *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP* " versioon 2.0 kuupäevaga 27. detsember 2005 või hilisem), IT-etalonturbe meetmed või muu tootjapoolne dokumentatsioon.Käesoleva meetme järgnevates lõikudes loendatakse mõningaid seadistusi ja nõudeid. Neid ei kajastata Windows Server 2003 teistes meetmetes, kuid nad mõjutavad põhikonfiguratsiooni turvalisust. Nendega tuleks kontrollnimekirja koostamisel samuti arvestada.

Olulised turvalisusega seotud funktsioonid

Kõvaketta partitsioone tuleks esimesel formaatimisel formaatida ainult NTFS-iga. Windows Server 2003 ja Server 2008 installeerimisprogramm tagab vajadusel installeerimise käigus süsteemi partitsioonide konverteerimise. Töösoleva süsteemi puhul tuleks siiski hoiduda FAT32-partitsioonide tagantjärele konverteerimisest ja otsustada kohe NTFS-i kasuks. Töömälu saalimisfailist saab ekstraheerida krüpteerimata andmeid. Saalimisfail tuleks igal väljalülitamisel automaatselt kustutada:

Start | *Control Panel* | *Administrative Tools* | avage konsool *Local Security Policy* | valige sõlm *Local Policies* | *Security Options* | *Shutdown: Clear virtual memory pagefile*

Juhtudel, kui server pole volitusteta juurdepääsude eest piisavalt kaitstud, on ohtlikud ka automaatse riistvaratuvastuse (*Plug and Play*) ning *Autorun* 'i (programmide automaatne käivitamine) funktsioonid. Kõik ebavajalikud ühendused tuleb desaktiveerida (nt BIOS -is ja Windowsi seadmehalduris). Kaaluda tuleks ka võimalust vahetatavate andmekandjate kettaseadmed eemaldada või füüsiliselt tõkestada. Võimalik on ka kontrollida vahetatavaid andmekandjaid teiste firmade tarkvaratööriistade abil. Windows Server 2003 ei paku selleks piisavaid vahendeid. Windows Server 2008 kasutuselevõtuga saab seda osaliselt konfigureerida. Alates Windows Server 2008 kasutuselevõtust saab grupipoliitikaobjektidega vähemalt osaliselt konfigureerida ka vahetatavaid andmekandjaid. Mitme serveri turvaline käitamine eeldab sünkroonset süsteemiaega. Selleks võib kasutada süsteemis olevat *Network Time Protocol* -i (NTP) klienti. Kasutajatel on alati oma objektidele erivolitused. Kui administratiivne kasutaja loob objekti, on standardi-

na omanikuks lokaalne turvagrupp *Administraatorid*. Gruppide kui objektide omanike seiret ei saa optimaalselt korraldada. Andmekandjate kontingente juhitakse samuti diskreetsete kasutajate failiomanduste alusel. Kui grupid on andmete omanikud, esineb kontingentide eksitavaid sissekandeid ja seiretulemusi (alates Windows Server 2003 R2-st). See probleem tuleks esmajoones lahendada sobivate kontseptsioonidega, mis puudutavad selliseid valdkondi nagu seireseadistused, volitused (nt volituste kontseptsioon) ja andmekandjate kontingendid (nt failiserveri osakontseptsioon).

Kui ei lähe tarvis ühilduvust Windows NT 4.0, Windows ME/98 või varasemaga, tuleks kaaluda võimalust lubade anonüümne loendamine välja lülitada:

Start | *Control Panel* | *Administrative Tools* | avage konsool *Local Security Settings* | valige sõlme *Local Policies* | *Security Options* | *Network Access: Do not allow anonymous enumeration of SAM accounts and shares* väärtuseks *Enabled*.

Täiendavad turvakomponendid

Windows Serverite muutmata installeerimisandmekandjate peal on olemas piiratud käsuviiba keskkond (*Recovery console*), mida on võimalik serveril käivitada operatsioonisüsteemi asemel. Selle abil saab installeeritud Windowsi operatsioonisüsteemi konfiguratsiooni muuta. Autentimiseks küsitakse Windows Serverite installeerimisel standardina sisse seatavat administraatorikonto parooli. See töötab sõltumata sellest, kas konto on ümber nimetatud või desaktiveeritud. Taastamiskonsooli saab paigaldada otse kõvakettale ja see käitub nagu täiendavalt installeeritud operatsioonisüsteem. Mõlemal juhul kujutab see endast sekkumist buutimisse, mistõttu on see ebapiisavalt kaitstud. Taastamiskonsooli installeerimine ei tohiks seega toimuda meelevaldselt, vaid peab olema reguleeritud. Standardinstalleerimise järgsed turvaseadistused (*Start* | *Control Panel* | *Administrative Tools* | avage konsool *Local Policies* | valige sõlm *Local Policies* | *Security Options* | *Recovery Console*) tuleks säilitada. Pärast tüüpinstalleerimist on aktiivne *Internet Explorer Enhanced Security Configuration* (*Control Panel* | *Software* | *Windows Components*). Seda komponenti tohib desaktiveerida ainult siis, kui mõni Internet Exploreril põhinev rakendus (mõne teise firma oma), mida serveril vajatakse, sellega ei ühildu. Windowsi tulemüür laetakse alates Windows Server 2003 SP1-st buutimisel koos TCP/IP-protokolliga ja aktiveeritakse – nõnda kaitstakse TCP/IP-protokolli juba buutimise ajal paremini. Teenuse *Windows-Firewall/ Internet Connection Sharing* seadistus peab selleks olema *Automatic*.

Pärast buutimist on tulemüüri funktsioon (mitte teenus ise) standardina taas desaktiveeritud. Kohtvõrgu turvaintsidentide vastu (kahjulike programmide leviku ja seest tulevate rünnete vastu) on server kaitsetu. Seega tuleks turvalise baaskonfiguratsiooni puhul kaaluda võimalust aktiveerida Windowsi tulemüür. Selleks võib sihilikult tüüpilised teenused ja funktsioonid lokaalses grupipoliitikas (*Start* | *Run . . .* | *gpedit.msc*) kasutusse lubada (*Computer Configuration* | *Administrative Templates* | *Network* | *Network Connections* | *Windows Firewall*) või konfigureerida SCW abil. Windowsi tulemüür toetab RPC-teenuseid, mis töötavad eeldefineeritud kontode *Local System*, *Local Service* ja *Network Service* kaudu, näiteks kaugadministreerimise jaoks. RPC-teenustega lisatarkvara tuleb esmalt testida.

Ebavajalike funktsioonide väljalülitamine

Windows Server süsteemis on sageli aktiveeritud põhi- ja abifunktsioonid, mida ei lähe alati tarvis. Kehtib põhimõte: desaktiveerida, et vähendada võimalusi rünneteks ja kahandada ebavajalikke riske. Selle tulemusel võib langeda Windows

Server 2003 paindlikkus ja kasvada administreerimise töömaht. Turvalisuspõhjustel tuleks desaktiveeritud funktsioone sellegipoolest aktiveerida ainult koos vastava põhjenduse/dokumentatsiooniga. Tuleb täpselt kaaluda, millised funktsioonid on Windows Server 2003 või Server 2008 konkreetse kasutusotstarbe jaoks vajalikud ja aktiveerida ainult need. Ebavajalike funktsioonide info asub ka tootja dokumentatsioonis „*Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP*“ versioon 2.0 kuupäevaga 27. detsember 2005 või hilisem, mainitud Exceli-failis *Windows Default Security and Services Configuration.xls*. Ebavajalikud funktsioonid tuleb reeglina desaktiveerida. Teenuste liigne väljalülitamine võib süsteemi viia töökõlbmatusse seisu. Süsteemi käideldavuse säilitamiseks tuleb eelnevalt läbi viia vastavad testid.

Dokumentatsioon
Põhikonfiguratsiooni dokumentatsioon peab vastama muudatuste halduse nõuetele. See peaks sisaldama kõiki kasutatud malle koos versiooni numbrite ja kirjeldusega. Iga serveri puhul peab olema näha, millised mallid talle mõjuvad.

Täiendavad kontrollküsimused:

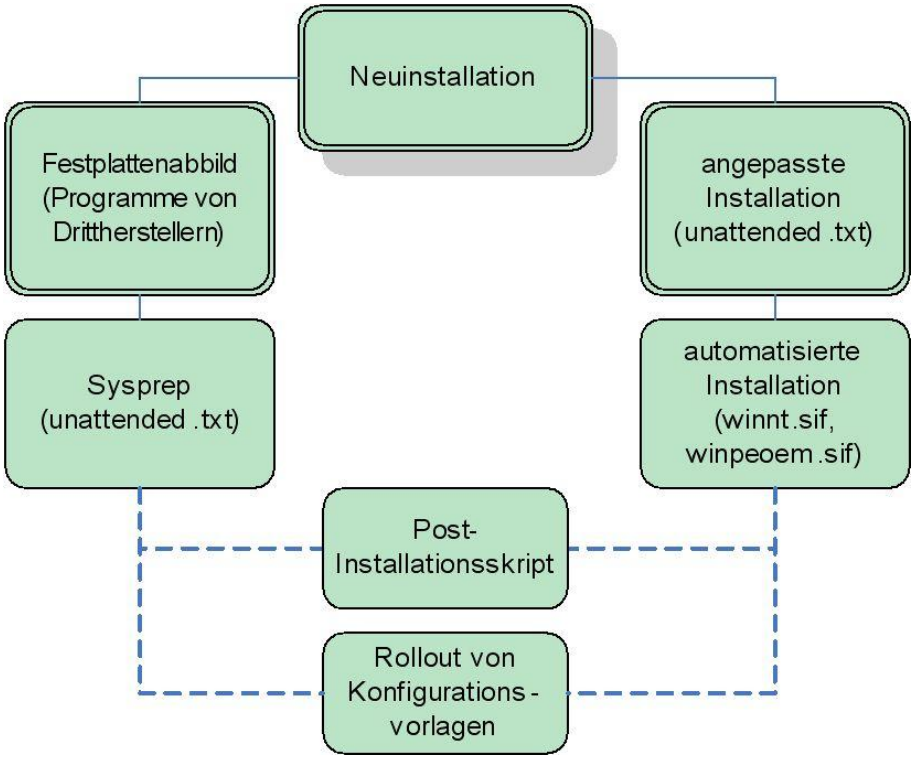
- Kas on olemas kontrollnimekiri või mõni muu dokument, milles on dokumenteeritud kõik seadistused?
- Kas kõikide vajalike seadistuste jaoks on vajaduse korral olemas turvamallid ja administratiivsed mallid?
- Kas grupi liikmelisuse, süsteemisiseste kontode ja volituste standardseadistused on säilitatud muutmata kujul?
- Kas kõik ebavajalikud riistavaraühendused on desaktiveeritud?
- Kas süsteemiaeg on teiste IT-süsteemide ajaga sünkroniseeritud?
- Kas on olemas kontseptsioon, mis ei lase gruppidel olla objektide omanikud?
- Kas taastamiskonsooli jaoks on olemas poliitika?
- Kas Windowsi tulemüüri teenus aktiveeritakse buutimise ajal automaatselt?
- Kas kõik ebavajalikud funktsioonid on välja lülitatud?
- Kas muudatuste halduse jaoks on olemas dokumentatsioon?

M 4.281 Windows Serveri turvaline installeerimine ja ettevalmistus

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator

Ettevalmistamine hõlmab kõiki aktiivsele kasutamisele eelnevaid samme pärast serveri või serverigrupi planeerimist ja soetamist. Eriti kriitilise tähtsusega on operatsioonisüsteemi installeerimine. Selles faasis Windows Server 2003 kaitsemeetmed ei toimi. Paljusid IT-turvapoliitika nõudeid saab täitma hakata alles pärast seda, kui server on installeeritud. Samas aga määratakse hilisema käitamise olulised parameetrid juba installeerimise ajal. Seetõttu tuleb koostada meetmele M 2.318 Serveri turvaline installeerimine vastav installeerimise kontseptsioon, mis arvestaks Windows Server 2003 spetsiifiliste omadustega. Serverigrupi installeerimisel või korduvate installeerimistööde puhul on oluline, et vastavad protsessid saaksid kulgeda automaatselt ja standardiseeritult, lisaks mõjutavad installeerimist ja ettevalmistamist ka olemasolev IT-keskkond ja leiduda võivad tarkvara haldussüsteemid. Sellised käsitlused ületavad sageli üksiku serveri installeerimise kontseptsiooni piire. Seega on soovitatav koostada põhjalik, korduvalt kasutatav ettevalmistamise kontseptsioon, mis arvestaks ka juba olemasolevate installeerimise kontseptsioonidega. Installeerimise ja ettevalmistamise kontseptsioonid peavad olema välja töötatud sellisel kujul, et administraatorid saaksid oma installeerimisülesannete jaoks kasutada konkreetseid juhiseid. Lisaks muutmata kujul eksisteeriva Windows Server 2003 andmekandja manuaalsele installeerimisele tuleb eristada veel kahte erinevat ettevalmistamise varianti. Nendeks variantideks on kõvaketta kujutise (*Image*) kasutamine ja installeerimine mõnest installeerimisallikast, kasutades installeerimisprogrammi. Mõlemad variandid pakuvad automatiseerimiseks ja standardiseerimiseks erinevaid võimalusi.

Järgneval joonisel kujutatakse nende ettevalmistamisvariantide võimalikku kulgu.



Joonis: ettevalmistamise võimalused

Neuinstallation – uus installeerimine; *Festplattenabbild* (*Programme von Drittherstellern*) – kõvaketta kujutis (kolmandate tootjate programmid); *Angepasste Installation* – kohandatud installatsioon; *Automatisierte Installation* – automatiseeritud installeerimine; *Postinstallationsskript* – installeerimisjärgne skript; *Rollout von Konfigurationsvorlagen* – konfigureerimismallide levitamine

Ülalolevalt jooniselt saab tuletada ettevalmistamise peamised vahendid ja järjekorra, mille alusel neid ette valmistada. Kasutusotstarvet saab varieerida ja täiendada lisatarkvaraga. Administraator peaks oskama kasutada vähemalt siin esile toodud vahendeid, kuna need on peaaegu kõikide meetodite aluseks.

Installeerimise kontseptsiooni olulised aspektid

Üksiku serveri installeerimise kontseptsioonis tuleb arvestada mitme faktoriga:

- Buutimine ja installeerimise käivitamine.
- Massmäluseadmete draiverite ja vajadusel ka võrgudraiverite valmis seadmine buutimisprotsessiks.
- Installeerimise allika liik (andmekandja, võrk).

- Remondipakettide (*Service Pack*) integreerimine installeerimisallikasse (nn *slipstreamed*).
- Toote võtme valmispanek.
- Riistvara draiverite valmispanek.
- Tooteuuenduste paigaldamine (paigad).
- Vajadusel domeeniga liitumine.
- Serverirollide konfigureerimine.
- Turvalisuse seisukohast oluliste seadistuste tegemine vastavalt turvapoliitikale.
- Windows Server 2003 aktiveerimine.

Ettevalmistamise kontseptsiooni puhul arvestatakse nende ja täiendavate aspektidega terve süsteemi lõikes. Tarkvara haldamiseks ja jaotamiseks kasutatavad levinud tooted integreerivad ja automatiseerivad mõningaid Windows Server 2003 peamisi mehhanisme, nt vastusfaile või draiverite ettevalmistamist. Järgnevalt selgitatakse mõningaid üldkehtivaid turvalisuse aspekte.

Turbeaspektid

Kõvaketta kujutis luuakse mõnest täielikult installeeritud, töökorras serverist ja kantakse üle teisele serverile. Selle meetodi üheks probleemiks on peegeldatud süsteemide ühesugune turvatunnus (SID). Windowsi keskkonnas autentimiseks on erinevad SID-d hädavajalikud. SID-i hilisem muutmine (*Sysprep* või teiste firmade programmidega) tungib sügavale süsteemi ja puudutab mitmeid turvalisuse seisukohast kriitilisi objekte. Lisaks on kõvaketta kujutis riist- ja tarkvarakonfiguratsiooni muudatuste suhtes paindumatu. Peegeldatud süsteemid tuleb aktiveerida, seega tuleks kasutada mitmik- või hulgilitsentsiga programme. Peegeldatud süsteemide usaldusväärset tööd tuleb kontrollida sobivate testidega. Kujutised võimaldavad saavutada kõrgetasemelist standardiseerimist ning kaitset installeerimisprobleemide eest. Neid on kerge hallata ja arhiveerida. Tarkvara haldamise programmid võivad kõvaketta kujutiste paigaldamisel teatud süsteemiparameetreid kohandada. Edasine kohandamine toimub *Sysprep* abil (koos vastusfailiga) ja installeerimisjärgsete skriptidega. Selle kontseptsiooni eelised avalduvad eriti selgelt juhtudel, kus eksisteerib suur hulk kujutisi, mida on tarvis ainult natuke muuta.

Automaatselt kohandatud installeerimised põhinevad installeerimisprotseduuri vastusfailil. Need pakuvad riist- ja tarkvarakontseptsiooni jaoks suurt paindlikkust ja võimalust rakendada erinevaid mooduleid ning neid on kerge kohandada. Installeerimisprotsess on küll vigade ja kompromiteerimiskatsete suhtes vastuvõtlikum, kuid samas luuakse iga installatsiooni kohta individuaalne logi. Täieliku automatiseerimise jaoks on soovitatav kasutada ühtse tootevõtmega litsentsiprogramme. Installeerimise lõppedes tuleb installeerimise logid varundada. Logideks on *setuplog.txt* ja kõik failid laiendiga *.log*, mis asuvad süsteemi juurkataloogis (enamasti *C:\WINDOWS*), ning kõik *.log* -failid kataloogis *C:\WINDOWS\security\logs*. Kõikidel juhtudel tuleb analüüsida faili *setuperr.log*. Vastusfailid (*unattended.txt*, *winnt.sif, winpeoem.sif, ini* -failid jne) sisaldavad kriitilise tähtsusega konfiguratsiooniinfot, mida on volitusteta isikutel võimalik ära kasutada sissemurdmiskatseteks. Installeerimise andmekandjaid ning kohandatud vastusfailidega installeerimisallikaid tuleb kõikidel juhtudel kaitsta volitamata juurdepääsude eest, st nende suhtes tuleb kehtestada piiravad volitused. Vastusfaili koostamiseks on ette nähtud *Setup Manager* (fail *SetupMgr.exe* installeerimis-CD-l või Windows Server 2003

R2 CD1 kataloog *\SUPPORT\TOOLS\DEPLOY.CAB*). Juurdepääs peaks piirduma administraatoritega ning olema allutatud versiooni kontrollile. Eriti oluline on ettevalmistamisfaasis kasutatavate installeerimiskontode õige planeerimine. Need on sarnase kriitilise tähtsusega nagu administratiivsed kontod ja vajavad sama tugevat kaitset. Neil kontodel peavad olema minimaalsed volitused, sisselogimise võimalused peavad olema piiratud.

Turvalisust suurendab tooteuuenduste laadimine juba installeerimise ajal. Siiski ei tohiks uuendusi laadida otse internetist (*Windows Update*). Eelistada tuleks *Dynamic Update* 'i võimalust, mis kasutab lokaalset allikat ja võimaldab uuenduste individuaalset ja teadlikku kinnitamist. Selleks tuleb vastusfaili käsitsi sisestada valik *DUShare* . *DUShare* viitab installeerimisallika kaustale, mis sisaldab värskenduste pakette *.cab* -failide kujul. Selle meetodi asemel võib tootevärskendusi paigaldada ka pärast *Windows Update* 'i installeerimist ja installeerimisjärgsete skriptide abil lokaalsest värskenduste serverist. Ettevalmistamise kontseptsioonis tuleks defineerida üks kirjeldatud meetoditest. Tootja dokumentatsioon vastusfailide teema kohta asub installeerimis-CD-l failides *ref.chm* ja *deploy.chm* või Windows Server 2003 R2 CD1 kataloogis *\SUPPORT\TOOLS\DEPLOY.CAB*. Alates Windows Server 2003 SP1-st on installeerimise ajal ja pärast installeerimist kohalik tulemüür aktiivne ja piiravalt seadistatud seni, kuni värskendamisprotseduur on korra läbitud. Alles seejärel tagatakse täielik ühenduvus. See režiim kaitseb serverit, ajal, mil toodet aktiveeritakse ja uuendatakse otse internetist. See lahendus on vähese turvalisuse jaoks piisav, kuid ei asenda eraldatud installeerimisvõrku.

Kooskõla turvapoliitikaga

Ettevalmistamise protseduur peab tagama, et igapäevase käitamise alustamisel vastaks süsteem kehtiva turvapoliitika nõuetele. Turvamallid kantakse tavaliselt serverile üle ja aktiveeritakse grupipoliitika ja *Active Directory* abil. Alternatiivse või täiendava lahendusena saab malle paigaldada ka installeerimisjärgsete skriptidega. Installeerimise tulemust tuleb testida kehtivate mallidega ja muude kehtivate turvamallidega. Mallide ja seadistuste kehtestamisel peab installeerimise/ettevalmistamise kontseptsioonis olema kindel koht.

Dokumentatsioon

Ettevalmistamise kontseptsioon tuleb dokumenteerida põhjalikult ja selgelt. Iga serveri kohta peab eksisteerima kehtiv installeerimisjuhis.

Täiendavad kontrollküsimused:

- Kas IT-koosluses käitatavate serverite arv nõuab ettevalmistamise kontseptsiooni?
- Kas on koostatud ettevalmistamise kontseptsioon, mis arvestab installeerimist *Image* 'i või vastusfailiga?
- Kas vastusfailide puhul on kindel, et need ei sisalda käitamiskeskkonnast pärit, loetavas tekstivormis paroole?
- Kas kasutatud installeerimiskontosid on võimalik kompromiteerida ja kuritarvitada?

M 4.282 Windows Serveri IIS põhikomponentide turvaline konfiguratsioon

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator

Internet Information Services (IIS) 6.0 on Windows Server 2003-e oluline komponent, ilma milleta ei saa paljusid operatsioonisüsteemi olulisi funktsioone üldse kasutada või saab neid kasutada ainult piiratult. IIS-i täiendati alates 5. versioonist uute tehnoloogiatega, see jaotati moodulitesse ja eraldati suuremalt jaolt operatsioonisüsteemi tuumast. Uus süsteemidisain muudab IIS-i vastupidavamaks ja tõstab operatsioonisüsteemi tõrkekindlust. IIS on Windows Server 2003 keskkonna alla integreeritud veebipõhiste rakenduste rakendusserveri kontekstis. Vastavalt sellele nimetatakse vastavat komponenti Windows Server 2003-s *rakendusserveriks*. IIS on rakendusserveri komponent. Komponent *rakendusserver* on pärast operatsioonisüsteemi tüüpinstalleerimist täielikult desaktiveeritud. Järgnevalt kirjeldatud soovitused ei kirjelda täpsemalt rakendusserveri või intraneti/interneti serveri installeerimist. Selle asemel tuleks neid kasutada alati siis, kui mõni muu Windows Server 2003 komponent või täiendav rakendus nõuab IIS-i installeerimist abiteenusena. Käesolev meede viitab teatud aspektidele, millega tuleb arvestada IIS-i põhikomponentide konfigureerimisel.

Milliseid komponente võib installeerida?

Serveril tohivad olla aktiivsed ainult *COM+-võrgujuurdepääs* ning *interneti informatsiooniteenused* (IIS). Viimaste puhul tuleb aktiveerimisel piirduda *ühiste failide*, *informatsiooniteenuste halduri* ja *WWW-teenustega*; vajadusel võib täiendavalt kasutada veel vaid *internetis printimist*.

Täiendavad IIS-i teenused HTTP-serveri kõrval

Rakendusserveri all on üles loetletud levinud protokollid SMTP, NNTP ja FTP ning teadete järjekorra teenus. Mõned tööriistad ja serverirakendused nõuavad nende installeerimist. Nende protokollide ja teenustega on seotud täiendavad ohud, seega tuleb lisaks siinnimetatud soovitustele võtta tarvitusele täiendavad meetmed lähtuvalt IT-etalonturbele põhineva modelleerimise tulemustest (vt M 5.131 Windows Server 2003 IP-protokollide kaitse). *Active Directory* domeenikontrollerile tuleks installeerida ainult vajalikud IIS-i teenused ja protokollid.

Aluskonfiguratsiooni kaitse

IIS-i installeerimine loob süsteemiketta juurkataloogi kataloogid *C:\Inetpub* ja *C:\Inetpub\wwwroot*. Mõlemad kaustad tuleks ümber nimetada. Turvagrupp *Kasutaja* tuleb eemaldada *C:\Inetpub\wwwroot* ja kõikide selle alamkaustade turvasätetest. Kaust *AdminScripts* tuleks tõsta kasutaja poolt defineeritud kausta. Reeglina tuleb igapäevaselt töötavas serveris loobuda kõikidest näidis- ja testskriptidest, olgu need siis ise tehtud, internetist laetud või tarkvaraarenduspakettidest võetud. Samad meetmed kehtivad ka järgnevatele kaustadele, kui need on olemas:

- *C:\inetpub\ftproot* (FTP-server)
- *C:\inetpub\mailroot* (SMTP-server)
- *C:\inetpub\nntpfile* (NNTP-server)

Kõik virtuaalsed standardserverid, standardne veebileht ja standardne FTP-lehekülg tuleb välja lülitada, kui neid ei vajata. Standardset veebilehe tuleks enamatel juhtudel hoida välja lülitatud seisundis ning uusi veebilehti tuleks lisada ainult selgelt määratletud otstarvete jaoks, nagu WebDAV-kinnitused. Interneti infoteenuste halduri paljud kataloogid viitavad operatsioonisüsteemi funktsioonidele, näiteks internetis printimisele või sertifikaaditeenustele. Põhikataloogid on seega enamasti seotud operatsioonisüsteemi süsteemikaustadega. Seega tuleks vastava põhikataloogi turvaseadistustest reeglina eemaldada turvagrupp nimega *User*. Kui teatud ressursid peavad olema ka kasutajate jaoks saadaval, nt internetis printimine või IIS-il põhinev kasutajaparooli muutmine, siis tuleb selleks kavandada vastav volituste kontseptsioon ja see ellu viia.

Dünaamilise sisu kasutamine

Sertifitseerimisteenused ja muud Windowsi komponendid sisaldavad osalt graafilisi kasutajaliideseid, mis töötavad ASP-ga. Seetõttu pole ASP desaktiveerimine alati võimalik. Windows Server 2003 puhul on ASP võimalused operatsioonisüsteemi mõjutada standardina tugevalt piiratud (aktiveeritud *IISLockdown*). Kontrollitud tingimustes on seega nende komponentide turvaline kasutamine võimalik ilma suurema töövaevata. Esmajoones tähendab see seda, et ASP-d kasutatakse eranditult administratiivsetel ja infrastruktuurilistel eesmärkidel. Lisaks peavad eksisteerima sobiv administreerimise kontseptsioon ja vastav turvapoliitika. Juurdepääsu kasutaja tasandile piiratakse, logitakse ja kontrollitakse. Vastasel korral esineb täiendavaid riske, mille jaoks läheks tarvis vastavaid meetmeid. Dünaamilise sisu käivitamiseks käivitab IIS eraldiseisvaid protsesse. Erinevaid rakendusi tuleks vastava protsessihalduse abil käitada üksteisest eraldatult.

Juurdepääsu piiramine ja turve

Juurdepääs virtuaalserveritele ja kataloogidele pole standardina piiratud, kuigi IIS-i teenuste poole pöördutakse ainult lokaalsest arvutist või teatud klientide poolt võrgust. Lisaks sellele ei takistata paroolide edastamist loetavas tekstivormis. Seega tuleks piiravad seadistused määrata põhiseadistusteks.

Autentimismeetodid

LAN'is on *integreeritud Windows autentimine* kõige turvalisem ja mugavam meetod. See töötab suurema osa levinud brauseritega, näiteks Internet Exploreri ja Firefoxiga. Kui osa LAN'ist on kaitstud turvalüüsiga, siis tuleb kontrollida *integreeritud Windows autentimise* tuge. Kui IT-turvapoliitika seda võimaldab ja ohtudega (vt G 5.133 Veebipõhiste administreerimisvahendite volitamata kasutamine) osatakse piisavalt arvestada, saab teatud valdkondades kasutada *Digest autentimist* (sisselogimisinfo krüpteeritud saatmine domeenikontrollerite abil vastavalt RFC 2617-le). Kui see on võimatu, tuleb kogu ühendus luua krüpteeritud kanali kaudu. *Digest autentimise* eeldusteks on:

- Windows Server 2003 skeemitäiendusega *Active Directory*
- Windows Server 2003 kõikidel lokaalse *Active Directory* lehekülje domeenikontrolleritel
- HTTP 1.1 tugi klientidel (nt MS Internet Explorer alates versioonist 5)
- HTTP 1.1 tugi turvalüüsidel

Windows Server 2003 puhul on *Digest* integreeritud kui *Security Service Provider Interface* (SSPI) (*laiendatud Digest autentimine*). Eelduseks on, et nii IIS kui ka domeenikontroller peavad töötama Windows Server 2003 all. IIS-iga serveris tuleb SSPI määrata *Digest* 'i jaoks skripti abil, kuna Windows Server 2003 lülitub tagasi vanemale, Windows 2000-e *Digest* 'i moodulile. Võimalik on ka autentimise täielik ebaõnnestumine, kui Windowsi domeeni konfiguratsioon pole homogeenne. Käsuviiba sisestus on: *cscript adsutil.vbs SET W3SVC/UseDigestSSP true.* Konfigureerimisskript *adsutil.vbs* asub kataloogis *AdminScripts*. Skriptide kasutamise info leiate meetmest M 2.367 Käskude ja skriptide kasutamine alates Windows Server 2003-st .

Krüpteerimine turvalises kanalis (SSL/TLS)

Turvaline kanal on sageli ainus võimalus, kuidas saavutada kolmandate tootjate administreerimistööriistade puhul krüpteeritud parooliedastust.

Iga veebileht (edaspidi virtuaalserver) peab omama kehtivat sertifikaati ja võimaldama krüpteeritud kommunikatsiooni turvalise kanali kaudu.

Kõrge või väga kõrge kaitsevajadusega serverite puhul võib aktiveerida kliendisertifikaatide nõudmise. Edasiste süsteemide (nt kiipkaartide) abil on seega võimalik kasutada kahefaktorilist autentimist.

Seire

Logimine tuleb aktiveerida kõikide virtuaalserverite ja veebilehtede omaduste dialoogaknas. Standardseadistus, üks logifail päevas, tuleks jätta muutmata, kui IT-turvapoliitika ei nõua pikaajalisi logisid. Alates Windows Server 2003 SP1-st tuleks lisaks kasutada *Metabase* seiret. Selleks kasutatakse konfigureerimisskripti *iiscnfg.vbs*. Käsuviiba sisestus on järgmine: *iiscnfg.vbs /enableaudit W3SVC//ROOT,* mis aktiveerib veebilehe konfiguratsiooni ja allasuvate virtuaalkataloogide seire. on virtuaalserveri number. See on interneti infoteenuste halduris dokumenteeritud loetletud veebilehtede kõrval sõlmes *Websites*. Lõpuks, kui seda veel tehtud ei ole, tuleb serveril aktiveerida objektiseire grupipoliitika (vt M 2.365 Windows Server 2003 süsteemiseire planeerimine).

Dokumentatsioon

Dokumenteerida tuleks vähemalt see, milline server on millise administratiivse tööriista pöördumiskohaks, millised on selleks seadistatud autentimismeetodid ja milliseid täiendavaid ressursse ehk juurdepääsusid võib tööriist veel vajada. Kõrvalekalded nimetatud algseadistustest või installeerimise standardist tuleb dokumenteerida ja põhjendada.

Täiendavad kontrollküsimused:

- Kas installeeritud on ainult vajalikud IIS-i teenused ja protokollid?

- Kas aluskonfiguratsioon on turvaline ja juurdepääs virtuaalsetele serveritele ja kataloogidele piiratud?
- Kas kasutatakse ainult Windowsisse integreeritud või täiendatud *Digest* autentimist?
- Kas kõikide virtuaalserverite ja veebilehtede logimisfunktsioon on sisse lülitatud?
- Kas konfiguratsiooni kohta on koostaud dokumentatsioon (kõrvalekalded installeerimise standardist)?

M 4.283 Windows NT 4 Serveri ja Windows 2000 Serveri turvaline migratsioon Windows Server 2003-ks

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator

Vanema versiooni uuendamine versioonile Windows Server 2003 toimub tihti erinevatel põhjustel ja erinevate eesmärkide täitmiseks. Töökorralduslikust ja tehnilisest küljest vaadatuna on lähtepunktid väga mitmekülgsed. Seega tuleb serveriuuendust hoolikalt planeerida, lähtudes soovitud eesmärkidest. Arvestada tuleb nõuetega meetmetes M 2.315 Serveri kasutuselevõtu planeerimine ja M 2.319 Serveri üleviimine . Windows NT serveri üleviimisel kehtib suur osa reeglitest.

Erinevate üleviimisteede eelised ja puudused

Üleviimistee kasuks otsustamisel tuleb eriti hoolikalt kaaluda olemasoleva serveri uuendamise (*In-place Upgrade*) ning uue installatsiooni eeliseid ja puudujääke. Näiteks võib uuendatud server kaasatuleva „vana taaga“ või vananenud kontseptsioonide tõttu oluliselt erineda uuena installeeritud Windows Server 2003 süsteemist. Oluline on ka uuendatava serveri lähteversioon. Uuendatud Windows Server 2003 standardsed turvaseadistused ei vasta uue installatsiooni standardsetele seadistustele. Sõltuvalt lähteversioonist ja *Service Pack* -ist on installeerimisprogrammi seadistused erinevad. Seega, kui Windows NT 4.0 Server uuendatakse versioonile Windows Server 2003, erinevad seadistused olukorrast, kus Windows 2000 Server uuendatakse versioonile Windows Server 2003. Homogeense IT-turvapoliitika elluviimiseks tuleb turvakonfiguratsioone lähteolukorraga (versiooni, rolli, ja konfiguratsiooniga) arvestades kohandada.
Olemasoleva serveri uuendamine nõuab üldjuhul vähem tööd, kuna olemasoleva kasutajad, grupid ja õigused säilivad. Faile ja rakendusi pole tarvis uuesti installeerida. Äsja formaaditud kõvakettale installeerimisel saavutatakse seevastu aga suurem jõudlus. Andmekandjate partitsioone saab kohandada tegelike vajadustega vastavaks. Väga kõrgete käideldavusnõuetega serverite puhul tuleks valida uus installeerimine. Vastasel korral tuleks pärast eelnevat andmete varundamist kindlast partitsioonid täielikult defragmentida.

Ettevalmistused

Tuleb arvestada tootjainfoga, eriti aga installeerimise andmekandjatel leiduva dokumentatsiooniga (nt kataloogiga*DOC* Windows Server 2003 installeerimise andmekandjal). Enne uuendamist tuleb kontrollida, kas kõik eeldused on täidetud. Selle juurde käib ka operatsioonisüsteemide erinevate versioonide täiendamisvõimalus (*upgrade*). Süsteeminõuete ja riistvara ühilduvuse kohta saab infot tootja käest, kasutada võib ka Windows Server 2003 installeerimise andmekandjal leiduvat programmi *Setup*, et kontrollida *süsteemi ühilduvust*. Lisaks tootja soovitatud nõuetele tuleb arvestada käitamiseks vajaminevat jõudlust (kõvaketas, töömälu jne). Info olemasolevate seadmete ja draiverite kohta võib aidata olukordades, mis nõuavad käsitsi sekkumist. Serveri kohta tuleks koostada inventarikataloog,

kuhu oleks dokumenteeritud selle komponendid (nt nimetus, tüüp, arv, IRQ, E/A-aadress jne). Kui tootja pakub nende komponentide jaoks draivereid, tuleks need juba ette valmis soetada. Windows Server 2003 võib nõuda uute draiverite kasutamist, mis ühilduvad ainult uuemate BIOS-i versioonidega, tekitades BIOS-i uuendamise vajaduse. See peaks siiski toimuma ainult sel juhul, kui on uuritud, millised draiveri versioonid vajavad milliseid BIOS-i versioone. Kui uuendataval serveril leidub:

- klastreid,
- andmehulkade kogumeid,
- peegeldatud andmehulkasid,
- *Stripeset* -e või
- FAT/FAT32-partitsioone,

vajavad need eriti hoolikat tähelepanu. Seejuures ei soovitata kasutada FAT-i.

Tarkvara, mida soovitakse uuendatud serveris edasi kasutada, tuleb eelnevalt testida, et veenduda selle ühilduvuses. Muuhulgas on selliseks tarkvaraks viirusetõrjeprogrammid, varundus- ja haldussüsteemid ning krüpteerimisrakendused. Üleviidava serveri nimed, nimeteenused ja võrguseadistused peavad olema sellised, et mitte üheski faasis ei esineks konflikte ega muid ohtusid. Käitatav Windows Server 2003 peaks (erandiks on taastamiskonsool) reeglina sisaldama ainult üht installeeritud operatsioonisüsteemi ja ainult NTFS-partitsioone. Planeerimisfaasi teadmistest ja nõuetest tuleks koostada kontrollnimekiri, mis on üleviimise testi ajal ja ennekõike pärast lõpetatud üleviimist dokumenteeritud tõendiks funktsioonide toimimise kohta.

Läbiviimine

Pärast kõikide testide edukat lõpetamist tuleks käitatava serveri üleviimine kooskõlastada igapäevaste tööprotsesside toimimisega. Kokkulepitud ajal tuleb server installeerimise ajaks käitamisest eemaldada. Tuleb tagada aktuaalne ja täiemahuline andmete varundamine. Installeerimiseks tohib kasutada ainult turvalisest allikast saadud tarkvara (vt M 2.273 Turvalisust mõjutavate paikade ja värskenduste kiire paigaldamine). Uusimad teeninduspakid, turvapaigad ja draiverid peavad olema käepärast. Kõige turvalisem on hoida neid sobival vahetataval andmekandjal (nt CD-l või DVD-l) ja see tagab hiljem ka kõige parema ülevaate. Installeerimise ajal vajab server aktiivset võrguühendust. Võimaliku puhvertoiteallika jadaühendus tuleb igaks juhuks juba eelnevalt lahti ühendada, kuna vastasel korral võib liidese tuvastamine tekitada probleeme. Vältida tuleb interneti kaudu tehtavat *dünaamilist uuendust* ning planeerimata värskendusi, kuna aktiivselt käitatavate serverite uuendamisega kaasnevad eripärad, mis nõuavad individuaalseid otsuseid ja individuaalset sekkumist. Serveri installeerimise ajal vajalikud internetiühendused nõuavad täiendavaid turvameetmeid ja tekitavad ohtusid, mida on võimalik vältida. Lisaks pole võimalik garanteerida nende käideldavust.

Abivahendid

Serveri üleviimist uuele riistvarale toetavad Microsofti tarkvaratööriistad. Enne

nende tööriistade kasutamist tuleb tootjaga suheldes selgitada, millist tuge pakuvad nad probleemide korral. Tööriistad tuleb valida ülimalt hoolikalt ja eelnevalt läbi testida. Samuti võib kasutada mõne teise firma tööriistu:

- *File Server Migration Toolkit* (FSMT) on mõeldud vanemate failiserverite üleviimiseks ja konsolideerimiseks. Lisaks andmetele viiakse *FSMT* abil üle ka NTFS-i ja kinnitamise tasandi volitused.
- *Microsoft Print Migrator* viib üle printeridraiverid ja nende konfiguratsiooni, kuid turvavolitusteta.
- Domeenide üleviimise ja konsolideerimise jaoks on olemas *Active Directory Migration Tool* (ADMT).
- Füüsilise serveri operatsioonisüsteemi ja installeeritud rakenduste üleviimiseks virtuaalmasinasse MS Virtual Server 2005 all võib kasutada tööriista *Virtual Server Migration Toolkit* (VSMT).

Järeltööd

Pärast oluliste töösammude lõpetamist, näiteks pärast Windows Server 2003 taaskäivitamist, tuleb sündmuste kuvasid kontrollida kriitiliste vigade ja juhiste osas. Sõltuvalt toote versioonist ja litsentsitingimustest võib olla vajalik toote aktiveerimine. Sellekohase info leiate IT-etalonturbe abivahendite alt (vt *Sobilike litsentseerimismeetodite valimine Windows XP/Server 2003 all* teemas *Windows Server 2003 abivahendid*).

Turvakonfiguratsioon

Windows Server 2003 all toimub turvakonfiguratsiooni seadistamine erinevate tööriistadega, mille konfigureerimisvõimalused osaliselt kattuvad. Määratleda saab enda poliitikaid ja malle:

- Pärast uuendamist tuleb serveril *Turvakonfiguratsiooni abilise* (SCW) abil rakendada ette valmistatud turvakonfiguratsioon. Vastava serveri roll peab olema selleks ajaks juba kindlaks määratud.
- *Microsoft Management Console* (MMC) abil koostatakse funktsiooni *Turvakonfiguratsioon- ja analüüs* või *Turvamallid* abil mallid turvaseadistuste jaoks ja kasutatakse neid vastavalt vajadusele. Neid malle saab kasutada ka läbi grupipoliitikate. *Windows Server 2003 Security Baseline* (saadaval tootja veebiversioonina) sisaldab soovitatavaid turvamalle, kirjeldusi ja dokumendimalle. Neid soovitusi tuleb siiski alati kohandada vastavalt konkreetsele olukorrale (vt M 4.280 Turvaline põhikonfiguratsioon alates Windows Server 2003-st ja M 2.366 Windows Server 2003 turvamallide kasutamine).

Sündmuste kuvasid tuleb kontrollida pärast igat turvakonfiguratsiooni. Windows Server 2003 all on Internet Explorer standardina seadistatud nõnda, et selle tur-

valisuse oleks kõrge. Sellest tulenevaid piiranguid saab tühistada, määrates internetiaadresse tsooni *Usaldusväärsed leheküljed* või kasutades UNC-andmeteid tsoonis *Lokaalne intranet*. Internet Exploreri konfigureerimiseks peavad kasutajal olema vastavad volitused. Windows Server 2003 all võeti kasutusele täiendavad lokaalsed grupid ja kasutajad, millega tuleb arvestada, näiteks *Remote Desktop-i kasutajad*, *Võrgukonfiguratsiooni operaatorid*, *Support_388945a0* (desaktiveeritud).

Kasutajaprofiilide kataloogi andmetee on võrreldes Windows NT 4.0-ga muutunud. Olemasolevaid skripte ja meetodeid tuleb seepärast vajadusel kohandada.

Täiendavad kontrollküsimused:

- Kas üleviimise plaan on olemas?
- Kas turvalised installeerimise andmekandjad on käepärast?
- Kas Windows Server 2003-e installeerimise andmekandjalt installeerimisel kasutati valikut *Kontrolli süsteemi ühilduvust*?
- Kas turvakonfiguratsioon on tehtud ja dokumenteeritud?

M 4.284 Teenuste rakendamine

Algatamise eest vastutavad: IT-juht
Rakendamise eest vastutavad: administraator

Teenuseid käivitatakse teatud kontode (niinimetatud töökontode) turvakontekstis. Pöördumine ressursside poole toimub töökontodega, mis sarnanevad kasutaja ja kasutajakontoga. Käivitatud teenused jäävad aktiivseks, seega jääb ka vastav töökonto püsivalt sisselogituks või siis uuendatakse sisselogimisinfot regulaarselt tsentraalse teenusejuhtimise abil. Lisaks on serveris tavaliselt tegu tööks oluliste tsentraalsete teenustega. Töökontod on seega tavalistest kasutajakontodest rohkem paljastatud. Kui teenuste vahel esineb sõltuvussidemeid, võib näiliselt väheoluline kompromiteeritud teenus põhjustada töö jaoks olulises teenuses avarii. Sel põhjusel tuleb teenuseid ja töökontosid hallata spetsiaalsete reeglite alusel.

- Töökontode jaoks ei tohi mitte mingil juhul kasutada eeldefineeritud administraatorikontot.
- Iga teenus peab töötama isikliku töökontoga. Erandiks on eriotstarbelised, eeldefineeritud kontod *NT AUTHORITY\LocalService, NT AUTHORITY\NetworkService*. Neid hallatakse sisemise teenusejuhtimise kaudu ja need pakuvad igale teenusele isoleeritud turvakonteksti. Autentimist reguleeritakse süsteemisiseselt teenusejuhtimisega. Paroolisisestusi ignoreeritakse.Kõrgete volitustega, kuid kompromiteeritud töökontot on lihtsam isoleerida, kui seda kasutab ainult üks teenus. Praktikas võivad serverirakendused kasutada teenuste gruppi ühe ja sama konto kontekstis. Siin tuleb olukorrale vastavalt kaaluda, kas see ühildub süsteemi kaitsevajadusega ja kui palju saab määrata erinevaid töökontosid, ilma et see mõjuks soovitud funktsioonidele negatiivselt.
- Igal töökontol peavad olema ainult hädavajalikud volitused. Seepärast tuleb kohalike teenuste jaoks esmajoones kaaluda kontot *NT AUTHORITY\LocalService* ja võrgujuurdepääsuga teenuste jaoks kontot *NT AUTHORITY\NetworkService*. Standardina on neil samad volitused nagu eeldefineeritud grupil *Authenticated user* (tavakasutaja).

Versiooniga Windows Server 2008 R2 võeti kasutusele kaks spetsiaalset kontot: hallatav teenusekonto ja virtuaalkonto.

- Hallatavaid teenusekontosid käsitletakse Windows Server 2008 R2-s hallatavate domeenikontodena, mis võimaldavad paroolide automaatset haldamist.

Lisaks on domeenikontodest võimalik koostada klasse, mida saab haldustööde otstarbel delegeerida ka neile, kes pole administraatorid. Seda tüüpi kontot kasutatakse enamasti rakenduste, nt SQL-serveri ja IIS-i haldamiseks.

- Virtuaalseid kontosid käsitletakse Windows Server 2008 R2-s hallatavate lokaalsete kontodena. Nende kontode puhul ei ole paroolihaldus vajalik. Sisselogimine toimub domeeni piires ning võrgu ressurssidele juurdepääsuks kasutatakse arvuti identiteeti.

Erinevalt seni teenuste haldamiseks kasutatud kontodest, nt Local Service, Network Service ja Local System, saab hallatavat teenusekontot hallata tsentraalselt, sest see salvestatakse Active Directory organisatsiooniüksusse Managed Service Accounts. Siinkohal tuleb arvestada, et teenusekontode uus funktsioon eeldab, et hallatavas süsteemis kasutatakse versiooni Windows Server 2008 R2. Iga süsteemi kohta lubatakse rakendada ainult ühte hallatavat teenusekontot. Funktsioonide täielikuks kasutamiseks peab ka domeen töötama nn Windows Server 2008 R2-režiimis (domeeni funktsioonitasand). Domeenide puhul, mis ei ole lülitatud ei Windows Server 2003 režiimi ega Windows Server 2008 režiimi, tuleb vajaduse korral teha muid konfigureerimistöid. Kuni versioonini Windows Server 2008 (ja 2008 kaasa arvatud) tuleks domeenikontodele eelistada lokaalseid kontosid. Domeenikontode kasutamisel ei tohi neil olla rohkem domeenivolitusi kui vaja, lisaks tuleb tagada domeenikontrollerite piisav käideldavus. Kohalikke kontosid tuleks eelistada domeenikontodele. Domeenikontode kasutamise korral ei tohi neil olla tarvilikust rohkem domeenivolitusi, lisaks tuleb tagada domeenikontrollerite vastav käideldavus. Töökontode puhul tuleb kohalik sisselogimine keelata (*Start* | *Control Panel* | *Administrative Tools* | *Local Security Policy* |*Local policies* | *User Rights Assignment* | *Deny logon locally* või domeeni grupipoliitika kaudu).

- Administraatoritasandi teenustega rakendusi tuleb käitada eraldi serveril. Mida rohkem selliseid rakendusi ühel serveril on, seda väiksem on saavutatav turvalisus. Näidetena võib tuua varundusservereid või domeenikontrollereid, mis saavad oma põhiteenuseid pakkuda ainult täielike administreerimisõigustega.
- Windowsis sisalduvate teenuste eelseadistatud kontosid ei tohi muuta.
- Kasutud või potentsiaalselt ohtlikud teenused tuleb desaktiveerida.
- Paljusid skripte ja muid käivitatavaid faile saab installeerida ja käivitada teenusena. Tavajuhtudel tuleks sellest hoiduda.
- Iga üksikjuhtumi puhul tuleb eraldi kindlaks teha, kuidas mõjutab teenusena käivitatud protsess (nt skript või programm) süsteemi stabiilsust ja turvalisust. Näiteks võib *Teenuse lõpetamine* või *Teenuse taaskäivitamine* põhjustada andmete rikkumist, kuna protsess ei suuda sellistele sündmustele iseseisvalt reageerida, vaid lihtsalt kustutatakse. Ka siin kehtib reegel: vähim võimalik turvakontekst vähendab riski. Sellise meetodi kasutamist tuleb kontrollida testimiskeskkonnas. Töökontode jaoks tuleks kaaluda tugevate seireseadistuste (*System Access Control List*, SACL) rakendamist, et märgata ootamatut käitumist.
- Töökontode paroolide jaoks ei sobi tavalised, kasutajaparoolide reeglid. Alljärgnev tabel on näide installeerimisjärgsest standardseadistustest.

Paroolisuunis	Standard-seadistus domeenikontrolleritel	Sobivus töökontode jaoks
Paroolide ajalugu	24	jah
Parooli maksimaalne vanus (päevades)	42	ei sobi
Parooli minimaalne vanus (päevades)	1	jah

Parooli minimaalne pikkus	7	ebapiisav
Parool peab vastama keerukusnõuetele	aktiveeritud	jah
Paroolide salvestamine reversiivse krüpteeringuga	desaktiveeritud	jah

Paroolil peab olema kahekohaline pikkus (võimalik kuni 127 märki). See ei tohi automaatselt aeguda (konto seadistuste all valik Parool ei aegu) vaid selle asemel tuleks parooli regulaarsete hooldustsüklite ajal muuta. Paroole tuleb hoida turvalises kohas (vt M 2.22 Paroolide deponeerimine). Suurema hulga teenuste ja serverite puhul võib paroolide deponeerimine ja muutmine (koos teenuste funktsioonitestidega) olla väga töömahukas ning see ei pruugi enam tagada suuremat turvalisust. Töökontode paroolide haldamise abiprogrammid võivad olla väga tõhusad abivahendid, kuid need sisaldavad ka riske. Paroolide vanus ja nende haldamise meetod tuleb kindlaks määrata vastavalt kaitsevajadusele ja töömahule ning poliitikas dokumenteerida.

Dokumentatsioon

Kõikide teenuste jaoks, mis ei tööta eeldefineeritud kontoga, tuleb määratleda töökontod ja volitused.

Täiendavad kontrollküsimused:

- Kas eeldefineeritud kontosid kasutatakse administraatorivolitustega?
- Kas töökontodel on ainult hädavajalikud õigused?
- Kas töökontode paroolide muutmiseks on välja töötatud vastav protseduur?

M 4.285 Mittevajalike Windows Server 2003 klientfunktsioonide deinstalleerimine

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator

Windows Server 2003 standardne installatsioon sisaldab mitmeid funktsioone. Serveril on nad kasutud ja tuleks deinstalleerida, või, kui see on võimatu, vähemalt desaktiveerida, et vähendada rünnete ja nendega kaasnevate asjatute riskide võimalusi.

Programmide deinstalleerimine Start | Programs | Accessories kaudu

1. Logige serverisse administraatorina.
2. Looge failist C:\WINDOWS\inf\sysoc.inf varukoopia, näiteks failina Copy of sysoc.inf
3. Muutke failis C:\WINDOWS\inf\sysoc.inf järgnevaid ridu ja salvestage:
OEAccess=ocgen.dll,OcEntry,oeaccess.inf,hide,7
muutke reaks
OEAccess=ocgen.dll,OcEntry,oeaccess.inf„7
ja
MultiM=ocgen.dll,OcEntry,multimed.inf,HIDE,7
muutke reaks
MultiM=ocgen.dll,OcEntry,multimed.inf„7
4. Minge Start | Control Panel | Software | Add/Remove Windows Components alla ja eemaldage märgid järgnevatest kastidest:
- Outlook Express
- Accessories and Utilities / Multimedia / Audiorecorder
- Accessories and Utilities / Multimedia / Mediaplayer
- Accessories and Utilities / Communication / Telephone
4. sammu tarkvaravalikud muutuvad nähtavaks alles sammudega 1 kuni 3.

Media Playeri, Outlook Expressi ja Netmeetingu desaktiveerimine

Integreeritud komponentide nagu Media Player, Outlook Express ja Netmeeting deinstalleerimisvõimalused ei eemalda programme täielikult, mistõttu säilib võimalus neid juhuslikult käivitada. Seepärast tuleks need programmid desaktiveerida tarkvarapiirangute poliitikatega (vt meedet M 4.286 Windows Server 2003 Software Restriction Policy rakendamine). Kui kasutatakse Active Directory't ja grupipoliitikat, siis tuleb seadistuste tõhusust üksikul serveril tagada grupipoliitika õige konfiguratsiooniga (vt M 2.231 Windowsi grupipoliitika planeerimine).

Lokaalset tarkvara piirava poliitika kohandamine:

1. Avage Start | Control Panel | Administrative Tools | Local Security Policy kaudu lokaalne turvapoliitika.
2. Liikuge harusse Software Restriction Policies | Additional Rules.
3. Lisage järgnevatele andmeteedele uued andmeteede reeglid turvaastmega Disallowed:
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%\NetMe

%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%\Outlook Express
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%\Windows Media Player

Kui mõni desaktiveeritud programmidest laeti seni operatsioonisüsteemi käivitamisel automaatselt, võib esineda veateateid. Vastavad Autostart -funktsioonid tuleb enne poliitika aktiveerimist välja lülitada, näiteks msconfig.exe abil. Lisaks tuleb piirata Windowsi klientkomponentide internetis toimuvat andmesidet. Selleks tuleb lokaalses grupipoliitikas (Start | Run ... | gpedit.msc) valida haru Computer Configuration | Administrative Templates | System | Internet Communication Management | Internet Communication settings. Siin tuleb kõik funktsioonid desaktiveerida. Aktiivseks peavad jääma ainult Automatic Root Certificates Update ja Windows Update, juhul, kui serveri jaoks pole määratud vastavaid alternatiivseid meetodeid.

Kui serveris on aktiivsed veel mõned ebavajalikud klientrakendused ja klientfunktsioonid, siis tuleb ka need deinstalleerida või desaktiveerida.

Täiendav kontrollküsimus:

- Kas server sisaldab üleliigseid klientfunktsioone?

M 4.286 Windows Server 2003 Software Restriction Policy rakendamine

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator

Kasutajad puutuvad sageli kokku tundmatu tarkvaraga eriti just interneti (WWW, e-post jne) intensiivse kasutamise tõttu. Sellistel juhtudel peavad kasutajad otsustama, kas nad tahavad seda tarkvara kasutada või mitte. Kahjulikud programmid maskeerivad end sageli nt nn trooja hobusteks eesmärgiga panna kasutaja neid installeerima ja käivitama. Kasutajal on sageli raske otsustada, millist tarkvara tohib käivitada. Tarkvara piiramise poliitikaga saab IT-keskkonda kaitsta soovimatu või ebausaldusväärse tarkvara eest. Pärast Windows Server 2003 tüüpinstalleerimist tuleks koostada vähemalt lokaalne tarkvara piiramise poliitika:

- *Start* | *Control Panel* | *Administrative Tools* | *Local Security Policy* | all valida *Richtlinien für Softwareeinschränkung* kontekstimenüüs valik *New Software Restriction Policies*

Seadistused *Trusted Publishers* all:

- *enable administrators for local computer*,
- aktiveerige *Publisher* ja *Time Stamp*.

Failitüübid, mida tarkvara piiramise poliitika mõjutab, on *Designated File Types*. Seepärast tuleb nimekirja *Designated File Types* regulaarselt uuendada. Lähtematerjalina võib kasutada näiteks IT-koosluse viirusetõrjepoliitikat, milles on defineeritud kriitilised faililaiendid. Muid seadistusi pole tavaolukorras tarvis muuta. Eriti oluline on eeldefineeritud reeglite muutmatajätmine, kuna vastasel korral võib süsteem muutuda kasutuskõlbmatuks. Poliitika peab kehtima alati kõikide kasutajate jaoks, kaasa arvatud administraatorid.

Täiendavate reeglite tüübid

Reegli tüüp	Selgitus	Turvameetme kindlus keskmine
Hash -reegel	Pöördumisel faili poole arvutatakse selle *hash*-väärtus ja võrreldakse seda eelnevalt salvestatud *hash*-väärtusega.	

	Reegel mõjub identsete *hash*- väärtuste puhul. Kui aga faili sisu vahepeal muudetakse, muutub ka *hash*-väärtus ja reegel ei mõju!	
Sertifikaadi reegel	Sertifikaadi reegel tuvastab tarkvara selle tootja autentimiskoodi sertifikaadi alusel ja lubab seda käivitada ka serveri kaitstud piirkondades, lähtudes seejuures turvalisuse astmest.	keskmine
Andmetee reegel	See reegel tuvastab tarkvara eelnevalt määratud failitee abil. Programmi ümbertõstmisel reegel enam ei kehti.	madal
Interneti tsoonide reegel	Tsoonireeglid kehtivad ainult .msi-failidele (*Windows Installer*'i paketid)	madal

Tarkvara piirava poliitika kasutamine

Tarkvara piiramise poliitika eeldab põhjalikku planeerimist ja testimist testimiskeskkonnas, eriti siis, kui turvaaste *Disallowed* on määratud standardiks. Rakendamisel tuleks eelistada *hash*- ja sertifikaadireegleid, kuna teereeglid ja internetitsoonide reeglid pakuvad kesist kaitsest programmide ja programmiteekide käivitamise eest. Lisaks tuleks kasutada *Microsoft Knowledge Base* infot, et välistada seal dokumenteeritud ootamatut ja soovimatut *hash*- reeglite kasutamise mõju. Tarkvara piiramise poliitikas võivad DLL-teegid olla algusest peale blokeeritud. Sel juhul tuleb määrata palju reegleid selgelt lubatud teekide jaoks. Pöördumisi DLL-teekide poole esineb programmi käivitamisel sageli ja iga kord tuleb kogu nimekiri läbi töötada. Seetõttu tuleb arvestada ka jõudlusega. Poliitikat tuleb esmajoones rakendada nähtavatel serveritel, millele on esitatud kõrgendatud turvanõudmised, näiteks nn *bastion host*'idel (ettevõtte võrgu avalikult ligipääsetavad arvutitel), et vähendada kahjulike programmide ründevõimalusi. Aktiveeritud poliitika ja vastavad reeglid ei asenda viirusetõrjeprogramme. Turvaintsidentide vältimiseks, näiteks seoses kahjulike programmidega, saab poliitikat kasutada tarkvara piiramiseks ennetava meetmena või hädaabimeetmena. Kui tarkvara piiramise poliitikat jaotatakse *Active Directory* grupipoliitika abil, tuleks selleks luua eraldi grupipoliitika objekt. Standardsete grupipoliitikate reegleid ei tohi muuta. Kui töö ajal esineb ootamatuid ja soovimatuid mõjusid, saab eraldi grupipoliitika objekti raskusteta desaktiveerida ja mõjuma hakkavad taas standardsed reeglid.

Dokumentatsioon
Kõik reeglid peale eeldefineeritud reeglite tuleb dokumenteerida. Vastav eesmärk tuleb samuti dokumenteerida.

Täiendavad kontrollküsimused:

- Kas ette nähtud failitüüpide nimekirja uuendatakse regulaarselt?
- Kas Windows Server 2003-el kasutatakse *hash*- reeglitel või sertifikaadireeglitel põhinevat tarkvara piiramise poliitikat ja kas see on dokumenteeritud?

M 4.287 IP-kõne vahetarkvara turvaline administreerimine

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator

IP-kõne vahetarkvara puhul on tegu serverisüsteemidega, mida tuleb kaitsta samade turvameetmetega, mida kasutatakse ka teiste serverisüsteemide jaoks. Lisaks sellele tuleb rakendada täiendavaid turvameetmeid, mis suudaksid vastu seista IP-kõne süsteemide eriomastele ohtudele. Enne kasutuselevõttu tuleb IP-kõne komponendid turvaliseks konfigureerida. Dokumenteerida tuleb esmakordsel installeerimisel läbitav protseduur. Järgnevalt tutvustatakse mõningaid punkte, millega tuleb arvestada, et saavutada turvalist konfiguratsiooni ja administreerimist.

Funktsioonid

IP-kõne süsteemid pakuvad sarnaselt traditsioonilistele kodukeskjaamade süsteemidele mitmeid erinevaid funktsioone. Enne IP-kõne süsteemi kasutuselevõtmist peab olema selge, millised funktsioonid on olemas ja milliseid neist läheb tarvis (vt M 2.372 IP-kõne kasutamise planeerimine). Ebavajalikud ja turvalisuse seisukohalt kriitilised funktsioonid tuleb desaktiveerida. Turvalisuse seisukohalt kriitiliste funktsioonide hulka kuuluvad näiteks aktiivse kõnega liitumine, ruumiseire funktsioonid ja vaheldumisi rääkimine.

Administreerimine ja juurdepääsud

Vahevara administreerimist ja konfigureerimist tuleb alati teostada kas konsoolist või turvaliste ühenduste kaudu. Administreerimine võib näiteks toimuda *Secure Shell* -i (SSH) või krüpteeritud VPN-ühenduse kaudu. Paljud IP-kõne süsteemid võimaldavad konfigureerimist läbi veebiliidese. Seejuures installeeritav veebiserver võib kujuneda täiendavaks turvariskiks. Seetõttu tuleks võimaliku veebipõhise konfigureerimisliidese puhul hoiduda veebiserveri käitamisest kriitilisel vahevaral, näiteks lüüsidel ja *Gatekeeper* -itel. Veebipõhine konfigureerimine peab alati toimuma turvatult, näiteks SSL-i või TLS-i kasutades. Administreerimiskontseptsiooni planeerimine vajab töörollide kontseptsiooni, mis hõlmab erinevaid volituste astmeid. Iga roll tuleb asendamise tagamiseks siduda vähemalt kahe inimesega. Sageli on võimalik IP-kõne komponente (nt tarkvaratelefone või vahevara-rakendusi) üldlevinud operatsioonisüsteemidega tavalistesse arvutitesse installeerida. Operatsioonisüsteemide administreerimine tuleb võimalusel eraldada IP-kõne rakenduste administreerimisest, määrates need ülesanded erinevatele inimestele. Süsteem peab konfiguratsiooni muudatusi logima selliselt, et manipulatsioonid oleksid aegsasti tuvastatavad. Logifailid ise peavad olema kaitstud selliselt, et nendega manipuleerimine oleks välistatud. Selleks tuleks piirata ka administraatorite juurdepääsuvõimalusi. Logiandmete kaitseks võib neid salvestada WORM-andmekandjatele või võimaldada juurdepääsu ainult revidentidele.

Andmevarundus

Töökindluse tagamiseks ja käideldavuse kiireks taastamiseks, samuti tervikliikuskontrollide läbiviimiseks on tingimata tarvis, et olemas oleks laiaulatuslik

andmevarunduse kontseptsioon. Seejuures tuleb jälgida, et isikuandmeid, näiteks isiklikke ühendamisandmeid varundades, hoitaks neid volitusteta juurdepääsude eest kaitstult, näiteks krüpteeritult.

Tarkvara turvalisus

Tuleb jälgida, et kasutatud tarkvara oleks alati uuendatud ja turvalisust puudutavad paigad paigaldataks viivitamatult. Eriti oluline on see operatsioonisüsteemi puhul. Tuleb tagada, et paigaldataks ainult originaalvärskendusi ja -paikasid. See kehtib nii soetamisel, näiteks tootja internetilehelt, kui ka IP-kõne komponendile paigaldamisel. Järgnevad meetmed raskendavad manipuleerimist andmeedastuse raames ning võimaldavad tuvastada manipulatsioone:

- kontrollsummade võrdlemine
- turvaliste sidekanalite kasutamine
- sertifikaatide kasutamine

Terviksüsteemi usaldusväärsuse tagamiseks on väga oluline, et tarkvara oleks korrektselt paigaldatud. Hoolika hindamisprotseduuri peaksid läbima ennekõike eriti just telefonisüsteemi olulised funktsioonid, näiteks kõnede suunamine ja lüüsifunktsioon digitaalsesse kaugekõnevõrku. See on vajalik seetõttu, et telefonisüsteemi põhifunktsioonide tarkvara, mis puudutab näiteks kõnede suunamist ja lüüsifunktsiooni digitaalsesse kaugekõnevõrku, oleks välja töötatud mõne end juba tõestanud töömudeli põhjal ning et sõltumatu osapool saaks seda kontrollida.

Operatsioonisüsteemi turvalisus

IP-kõne komponendid peaksid järgima kontseptsiooni, mille põhjal käitatakse erinevaid teenuseid erinevatel serveritel (vt M 4.97 Ainult üks teenus serveri kohta). Siiski ei ole teenuste täielik lahutamine alati võimalik, eriti näiteks just kompaktsete *Stand-alone* -süsteemide puhul, mis koosnevad tavaliselt ainult ühest riistavarakomponendist. Kasutatav operatsioonisüsteem peab olema minimaalne (vt M 4.95 Minimaalne operatsioonisüsteem) ja vahevaral käitatavate rakenduste arv võimalikult väike. Iga täiendav rakendus võib sisaldada puudujääke, mida võidakse rünnete jaoks kurjasti ära kasutada. Seega tuleb hoolikalt kontrollida, milliseid rakendusi läheb tarvis. Ebavajalikud rakendused tuleb deinstalleerida. Tarkvara, mida läheb tarvis ainult installeerimiseks (nt kompilaatorid), tuleb töö lõpetades kustutada. Samuti tuleb desaktiveerida ebavajalikud võrguteenused ja juurdepääsu alles jäänud võrguteenustele tuleb piirata lokaalsete paketifiltritega.

Täiendavad kontrollküsimused:

- Kas on tagatud, et värskendused ja paigad oleksid tootjalt kliendile edastamisel ja lokaalses andmevõrgus manipuleerimiskindlad?
- Kas IT-süsteemides desaktiveeriti kõik IP-kõne töö jaoks ebavajalikud teenused?
- Kas andmete varundamisel arvestatakse kogu olulise infoga?

M 4.288 IP-kõne lõppseadmete turvaline administreerimine

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator

Nii nagu IP-kõne vahevara, peavad ka IP-kõne lõppseadmed vastama arvukatele turvanõuetele. Vahevara turvameetmetest erinevad need turvalise konfigureerimise meetmete osas.

Usaldusväärsed püsivara värskendused

Paljud IP-kõne lõppseadmed pakuvad püsivara automaatset värskendust (*update*). Tuleb tagada, et uue püsivara paigaldamine lõppseadmetele toimuks alles pärast koodi autentsuse ja terviklikkuse edukat kontrollimist. Kui tootja pakub värskendustele kontrollsummasid või allkirjastab värskenduste pakette, tuleb enne installeerimist kontrollsummasid või signatuure kontrollida. Kui tootja kontrollsummasid ei paku, tuleb tagada, et värskendusi hangitaks ainult usaldusväärsetest allikatest.

Usaldusväärne konfigureerimine ja digitaalsed sertifikaadid

Suurem osa IP-kõnede lõppseadmeid pakuvad konfigureerimiseks erinevaid võimalusi. Selle näideteks on lõppseadme kohapealne konfigureerimine, veebipõhine konfigureerimine lõppseadmesse integreeritud veebiserveriga ning automaatne konfigureerimine, konfiguratsiooni http(s)- või TFTP-serverist „tõmbamine“ (*pull*).

Kohapealset konfigureerimist kasutatakse parktikas harva. See peab olema parooliga kaitstud. Kui seda ei kasutata, tuleks see desaktiveerida. Juurdepääs veebipõhisele konfiguratsioonile peab samuti olema parooliga kaitstud ja toimuma turvalise ühenduse, näiteks SSL-i või TLS-i kaudu. Täiendav kaitse saavutatakse kliendi autentimiseks kasutatava klientsertifikaadi abil. Automaatsest konfiguratsioonist TFTP-serveri kaudu tuleks loobuda ja see hoopiski desaktiveerida, kuna see pole piisavalt turvaline. Arvukaid ründevõimalusi pakub eriti just TFTP-serveri automaatne valimine DHCP-buutimise ajal. Automaatne konfigureerimine peab toimuma https-serveri kaudu. Https-server peab end autentima sertifikaadiga, mida lõppseade saaks enne konfiguratsiooni laadimist kontrollida. Tavaliselt installeeritakse serveri sertifikaat esmasel kasutuselevõtul käsitsi lõppseadmesse.

Turvafunktsioonid

Paljud IP-kõnede telefonid pakuvad võimalust paroolipõhiseks ühe- või mitmeastmeliseks juurdepääsukontrolliks (nt isiklik sisselogimine või ametkonna volitused). Tuleb otsustada, kas kasutajad peavad ennast kohustuslikus korras enne telefoni kasutamist sisse logima või mitte. Aktiveeritud paroolikaitse korral peab ilma sisse logimata olema võimalik helistada ainult hädaabinumbritele. Vältimaks seda, et seadmeid kasutaksid volitamata isikud, peavad kasutajad ka lühikese eemalviibimise korral telefoni sulgema. Turvafunktsioone, näiteks sisselogimise paroole või ametkonna volituste paroole, peab enne igapäevast kasutamist põhjalikult testima, et kontrollida nende õiget kasutuselevõtmist. Kasutajad peaksid neid autentimismehhanisme kasutama. Samas tuleb kasutajaid teavitada ka puudustest. Vastasel korral on oht, et turvalisus muutub vaid näiliseks. Tarkvaratelefone käitatakse reeglina tavaarvutites, mis täidavad veel ka teisi ülesandeid. Ka seda tuleb vastavalt hallata, et saavutada nõutud IT-turvalisuse tase. Selle alla kuuluvad

näiteks meetmed, mis ei lase mikrofoni aktiveerida kolmandal osapoolel. Kui seda nõuet ei täideta, võib ründe toimepanija mikrofoni aktiveerida ja kasutada seda pealtkuulamiseks.

Kuna keerukad töökohasüsteemid pakuvad arvukaid võimalusi rünneteks, ei tohi kõrgete ja väga kõrgete turvanõuete korral tarkvaratelefone kasutada.

Komponentide dokumentatsioonist leiab sageli informatsiooni täiendavate toetatavate turvafunktsioonide kohta. Sisse lülitatud turvafunktsioonid tuleb dokumenteerida.

Täiendavad kontrollküsimused:

- Kas on tagatud, et värskendused ja paigad on tootjalt kliendile edastamisel ja lokaalses andmevõrgus manipuleerimiskindlad?
- Kas võimalusel kontrolliti, et kolmas osapool ei saa aktiveerida tarkvaratelefoni mikrofoni?
- Kas on dokumenteeritud, milliseid turvafunktsioone lõppseaded pakuvad ja milliseid nendest funktsioonidest on kasutusel?

M 4.289 Ligipääsu piiramine IP-kõne komponentidele

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator

Internetipõhist otsejuurdepääsu firma või ettevõtte IP-kõne komponentidele on soovitav rakendada vaid väga vähestel juhtudel. Otsese juurdepääsuga, näiteks kui on loodud ühendus mõne sisevõrgu IP-aadressiga, pakutakse ründajale mitmeid võimalusi. Seega tuleb otsustada, milliseid IP-kõne arhitektuuri kasutavaid ühenduse loomise võimalusi pakutakse oma välistele kõnepartneritele. Esmalt tuleb kontrollida, kas IP-kõne otsest alustamist väljastpoolt on üldse tarvis. Sageli on piisav, kui kontakti võimaldatakse edasisuunava telefonivõrgu kaudu. Sellisel juhul ei tohi ükski sisevõrgu IP-kõne komponent olla avaliku andmevõrgu kaudu ligipääsetav. Ka lüüsile, mida käitatakse avaliku, edasisuunava telefonivõrgu ja kohaliku IP-kõne võrgu vahel, ei tohi avaliku andmevõrgu kaudu ligi pääseda. Olukord, kus IP-kõne välimised ligipääsuvõimalused otsustatakse aga täielikult ära kaotada, tekitab väliste kõnepartnerite jaoks märgatavaid puudusi. Juhul, kui neil on ühendus avaliku andmevõrguga, peavad nad sellegipoolest looma ühenduse avaliku, edasisuunava telefonivõrgu kaudu. Sellest toimingust tekkivad kulud on üldjuhul kõrgemad kui IP-kõnede aadresside otseühenduse kulud, näiteks SIP-URL-iga. Kuna selle puudusega käivad aga koos ka mitmed eelised, eriti just turvalisuse seisukohast kriitilistel kasutusjuhtudel, tuleks IP-kõnede välise ligipääsetavuse võimalikkust ja vajalikkust hoolikalt kaaluda. Olukordades, kus lubatakse ainult avaliku, edasisuunava telefonivõrgu kaudu tulevaid välisühendusi, saab vältida ka SPIT (*Spam over IP-Telephone*) ohtu. Kuna SPIT ei ole sel juhul enam andmevõrgu kaudu madalate kuludega edastatav, tekivad samad kulud nagu kasutaja puhul, kes ei kasuta IP-kõnesid.

Juhul, kui ühenduse loomine avalikku andmevõrku või avalikust andmevõrgust on siiski vajalik, tuleb see otsus koos riskidega dokumenteerida. Lisaks tuleb võtta tarvitusele vastavad turvameetmed. Näiteks võib kogu andmeside toimuda läbi kontsentraatori, mis võtab sarnaselt proksiserverile vastu ühenduspäringuid ja suunab neid edasi järgmisele süsteemile, näiteks täiendavale serverile või otse lõppseadmesse. Kontsentraatori kasutamisel tuleb arvestada järgnevate punktidega:

- Mõlemad, st nii signaal- kui ka kõneinfo, mis kulgevad avaliku ja privaatse andmevõrgu vahel, peavad liikuma läbi kontsentraatori. Individuaalsete ühenduste loomist tuleb takistada. Paketifiltrid ja turvalüüsid tuleb konfigureerida selliselt, et IP-kõne ühendus väliste sidepartneritega saaks toimuda ainult kontsentraatori kaudu. Näiteks võib kontsentraatorit käitada turvalüüsi demilitariseeritud tsoonis (DMZ). Sel moel saab vältida otseühenduse loomist lokaalsest võrgust avalikku võrku või avalikust võrgust lokaalsesse võrku.
- Puuduva signaalistandardi tõttu tuleks toetada võimalikult mitmeid välja suunatud signaaliprotokolle. Seetõttu peab kontsentraator toimima lüüsina lokaalses andmevõrgus kasutatud protokolli ja väliste kasutajate protokollide vahel.

- Kuritarvitamise takistamiseks peab kõne loomine sisemisest välimisse andmevõrku olema võimalik alles pärast kontsentraatoris autentimist.
- Kohapealse andmevõrgu piires loodavate ühenduste puhul ei ole kontsentraator tarvilik.
- Tuleb otsustada, milliseid funktsioone peale telefoniside tahetakse välistele osalejatele pakkuda.
- Kontsentraator peab tuvastama signaali- ja kõnepakette (nt liiga suuri andmepakette), mis ei ole protokollile iseloomulikud.
- Kuna avaliku andmevõrgu kaudu on võimalik kontsentraatorile otse ligi pääseda, tuleb esimesele kohale seada võimalikult turvaline konfiguratsioon.
- Avalikust andmevõrgust pöördusi tegevad kõnepartnerid peavad sellega ühenduse võtmiseks tundma kontsentraatori IP-aadressi. Sellest tulenevalt on võimalik avaldada kontsentraatori aadress ametkonna/ettevõtte DNS-serveri vastava sissekandega.
- Kõne- ja signaaliinfo vastuvõtmine, töötlemine ja edasisuunamine võib kulutada äärmiselt palju ressurssi. Seega peavad võrguühenduse ja süsteemi ressursid olema vastava jõudlusega.
- Kui kättesaadavusele esitatakse kõrgendatud käideldavusnõudmisi, peab kontsentraator olema liiasusega. Koormust jaotava liiasusega teostuse korral peavad ülejäänud süsteemid olema piisavalt suure jõudlusega, et võimaliku tõrke korral neile langeva koormusega toime tulla.

Paljud tootjad pakuvad selleks oma süsteeme. Avatud lähtekoodi valdkonnast täidab mitmeid neid nõudmisi tarkvaraline telefonisüsteem Asterisk, mida saab käitada eraldiseisva seadmena. Kontsentraatori täiendavaks eeliseks on võimalus vältida probleeme, mis esinevad NAT-i (*Network Adress Translation*) kasutamisel.

M 4.290 IP-kõne kasutamisest tulenevad nõuded turvalüüsidele

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator

Juhul, kui IP-kõnede jaoks kasutatakse IP-andmevõrku, tulenevad sellest täiendavad nõuded, eriti võrgu turvalisuse osas. Kõne- ja andmevõrkude range eraldamine on sageli võimatu, kuna näiteks töökohaarvutite tarkvaratelefonid pöörduvad kõnevõrgu IP-kõne serverite poole, *Groupware* -kliendid võimaldavad otse rakendusest valida salvestatud kontaktide numbreid ning IP-kõne servereid ühendatakse kataloogiteenustega, näiteks LDAP-ga (*Lightweight Directory Access Protocol*). Sellele lisaks võib esineda olukord, kus geograafiliselt eraldatud ametkonna, ettevõtte või organisatsiooni asukohad kasutavad organisatsioonisiseseks sideks keskset IP-kõne serverit ja vahetavad samal ajal selle ühenduse kaudu ka andmeid. Turvalüüs peab sisemist, turvalist süsteemi ebaturvalisest võrgust pärinevate volitusteta juurdepääsude eest kaitsma ja võimaldama samal ajal volitatud juurdepääsu kaitstud valdkondadele. Mõisteid, mis on turvaline või ebaturvaline võrk, milliseid ressursse tuleb kaitsta ja kuidas seda teha, kirjeldatakse organisatsiooni turvapoliitikas (vt lisaks B 3.301 Turvalüüs (tulemüür)). IP-kõne kasutamise planeerimisel tuleb kontrollida, kas olemasolevat turvalüüsi saab kohandada IP-kõne kasutamiseks. Juhul kui see pole võimalik, tuleb selleks otstarbeks soetada ja installeerida täiendav turvalüüs.

Turvalüüsi valimine ja sellele esitatavad nõuded

IP-kõne kasutamisel mõjutab turvalüüsi jõudlus mitte ainult turvalisust, vaid ka edastatava kõne kvaliteeti. IP-kõne puhul on tavapärane, et korraga töödeldakse suurt hulka väiksemahulisi andmepakette ning see koormab olulisel määral turvalüüsi, mistõttu võib kõne edastamisel esineda viivitusi ja katkevat heli. Kui signaali- ja kõneandmeid suunatakse edasi turvalüüsi kaudu, tuleb kasutada IP-kõne jaoks mõeldud turvalüüsi, mis suudab kasutatud signaaliprotokolle koos kõne alustamise ja lõpetamisega analüüsida ja vajalikke seisundeid salvestada. Logiandmete alusel (nt vajalikud UDP-pordid RTP abil edastatud kõneandmete jaoks) avatakse side kestuse ajaks vajalikud pordid. Lisaks sõltub õige süsteemi valimine alljärgnevatest faktoritest:

- Kui suur on võrk?
- Milliseid süsteemikomponente saab kasutada? Kas olemasolevad kommutaatorid võimaldavad kõne- ja andmevõrkude VLAN-eraldamist?
- Kas olemasolevad marsruuterid toetavad pääsuloendeid (ACL-e) või turvalüüside funktsioone?
- Millised turvalüüsid on andmevõrgus juba kasutusel?
- Kas tahetakse kasutada LAN-iga piirduvat IP-kõne võimalust või ka interneti kaudu toimuvat helistamist?
- Kui põhjalikud on IT-d haldava personali teadmised?
- Milliseid IP-kõne süsteemikomponente kasutatakse?
- Millised on turvaeesmärkide elluviimiseks kasutatavad finantsressursid?

Turvalüüsi kontseptsioon

Sõltumata sellest, kas IP-kõne kasutamise jaoks muudetakse olemasolevat turvalüüsi või soetatakse uus süsteem, võib see koosneda alljärgnevatest komponentidest:

- Seisundita paketifilter (*Stateless Packet Filter*) - Tavalisi paketifiltreid võib kasutada marsruuteritel, 3. kihi kommutaatoritel või turvalüüsidel, et eraldada andme- ja kõnevõrku, kuid nende filtreerimise funktsioonid oluliselt piiratumad kui seisundipõhistel filtritel või *Application Level* lüüsidel.
- Seisundipõhine filtreerimine (*stateful packet inspection*) - Seisundipõhised paketifiltrid suudavad side jaoks vajalikke tagastuspakette endast dünaamiliselt läbi lasta ja tagavad seega võrgu suurema turvalisuse. Nad salvestavad ühenduse seisundeid ja suudavad seetõttu tagastuspakette, mis kuuluvad loodud ühendusele, endast läbi lasta, ilma et selleks oleks tarvis konfigureerida täpseid pääsuloendeid.
- *Application Level Gateway* (ALG) - *Application Level Gateway* suudab filtreerida erinevalt eelnimetatud süsteemidest mitte ainult IP-aadresside ja portide, vaid ka rakenduse tasandil. *Application Level Gateway* eelis tuleb eriti esile RTP-pakettide edastamisel. RTP-ülekannete jaoks kasutatavaid UDP-porte vahetatakse signaliseerimise raames (SDP abil) lõpp-punktide vahel. Need pordid muutuvad tavaliselt iga uue kõne puhul ja vajavad turvalüüsis kinnitamist. Kuna ALG jälgib protokolliteadete vahetamist, milles lepitakse kokku IP-aadressid ja kasutatavad UDP-pordid, saab see filtrit dünaamiliselt kohandada ja seega vastava RTP-voo läbi lasta.

Võrreldes omavahel seisundita paketifiltreid, seisundipõhiseid paketifiltreid ja ALG-sid, tuleks plusside tõttu eelistada ALG-sid. Siseneva RTP-side võimaldamiseks peavad seisundita ja seisundipõhised turvalüüsid püsivalt avama suuri portidevahemikke, et kõneandmetega RTP-paketid läbi pääseksid. Selline konfiguratsioon on väga ebaturvaline. *Application Level Gateway* -d seevastu avavad ainult reaalselt vajaminevaid porte ainult sideühenduse ajaks ja pakuvad seega vähem ründevõimalusi. IAX-ile (*InterAsterisk eXchange*) sarnanevate protokollide kasutamine kergendab turvalüüside kontseptsiooni. Kuna seejuures edastatakse nii signaali- kui ka meediatranspordiinfot uudistevoo kaudu, läheb tarvis ainult ühte kindlat porti. Puuduva pordijagamise tõttu pole tarvis porte dünaamiliselt filtreerida.

Turvalüüsi konfigureerimine

IP-kõne kasutamiseks vajaminevad turvalüüsid on peaaegu samasugused nagu klassikalised turvalüüsid. Nende ülesehitamiseks ja turvaliseks käitamiseks tuleb rakendada moodulis B 3.301 Turvalüüs (tulemüür) kirjeldatud meetmeid. IP-kõne spetsiifikaga arvestavad seadistused tuleb sarnaselt meetmetele samuti võtta eelnimetatud moodulist. Nende konkreetne rakendamine on kirjas kasutatava toote dokumentatsioonis.

Täiendav kontrollküsimus:

- Kas turvalüüs on IP-kõne jaoks sobivaks kohandatud?

M 4.291 IP-kõne vahendustarkvara turvaline konfiguratsioon

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator

IP-kõne vahevara funktsioone ja turvalisust mõjutavad olulisel määral konfiguratsiooniparameetrite seadistused. Sageli läheb tarvis mitut sõltumatut IP-kõne komponenti, näiteks *Gatekeeper* 'it ja lüüse. Ühe komponendi ühe konfiguratsiooniparameetri kooskõlastamata muutmine võib tekitada koostöös teiste komponentidega tõrkeid. IP-kõne komponentide eest vastutavad administraatorid peavad pärast nende kasutuselevõttu tegema mitmeid täiendavaid muudatusi. Olukordades, kus töötajad lahkuvad ametiasutusest/ettevõttest või kui lisandub uusi töötajaid, tuleb teha muudatusi. Ka teise võrgusegmenti ümberkolimisel, näiteks kolides teise hoonesse, tuleb teha muudatusi. Seega tuleks valida konfiguratsiooniks liides, mille abil saavad administraatorid neid muudatusi teha võimalikult tõhusalt. Tavaliselt määratakse igale töötajale IP-kõne jaoks üks kasutajanimi ja üks parool. *VoiceMail* 'ide kasutamisel võib siinkohal sisestada meiliaadressi. Kasutajad peavad endale valima paroolid, mis pole liiga lühikesed ega liiga kergesti äraarvatavad. Aktiveerida tuleb seadistused, mis võimaldavad kasutada ainult turvalisi paroole. Kasutajatel, kellel on ainult statsionaarsed, muutumatu IP-aadressiga seadmed, peaks olema lubatud sisse logida ainult selle seadmega, mis on selle IP-aadressiga seotud.

Kasutajanime ja telefoninumbri sidumisel tuleb arvestada võimalike organisatsioonisiseste nõuetega. Oluline on ka selliste telefoninumbrite määramine, mis pole seotud ühegi kasutajaga. Selle näiteks on konverentsiruumides asuvad külalistele vabalt ligipääsetavad telefonid. Nende telefoniühenduste privileegid peavad olema võimalikult piiratud. Tavaliselt on vastuvõetavaks ja piisavaks piiranguks võimalus helistada ainult asutuse/ettevõtte piires. Sageli on võimalik määrata, milline kasutaja tohib kasutada milliseid signaaliprotokolle. Võimalusel tuleks kõigile kasutajatele määrata üksainus protokoll, kuna see vähendab administreerimise töövaeva. Kui lõppseadmed toetavad krüpteeritud signaaliprotokolle, tuleb arvestada sellega, et krüpteerimata sisselogimine on võimatu.

Kodukeskjaama kasutajatele saab määrata teatud õigusi (privileege) ning neid saab ka ära võtta. Näiteks saab piirata õigust helistada välismaale või tasulistele erinumbritele. Konfigureerimisel on eesmärgiks anda igale kasutajale ainult sellised õigused, mis on talle ette nähtud. Väikesed, ise välja töötatud ja oludele vastavad makrod võivad administraatorite konfigureerimisvaeva kergendada. Need makrod tuleb põhjalikult dokumenteerida. Makrode kasutamisel tuleb arvestada sellega, et enne kasutamist tuleb nende kvaliteeti põhjalikult kontrollida ja neid korralikult testida. Vastasel korral võivad makrod tekitada raskesti leitavaid konfiguratsioonivigu või kaasa tuua muid soovimatuid kõrvalmõjusid. Konfigureerimisel tuleb jälgida, et täiendavad ja ebaolulised teenused desaktiveeritaks/jääksid desaktiveerituks. Vastasel korral võidakse neid teenuseid ära kasutada rünneteks.

Logida saab paljusid erinevaid sündmuseid. Signaaliinfo alusel saab näiteks hinnata, milline kasutaja kui kaua telefoni kasutas ja kellele ta helistas. Kui meediainfot ei vahetata otse lõppseadmete vahel, vaid vahevara kaudu, on reeglina võimalik kõne sisu analüüsida ka tsentraalselt. Logimisfunktsioonid võivad ühest küljest aidata IP-kõne kasutamist analüüsida, teisest küljest ei tohiks logimisfunktsioonid siiski ei IT-turvalisust vähendada ega pakkuda võimalusi andmekaitse-

reeglite rikkumiseks. Seega tuleb süstemaatiliselt ja siduvalt kindlaks määrata, milline info tuleb logida ja kuidas logiandmeid regulaarselt analüüsida. Selles protsessis peavad kindlasti osalema andmekaitsespetsialist ja töötajate esindus. Kui analüüsis esineb ebakõlasid, tuleb neid lähemalt uurida ja põhjused vajadusel kõrvaldada.

Kõiki seadistusi tuleb kontrollida regulaarse revisjoni käigus.

Täiendavad kontrollküsimused:

- Kas kasutajate sissekannete aktuaalsust kontrollitakse regulaarselt?
- Kas on tagatud, et igale kasutajale antaks ainult temale mõeldud privileegid?

M 4.292 IP-kõne logimine

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator

IP-kõne kasutamisel saab logida erinevat infot. Enamasti tuleb sujuva töö tagamiseks logida IP-kõne vahevara teatud seisundiinfot. Selliste logiandmete regulaarne analüüsimine võimaldab hinnata seadmete õiget tööd ja tuvastada ründekatseid. Logiandmed võimaldavad sageli tuvastada ka ründe liiki, aidates niiviisi kohandada konfiguratsiooni. Logimisfunktsiooni hoolikas konfigureerimine on eriti oluline, kuna oluliste andmete leidmine on võimalik ainult suure andmehulga õige filtreerimise korral. Sõltuvalt logitava sündmuse liigist võib olla vajalik reageerida sellele võimalikult kiirelt. Seega tuleb logiandmeid analüüsida regulaarselt. Logimisfunktsioonid võivad ühest küljest aidata IP-kõne kasutamist analüüsida. Teisest küljest tekib aga oht, et logimisfunktsioonid võivad siiski vähendada IT-turvalisust ning pakkuda võimalusi andmekaitsereeglite rikkumiseks. Seega tuleb siduvalt kindlaks määrata ja dokumenteerida, milline info vajab logimist ja kuidas logiandmeid regulaarselt analüüsida. Selles protsessis peavad kindlasti osalema andmekaitsespetsialist ja töötajate esindus (vt M 2.110 Andmeprivaatsuse suunised logimisprotseduurides). Logimisse kaasatavate andmete ulatus ja nende kontrollimise kriteeriumid tuleks dokumenteerida ja organisatsioonisiseselt kokku leppida. Vajadusel tuleb varakult kaasata vastavad otsustavad komiteed.

Signaalide logimine

Signaalilogide analüüsist saab tuletada suurel hulgal informatsiooni. *Sip-Proxy* , *Gatekeeper* 'i või *Gateway* puhul tuleb salvestada järgnevad andmed:

- kes helistas kellele,
- kui kaua kõne kestis,
- kas kõne võeti vastu,
- millisest võrgust ja milliselt IP-aadressilt kõne toimus,
- millise meediatranspordiprotokolli ja millise koodeki osas kokku lepiti.

Seda infot saab kasutada näiteks kulude arveldamisel või IP-kõne infrastruktuuri optimeerimisel.

Meediatranspordi logimine

Võrgukeskkonnas, teatud sobivas punktis logimisel, on mõningatel tingimustel võimalik salvestada ka kõnesid. Kõnesid, mis lahkuvad võrgust teatud kindla punkti kaudu, näiteks läbi *Proxy*, saab logida otse selles punktis. Sisekõnede puhul ei ole *Proxy* sageli vajalik. Kõne sisu salvestamine on tavaliselt ka neil juhtudel võimalik, näiteks sides osalevates lõppseadmetes või marsruuterites. Tõhusalt krüpteeritud meediatranspordi korral, kus kõnepartnerid lepivad krüptograafiliste võtmete osas ise kokku, saab tsentraalses punktis vähem infot salvestada.

Süsteemi olekuinfo logimine

Lisaks eelpool nimetatud punktidele tuleks IP-kõne vahevaras võimalusel logida ka järgnevat infot:

- kõik otsesed sisselogimised eraldiseisvas süsteemis või IT-süsteemis,
- konfiguratsioonimuudatused,
- IP-kõne teenusesse ebaõnnestunud sisselogimised,
- süsteemivead,
- koormus,
- kasutajate haldust puudutavad muudatused (kasutajate loomine või kustutamine, kasutaja ja telefoninumbri vahelise seose muutmine, jne),
- IT-süsteemi tõrkeid põhjustada võivad riistvaravead,
- olulised IP-kõne rakenduse käitamiseks kasutatava IT-süsteemi sündmused. Lisainfot selle kohta leiate operatsioonisüsteemi vastavast IT-etalonturbe moodulist.

Logiandmete tsentraalne haldamine

Logiandmed tuleks võrgu kaudu edastada *syslog* -serverisse. See aitab logiandmeid tsentraalselt koguda, arhiveerida ja analüüsida, kuna eraldiseisvatel IP-kõne seadmetel puuduvad sageli selleks piisavad töövahendid. Lisaks on selle eeliseks, et seadme kuritarvitamisel ei saa ründaja juba edastatud logiandmeid otse muuta ega kustutada. Kui ülekanne *syslog* -serverisse toimub krüpteerimata kujul, on edastuskanalit võimalik pealt kuulata. Seega tuleks logiandmeid salvestada kas ainult serveris endas, või edastada krüpteeritult läbi eraldi võrgu (administreerimisvõrgu).

Aja sünkroniseerimine

Võimalusel peab kõikide logiandmete ajatempel olema õige. Ainult nii on võimalik neid andmeid tõhusalt analüüsida, eriti ründekatsete või edukate rünnete puhul. Seetõttu tuleks sisevõrgus kasutada vastavaid servereid, mis edastavad kõikidele süsteemidele õige aja. See võib toimuda näiteks NTP-teenusega (vt M 4.227 Lokaalse NTP -serveri kasutamine aja sünkroniseerimiseks).

Täiendavad kontrollküsimused:

- Kas logimisel ja analüüsimisel arvestatakse andmekaitse ettekirjutustega?
- Kuidas tagatakse kõikide seadmete õige süsteemiaeg?

M 4.293z Avalike pääsupunktide turvaline käitamine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT-juht
Rakendamise eest vastutavad: IT-juht, infoturbe spetsialist, administraator

Avaliku pääsupunkti eesmärgiks on tavaliselt võimaldada (võõrastele) kasutajatele lihtsat juurdepääsu internetti. Avaliku pääsupunkti püsivaks ja ohutuks tööshoidmiseks läheb tarvis kõikide kasutajate autentimist pääsupunktis. Tavapärased ja mööndustega turvalised meetodid on näiteks järgmised:

- Veebis autentimine - Siin sisestab kasutaja veebiliidesesse oma pääsuandmed (IP-aadressi, kasutajanime, parooli jne). Loomulikult peab see toimuma krüpteeritult SSL/TLS kaudu. Pärast edukat autentimist avaneb kliendile juurdepääs.
- PPTP (*Point to Point Tunnel Protocol*) - PPTP on tüüpiline VPN-ide tunneldusprotokoll ehk protokoll, mida kasutatakse selleks, et andmeid edastamisel krüpteerida, läbi tunneli edastada ja ühendust hallata. Krüptograafiliste meetmetena saab PPTP puhul valida krüpteerimiseks kas 40- või 128-bitilise RC4 ning autentimiseks PAP-i või CHAP-i. Selle tunneldusmeetodi tavapärases rakenduses on leitud turvaauke, eriti just seoses nõrkade paroolidega. Seega ei tohiks PPTP-d kasutada ilma täiendavate turvamehhanismideta.
- *IPSec* - *IPSec* pakub tugevaid krüptograafilisi meetodeid ja sidepartnerite vastastikust autentimist. Oleks mõistlik, kui see põhineks sertifikaatidel. Kuid esiteks pole nende kasutamine veel kõikides *IPsec* -i rakendusviisides ette nähtud ning teiseks tuleb need esmalt sobivalt luua ja jaotada (tavaline PKI-probleem).
- WLAN-põhised turvamehhanismid, näiteks WEP, IEEE 802.1X, WPA, WPA2, TKIP, IEEE 802.11i - Kõikide WLAN-põhiste turvamehhanismide puhul tuleb tagada sidekanali turvalisus. Need tuleb sobival viisil kombineerida. Selles valdkonnas toimuvate kiirete arengute tõttu ei sobi mitte kõik need meetodid kas oma leviku või turvapuudujääkide tõttu avalikes pääsupunktides kasutamiseks.

Avalike pääsupunktide teenusepakkujad peavad tagama sobiva autentimismeetodi kasutamise. Avalike pääsupunktide käitamisel tuleb lisaks rakendada järgnevaid turvameetmeid:

- Avalike pääsupunktidena kasutatavaid *Access Point* 'e ei tohi LAN-iga siduda otse, vaid ainult turvalüüsi kaudu.
- WLAN-klientide omavaheline kommunikatsioon, nn klientidevaheline kommunikatsioon, peab olema täielikult tõkestatud.
- Raadiolevi liidest tuleb jälgida raadioside analüüsisüsteemidega, et tuvastada võõraid *Access Point* 'e ja pääsupunkte.

- Autentimisandmeid tuleb raadiosidekanali kaudu, ehk siis WLAN-kliendi ja *Access Point* 'i vahel edastada alati krüpteeritult. Andmete edasisel ülekandmisel avaliku pääsupunkti *Access Point*'ist autentimissüsteemidesse (nt RADIUS-serverisse) tuleb kasutada sobivaid krüpteerimismeetodeid, näiteks SSL-i või *IPSec* -i, eriti kui kasutatakse avalikke võrkusid.
- Kui autentimiseks kasutatakse sertifikaate, peavad need olema allkirjastatud sobiva sertifitseerimisorgani poolt. Lisaks tuleb avaldada serverisertifikaadi sõrmejälg, et kasutaja saaks kontrollida ehtsust.
- Iga avaliku pääsupunkti käitaja peab pakkuma vähemalt üht sobivat meetodit raadiosidekanali krüpteerimiseks, et kasutajad saaksid oma andmeid kaitsta volitamata lugemise eest. Siiski – mitte kõik kasutajad ei hooli oma andmete ja süsteemide kaitsest. Samuti on võimalik, et neil puuduvad krüpteerimismeetodite kasutamiseks vajalikud tehnilised eeldused, seega peaks nende kasutamine olema valikuline. Siiski tuleks kasutajate tähelepanu juhtida krüpteeritud andmeedastuse võimalusele ja selle eelistele.
- Paljud kasutajad tahavad avaliku pääsupunkti, näiteks VPN-i kaudu ligi pääseda oma organisatsiooni võrgule. Siinkohal peab olema võimalik rakendada organisatsioonile omaseid turvareegleid. Seetõttu peab avaliku pääsupunkti tehniline teostus võimaldama tavaliste turvameetmete, nt *IPsec* -i kasutamist.

Lisaks peaksid avalike pääsupunktide haldajad regulaarselt kontrollima logisid, et tuvastada, kas esineb ebakorrapärasusi näiteks kasutajate arvus, et näha, kas sisse logitud külaliste arv ületab näiteks kasutajate arvu.

Avalike pääsupunktide funktsiooni pakkujad peavad lisaks sellele arvestama ka seaduste ja ettekirjutustega. Kasutajaid tuleb kasutustingimustest teavitada sobival viisil. Kasutustingimused peavad sisaldama infot selle kohta, kas kasutamine on tasuta või tasuline (koos vastavate hindaega), lisaks ka andmeid selle kohta, milliseid teenuseid (esmajoones turvamehhanisme) pakutakse avaliku pääsupunkti kasutamisel. Kasutaja peab kinnitama, et ta on kasutustingimused läbi lugenud ja nõustub nendega. Veebis autentimisel saab kasutustingimusi esitada veebilehel ja võimaldada seal samas nendega nõustumist. Avalike pääsupunktide kasutajate jaoks oluline turvapoliitika on kirjas meetmes M 2.389 Avalike pääsupunktide turvaline kasutus .

Täiendavad kontrollküsimused:

- Kas avaliku pääsupunkti kasutustingimused on igale kasutajale hõlpsasti leitavad ja mõistetavad?
- Kas avalikud pääsupunktid on LAN-ist eraldatud või kas avaliku pääsupunkti kasutaja juurdepääsu LAN-ile kaitseb vähemalt turvalüüs?
- Kas klientidevaheline kommunikatsioon on tõkestatud?
- Kas raadiolevi liidest kontrollitakse, et leida võõraid *Access Point* 'e ja avalikke pääsupunkte?
- Kas autentimispäringud ja ka raadiosidekanal on piisavalt krüpteeritud?

M 4.294 Pääsupunktide turvaline konfigureerimine

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator

Access Point 'e ei tohi mitte mingisugusel juhul kasutada tarnitud konfiguratsiooniseisundis, samuti ei tohi juurdepääsuparoolide või krüptograafiliste võtmete jaoks kasutada toote käsiraamatus mainitud seadistusi, näiteks SSID (*Service Set Identifier*) seadistusi. Sisse tuleb viia järgnevad muudatused, st kasutada tuleb individuaalseid, turvalisi väärtuseid:

- Kui võimalik, tuleb *Access Point* 'ide administratiivne õhuliides üldjuhul desaktiveerida.
- Kõik administreerimise paroolid peavad olema võimalikult keerulised ja neid tuleb regulaarselt vahetada.
- Ebaturvalised administreerimise juurdepääsud (nt Telnet, HTTP) tuleb võimalusel välja lülitada. Administreerimisvõimalusega juurdepääsu puhul peab kindlasti kasutama krüpteeritud ühendust (nt SSL-i või SSH-d).
- Eelseadistatud SSID-d, krüptograafilised võtmed või paroolid tuleb muuta kohe pärast kasutuselevõttu.
- SSID ei tohi sisaldada mitte mingisuguseid viiteid omanikule ega WLAN-i eesmärgile. Samuti ei tohi SSID seadistus olla „Any“, kuna sel juhul võib kommunikatsioonis osaleda iga suvaline WLAN-i komponent.
- SSID -*Broadcast* tuleb desaktiveerida, et vältida WLAN-i olemasolu asjatut ilmsikstulekut. Lisaks tuleb desaktiveerida seos SSID -*Broadcast* 'iga, et klient peaks seostamisel sisestama selgelt nõutava SSID.
- Sobivad krüpteerimismehhanismid peavad olema aktiveeritud. Samal ajal peab olema tagatud, et kõik WLAN-i komponendid seda ka toetaks. Ühenduse loomine WLAN-komponentidega, millel puuduvad või on ebapiisavad krüpteerimismehhanismid, peab olema tõkestatud.
- Krüptograafilised võtmed peavad olema võimalikult juhuslikult valitud ja neid tuleb regulaarselt vahetada. WPA-PSK või WPA2-PSK kasutamisel tuleb kasutada keerukat *Pre-Shared Key* 'd (PSK). Kui PSK-taoline krüptograafiline võti genereeritakse parooli abil, tuleb kasutada ülikeerukat parooli, milles on vähemalt 20 märki.
- *Access Point* 'i jaoks lubatud kommunikatsioonipartnerite piiramiseks tuleb kasutada MAC-aadressi tasandil pääsuloendeid (ACL'e). See on eriti kasulik väikeste kuni väga väikeste WLAN-süsteemide puhul. Ainukese vahendina ei taga see siiski eriti just WLAN-ide puhul (pealtkuulatavuse tõttu) reeglina piisavat turvalisust, kuna MAC-aadresse on lihtne muuta. Pääsuloendid WLAN-is on seega ainult nõrk, täiendav lisameede, mille kasutamine on mõistlik vaid teatud eriolukordades. Kuna selle kasu turvalisusele on väike, tuleks suuremates võrkudes kaaluda, kas sellega kaasnev suurem administreerimise töömaht on õigustatud või mitte.
- *Acces Point* 'i võimalik DHCP (*Dynamic Host Configuration Protocol*) Server tuleks, kui see on tehniliselt teostatav, välja lülitada. Kasutada tuleks

staatilisi IP-aadresse ja lubatud IP-aadressiala peaks olema võimalikult väike. Vastasel korral määrab DHCP server sissetungijale automaatselt mõne kehtiva IP-aadressi.
- Mitme *Access Point* 'i kasutamisel tuleb lähedal asuvate *Access Point* 'ide sageduskanalid valida võimalikult kattumisvabalt.
- Süsteemi konfiguratsiooni muudatusi tuleb testida ning need tuleb ka dokumenteerida.
- Regulaarselt tuleb kontrollida, kas kõik turvalisuse seisukohalt olulised värskendused ja paigad on installeeritud. Seda tuleb arvestada ka WLAN-klientide WLAN-riistvara vastavate seadmedraiverite puhul. Tarkvara uus versioon või paik tuleb paigaldada WLAN-i alles siis, kui seda on eelnevalt piisavalt testitud. Praktikas on juba juhtunud, et pärast tarkvara värskenduse paigaldamist hakkab WLAN-kommunikatsioon tööle kas ainult väga piiratult või lakkab üldse töötamast. Muudatuste halduses tuleb täpsustada teavitamis- ja infoprotseduurid, mis kirjeldavad, keda ja kuidas sellistest muudatustest teavitada. Samuti tuleb kohandada WLAN-infrastruktuuri dokumentatsiooni.
- Kui WLAN-komponente pikemat aega ei kasutata, tuleb need välja lülitada. *Access Point* 'id tuleb väljaspool tööaegu (nt ööseks ja nädalavahetusteks) automaatselt desaktiveerida.

WLAN-i haldustarkvara ja sidumine tsentraalse võrguhaldusega võimaldab neid ülesandeid abistada ja kontrollida.

Täiendavad kontrollküsimused:

- Kuidas toimub administreerimisotstarbeline juurdepääs süsteemile?
- Kuidas konfiguratsiooni muudatusi testitakse ja dokumenteeritakse?
- Kas on tagatud, et avastatud turvalünkadele välja töötatud paigad ja värskendused installeeritakse võimalikult operatiivselt?
- Kas on tagatud, et WLAN-i komponendid lülitatakse ka tegelikult välja, kui neid ei vajata pikema aja jooksul?

M 4.295 Traadita kohtvõrgu kliendi turvaline konfiguratsioon

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator, kasutaja

WLAN-ide turvalise käitamise tagamiseks peavad ka kõik sellega ühendatud kliendid olema turvaliselt konfigureeritud. Sobivad klientide IT-turvasuunised leiate IT-süsteemide kolmanda kihi moodulitest *IT-süsteemid*. Täiendavalt tuleb võtta tarvitusele järgnevad WLAN-i põhised turvameetmed:

- Eelseadistatud SSID-d, krüptograafilised võtmed ja paroolid tuleb ära muuta kohe pärast kasutuselevõttu. Paroolid peavad olema raskesti äraarvatavad.
- *Ad-hoc* -režiim tuleb välja lülitada, et kliendid saaks üksteisega suhelda ainult pääsuloendi abil, aga mitte otse.
- Kaitsmist vajavad andmed mobiilsetel lõppseadmetel tuleb krüpteerida. Selle jaoks on olemas mitmeid riistvara- või tarkvarapõhiseid tooteid, mis võimaldavad üksikuid andmeid, teatud alasid või tervet kõvaketast krüpteerida nii, et pääsuõigused on ainult nendel, kes suudavad andmeid dekrüpteerida.
- Klientide WLAN-liidesed, kui neid reaalselt tarvis ei lähe, peavad reeglina olema desaktiveeritud. Esmajoones peab see toimuma alati siis, kui kliendid on sisse logitud kaabliühendusega LAN-i. Juurdepääs klientsüsteemist majasisesesse LAN-i, kasutades tavalist siseühendust, peab olema võimalik ainult siis, kui sellele ei järgne tegevusi WLAN-is. Vastasel korral loob see ründajatele võimaluse tungida WLAN-liidese kaudu majasiseses võrgus olevatesse (ja autenditud) ühendustesse.
- VPN-ühenduste loomisel peab kliendi poolel olema täidetud mitmed turvanõuded. VPN-ühenduse kõrval ei tohi olla võimalik kasutada teisi kommunikatsiooniliideseid, et ebaturvalised kanalid ei õõnestaks näiliselt turvalist VPN-ühendust. Lisaks oleks kasulik mitte ainult eeldada, et klientide poolel on olemas teatud minimaalsed turvameetmeid, vaid ka nende täitmist kontrollida ning alles seejärel võimaldada juurdepääsu VPN-i kaudu. Seega tuleks enne seda, kui server võimaldab edasist kommunikatsiooni, kasutada tööriistu, mis kontrollivad klientide turvapoliitikast kinnipidamist.
- Regulaarselt tuleb kontrollida, kas kõik turvalisuse seisukohalt olulised värskendused ja paigad on installeeritud. Suurema tarkvaravärskenduse paigaldamine WLAN-kliendile WLAN-i kaudu võib olla problemaatiline, kuna ribalaius WLAN-is on võrreldes kaablitel põhineva LAN-iga oluliselt väiksem. Värskenduse paigaldamine võtab sel moel oluliselt kauem aega, lisaks võib see mõjutada ka teisi WLAN-i kasutajaid, kuna WLAN on *Shared Medium*. Võimalusel tuleks klient seega suurema tarkvaravärskenduse paigaldamiseks ühendada kaablipõhise LAN-iga. Lisaks võib tarkvaravärskenduse ülekandmise seada madalamale prioriteedile, juhul, kui seeläbi pikenev paigaldusaeg on vastuvõetav. Sel moel ei sega tarkvaratäiend olulisel määral teisi WLAN-i rakendusi.

Regulaarselt tuleb kontrollida, et turvalisuse seisukohast olulisi seadistusi ei oleks muudetud. Tuleb selgelt määratleda, kas ja millistel raamtingimustel tohivad WLAN-kliendid võõrastesse võrkudesse sisse logida (vt M 4.251 Töötamine võõraste IT-süsteemidega), eriti just siis, kui neil on juurdepääs tootmiskeskkonnale või kui neil hoitakse konfidentsiaalset infot.

WLAN-kliente ei tohi käitada ebaturvalistes keskkondades, näiteks avalikes pääsupunktides või ainult WEP-ga kaitstud WLAN-ides. WLAN-kliente, mis töötlevad kõrge turbevajadusega andmeid, tohib rakendada ainult sellistes WLAN-ides, mida käitatakse täielikult oma kontrolli all ja mis on vastavalt turvalise konfiguratsiooniga. Rakendamine teistes WLAN-ides tuleb keelata. Kõiki WLAN-komponentide kasutajaid tuleb informeerida kasutuse võimalikest riskidest ja probleemidest, samuti kasutatavate turvameetmete kasust ning piiridest. Kõik kasutajad peavad tundma WLAN-i kasutamise turvapoliitikat (vt M 2.382 Traadita kohtvõrgu turvajuhendi väljatöötamine). Mitte keegi ei tohi omada juurdepääsu sisemisele WLAN-ile, kui ta pole eelnevalt andnud kirjalikku nõusolekut, et nõustub WLAN-i turvapoliitikas sisalduvate kasutustingimustega.

Täiendavad kontrollküsimused:

- Kas kasutajaid on informeeritud, milliste turvaaspektidega peavad nad WLAN-i kasutamisel arvestama?
- Kas on tagatud, et avastatud turvalünkadele välja töötatud paigad ja värskendused installeeritaks võimalikult operatiivselt?
- Kas kliendid lülitavad WLAN-i liidesed välja, kui neid ei kasutata?

M 4.296 Traadita kohtvõrgu sobiva haldussüsteemi kasutamine

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator

Turvalisuse seisukohast optimaalse konfiguratsiooni tagamine kõikidele WLAN-i komponentidele eeldab nende hoolikat administreerimist. Kuna suure WLAN-i administreerimine võib olla töömahukas ja keeruline, tuleks kasutada WLAN-i süsteemihaldustööriistu. Need tuleks võimalusel integreerida olemasolevate IT- ja võrguhaldustööriistadega. Reeglina tuleks võtta kasutusele selline halduslahendus, mis võimaldaks WLAN-i kõrval ka *online* -dokumenteerimist. Sõltuvalt vajaminevast jõudlusest peab see pakkuma järgnevaid võimalusi:

- *Access Point* 'ide püsivaraseisundite dokumenteerimine
- WLAN-klientide WLAN-adapteri püsivaraseisundite dokumenteerimine
- turvakonfiguratsioonide dokumenteerimine
- asukohapõhiste konfiguratsioonide dokumenteerimine
- konfiguratsioonimuudatuste ajaloo haldamine

Selleks, et administraatoritel säiliks ülevaade kõikidest statsionaarsetest ja mobiilsetest süsteemidest ja rakendustest, ja et see toimuks võimalikult lihtsalt, peab süsteemihalduse lahendus suutma mobiilseid lõppseadmeid ja nende rakendusi automaatselt inventariseerida. Haldustarkvara peab iga lõppseadme kaasama konfiguratsiooni- ja kontrollprotseduuridesse, niipea kui see võrku sisse logib. Selle funktsiooni kasutamisel tuleb lähtuda käsiraamatu infost. Lisaks peavad haldussüsteemil olema protseduurid hoiatamiseks ja vigadega toimetulemiseks. Seejuures peavad administraatorid saama täita järgnevaid ülesandeid:

- hoiatusteadete analüüs, näiteks sagedased ebaõnnestunud autentimiskatsed *Access Point* 'is,
- veaotsingu statistika analüüs,
- meetmete rakendamine turvaintsidendi kahtluse korral,
- alarmi piirväärtuste kohandamine WLAN-kasutuse muudetud väärtustega.

Tuleb valida sobiv võrguhaldusprotokoll, näiteks SNMPv3 (vt M 2.144 Sobiva võrguhaldusprotokolli valimine). Salvestatud logiandmeid tuleb analüüsida regulaarselt, kuid vähemalt kord kuus. Logimise maht tuleb kooskõlastada töötajate esindajaga ja andmekaitsespetsialistiga. WLAN-i haldustarkvara või üldine võrguhalduslahendus peab pakkuma filtreerimisvõimalusi, et logiandmeid paremini analüüsida.

Täiendavad kontrollküsimused:

- Millal leidis viimati aset salvestatud logiandmete analüüsimine?
- Kas kõik WLAN-komponendid on inventariseeritud?

M 4.297 Traadita kohtvõrgu komponentide turvaline kasutamine

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator

WLAN-id on ründajatele atraktiivsed sihtmärgid ning nende turvaline käitamine eeldab väga hoolikat konfigureerimist. Kõik WLAN-i komponendid peavad olema konfigureeritud selliselt, et need oleksid rünnete eest võimalikult hästi kaitstud. Seni, kuni WLAN-i komponendid pole vastavalt konfigureeritud, ei tohi neid aktiveerida ega töökeskkonnaga ühendada. Kaitset vajavate WLAN-i komponentide hulka kuuluvad ka *Access Point* 'id, *Distribution System*, WLAN-i kliendid, operatsioonisüsteemid, millel WLAN-i komponente käitatakse, ja kasutatavad protokollid. Eriti oluline on siinkohal arvestada järgnevate punktidega:

- Erinevate WLAN-i komponentide administreerimiseks tuleb määrata vastutavad isikud.
- Pärast WLAN-i komponentide paigaldamist ja kasutuselevõttu tuleb aktiveerida kõik vajalikud turvamehhanismid.
- WLAN-i komponentide haldamine võib toimuda ainult turvalise ühenduse kaudu, st haldus peaks toimuma konsooli abil otse, eelneva tugeva autentimisprotsessiga (juhul kui juurdepääs toimub LAN-i kaudu), või siis krüpteeritud ühenduse abil (juhul kui juurdepääs toimub internetist).
- Kehtima peab reegel „Kõik, mis ei ole otseselt lubatud, on keelatud“. Näiteks ei tohi ükski kasutaja, keda pole pääsuloendis, WLAN-ile ligi pääseda. Pääsuõigused kataloogidele ja failidele peavad olema määratud võimalikult piiratult.
- Tuleb jälgida, et kasutatud tarkvara oleks alati uuendatud ja turvalisust puudutavad paigad paigaldataks viivitusteta.
- Süsteem peab konfiguratsiooni muudatusi logima selliselt, et manipulatsioonid oleksid aegsasti tuvastatavad. Logiandmed peavad olema kaitstud selliselt, et nendega manipuleerimine oleks võimatu.
- Kõik turvalisuse seisukohalt olulised sündmused tuleb logida. Selle alla käivad näiteks volitusteta juurdepääsukatsed ja võrgukoormuse ning võrgu ülekoormuse andmed. Salvestatud logifaile tuleb regulaarselt analüüsida. Logimise maht tuleb kooskõlastada töötajate esindajaga ja andmekaitsespetsialistiga.
- WLAN-i komponendid tuleb kaasata andmevarunduse kontseptsiooni. Turvaliselt hoiule pandud andmete taassisestamisel tuleb tähelepanu pöörata sellele, et WLAN-i turvaliseks kasutamiseks vajalikud failid nagu pääsuloendid, paroolifailid ja filtreerimisreeglid oleksid värsked.

Kasutuses olevate WLAN-i komponentide jaoks tuleks võimalusel luua standardkonfiguratsioon, milles kajastuksid WLAN-i turvapoliitika nõuded. Lisaks kergendab see suure arvu hallatavate seadmete puhul muudatuste tegemist. Ka kõrvalekalded nimikonfiguratsioonist on sedasi kiiremini tuvastatavad. Mõistlik on kasutada WLAN-i halduslahendust, mis tagab *Access Point* 'ide tõhusa konfiguree-

rimise. *Access Point* 'ide ja *Distribution System* 'i aktiivsete komponentide võrguhaldussüsteemiga sidumise ning seire võimalus peavad säilima. Lõpuks peab haldussüsteem suutma kontrollida ka autentimisserveri käideldavust. Vajadusel on võimalik juba kasutuses olevat võrguhaldussüsteemi täiendada WLAN-i haldusmooduliga.

WLAN-i haldussüsteem peab olema suuteline tuvastama võõraste *Access Point* 'ide ühendamist või *Distribution System* 'i kommutaatorite manipuleerimist. *Distribution* -kommutaatori vastav võrguport tuleb sellisel juhul kohe sulgeda. Samuti tuleb regulaarselt kontrollida *Access Point* 'ide ja *Distribution System* 'i konfiguratsiooni. Selleks tuleb süsteemikonfiguratsiooni hetkeseisu võrrelda dokumenteeritud ja kinnitatud konfiguratsiooniga. Kinnitamata muudatuste esinemisel tuleb süsteeme lähemalt uurida ja vajadusel isegi välja lülitada ning kontrollida, kas tegu võib olla ründega. WLAN-i komponentide turvalise töö tagamiseks tuleb nii WLAN-i turvapoliitikal põhinev aluskonfiguratsioon kui ka kõik tehtud muudatused hoolikalt dokumenteerida, et need alati mõistetavad oleksid. Lisaks turvakonfiguratsiooni dokumenteerimisele tuleb dokumenteerida ka *Access Point* 'ide püsivara seisundid ja asukohapõhised konfiguratsioonid.

Täiendavad kontrollküsimused:

- Kas on tagatud, et kõikidel WLAN-i komponentidel on vajalikud turvamehhanismid aktiveeritud?
- Kuidas tagatakse, et operatsioonisüsteemidele ja programmidele, mida kasutatakse WLAN-i komponentidel, on paigaldatud kõige värskemad turvapaikade versioonid?
- Millist kanalit pidi astuvad administraatorid ja auditi läbiviijad ühendusse tulemüüri ja selle komponentidega?
- Kas andmete varundamisel arvestatakse kogu olulise WLAN-i komponentide kohta käiva infoga?

M 4.298 Traadita kohtvõrgu komponentide regulaarne audit

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator

WLAN-i infrastruktuuri kõikide komponentide puhul tuleb regulaarselt kontrollida, kas kõik määratletud turvameetmed on rakendatud ja õigesti konfigureeritud. Lisaks *Access Point* 'idele on siin olulised *Distribution System* 'i komponendid, turvalisuse infrastruktuuri elemendid (kaasa arvatud autentimisserver) ja WLAN-i haldussüsteemi elemendid. WLAN-i haldussüsteem peab sõltuvalt funktsioonist haldama mitte ainult *Access Point* 'ide hetkekonfiguratsiooni, vaid ka *Distribution System* 'i komponente, ning pidama ajaloo halduse abil arvet ka varasemate konfiguratsioonide üle (vt M 4.296 Traadita kohtvõrgu sobiva haldussüsteemi kasutamine). Samuti tuleb regulaarselt kontrollida tsentraalsete turvasüsteemide, näiteks autentimisserveri või *Distribution System* 'i ja LAN-i vahelise punkti ühenduselemendi turvalisust. Pistelist kontrolli vajavad eriti just avalikult ligipääsetavates alades asuvad seadeldised, et tuvastada lahtimuukimis- või manipulatsioonikatseid (eriti *Access Point* 'ide puhul). WLAN-i kompromiteerimise tõestuseks võib olla nt *Access Point* 'i ja *Distribution* -kommutaatori vahele paigaldatud jaotur (*hub)* . Sellised diagnostika eesmärgiga seadeldised tohivad olla ligipääsetavad ainult volitatud personalile ning need tuleb pärast mõõtmiste lõppemist kohe eemaldada. Lisaks tuleb regulaarselt kontrollida WLAN-i kliente. Suurema arvu puhul tuleks seda teha vähemalt pisteliselt. Esmalt tuleb kontrollida WLAN-i adapteri konfiguratsiooni ja IEEE 802.1X *Supplicant* 'i (või VPN-i klienti, kui seda kasutatakse WLAN-is). Lisaks tuleb sõltuvalt süsteemist kontrollida ka operatsioonisüsteemi *Patch Level* 'it, kliendi WLAN-i adapteri draiveri ajakohasust, isikliku tulemüüri reguleerimispõhimõtteid, kasutatava viirusetõrje ajakohasust, ning samuti WLAN-i kaudu kasutatavate rakenduste turvaseadistusi.

Ebakorrapärasuste või kitsaskohtade tuvastamisel tuleb need dokumenteerida, ja seejuures tuleb kirja panna ka see, kuidas neid leida. Üksikute WLAN-i komponentide regulaarsete auditite kõrval tuleb regulaarselt üle vaadata ka WLAN-i turvapoliitika. Eriti tuleks hinnata seda, kas WLAN-i kaitseks kasutusele võetud meetmed vastavad tehnika tasemele ja kas nende aluseks olev kaitsevajadus on veel kehtiv. Lisaks tuleb kontrollida, kas kõik kasutajad tunnevad ja rakendavad WLAN-i turvameetmeid.

Täiendavad kontrollküsimused:

- Kas turvaauditeid tehakse regulaarselt?
- Kas leitud kõrvalekaldumised pannakse kirja ja uuritakse?

M 4.299z Autentimine printerite, koopiamasinate ja multifunktsionaalsete seadmete kasutamisel

Turvameetme kasutuselevõtmise eest vastutavad: IT-juht, infoturbeosakond
Turvameetme rakendamise eest vastutab: Administraator

Büroo normaalses igapäevases töös on sageli lihtne konfidentsiaalsete dokumentide väljatrükke vahetult printeri juures üle vaadata, sest neid ei ole veel ära viidud. Seetõttu tuleb tarvitusele võtta meetmed, mis raskendavad juurdepääsu võõrastele dokumentidele. Üldiselt peaksid väljaprinditud või kopeeritud dokumentidele saama juurdepääsu ainult volitatud isikud. Volitatud isikute ring tuleks hoida võimalikult väiksena.

Autentimine printeri juures
Kui juurdepääsu võrguprinterile ei ole võimalik piirata, tuleks kaaluda selliste seadmete kasutamist, millel on kasutajate autentimist võimaldav funktsioon. Kui see funktsioon on aktiveeritud, prinditakse dokument välja alles pärast seda, kui kasutaja, kes andis vastava printimiskäsu, on end seadme juures identifitseerinud ja autentinud. Praktikas kasutatakse autentimiseks sageli kiipkaarte või PINe. PINid saab seejuures olenevalt seadme tüübist määrata kasutaja- või dokumendipõhised. Viimase variandi puhul fikseeritakse PIN alles printimiskäsu andmisel. Alles pärast seda, kui see PIN on seadmesse sisestatud, prinditakse välja dokument, mille puhul antud PIN kehtib. Printimiskäsud, mis küll anti, kuid mida ei realiseeritud, tuleb regulaarselt tühistada. Printerid tuleks konfigureerida nii, et vale PINi mitmekordsel sisestamisel tühistatakse printimiskäsk automaatselt. Turvalist kasutamist saab tagada ka siis, kui prinditav dokument edastatakse töökohaarvutist printerisse krüpteerituna ja salvestatakse krüpteeritult vahemällu. Alles pärast seda, kui otse printeris juures on toimunud edukas autentimine, dokument dekrüpteeritakse ja prinditakse välja.

Autentimine koopiamasina juures
On ka koopiamasinaid, millel on sarnane autentimisfunktsioon olemas, enamasti valikulise lisavõimalusena. Seadme kasutaja saab kopeerida alles pärast seda, kui kiipkaart on tuvastatud või PIN sisestatud. Kuigi need autentimisfunktsioonid on mõeldud peamiselt kulude aruannete jaoks, raskendavad need lisavõimalused koopiate tegemist tundmatute isikute poolt. Kui võrguprinteritega prinditakse või koopiamasinatega paljundatakse sageli kõrge konfidentsiaalsusastmega dokumente, tuleks mõelda autentimisvõimalusega seadmete kasutamisele.

Täiendavad kontrollküsimused:

- Kuidas takistatakse seda, et volitamata isikud pääsevad väljatrükkidele juurde?
- Kas on olemas kontrollmehhanismid, mille abil takistatakse dokumentide volitamata kopeerimist?

M 4.300z Printerite, koopiamasinate ja multifunktsionaalsete seadmete infoturve

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: administraator, kasutaja

Väljaprintimiseks tuleb vajalik info edastada töökoha arvutist printerisse. Kopeerimisel toimub edastamine tavaliselt seadmesiseselt skänneri ja salvesti vahel. Ründe läbiviija võib üritada salvestile ligi pääseda või infot printerisse edastamisel pealt kuulata. Suuremate seadmete puhul kasutatakse prinditava info ajutiseks salvestamiseks vahemäluna sageli kõvakettaid. Sõltuvalt seadistustest ei salvestata vahemällu infot mitte ainult ajutiselt, vaid ka püsivalt. Tuleks tagada, et pärast printimist kustutataks info vahemälust. Selleks on paljudel koopiamasinatel oma kustutusfunktsioon. Kõikidele kasutajatele tuleb meelde tuletada, et nad kasutaksid seda funktsiooni pidevalt (vt M 2.398 Printerite, koopiamasinate ja multifunktsionaalsete seadmete kasutusjuhised). Juhul kui kõrgema konfidentsiaalsusastmega infot prinditakse või kopeeritakse sagedasti, tuleb arvestada sellega, et lihtne kustutamine jätab võimaluse kustutatud andmete taastamiseks. Teatud seadmetel on olemas mehhanismid „turvalise kustutamise“ tagamiseks. Seejuures on tegu kustutamisega koos täiendava ülekirjutamisfunktsiooniga. Kui seadmel on selline funktsioon olemas, tuleb see sisse lülitada. Vastasel korral tuleb leida sobiv alternatiivlahendus.

Võimalusel tuleb rakendada meetmeid, mis raskendavad ründe läbiviijal juurdepääsu salvestile või muudavad kõvaketaste eemaldamise keerulisemaks. Selleks, et oleks võimalik ära tunda, kas keegi on püüdnud sisemist salvestit eemaldada või seda manipuleerida, tuleks seadmed plommida. Üldjuhul tuleks printerid ja koopiamasinad paigaldada selliselt, et kellelgi ei oleks võimalik neid märkamatult manipuleerida. Täiendava kaitse jaoks on soovitav salvestada info sisemisele salvestile krüpteeritult. Paljudel printeritel ja koopiamasinatel on vastav funktsioon olemas. Kui kasutatav seade toetab krüpteeritult salvestamist, tuleks vastav funktsioon sisse lülitada.

Kommunikatsioon töökoha arvutite, prindiserverite ja võrguprinterite vahel toimub enamasti andmevõrgu kaudu, mille puhul tuleb arvestada samade ohtudega nagu ka teiste andmeühenduste puhul. Kommunikatsiooni pealtkuulamise takistamiseks tuleks printimisülesandeid edastada võimalusel krüpteeritult. Teatud osa printimisprotokolle, näiteks *Unixi* süsteemides levinud LPR/LPD protokoll *(Line Printer Remote / Line Printer Daemon)*, ei toeta krüpteerimist. Sarnane olukord on *Windowsi* all *SMB/CIFS (Server Message Block / Common Internet File System)* puhul. Seetõttu tuleks valida mõni krüpteerimist toetav protokoll nagu IPP *(Internet Printing Protocol)*, näiteks TLS/SSL *(Transport Layer Security / Secure Sockets Layer)* koos IPP-ga.

Unixi süsteemide all tuleks rakendada näiteks *Common Unix Printing Sys-tem (CUPS)* meetodit, mis kasutab uuemate versioonide puhul kliendi ja prindiserveri vahelise kommunikatsiooni ettevalmistamiseks IPP protokolli. Vastava konfiguratsiooni abil saab aktiveerida TLS/SSL-i.

Täiendavad kontrollküsimused:

- Kas võrguprinterid/koopiamasinad toetavad informatsiooni salvestamist krüpteeritud kujul?
- Millist printimisprotokolli rakendatakse ja kuidas kaitstakse printimisülesandeid nende edastamisel?
- Kas on kasutusele võetud printerite ja koopiamasinate sisemiste salvestikomponentide eemaldamist raskendavad meetmed?

M 4.301 Juurdepääsu piiramine printeritele, koopiamasinatele ja multifunktsionaalsetele seadmetele

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator

Printeritele, koopiamasinatele ja multifunktsionaalsetele seadmetele tehtavate rünnete raskendamiseks tuleb juurdepääsu nendele seadmetele piirata.

Järgnevalt kirjeldatakse mõningaid aspekte, millega tuleks arvestada printerite ja koopiamasinate turvalise kasutamise tagamisel:

- Piirdumine võimalikult väheste pääsuõigustega. Kui võimalik, tuleks ainult vähestele administraatoritele anda täielikud pääsuõigused. Seejuures tuleks töötajatele jagada alati ainult sellised pääsuõigused, mis on tööülesande täitmiseks hädavajalikud (vt M 2.8 IT-rakendustele ja andmetele pääsuõiguste andmine).
- Administreerimise pääsuõiguste piiramine. Administreerimistegevuse ja selle konfigureerimise pääsuõigused tuleks anda ainult volitatud isikutele. Juurdepääs peaks olema võimalik alles pärast autentimist, näiteks pärast parooli või PIN-koodi sisestamist. Kui printeri, koopiamasina või multifunktsionaalse seadme administreerimine toimub võrgu kaudu, tuleb tagada, et ka sellisel juhul toimuks administraatorite autentimine. Kui süsteem ei toeta autentimist, tuleb rakendada sobivaid asendusmeetmeid.
- Administreerimise kaitsmine kaugpääsu korral. Kõik administreerimise juurdepääsud peaksid võimalusel toimuma ainult krüpteeritud kanali kaudu, et vältida paroolide või muu kaitset vajava informatsiooni pealtkuulamist. Näiteks saab osade seadmetüüpide puhul konfiguratsiooniandmete edastamist krüpteerida HTTPSi või SMNPv3 abil. Niisugusel juhul tuleks krüpteerimata kommunikatsiooni takistada, näiteks HTTP-liidese konfigureerimise väljalülitamise abil.
- Ebavajalikest funktsioonidest loobumine. Ka printerid, koopiamasinad ja multifunktsionaalsed seadmed pakuvad üldjuhul rohkem funktsioone, kui neid tavakasutuses tarvis läheb. Vastavad funktsioonid võivad tekitada asjatuid riske. Seega tuleks kõik ebavajalikud funktsioonid kas välja lülitada või piirata nende kasutamist nii palju kui võimalik.
- Paketifilter. Printerite valikus leidub ka integreeritud paketifiltritega seadmeid, mille paketifiltrite kaudu saab filtreerida ühendusi nende IPaadresside või portide numbrite alusel. Blokeerige võimalusel kõik pordid, mida ei lähe tarvis printeri kasutamiseks või konfigureerimiseks. Kui seade toetab krüpteerimist, tuleks krüpteerimata kommunikatsiooni vastava seadmega maksimaalsel võimalikul moel takistada, näiteks vastava pordinumbri abil. Printiserverite kasutamisel tuleb arvestada sellega, et printeriga tohib ühendust luua ainult nende serverite kaudu. See raskendab volitamata IT-süsteemide jaoks juurdepääsu loomist printeritega. Erandiks on süsteemid, mille kaudu toimub printerite konfigureerimine. Vastavad süsteemid peavad loomulikult printerile ligi pääsema. Paketifiltrid tuleb üldjuhul konfigureerida selliselt, et need kehtestaks võimalikult suured piirangud. See kehtib ka ühenduse loomise kohta võrguprinteritest teistesse IT-süsteemidesse.

Näiteks tuleks paketifiltrid konfigureerida selliselt, et võrguprinter ei saaks luua ühendust väljaspool LANi asuva IT-süsteemiga. Niimoodi raskendatakse soovimatut andmevahetust väliste IT-süsteemidega, näiteks Internetti ühendatud arvutitega.

Olenemata kohalikest paketifiltritest tuleb keskses tulemüüris blokeerida kommunikatsioon printerite ja väliste võrkude vahel.

- Võrgu segmenteerimine. Sageli on soovitatav kõik printerid, koopiamasinad ja multifunktsionaalsed seadmed ühte loogilisse võrku kokku koondada. Sageli kergendab see konfigureerimist ja administreerimist. Selle põhimõtte järjekindlal rakendamisel saab vastutavate marsruutrite ja rakenduslüüside abil täpselt kontrollida printerite ja teiste võrgusegmentide vahelist kommunikatsiooni (niihästi IP-pakettide vastuvõtt kui ka saatmine).

Kontrollküsimused:

- Kuidas kaitstakse juurdepääsu konfiguratsioonile?
- Kuidas kaitstakse printerite, koopiamasinate ja multifunktsionaalsete seadmete kaugkonfiguratsiooni?
- Kas on rakendatud meetmeid, mis ei lase printeritel Internetiga ühendusi luua?

M 4.302 Printerite, koopiamasinate ja multifunktsionaalsete seadmete logimine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: administraator

Printerite, koopiamasinate ja multifunktsionaalsete seadmetega seotud tegevusi tuleks mitmel põhjusel jälgida ja logida. Ühest küljest aitab sisselülitatud logifunktsioon varakult tuvastada ja kõrvaldada potentsiaalseid kitsaskohti. Teisest küljest aitab logimine avastada turvapoliitika rikkumisi (vt M 2.398 Printerite, koopiamasinate ja multifunktsionaalsete seadmete kasutusjuhised) või asetleidnud turvaintsidente tagantjärele uurida. Lisaks saab jälgimist tihti kasutada ka selleks, et märgata varakult kulumaterjalide lisamise vajadust. Printerite, koopiamasinate ja multifunktsionaalsete seadmete logimisfunktsiooni kasutamseks tuleks leida vastused vähemalt järgnevatele olulistele küsimustele:

- Millist informatsiooni tuleks logida?
- Kuidas tuleks logida?
- Kes on volitatud/vastutav logide analüüsimise eest?
- Kuidas ja millal toimub logide analüüsimine?
- Keda tuleks teatud sündmuste esinemise korral teavitada?
- Kui kaua tuleb ja tohib logiandmeid säilitada ja kuidas toimub nende kustutamine?

Logimisse kaasatud informatsioon peaks olema hoolikalt välja valitud. Liiga suure infokoguse salvestamise korral võib juhtuda, et analüüsimisel jäävad olulised sündmused märkamata. Liiga väheste logiandmete korral võib juhtuda, et oluline informatsioon jääb salvestamata. Turvalisuse vaatepunktist on logimise jaoks eriti olulised järgnevad sündmused, mille loetelu on sorteeritud langevas järjekorras vastavalt nende prioriteedile:

- Alati tuleb logida konfiguratsiooni seadetes asetleidnud muudatused.
- Logida tuleks ebaõnnestunud autentimiskatsed ning kõrgema konfidentsiaalsusastme korral ka õnnestunud autentimiskatsed. See kehtib niihästi kohapeal toimunud sisselogimiste kui ka võrgu kaudu loodud ühenduste kohta.
- Alati tuleb kontrollida süsteemi ressursse ja tööohutuse väärtusi, et neis ei esineks kriitilisi väärtusi. Selle alla kuuluvad näiteks temperatuuri, koormuse ja salvesti vaba ruumi kohta käiv info.
- Varustusprobleemide vältimiseks tuleks logida paberi ja tooneri kuluinfot ja seda analüüsida.
- Täiendavalt võib salvestada informatsiooni ka selle kohta, kes millisel kellaajal printis või seadet kasutas.

Sõltuvalt seadmest ja kasutamisolukorrast võib logimismahu määramisel olla otstarbekas teatud sündmused välja jätta või hoopis täiendavalt jälgida veel lisasündmusi, nagu nt seadme sisse- ja väljalülitamist. Praktikas sõltub logimise ulatus ka sellest, millisel määral vastav seadmetüüp erinevate sündmuste logimist tehniliselt toetab. Kui logitava informatsiooni ulatus on kindlaks määratud, tuleb välja selgitada, kuhu logiandmed salvestatakse. Võimalusel tuleks selleks kasutada keskseid logiservereid. Vastasel korral tuleb logiandmed salvestada üksikutesse seadmetesse. Võrguühendusega IT-süsteemide logimisel tuleks rakendada aja sünkroniseerimist. Niimoodi on võimalik võrrelda asetleidnud sündmusi usaldusväärselt teiste süsteemide logiinfoga (vt M 4.227 Lokaalse NTP -serveri kasutamine aja sünkroniseerimiseks). Logiandmeid ei tule mitte ainult salvestada, vaid ka süstemaatiliselt analüüsida. Ka selle jaoks tuleb määrata vastutusalad ja kohustuslikud toimingud. Vastavad soovitused leiate muuhulgas meetmest M 2.64 Logifailide kontroll .

Kui logidest leitakse ootamatuid või silmatorkavaid sündmusi, tuleb vastavalt reageerida. Korduvad ebaõnnestunud autentimiskatsed võivad viidata võimalikule ründele või ebapiisavalt informeeritud kasutajale. Kuid ka tavasündmused võivad nõuda reageerimist. Näiteks kulumaterjalide minimaalse täituvuse saavutamisel tuleb õigeaegselt lisada/vahetada materjale. Sellest tuleks õigeaegselt teatada vastutavale administraatorile või muule kulumaterjalide eest vastutavale isikule. Isikuandmete arhiveerimisel tuleb kinni pidada vastavatest seadustest ja eeskirjadest. Lisainfot leiate meetmest M 2.110 Andmeprivaatsuse suunised logimisprotseduurides .

Täiendavad kontrollküsimused:

- Kuidas rakendatakse logifunktsiooni printerite, koopiamasinate ja multifunktsionaalsete seadmete puhul?
- Kuidas toimub logide analüüsimine?
- Kas logide analüüsimisel arvestatakse andmekaitse ettekirjutustega?
- Kuidas tagatakse kõikide seadmete õige süsteemiaeg?

M 4.303 Võrgutoega dokumendiskännerite kasutamine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator

Dokumendiskänneri abil saab analoogset infot digitaliseerida, näiteks paberdokumenti IT-süsteemi kopeerida, arhiveerida või edasi töödelda. Eriti neil juhtudel, kus vastavat seadet kasutatakse harva, on iga töökohaarvuti juurde skänneri paigaldamise asemel majanduslikult palju tasuvam ühe või mitme keskse seadme paigaldamine. Sobivate turvameetmete valimisel tuleb vahet teha skaneerimisarvutite ja võrgutoega dokumendiskännerite vahel. Skaneerimisarvuti on tavaline PC, mis on üldjuhul ühendatud LANiga ja mille külge on ühendatud lokaalne skänner. Skaneerimisarvuteid kasutatakse sageli võrguprinteritega sarnastes ruumides ja vajadusel saavad neid kasutada erinevad kasutajad. Lisaks on skaneerimisarvutisse tavaliselt paigaldatud sisseskaneeritud info järeltöötlemiseks vajalik tarkvara, näiteks OCR- või pilditöötlusprogramm. Võrgutoega dokumendiskännerid („bürooskännerid“) on kompaktsed seadmed, mis võimaldavad paberdokumente ja muud sarnast lihtsal moel sisse skaneerida ja kasutajatele edasiseks töötlemiseks LANi kaudu edasi saata, näiteks meili teel. Vastav funktsioon on sageli integreeritud ka faksiseadmetesse. Üldjuhul on võrgutoega dokumendiskännerite funktsionaalsus skaneerimisarvutite omast väiksem. Tavaliselt saab skaneerida ainult lihtsaid standardformaadiga paberdokumente, mille järeltöötlemine vahetult seadme enda abil on enamasti võimatu.

Skaneerimisarvuti

Kui skaneerimiseks kasutatakse tavalist PCd, tuleb rakendada IT etalonturbe kataloogi 3. mooduli osi, mis käsitlevad lähemalt kliente. Skaneerimisarvuteid saab rakendada kasutusvõrgus, testvõrgus või ka üksikrežiimil töötavas süsteemis, mille puudub võrguühendus. Need peaksid olema seadistatud selliselt, et kasutajal oleks kohustus ennast autentida. Sisseskanneeritud andmed saab töökoha arvutisse toimetada võrgu kaudu või kaasaskantava andmekandja abil. Skaneerimise analoogmaterjale (pabereid, kilesid jne) ei tohi seadme juurde järelvalveta laokile jätta. Ka digitaalsed skaneerimistulemused tuleb üldkasutatavatest kataloogidest pärast nende edastamist soovitud sihtsüsteemi (näiteks vastava kasutaja töökohaarvutisse) kustutada.

Võrgutoega dokumendiskännerid

Nende kompaktsete seadmetega saab dokumente skanneerida ka siis, kui üksgi arvuti ei ole seadmega ühendatud. Seejuures muudetakse dokumendid levinud failiformaatides pildifailideks. Edasise töötlemise jaoks peavad seadmed saatma sisseskanneeritud dokumendid edasi teistele võrgus olevatele IT-süsteemidele.

Üldjuhul toetavad seadmed järgnevaid edastamis- ja salvestamisfunktsioone:

- Võrguketastele salvestamine - Sisseskaneeritud dokumendid edastatakse vahetult võrguprotokolli kaudu failiserverisse. Tavaliselt toetatakse NFS- ja SMB-litsentse või edastamist FTP kaudu. Üldjuhul tuleb tagada, et juurdepääsuõigustega inimeste arv, kellel on õigus sisseskaneeritud andmete sihtkausta kasutada, oleks võimalikult väike. Kõrgema kaitsevajaduse korral võib olla vajalik, et sisseskaneeritud infole pääseks ligi ainult info sisseskaneerinud kasutaja. Mitte kõik skännerid ei võimalda andmete salvestamist

kasutaja poolt serveril määratud alasse. Kui salvestada saab ainult ühiskasutuses olevasse kausta, tuleb dokumendid võimalikult kiirelt sellistest avalikest kaustadest kustutada. Kasutajaid tuleb vastavalt juhendada. Lisaks tuleks vastavaid katalooge kord päevas automaatselt kustutada. Kasutajad peavad olema kustutamise hetkest teadlikud ning kustutamise aeg tuleb valida selline, kus ükski kasutaja ei töötaks skänneritega.

- Scan-to-Mail -selle funktsiooni puhul saab kasutaja skaneerimisel sisestada meiliaadressi või kasutajatunnuse, millele vastab kindel meiliaadress. Loodud fail saadetakse eelseadistatud SMTP-serveri kaudu vastavale meiliaadressile. Kuna sel moel võib konfidentsiaalne info võrgust anonüümselt lahkuda, tuleb jälgida, et väliste meiliaadresside sisestamine oleks tõkestatud. Targem oleks ka SMTP-server konfigureerida selliselt, et võrgutoega dokumendiskännerid ei saaks saata meile välistele meiliaadressidele.
- Scan-to-Print -antud juhul saadetakse dokument otse printerisse, seega kasutatakse skänneri-printeri kombinatsiooni digitaalse koopiamasinana. Kui seadmed ei asu koos, on oht, et skaneerimise ajal saab volitamata isik dokumendid printerist eemaldada. Seetõttu tuleks süsteemid võimalusel seadistada selliselt, et printimine algaks alles siis, kui kõik vastava dokumendi leheküljed on skaneeritud. Vastasel korral möödub esimese lehekülje skaneerimise ja kogu materjali printerist äratoomise vahel liiga palju aega.
- Scan-to-Fax -Scan-to-Fax meetod võimaldab skaneeritud dokumente saata otse faksiga. Selleks sisestatakse skanneerimisel faksi number. Loodud dokument saadetakse sel juhul teele kas integreeritud modemi kaudu või siis loob skänner LANi kaudu ühenduse faksiserveriga. Kasutades skännereid, millel on integreeritud faksi-, modemi- või andmete kaugedastuse liidesed, tuleb rakendada erilisi turvameetmeid, et nende liideste kaudu ei saaks luua soovimatut kommunikatsiooniühendust väliste võrkudega. Vastavaid soovitusi on kirjeldatud meetmes M 5.146 Multifunktsionaalsete seadmete lahutamine võrgust . Võimalusel tuleks kasutada keskset faksiserverit liidesena skänneri ja telefonivõrgu vahel. Vastaval juhul tuleb rakendada eriti just neid soovitusi, mida on kirjeldatud moodulis B 5.6 Faksiserver . Kui kasutatavad komponendid seda toetavad, tuleks sideühendused võimalusel krüpteerida, et edastatava info pealtkuulamine oleks raskendatud. Infot ülekande kaitsmise kohta leiate ka meetmest M 4.300z Printerite, koopiamasinate ja multifunktsionaalsete seadmete infoturve . Skännereid tuleks kaitsta ka võrgust tulevate rünnete eest. Niisugustel juhtudel tuleks arvestada meetmega M 4.301 Juurdepääsu piiramine printeritele, koopiamasinatele ja multifunktsionaalsetele seadmetele .

Pärast skanneerimist ei tohi süsteemi jääda jääkinfot. Seadme dokumendimälu kustutamine peaks toimuma pärast skaneerimise lõppu võimalikult automaatselt. Kui see pole teostatav, tuleb kasutajate tähelepanu juhtida sellele, et pärast seadme kasutamist tuleb dokumendimälu kustutada käsitsi, et järgneval kasutajal ei oleks võimalik näha eelnevalt sisse skaneeritud infot. Vastavaid turvameetmeid tuleb rakendada ka muude skaneerimise käigus kasutatavate salvestuskohtade, näiteks võrguketaste puhul.

Kontrollküsimused:

- Kas skaneeritud info edastamine töökoha arvutisse toimub turvaliselt?

- Kas skänneri kõik salvestuskohad kustutatakse pärast seadme kasutamist?

M 4.304z Printerite haldamine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: administraator
Ametiasutused ja ettevõtted vajavad tihti suurel hulgal printereid ja nendele sarnaseid seadmeid erinevate kasutusotstarvete jaoks. Selleks tuleb valida sobivad printimissüsteemid ja määrata riistvaraliste komponentide (printerite, koopiamasinate) paigutus. Järgnevalt tutvustatakse tüüpilisi printimissüsteeme, nende komponente ja vastavate süsteemide kommunikatsioonisuhteid. Printimissüsteemid koosnevad tavaliselt kliendi- ja serveripoolsetest tarkvarakomponentidest.

Printimissüsteemid

Rakendus saadab ainult väga harva printimisülesande otse printerisse, tavaliselt kasutatakse rakenduse ja printeri vahel printimissüsteemi. Sealjuures peab neil printimissüsteemidel olema võrgu tugi ning peab olema tagatud, et mitmel kliendil oleks juurdepääs ühele printerile. Ka eranditult lokaalse paigutusega süsteemi puhul läheb tarvis printimissüsteemi tarvis. Sel juhul saadab klient printimisülesande prindiserverisse süsteemisiseselt. Printimissüsteem saab muuhulgas täita järgnevaid ülesandeid:

- printimisülesande vastuvõtmine rakenduselt,
- printimisülesannete haldamine ootenimekirja abil (Spooling),
- lisainfoga täiendamine, nt eraldusleheküljed,
- ülesande kohandamine paberi formaadiga või muude näitajatega vastavaks,
- ülesande muutmine printeri jaoks arusaadavasse formaati, näiteks PostScript või PCL,
- loogiliste ja füüsiliste printerite haldamine,
- kasutajate haldamine ja
- logimine.

Printimissüsteemide teostamiseks on erinevaid võimalusi ning ühe või teise eelistamine sõltub operatsioonisüsteemist. Printimissüsteemide omavaheline ühilduvus on oluliseks eeliseks eriti just heterogeensete IT-varade puhul. Mitmed süsteemid pakuvad liideseid teiste printimissüsteemide ühenduste jaoks. Seeläbi pääseb näiteks Unix -süsteem ligi printerile, mida haldab Windows-süsteem. Sõltuvalt operatsioonisüsteemist on enim levinud järgnevad printimissüsteemid:

- Berkeley Printing System,
- Common Unix Printing System (CUPS) ja
- printeri kasutamine SMB protokolli abil Windowsi all.

Heterogeensete võrgulahenduste puhul tuleks valida printimissüsteem, mida toetavad kõik operatsioonisüsteemid. Alternatiivina võib olla otstarbekas rakendada mitut erinevat printimissüsteemi, mis suudavad vajadusel omavahel suhelda. Printimissüsteemi kasuks otsuse langetamist tuleb põhjendada ja dokumenteerida.

Komponendid

Rakenduse poolt loodud ja printerisse saadetav printimisülesanne peab läbima oma teekonnal mitu vahesammu. Nende sammude jaoks läheb tarvis üksikuid komponente, mida järgnevalt ka tutvustame:

- Printimisklient - Printimiskliendi puhul on tegu tarkvarakomponendiga, mis on paigaldatud töökoha arvutisse. Tavaliselt saab printimisklient vastava korralduse rakenduselt ja edastab printimisülesande prindiserverisse. Paljudel juhtudel saab kasutatava printeri välja valida printeri nime alusel. Erandiks on printimine printerikogude abil, mille puhul saab prindiserver iga printimisülesande jaoks määrata erineva printeri. Sageli saab printimisklient määrata lisafunktsioonide kasutamist, näiteks kahepoolset printimist ja klammerdamist. Selleks saadab printimisklient printimisandmed prindiserverisse. Vastava informatsiooni, kuidas printerit juhtida ja milliseid formaate printer toetab, saab printimissüsteem reeglina printeri installeerimise käigus.
- Prindiserver - Prindiserver võtab kliendi printimisülesanded vastu ja tegeleb nende haldamisega. Ülesanded lisatakse ootenimekirja ja edastatakse seejärel printerile. Sõltuvalt seadistusest edastatakse mitme trükiülesande puhul korraga esimesena vastuvõetud dokument printerile esimesena või siis lähtutakse vastavatest tähtsuse järjekordadest. Mõningatel juhtudel saab trükiülesannete täitmiseks määrata ka täpsed ajavahemikud. Dokument valmistatakse printimiseks ette tavaliselt otse prindiserveris. Ettevalmistamiseks vajab printimissüsteem seadmepõhist printeriinfot ja filtreid. Näiteks võib see printeriinfo olla määratletud PPD (PostScript Printer Description) kujul. Üldistatult on tegu spetsifikatsiooniga, mis määrab, milliseid formaate ja funktsioone printer oskab kasutada. Konkreetsete parameetrite näideteks on paberi formaadid, lahutusvõime, kirjastiilid, kahepoolne printimine, klammerdamine, augustamine ja värviline printimine. Selle spetsifikatsiooni alusel saab luua printimiskorralduse, mis edastatakse printerile. Printimisülesande ettevalmistamise alla kuulub ka failiformaadi konverteerimine vastava printeri poolt mõistetavasse formaati. Kui sisendformaadiks on näiteks PostScript ja printer PostScripti ei toeta, tuleb dokument konverteerida printeri jaoks arusaadavasse väljundformaati. Väljundformaat võib olla näiteks PDF, PCL ja PostScript.
- Printer - Printer võtab ettevalmistatud dokumendi prindiserverilt vastu ja trükib selle välja. Eristada on võimalik loogilisi ja füüsilisi printereid. Füüsiliste printerite puhul kasutatakse järgnevaid ühendusviise. Lokaalsed printerid: lokaalsetel printeritel on jada-, paralleel- või USB-liides ja need ühendatakse otse klientsüsteemiga. Võrguprinterid: ühendus printeriga luuakse võrgu kaudu. Lokaalsete printeritega prindiserver: printer ühendatakse lokaalselt prindiserveriga, mille on võrguühendus. Seejuures saab prindiserveri realiseerida eraldiseisva seadmena või klassikalise serverina. Niisugusel juhul võtab prindiserver sageli enda kanda konverteerimisülesande võrgu ja kohaliku ühenduse vahel, näiteks USB- Ethernet sillana.

Loogilistel printeritel võivad printimissüsteemis olla erinevad ülesanded. Praktikas võib sageli eest leida järgmisi lahendusi:

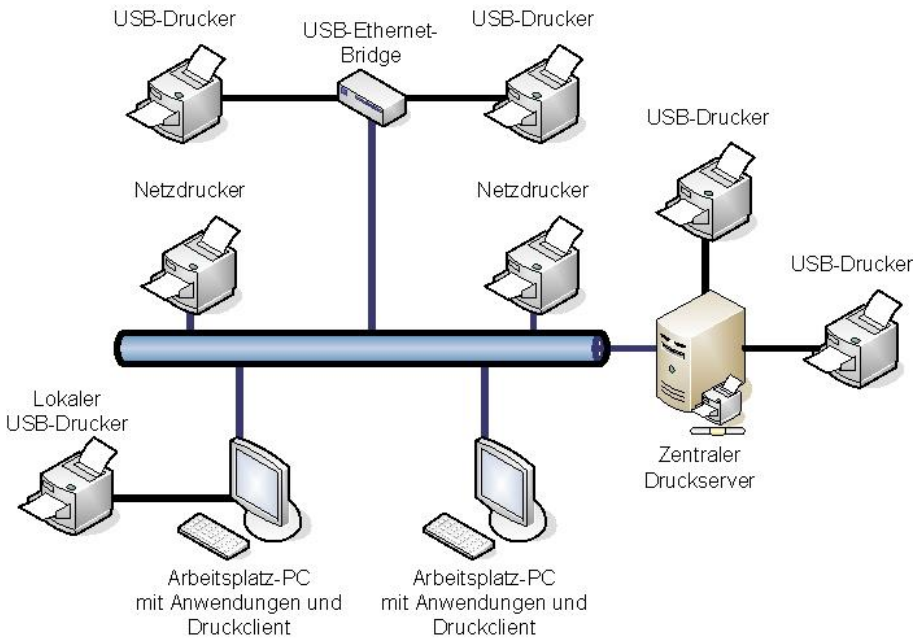
- Mitut füüsilist printerit rakendatakse ühe loogilise printerina. Lisaks tõhusamale printimisele (võimaldab printida samaaegselt), saab ühe printeri väljalangemise korral ilma erilise konfigureerimisvajaduseta kasutada mõnda

teist printerit. Soovitav on ühte gruppi koondada ainult sarnaste omadustega printerid.

- Üht füüsilist printerit kasutavad mitu loogilist printerit, mis on installeeritud erinevate prindiserverite alla. Niisugune olukord on võimalik, kui korraga kasutatakse mitut prindiserverit. Ühe prindiserveri väljalangemisel saab printimist jätkata suurema konfigureerimisvajaduseta, minnes üle mõne teise prindiserveri kasutamisele.
- Lisaks saab loogilisi printereid kasutada ühele füüsilisele printerile erinevate seadistuste lõikes erinevate printeri nimede määramiseks. Näiteks saab ühe füüsilise printeri jaoks defineerida kaks loogilist printerit: üks ühepoolse ja teine kahepoolse printimise jaoks. Kõik loogilised printerid tuleb dokumenteerida.

Kommunikatsioonisuhted

Nagu alljärgnevalt jooniselt on näha, tekivad printimissüsteemi eri komponentide vahel erinevad sideühendused.



Joonis: printeri arhitektuur printimisklientide, prindiserverite, lokaalsete ja võrgupõhiste printeritega

Joonis: USB Drucker – USB-printer, USB- Ethernet -Bridge – USB-Ethertnetsild, Netzdrucker – võrguprinter, Zentraler Druckserver – tsentraalne prindiserver, Arbeitsplatz-PC mit Anwendungen und Druckclient – töökoha PC koos rakenduste ja printimiskliendiga

Kommunikatsioon printimiskliendi ja prindiserveri vahel

Vastava sideühenduse saab luua printimiskliendi ja prindiserveri ning ka erinevate prindiserverite vahel. Sõltuvalt kasutusalast vahetatakse printimisinfot võrgu kaudu või lokaalselt (printimisklient ja prindiserver töötavad ühe seadme all).

Sõltuvalt printimissüsteemist saab rakendada järgnevaid protokolle:

- HTTP (Hypertext Transfer Protocol),
- IPP (Internet Printing Protocol),
- LPR/LPD (Line Printer Remote / Line Printer Daemon),
- SMB (Server Message Block) ja
- Appletalk või Bonjour.

Sobivate protokollide väljavalimisel tuleb lähtuda kasutatavatest printeritest ja valitud printimissüsteemist. Võrgu piires tuleks vältida paljude erinevate printimisprotokollide kasutamist. Vastav otsus tuleb dokumenteerida. Ka haldamise jaoks tuleb osade printimissüsteemide vahel infot vahetada. Näiteks tuleb kliente regulaarselt informeerida saadaolevate printerite ja nende seisundi kohta. Sõltuvalt printimissüsteemist saab kasutada järgnevaid strateegiaid:

- Broadcasting: server saadab regulaarsete ajavahemike tagant iseseisvalt teateid kõikidele Broadcast -domeeni klientidele.
- Polling: printimisklient esitab serverile infopäringu. Broadcasting lihtsustab administreerimist, kuid on seotud muude probleemidega. Kui kliendid ja server asuvad erinevates Broadcast -domeenides, ei jõua andmepaketid kõikide klientideni. Praktilise kasutamise käigus võib esinda probleeme ka siis, kui prindiserveril on mitu võrguliidest ja Broadcast -paketid edastatakse valedele liidestele. Konfiguratsiooni jaoks tuleb valida sobiv meetod ja dokumenteerida.
- Kommunikatsioon prindiserveri ja printeri vahel. Prindiserveri ja printeri vaheliseks kommunikatsiooniks läheb samuti sobivaid protokolle tarvis. Need sõltuvad printerite omadustest ja ühenduse liigist. Erinevad protokollid toetavad näiteks järgnevaid funktsioone:
- kommunikatsioon paralleelliidese kaudu,
- USB-ühendus,
- töö jadaliidese kaudu ja
- võrgupõhine kommunikatsioon printeritega, näiteks HP JetDirect protokolli või IPP (Internet Printing Protocol) abil.

Mõned printimissüsteemid võimaldavad printereid seadistada ka prindiserveri kaudu. Lisaks tootjapoolsetele protokollidele kasutatakse siinjuures sageli Simple Network Management protokolli (SNMP). Tuleb valida protokollid, mis vastavad asutuse nõuetele ja sobivad kokku kasutatavate komponentidega. Vastavad otsused tuleb dokumenteerida.

Printimislahenduse projekteerimine

Lisaks printimissüsteemi valikule on oluline ka üksikute komponentide (näiteks klientide, serveri ja printeri) paigutus. Suuresti üldistades saab printeriarhitektuuris eristada järgnevaid põhilahendusi:

- Lokaalsed printerid: niihästi printimisülesannet loonud rakendust kui ka prindiserverit ja printimisklienti kasutatakse koos ühe IT-süsteemi all. Printer on IT-süsteemiga ühendatud USB-, paralleel- või jadaliidesega.
- Võrguprinteriga töökohaarvuti: ühe või mitme IT-süsteemil all on lisaks printimisülesandeid saatvale rakendusele ka printimisklient ja prindiserver. Üksikute IT-süsteemide prindiserverid saadavad printimisülesanded edasi võrgutoega printerile.

- Keskne prindiserver: töökoha süsteemidele on installeeritud ainult printimiskliendid. Need võtavad printimisülesande vastu ja saadavad selle võrgu kaudu edasi kesksele prindiserverile. Sellel prindiserveril toimub printimisülesannete haldamine. Prindiserver saadab ülesanded edasi lokaalsetele või võrgupõhistele printeritele, kus need välja trükitakse.
- Kombinatsioonid: ülalmainitud paigutustest on võimalikud arvukad kombinatsioonid. Üheks näiteks on lokaalse printeri ühendamine töökoha arvutiga väiksemate printimisülesannete jaoks ja keskse prindiserveri paralleelne kasutamine suurte printimisülesannete jaoks.

Printimislahenduse kohta langetatud otsused tuleb dokumenteerida.

M 4.305 Salvestusvõimaluste piiramine (Quotas)

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: administraator, vastutav spetsialist

Isegi kui IT-süsteemi soetamisel lähtuti nõudest, et süsteemil peab olema piisavalt mälumahtu, tuleb paljudel juhtudel pikema kasutuse järel ilmsiks, et sellest siiski ei piisa. IT-süsteemide puhul, mida kasutavad erinevad töötajad, tuleks olemasolevad ressursid ära jagada selliselt, et kõik saaksid oma tööd teha võimalikult optimaalselt. Kasutajad soovivad tihti saada rohkem salvestusruumi kui nad parasjagu kasutavad. Lisaks erinevate rakenduste pidevalt kasvavale salvestusvajadusele on selle põhjuseks ka tõsiasi, et paljud kasutajad suudavad vaid väga raskelt oma vanadest ja mittevajalikest failidest loobuda. Juhul kui ei kehtestata salvestusmahu piiranguid ja arhiveerimispõhimõtteid, tekib oht, et olemasolev salvestusruum raisatakse ära kas suure kogusele vananenud andmetele või hakatakse andmeid salvestama koguni kasutajate endi kaustadesse. Lihtsaks lahenduseks, kuidas kasvavaid vajadusi rahuldada, oleks võimaldada töötajatele alati rohkem salvestusruumi kui nad konkreetselt vajavad. Praktikas pole see aga alati sugugi teostatav.

Kasutajatele või kasutajagruppidele, aga ka rakendustele saab kehtestada salvestusmahu kasutamise piirangud (*Disk Quotas*), mida nad ei tohi ületada. Seetõttu tuleks serverites ja kõikides IT-süsteemides, millel on mitu kasutajat, või mille peal käitatakse paralleelselt mitut rakendust, piirata olemasolevat salvestusruumi kasutajate ja rakenduste jaoks vastavate salvestuskvootidega. Siia alla kuuluvad nt serverid (faili-, veebi- ja meiliserverid) ja mitme kasutajakontoga varustatud kliendid. Klientide puhul, mille andmete partitsioon on süsteemi partitsioonist eraldatud ning andmeid kasutab vaid üks kasutaja, tuleks *Disk Quoata*'de kasutamisest loobuda. Siinkohal on oluline määratava kvoodi suurus. Juhul kui kõikidele kasutajatele soovitakse anda ühesugune salvestusmahu kvoot, saab vajaliku mahu välja arvutada, jagades olemasoleva salvestusmahu kasutajate arvuga. Sellele lisaks tuleks aga salvestusruumist teatud osa siiski ka reservi jätta. Problemaatiliseks võib olukord kujuneda siis, kui *Disk Quota* maht valitakse liiga väike. Juhtudel, kus kasutajatele on antud liiga vähe salvestusruumi, võivad nad hakata piirangutest möödahiilimiseks infot salvestama erinevatesse kaustadesse, mis pole selliseks tegevuseks üldse ette nähtud. Näidetena salvestamiseks ebasobivatest asukohtadest kasutatakse tihti nt ajutisi kaustu, või ka teisi, kõikide kasutajate jaoks kirjutusõigusega varustatud kaustu. Kui failiserveri salvestusmaht on liiga piiratud, kasutavad paljud inimesed lahendusena lokaalseid kõvakettaid. Paljudel juhtudel tähendab see aga ettekirjutuste rikkumist ning selle tagajärjel võib nt tekkida olukord, et vastavad andmed jäävad tsentraalselt toimivast andmevarundusest (*Backup* 'ist) lihtsalt välja. Ühelt poolt on tarvis konkreetselt määratleda, millistesse kohtadesse tohib erinevat infot salvestada, ning teiselt poolt, kui kaua tohib ühe faili erinevaid versioone igapäevaselt kasutatavas süsteemis säilitada.

Lõpetatud projekte kajastavaid andmehulki ei tuleks mitte „igaks juhuks“ igapäevaselt kasutatavas süsteemis alati käepärast hoida, vaid hoopis korrakohaselt arhiveerida. Vastasel juhul tuleks kehtestada, kui palju salvestusruumi erinevate kasutajagruppide ja rakenduste käsutusse antakse. Sellele lisaks tuleks aga

teatud osa siiski ka reservi jätta. Samuti peab olema selge, kuidas leiab aset suurema salvestusmahu eraldamine kasutajale juhul, kui tal tekib selleks spetsiaalne vajadus. Kindlaksmääratud väärtused tuleb dokumenteerida. Lisaks tuleb neid ka regulaarselt kontrollida ja värskendada. Pärast *Disk Quota* suuruse kindlaksmääramist tuleks mõelda, kuidas ja mil moel tuleks reageerida vajaduste tekkele, mis nõuavad salvestusmahu suurendamist. Vastavat otsust mõjutab kvoodi tüübi valimine. *Hard Quota* 'de puhul määratakse kindlaks ülempiirid, mis võtavad kasutajatelt võimaluse kasutada rohkem salvestiruumi kui neile on ette nähtud. *Soft Quota* võimaldab seevastu kasutajatel eelnevalt kehtestatud *Disk Quota* piiri kindlaksmääratud aja jooksul ja kindlaksmääratud mahus ületada. *Disk Quota* mahu ületamisel peab süsteem sellest teavitama vähemalt kasutajat ennast, nt meili teel. Siinkohal tuleks kaaluda ka administraatori teavitamist, et tal oleks võimalik potentsiaalsetele probleemidele õigeaegselt reageerida. Lisaks on tarvis kindlaks määrata, kas ja kuidas eraldatakse üksikutele kasutajatele täiendavat salvestusruumi. Vastav protseduur peab olema reguleeritud ja mõistetav. *Disk Quota* mahtusid ei tuleks suurendada lihtsalt „hõikamise“ peale.

Paljude enamlevinud operatsioonisüsteemidega on kaasas ka vastavad abivahendid, mille abil saab *Disk Quota* 'sid seadistada. Siiski tuleks kontrollida, kas *Disk Quota* sisseseadmiseks ja haldamiseks on võib-olla tarvis rakendada veel ka täiendavat tarkvara.

Täiendavad kontrollküsimused:

- Kas on olemas dokumentatsioon, mis näitab, kui palju salvestusruumi on kasutajatel ja rakendustel kasutada?
- Kas on reguleeritud, millistel asjaoludel eraldatakse kasutajatele täiendavat salvestusruumi?

M 4.306z Paroolisalvestusvahenditega ümberkäimine

Algatamise eest vastutavad: IT-juht, IT turvaosakond

Rakendamise eest vastutavad: kasutajad, IT turvaosakond

Enamik inimesi peab iga päev nii tööl kui ka eraelus meeles pidama paljusid PIN-koode, paroole ja muid autentimiseks vajalikke andmeid. Sellega tekib tihti probleeme. Tüüpilised näited on paroolide unustamine, mille tagajärjel tuleb need keeruliste ja aeganõudvate protsesside abil jälle ümber muuta, või paroolide üleskirjutamine ja nende ebaturvaline hoidmine. Selliste probleemide vältimiseks on saadaval terve rida tehnilisi abivahendeid, mille abil on võimalik hallata suurt hulka PIN-koode ja muud autentimiseks vajalikku salajast infot. Vastavad paroolisalvestusvahendid on saadaval nii puhtalt tarkvaralahendustena kui ka kombineeritult eraldiseisva riistvaraga.

Paroolisalvestusvahendite rakendamisel tuleb arvestada erinevate aspektidega (vt lisaks M 2.22z Paroolide deponeerimine):

- Igasugune paroolide deponeerimine või salvestamine on alati seotud organisatoorsete töödega. Paroolide muutumisel tuleb paroolid ära muuta ka paroolisalvestusvahendis. Sealjuures ei tohi kahe silma vahele jätta ühtegi parooli.
- Enne paroolisalvestusvahendi kasutuselevõttu tuleb hinnata paroolide kaitsevajadust. Kõrge kaitsevajadusega paroolide salvestamiseks ei sobi kõik paroolisalvestusvahendid. Teisalt jällegi aitavad need vahendid kasutajatel välja valida iga rakenduse jaoks erinevaid ja sellele vaatamata siiski ka piisavalt keerulisi paroole. Kasutades paroolide salvestamiseks tehnilisi abivahendeid, tuleks nende valikul lähtuda alljärgnevalt loetletud nõuetest:
- Volitamata isikute juurdepääs salvestatud paroolidele peab olema välistatud. Iga paroolisalvestusvahendi kasutamine peaks kajastuma ka logis.
- Paroolisalvestusvahend peab olema lihtsalt ja intuitiivselt kasutatav. Deponeeritavate paroolide pikkusele ja komponentidele ei tohiks olla mingisuguseid piiranguid. Toode peaks võimaldama kasutada pikki ja keerulisi peaparoole ning vastav nõue peaks kajastuma ka tootele esitatavates tehnilistes nõuetes.
- Paroolisalvestusvahend ei tohiks mingil tingimisel võimaldada kasutajatel ennast sisse logida peaparooli sisestamata, samuti ei tohiks lahenduses olla võimalust peaparooli automaatselt „meelde jätta".
- Salvestusvahend peaks suutma sisseloginud kasutaja pärast kindlaksmääratud aja möödumist, mil ühtki tegevust ei toimu, automaatselt välja logida.
- Paroolide salvestamine võib toimuda ainult krüpteeritult. Selleks tuleb kasutada tunnustatud krüpteerimisprotseduuri, millel on piisav võtmepikkus.
- Enne paroolisalvestusvahendi soetamist tuleks erialastest väljaannetest ja internetist järele uurida, kas vastava toote kohta on ilmunud artikleid, testikirjeldusi või koguni kirjeldusi edukaks osutunud rünnete kohta. Samuti tuleks vastavatest allikatest regulaarselt uurida, kas toote puhul ei ole vahepeal ilmsiks tulnud mõnda turvaauku.
- Kahjuks on avastatud ja leidub ka jätkuvalt paroolisalvestustooteid, mille puhul on tuvastatud jämedat turvanõuete rikkumist. Näiteks salvestavad sel-

lised tooted peaparoolid loetava teksti kujul kas seadme töömällu või selle vahemällu. Sel põhjusel tuleks võimaluse korral kasutada vaid selliseid paroolisalvestustooteid, mille turvalisust on eelnevalt kontrollitud (vt M 2.66z Sertifikaatidega arvestamine IT soetamisel).

- Kuna paroolisalvestusvahendi juurdepääs peab olema väga hästi kaitstud, võib olla mõistlik kasutada selleks tooteid, mis on varustatud spetsiaalse turvariistvaraga, nt paroolisalvestusvahendid, mille platvorm on kas USB-pääsmik või kiipkaart.
- Paroolisalvestusvahendi kasutamine võib olla mõistlik lahendus ka kaitseks klahvivajutusi salvestava klahvilogeri tüüpi nuhkvara vastu, milleks tuleks valida lahendus, kus parool sisestatakse ekraanile kuvatud klaviatuurilt hiire abil. Lahendus peaks pakkuma võimalust nii numbrite kui ka tähtede ja viitemärkide kasutamiseks, et valitavad paroolid oleksid võimalikult mitmekülgsed. Samas jällegi on vajalik, et kõik tähemärgid kuvataks ekraanile dünaamiliselt, st pärast igat sisestust peaksid tähemärgid olema paigutatud mõnda teise kohta. Kasutaja jaoks muudab see paroolide sisestamise küll aeglasemaks, kuid samas muudab see paroolide tuvastamise ekraani kindlate asukohtade kaudu kahjurvara jaoks jällegi keerulisemaks.
- Peaparoolide sisestamine peab olema kiire ja lihtne. Eriti hoolikalt tuleks peaparooli sisestamise protseduuri kontrollida seadmetel, millel on integreeritud sisestusklahvid või mis on varustatud ekraanile kuvatavate klaviatuuridega. Juhul kui sisestamisele kulub liiga palju aega, nt kui üksikute tähemärkide valimine on väga keeruline, on võimalik peaparooli väga kergesti välja nuhkida ning on oht, et see hakkab õõnestama kasutajatepoolset vastuvõtlikust selle kasutamise suhtes.
- Välise toiteallikaga, nt patareiga varustatud paroolisalvestuslahenduse kasutuselevõtul tuleks uurida, mis juhtub paroolidega siis, kui elektritoide peaks katkema. Võib juhtuda, et selliste lahenduste puhul on tarvis andmetest luua täiendavad varukoopiad, mida on samuti tarvis piisavalt kaitsta. Lisaks tuleks paroolisalvestusvahendite kasutamisel muu hulgas kinni pidada järgmistest raamtingimustest:
- Paroolisalvestusvahendite kasutamisele peab eelnema edukas sisselogimine. Ka siin kasutatakse üldjuhul paroole ja PIN-koode. Loomulikult tuleb hoolitseda, et need vastaksid kõrgeimatele kvaliteeditingimustele. Selleks kasutatavad peaparoolid peavad olema pikad ja keerulised (vt M 2.11 Paroolide kasutamise reeglid).
- Ebaõnnestunud sisselogimiskatsete järel peaks süsteem teavitama juurdepääsu keelamisest lühikeste veateadetega ilma detailidesse laskumata. Eriti oluline on see, et ebaõnnestunud sisselogimiskatsete järel ei tohi aru saada, kas vale oli sisestatud kasutajatunnus või sisestatud parool (või mõlemad). Pärast parooli kolmekordset valesti sisestamist ühe kasutajakonto kohta peaks autentimissüsteem vastava kasutajakonto juurdepääsu sulgema (kas teatud ajaks või ka püsivalt). Järgnevate ebaõnnestunud sisselogimiskatsete järel ei tohi süsteem paljastada infot kasutajakonto sulgemise kohta. Vastav info peab kasutajani jõudma eraldi kanali kaudu.
- Veel parem on, kui ebaõnnestunud sisselogimiskatsete järel ei kuva süsteem kasutajale mitte veateadet, vaid näitab ainult tavapärast kasutajaliidest. Kui järgnevalt kuvatakse ehtsatena näivaid, kuid väärtusetuid tulemusi, pole ründajal võimalik kohe tuvastada, kas nähtav parool oli õige või mitte.

- Paroolisalvestusvahendeid tuleks võimaluse korral kasutada ainult usaldusväärsetes IT-süsteemides, st süsteemides, mille järelevalve jääb enda pädevusse ehk süsteemides, mida oma institutsioonil on õigus kontrollida. Nendeks võivad olla nt mobiiltelefonid, pihuarvutid või spetsiaalsed autentimisserverid.
- Väliseid veebipõhiseid teenuseid tohiks paroolide salvestamiseks kasutada vaid juhul, kui teenusepakkuja usaldusväärsuse ja paroolide kaitsevajaduse omavaheline suhe jääb vastuvõetavatesse piiridesse. Mingil juhul ei tohiks siia salvestada kõiki krediitkaartide andmeid koos PIN-koodidega, kuna selliste teenuste usaldusväärsust ja turvalisust on väga raske kontrollida.
- Kasutada tohiks ainult selliseid paroolisalvestusvahendeid, mille turvalisust on institutsioon kontrollinud ja millele on antud kasutusluba. Institutsiooni sees tuleks kõiki töötajaid teavitada, kas paroolisalvestusvahendite kasutamine on lubatud või mitte. Kui see on lubatud, tuleks edastada ka info, milliseid konkreetseid vahendeid tohib kasutada. Lisaks peaksid olema välja töötatud reeglid, kus on kirjas, millist liiki paroole tohib nende abil salvestada ja milliseid raamtingimusi tuleb selle käigus järgida.

Kontrollküsimused:

- Kas paroolisalvestusvahendite rakendamise ja kasutuse kohta on olemas vastavad reeglid?
- Kas salvestatud paroolid on värsked?
- Kuidas kontrolliti paroolisalvestusvahendite turvalisust?

M 4.307 Kataloogiteenuste turvaline konfigureerimine

Algatamise eest vastutavad: IT-juht, IT-turbespetsialist

Rakendamise eest vastutavad: administraator

Pärast kataloogiteenuse täielikku installeerimist (vt M 4.308 Kataloogiteenuste turvaline installeerimine) peaks see jääma turvalisse seisundisse, et sellele järgnevas konfigureerimise etapis oleks võimalik kataloogiteenusele juurde pääseda ainult volitatud administraatoritel. Installeerimisele järgnevas konfigureerimisetapis on võimalik süsteemi sõltuvalt kasutusvaldkonnast täiendada paljude erinevate funktsioonidega, mis võivad väljuda tavapärase kataloogiteenuse piiridest. Konfigureerimistööde raames tuleb sobivate parameetrite abil tagada funktsioonide piisav turvalisus.

Kataloogiteenustega seotud tüüpilised konfigureerimisülesanded on:

- Kataloogipuu hierarhia konfigureerimine,
- Objekt-juurdepääsude konfigureerimine,
- Pärimisfiltrite konfigureerimine,
- Administreerimisrollide konfigureerimine,
- Administreerimisülesannete delegeerimise konfigureerimine,
- Kasutajate ja kasutajagruppide konfigureerimine,
- Võtme-objektide jagamine,
- Kataloogiteenuse klient-juurdepääsu konfigureerimine,
- Kataloogiandmebaasi partitsioonide loomise konfigureerimine,
- Kataloogiteenuse replikeerimise konfigureerimine,
- Võõraste kataloogiteenustega sünkroniseerimist võimaldava liidese konfigureerimine,
- Süsteemiseire konfigureerimine.

Kõik nimetatud ülesanded puudutavad kataloogiteenuse enda tarkvara. Siinkohal ei tohi unustada, et ka süsteemi aluseks olev operatsioonisüsteem peab olema konfigureeritud turvaliselt, eriti mis puudutab selle juurdepääsu serverile, võrguühendusi ja failisüsteemi. Kataloogiteenuste konfigureerimise käigus on võimalik süsteemi sõltuvalt kasutusvaldkonnast täiendada paljude erinevate moodulitega, mis võivad väljuda tavapärase kataloogiteenuse piiridest.

Siia alla kuuluvad:

- LDAP-serverimoodul, mis võimaldab LDAP-klientidele juurdepääsu kasutajainfole
- Tarkvaratööriist, mis võimaldab administratiivset juurdepääsu veebilehitseja vahendusel
- Kataloogiteenuse administreerimisplatvormina toimiv konsool (tööriist)
- Sertifitseerimisserver, mis installeeritakse kataloogiteenuse serveri esmapaigalduse käigus kataloogipuu alla
- Vajadusel veel ka täiendavad moodulid.

Sõltuvalt kasutusvaldkonnast ja kataloogiteenuse serveri pakutavatest funktsioonidest tuleb kontrollida, milliseid lisamooduleid oleks kataloogiteenuse käitamiseks tarvis. Mooduleid, mida kasutama ei hakata, ei tuleks ka installeerida, kuna iga installeeritud moodul võib väärkonfiguratsioonide korral endaga kaasa tuua turvalisusega seotud probleeme. Iga aktiveeritava mooduli kohta tuleb läbi viia asjakohane turvalisuse planeerimine. Seejärel tuleb planeerimisel saadud tulemused ka sobivate konfiguratsiooniparameetrite toel ellu viia (vt M 2.405 Kataloogiteenuse turvapoliitika koostamine). Kataloogiteenust pakkuva süsteemi turvalisus sõltub lisaks muule veel ka juurdepääsuks rakendatava klienttarkvara turvalisusest. Seetõttu tuleb kataloogiteenust pakkuva süsteemi turvalise konfiguratsiooni loomisesse kaasata ka klientide poolt kasutatavad arvutid ja programmid. Kataloogiteenuse administratiivsete juurdepääsude kaitsmiseks tuleb rakendada spetsiaalseid turvameetmed.

Kõikidel juhtudel tuleks kindlasti kinni pidada järgmistest üldistavatest juhistest:

- Installeeritud kliendi kaitsmiseks tuleb konkreetse, süsteemi aluseks oleva operatsioonisüsteemi turvalisuse tagamiseks rakendada IT etalonturbe kataloogide asjakohaseid mooduleid.
- Kui klienttarkvara puhul on ette nähtud, et see peab looma kataloogiteenusega LDAP-ühenduse, mis peab olema kaitstud SSLi abil, peab klient saama vastava juur-sertifikaadi, mille alusel saab ta kontrollida SSLserveri-sertifikaadi autentsust.
- Installeeritud kataloogiteenuse turvalisus sõltub lisaks muule veel ka administreerimiseks rakendatavate klientide terviklusest. Seetõttu on nende klientide turvaliseks muutmine väga oluline.

Eksisteerib ka võimalus luua oma tarkvara, mis suhtleb kataloogiteenusega mõne standardse LDAP-liidese (või muude, selleks loodud liideste) vahendusel.

Kataloogiteenust pakkuv süsteem ei koosne reeglina mitte ainult ühest kataloogiteenuse serverist, vaid paljudest omavahel ühendatud serveritest (vt M 2.403 Kataloogiteenuste kasutuselevõtu planeerimine). Kataloogiteenuse andmebaas võib olla üksikute partitsioonide näol laiali jaotatud erinevatele serveritele. Lisaks võivad üksikud serverid kataloogiteenuste andmebaase omavahel ka replikeerida. Seeläbi, et ühest andmebaasi partitsioonist hoitakse mitmeid koopiaid erinevatel serveritel, on võimalik tekkivat koormust paremini jagada. Kataloogiandmetest tehtud koopiate värskuse tagamiseks peavad serverid omavahel vahetama infot andmetes asetleidnud võimalike muutuste kohta. Selleks on tarvis luua eraldi replikeerimise kontseptsioon.

Muuhulgas tuleb siinkohal arvestada järgmiste asjaoludega:

- Kas kataloogiteenust pakkuvaid servereid käitatakse Master-Slave -režiimis või hoopis Multi-Master-Replication režiimis?
- Milliseid replikeerimistüüpe konfigureeritakse?
- Millistele serveritele tuleks kataloogiteenus replikeerida?
- Millist kataloogiteenuse infot tuleks replikeerida (filtrite defineerimine)?

- Kas kataloogiteenusest tehtud replikatsioonidesse lubatakse sisse viia muudatusi ning kas need tuleks originaali üle kanda (kas defineerida tüübina Read/Write või Read-Only)?

Kuna süsteem seisab reeglina pidevalt silmitsi muudatustega, mis tulevad selle igapäevasest käitamisest, tuleb ka süsteemi turvalisust pidevalt kontrollida ja uuesti konfigureerida. Täiendavaid juhiseid leiate selle kohta meetmest M 4.311 Kataloogiteenuste turvaline käitamine .

Kontrollküsimused:

- Kas kõik kataloogiteenust pakkuvad serverid on konfigureeritud vastavalt neile ettenähtud rollidele?
- Kas konfiguratsiooni on kaasatud ka klientide arvutid ja programmid?

M 4.308 Kataloogiteenuste turvaline installeerimine

Algatamise eest vastutavad: IT-juht, IT-turbespetsialist

Rakendamise eest vastutavad: administraator

Pärast seda, kui kõik kataloogiteenuste kasutuselevõtuks vajalikud raamtingimused on läbi töötatud (vt M 2.403 Kataloogiteenuste kasutuselevõtu planeerimine), tuleb vastavatesse serveritesse installeerida kataloogiteenuse komponendid ja selle kliendid. Installeerimisfaasis ei ole kataloogiteenust pakkuv server täielikult konfigureeritud, mis tähendab, et planeeritud turvaseadistused veel ei toimi. Seetõttu on soovitatav viia esmakordne konfigureerimine läbi kas kaitstud keskkonnas või paigaldada alternatiivlahendusena juba ettevalmistatud standardne konfiguratsioon. Siinkohal tuleks arvestada, et aluskonfiguratsioonina ei ole mitte kunagi soovitatav otse kasutusse üle võtta tootja poolt tarnitud standardset konfiguratsiooni, kuna kogemused on näidanud, et need ei ole piisavalt töökindlad. Sama kehtib ka juhul, kui kataloogiteenust on tarvis üleviimise raames (vt M 2.408 Kataloogiteenuste üleviimise planeerimine) värskendada või uuesti installeerida. Kataloogiteenust pakkuva serveri installeerimisel juba olemasoleva kataloogipuu alla tuleb piiritleda selle täpne kontekst. Serveri hilisem liigutamine puu koostises on võimalik ainult suure töö ja vaevaga. Installeerimise käigus konfigureeritakse esmakordselt ka lokaalselt toimivad turvaseadistused. Tähtsamate algseadistuste hulka kuuluvad:

- Kataloogiteenuse puu määratlemine
- Kataloogiteenuse juurdepääsuõigused
- Kataloogiteenuse pärimise seadistused
- LDAP-juurdepääsu turvaseadistused

Installeerimise käigus on osasid seadeid võimalik ise määrata, osadele määrab süsteem standardsed algväärtused. Mõningaid seadistusi võib olla tarvis teha ilma krüpteeritud juurdepääsuta ning alles seejärel saab hakata kasutama SSL-iga kaitstud LDAP-juurdepääsu. Sõltuvalt sellest, milliseid kataloogiteenuse mooduleid parasjagu kasutama hakatakse, tuleb iga mooduli jaoks luua turvaline installeerimise konfiguratsioon, mis takistaks juurdepääsusid senikaua, kuni server on esmakordse konfigureerimise faasis ning kuni kehtestatud turvapoliitikad on ellu rakendatud. Täiendavaid juhiseid leiate selle kohta meetmest M 4.307 Kataloogiteenuste turvaline konfigureerimine . Üldjuhtudel tuleb installeerimise käigus arvestada turbe seisukohast järgmiste aspektidega:

- Kataloogiteenuste objektidega seotud juurdepääsuõigusi tuleb süsteemides, mis on kas eelnevate versioonide poolt värskendatud või teiste kataloogisüsteemide poolt üle võetud, kindlasti värskendada.
- *Upgrade* -mehhanismid võivad muuta standardseid seadistusi, nt kaasata olemasoleva kataloogiteenuse struktuuri alla mõne täiendava kataloogiteenuse.

- Juhul kui juba olemasoleva kataloogiteenuse puu alla soovitakse lisada uut serverit, võimaldab pärimismehhanism selle esmakordset konfigureerimist märgatavalt lühendada. Siinkohal tuleks kriitilise pilguga kontrollida, kas pärimismehhanism pole teinud soovimatuid seadistusi, mille tagajärjel võivad tekkida turvalekked.
- Kataloogiteenust pakkuvate serverite installeerimisel tuleb olla eriti ettevaatlik, kuna hiljem hakkavad need igapäevatöös salvestama kaitset vajavat infot.

Kataloogiteenust pakkuvaid servereid tohib installeerida vaid selliste serverite alla, mis asuvad füüsiliselt turvalises keskkonnas, nt kas mõnes serveriruumis või serverikapis. See kehtib eelkõige selliste kataloogiteenust pakkuvate serverite puhul, kuhu salvestatakse andmeid, mis on eriti kõrge kaitsevajadusega.

Täiendavad kontrollküsimused:

- Kas kataloogiteenust pakkuvad serverid asuvad füüsiliselt kaitstud keskkonnas?
- Kas on olemas kontseptsioon, mis sätestab, milliseid administreerimis- ja pääsuõigusi on tarvis kataloogiteenuse installeerimise käigus selle turvaseadistuste all konfigureerida?
- Kas kataloogiteenuste objektidega seotud juurdepääsuõigusi on värskendatud ka neis süsteemides, mis on kas värskendatud eelnevate versioonide poolt või teiste kataloogisüsteemide poolt üle võetud?

M 4.309 Kataloogiteenuste pääsuõiguste seadmine

Algatamise eest vastutavad: IT-juht, IT-turbespetsialist
Rakendamise eest vastutavad: administraator

Kataloogiteenus salvestab institutsiooni töös reeglina palju infot, mida on tarvis kindlasti ka kaitsta, nt kasutajaandmeid. Seetõttu on vältimatu, et vastavale infole tuleb juurdepääs võimaldada ainult neile rakendustele, kasutajatele ja administraatoritele, kes on selleks volitatud. Selle tagamiseks on hädavajalik hakata juba eelnevalt koostatud turvapoliitikas määratletud pääsuõiguste jagamist (vt M 2.405 Kataloogiteenuse turvapoliitika koostamine) järjekindlalt ja läbivalt ellu rakendama. Õiguste jagamine toimub reeglina pääsuloendite ehk *Access Control Lists* (ACLide) abil. Pääsuõigusi on võimalik jagada nii objektipõhiselt kui ka atribuutide alusel. ACLide abil on võimalik õigusi jagada ainult positiivsest kontekstis, st õiguste andmisega kaasneb juurdepääsu kasutusõigus. Pääsuloendi abil pole võimalik määrata, et teatud konkreetne kasutaja jäetakse vastavatest õigustest ilma. Pääsuõiguste jagamisel seotakse vastavad õigused konkreetse omanikuga. Sealjuures tehakse iga sihtobjekti kohta sissekanne, millistel objektidel on lubatud sellel juurde pääseda. Selle alusel saab omakorda ka välja lugeda, millistele sihtobjektidele on teatud konkreetsel objektil õigus ligi pääseda.

Pääsuõiguste pärimine toimub vastavalt kataloogiteenuse puustruktuurile. Antud väide kehtib esmalt siiski vaid objektidega seotud õiguste kohta. Atribuutide õigused pärandatakse vaid juhul, kui need on eraldi selliselt konfigureeritud. Objektide pääsuõiguste automaatset pärandamist nende laps-objektidele saab reguleerida nn maskide või filtrite konfigureerimisega. Kuna “Self”-volitusega on võimalik muuta ka oma enda atribuutväärtusi, on tegu turvalisuse seisukohast kriitilise toiminguga, mida tuleks samuti filtri abil kontrollida. Kataloogipuus jagamisel partitsioonidesse tekib pärimisahelas esmalt lünk, kuid selle sulgeb automaatselt inherentse ACLi järgiühendamine. Juurdepääsu loomise katsel hakkavad tööle nn efektiivsed õigused, st need pääsuõigused, mis tekivad eelpool mainitud pääsuõiguste jagamise mehhanismide tagajärjel. Vastavad efektiivsed õigused arvutatakse iga juurdepääsu korral dünaamiliselt või hoitakse serveri vahemälus (*Cache*). Administraatoritel peaks olema võimalus vaadata halduskonsooliga üksikutele objektidele hetkel kehtivaid efektiivseid õigusi ning nad peaksid neid ka pisteliselt kontrollima.

Üheks oluliseks aspektiks kataloogiteenusega seotud õiguste jagamisel on kasutaja- ja grupikontide konfigureerimine. Kasutaja- ja administraatorigruppide õige defineerimise abil on võimalik õiguste jagamist korraldada palju lihtsamalt ja läbipaistvamalt. Seda on soovitatav teha, kuna üldjuhul on teada, et mida keerukamaks muutub hallatav süsteem, seda suuremaks muutub ka väärkonfiguratsioonide oht. Lihtsama ja järjepideva konfiguratsiooni tagamiseks tuleks kasutajate ja kasutajagruppide seadistamisel rakendada malle (*Templates*). Kataloogiteenused võimaldavad administreerida nii rollide kui ka funktsiooni põhjal. Juhul kui vastavaid administratiivseid rolle ei ole veel loodud, on selleks tarvis täiendada kataloogiteenuse skeemi. Administratiivseid tööülesandeid on võimalik delegeerida selliselt, et neid saaksid täita kõik ühe kindla kasutajagrupi (administraatorigrupi) liikmed. Sel moel toimib ka administreerimisülesannete delegeerimine.

Juhul kui kahte või enamat kataloogiteenuse puustruktuuri on tarvis liita omavahel üheks puustruktuuriks, tuleb pärast liitmist selle tagajärjel tekkinud efektiivsed

õigused üle kontrollida. Sama tuleks teha ka pärast seda, kui kataloogiteenuse puustruktuuris on liigutatud partitsioonide asukohti. Samuti tuleks kontrollida ja vajadusel ümber konfigureerida pääsuõigused, nt kui Windowsi domeen migreeritakse eDirectory-puustruktuuri alla.

Täiendavad kontrollküsimused:

- Kas kasutajate- ja administraatoritegrupi pääsuõigused konfigureeriti kooskõlas eelnevalt koostatud turvapoliitikaga?
- Kas sihtobjektide suhtes reaalselt tekkinud efektiivseid õigusi on pisteliselt kontrollitud?
- Kas administraatorirollid ja administreerimisvolituste delegeerimine on konfigureeritud läbivalt ühtemoodi?

M 4.310 Kataloogiteenuste LDAP-pöörduste seadmine

Algatamise eest vastutavad: IT-juht, IT-turbespetsialist
Rakendamise eest vastutavad: administraator

LDAP (Lightweight Directory Access Protocol) on protokoll, mis võimaldab juurdepääsu kataloogiteenuse andmetele. LDAP töötati algselt välja alternatiivina DAP (Directory Access Protocol) protokollile, mis defineeriti omal ajal X.500-Directory standardite raames. Aluseks olev andmemudel ja protokolli raames võimaldatavad operatsioonid võeti seejuures suures osas üle standardist X.500. Protokolli praegune kõige värskem versioon LDAP Version 3 on kataloogiteenuste juurdepääsude puhul muutunud vahepeal domineerivaks standardiks. Peaaegu kõikidel kataloogiteenustel on olemas LDAP-liides. Selle olemasolu pakub nt järgmisi kasutusvõimalusi:

- Kataloogiteenuse kasutamine internetikeskkonnas, näiteks nn sertifitseerimisandmebaasina. Kasutajatele võimaldatakse juurdepääs internetis, milleks tuleb kasutada sobilikku LDAP-võimelist tarkvaraklienti.
- Kataloogiteenuse kasutamine organisatsiooni intraneti keskkonnas kasutajakontode või ressursside haldamiseks võrgus. Lisaks kasutajate otsejuurdepääsudele LDAP-kliendi vahendusel on võimalik kasutada ka võrgurakendustel toimivaid juurdepääsusid.

Mõlemal juhul tuleb LDAP-juurdepääs konfigureerida vastavalt eelnevalt koostatud turvapoliitikale (vt M 2.405 Kataloogiteenuse turvapoliitika koostamine).

Kataloogiteenused lubavad LDAP-klientidel ennast üldjuhul ka anonüümselt sisse logida. Eelseadistusega on LDAP-klient varustatud pääsuõigustega, mis on objekti kohta kataloogiteenusesse sisse kantud. Tegemist on virtuaalse objektida, mille ainukeseks ülesandeks on kataloogiteenuse pääsuõiguste jagamine. Iga juurdepääs kataloogipuus olevatele objektidele leiab automaatselt aset nende õigustega, mis on vastavale “public” objektile antud.

Juhul kui anonüümselt sisseloginud kasutajatele soovitakse anda täiendavat ligipääsu kataloogipuu üksikutele alamvaldkondadele, tuleb selleks luua eraldi kasutajakonto. Vastav kasutajakonto tuleb registreerida anonüümse LDAP-juurdepääsu jaoks nn Proxy-User’ina. Nimetatud anonüümne juurdepääs ei eelda autentimist, mistõttu pole vastavat kontot tarvis varustada ka parooliga. Siinkohal tuleks jälgida, et vastavale kasutajakontole endale poleks antud õigust ise parooli kasutusele võtta, kuna vastasel korral võib üksik klient anonüümse juurdepääsu täielikult blokeerida. Lisaks tuleks juhul, kui pääsuõigusi ei lähe enam tarvis, varustada vastav Proxy-User võimalikult piiratud pääsuõigustega või need täielikult tühistada.

Eriti anonüümse juurdepääsu korral peaksid otsinguvõimalused LDAP-juurdepääsu kaudu olema piiratud. Kui server edastab näiteks pärast nime sisestamist sinna juurde kuuluva e-posti aadressi või e-posti aadressile kuuluva

sertifikaadi, peaks otsingufiltreid olema võimalik kasutada üksnes piiratult. E-posti aadress ja ainult see (mitte sinna juurde kuuluv eraldusnimi (distinguished name)) tuleks päringu teinud kliendile anda üksnes pärast täieliku nime või piisavalt pika nimeosa sisestamist. Sertifikaat tuleks vastu saata üksnes pärast täieliku e-posti aadressi sisestamist. Tuleks kaaluda, et mitte lubada kohahoidjaid (Wildcards), sest nende päringute kaudu ei saa koostada asutuse kõikide e-posti aadresside täielikku nimekirja. Alternatiivselt võib väljaantud tulemuste arvu piirata madala limiidiga. Soovitatakse limiiti 1 ja 5 vahel. Vastasel korral on anonüümsed kasutajad olukorras, et nad võivad lugeda kõiki kataloogiteenuse andmeid või vähemalt suurt osa sellest ja saavad nii väärtuslikku teavet, mis võivad saada rämpsposti või Social Engineering-tüüpi rünnete aluseks (vt G 3.89 Kataloogiteenuse LDAP-juurdepääsu väär konfiguratsioon).
Juba kataloogiteenuse kasutuselevõttu planeerides tuleb langetada otsus, millistele andmetele võimaldatakse juurdepääs ennast anonüümselt sisselogivatele kasutajatele (vt lisaks M 2.405 Kataloogiteenuse turvapoliitika koostamine). Vastavalt sellele otsusele tuleb konfigureerida ka Proxy-User 'ite juurdepääsud, rakendades selleks vajalikus mahus piiranguid.

Kataloogiteenuse rakendamisel LDAP-serverina internetikeskkonnas, tuleks puudutatud servereid kaitsta turvalüüsiga. Teenuse kasutamine peaks olema konfigureeritud selliselt, et LDAP-serveritesse edastataks ainult selliseid andmepakette, mis on LDAP-serverite käitamiseks hädavajalikud. Enamikel juhtudel on nende puhul tegu TCP-pakettidega, mis edastatakse portidesse 389 ja 636, mis on LDAP ehk LDAP üle SSLi standardsed pordinumbrid. Andmete puhul, millele ei tohi anonüümselt juurde pääseda, tuleb tingimata rakendada vastava LADP-kliendi autentimist. Vastav klient autendib ennast registreeritud kasutajate nimekirjas. Vältimaks kasutajatunnuste saatmist loetava teksti kujul üle Interneti, tuleks kasutada asjakohaseid seadistusi. Vastavate seadistusega säilivad aga siiski ka anonüümsed LDAP-ühendused, samamoodi nagu ka säilib ka kasutajate sisselogimisvõimalus LDAPga üle SSLi.

Enamikel juhtudel on soovitatav sideks ja edastuseks kasutada SSLi. Selleks otstarbeks kasutatakse nii ühe- kui ka mõlemapoolset autentimist. Kahepoolse autentimise all peetakse silmas seda, et ka klient peab olema varustatud kehtiva sertifikaadiga, mille juurde kuuluva privaatvõtme abil genereeritakse seansivõti (Session Key). See on võimalikest konfiguratsioonidest kõige turvalisem. Alternatiivina võib klienti autentida ka parooli abil. Edastatava parooli konfidentsiaalsuse tagab serveriga loodava ühenduse krüpteerimine SSLiga. Selleks, et sisseseatud usaldussuhteid oleks võimalik jälgida ka lokaalselt, peavad kasutajad kõikidel juhtudel oma LDAP-klienti, st veebilehitsejasse importima CA-juursertifikaadi, (vt M 5.66 TLS-i/SSL-i kasutamine). Juhul kui SSLi ei rakendata, on võimalik kasutajate paroole kataloogiteenusesse üle kanda loetava teksti kujul üle Interneti (vt lisaks M 5.147 Turvalise kommunikatsiooni tagamine kataloogiteenuste abil). Seda tuleks alati vältida.

Kataloogiteenus pakub võimalust LDAP raames kasutatavate standardseid objektiklasse taasluua teistes kataloogiteenuse enda sees kasutatavates objektiklassides. Antud võimalus muutub oluliseks, kui LDAP-kliendid kasutavad otsingu käigus standardseid LDAP-objektiklasse, kui vastavad andmed asuvad kataloogitee-

nuste objektiklasside atribuutide all hoopis teistsuguste nimedega. Seetõttu tuleks LDAP-klientide esmakordsel kasutamisel või kataloogiteenuse skeemi muutmise järele kontrollida, kas LDAP-objektiklasside kajastamine on kataloogiteenuste objektiklassidega kooskõlas ning kas rakendatavad LDAP-rakendused töötavad korrektselt.

Kontrollküsimused:

- Kas Kas kõik kataloogiteenuse serverid, mida on võimalik kasutada LDAP toel üle interneti, on turvalüüsiga kaitstud?
- Juhul kui LDAP-grupi jaoks on konfigureeritud Proxy-User, kas vastava Proxy-User'i pääsuõigused on piisavalt suurte piirangutega?
- Kas sidet ja edastusi LDAP kaudu kaitstakse piisavalt?
- Kas otsing LDAP kaudu on piiratud, et takistada turvalisuse suhtes tundliku teabe väljastamist?

M 4.311 Kataloogiteenuste turvaline käitamine

Algatamise eest vastutavad: IT-juht, IT-turbespetsialist
Rakendamise eest vastutavad: IT-juht, administraator

Keeruliste süsteemide käitamisel tuleb muuhulgas pidevalt tegeleda nende turvalisusega, kuna nende igapäevase kasutusese raames tuleb aeg-ajalt kindlasti teha hädavajalikke muudatusi. Selleks ei piisa ainult turvalise aluskonfiguratsiooni loomisest (vt M 4.308 Kataloogiteenuste turvaline installeerimine ja M 4.307 Kataloogiteenuste turvaline konfigureerimine). Pärast installeerimist ja esmakordset konfigureerimist, mis tehakse vastavalt eelnevalt loodud kataloogiteenuste kontseptsioonidele ja turvapoliitikatele, hakatakse kataloogiteenuse servereid reeglina kasutama võrgukeskkonnas. Sellise võrgu turvalisus sõltub ühelt poolt kindlasti ka aluskonfiguratsioonist. Kuid lisaks aluskonfiguratsioonile määrab võrgu turvalisuse veel ka see, kuidas tehakse jooksva töö käigus vajalikke konfiguratsioonimuudatusi. Siinkohal on eriti oluline arvestada võimalike kõrvalmõjudega, mis võivad sõltuvalt olukorrast tahtmatult tekitada turvaauke. Kataloogiteenusesüsteemi käitamise raames tuleks infoturbe seisukohast pöörata tähelepanu järgmistele aspektidele:

- Süsteemi turvalisuse seisukohast on kataloogisüsteemi puhul tähtis selle kasutajate ja volituste järjepidev haldamine. Vajalike tööülesannete keerukust mõjutab siinkohal suuresti halduskontseptsiooni ülesehitus. Kuna keerulisemate protsesside puhul on vigade tekke tõenäosus suurem, tuleks administratiivsed ülesanded koostada võimalikult lihtsad. Turvalist süsteemiseisundit toetab pääsuõiguste kontseptsioon, mis on üles ehitatud gruppidele. Antud põhimõte lihtsustab olulisel määral andmebaaside pääsuõiguste haldamist ning lisaks on see ka palju vähem vastuvõtlik vigadele. Eriti oluline on siinkohal jälgida, et tavakasutajatele keelataks igasugune juurdepääs administraatorite tööks vajalikele haldustööriistadele.
- Kataloogiteenuste muudatused leiavad aset peamiselt siis, kui olemasoleva kataloogiteenuse puustruktuuri alla on tarvis importida võõraid LDAP-katalooge. Uued imporditud kataloogid pole reeglina veel olemasolevate turvastruktuuride töösse kaasatud. Kehtestatud turvapoliitika järjekindla rakendamise tagamiseks tuleb kiirkorras värskendada turvaseadistuste konfiguratsiooni. Volitusi, mis lubavad uute kataloogide importimist ja kataloogide replikeerimist, tuleb jagada võimalikult suurte piirangutega.
- Kataloogiteenuse juurdepääsu kontrollimehhanismide rakendamisel võivad mängida olulist rolli krüptograafilised sertifikaadid. Kui sertifikaadi väljastamise koht on installeeritud kataloogiteenust pakkuvale serverile, on iga uue objekti jaoks võimalik automaatselt genereerida eraldi võtmepaar ja see kataloogiteenusesse hoiule panna. Seetõttu on äärmiselt oluline, et vastavat kataloogiteenust pakkuvat serverit käitataks puustruktuuri all võimalikult turvaliselt. Kaitsta ei tule mitte ainult seal asuvaid andmeid, vaid ennekõike ka nende käideldavust, nt selleks sobiva replikeerimise teel.
- Viirusetõrje seisukohast nõuab kataloogiteenus spetsiaalset strateegiat, mis

tagaks, et süsteem ei registreeriks viirusetõrjetarkvara tööd replikeeritud andmeversioonidega tavapäraste muudatustena, kuna selline olukord tekitab ebavajalikke andmeedastusi. Kõige halvemal juhul võib selle tagajärjel kaotsi minna kataloogi andmemahu terviklus, mis võib vastava kataloogiteenuse lõpuks isegi kasutuskõlbmatuks muuta.

- IT-süsteemi turvalisus toetub alati serverite ja võrgukomponentide rakenduskeskkonna füüsilisele turvalisusele. Seetõttu tuleb kataloogiteenust pakkuvad serverid üles seada turvalisse keskkonda, vt nt moodulit B 2.4 Serveriruum .
- Süsteemi turvaseisundi mõistmiseks on hädavajalik rakendada pidevat seiret. Serveri turvaseadistusi ja logiandmeid tuleks regulaarselt kontrollida. Niisuguse seire eesmärgiks on tuvastada kehtivate turvaeeskirjade rikkumised, avastada võimalikud olemasolevad turvaaugud ja tuvastada potentsiaalsed, turvaauke tekitavad väärkonfiguratsioonid. Vajaminevat seirekontseptsiooni tuleb siinkohal käsitleda turvakontseptsiooni ühe osana. Keerukamate süsteemide nagu nt kataloogiteenuste puhul ei ole mõeldav, et seirega tegelevad vaid mõned üksikud administraatorid, st seire peab aset leidma automatiseeritud kujul vastavate süsteemikomponentide või kolmandate tootjate toodete poolt. Siinkohal tuleb arvestada, et seoses süsteemis asetleidvate muudatustega tuleb vastavalt kohandada ka seiresüsteemi. Logifailide ja turvaseadistuste analüüsimine võib toimuda nii käsitsi kui ka tarkvara toel. Seiret puudutavad soovitused on kokku kogutud meetmesse M 4.312 Kataloogiteenuste monitooring .

Kõikide kataloogiteenuse käitamiseks vajalike poliitikate, suuniste ja protsessi-de dokumenteerimine on oluline ka turbe seisukohast. Selleks tuleks koostada käitamist kajastavad käsiraamatud ning süsteemis tehtava muudatuse korral tuleks neid vastavalt täiendada. Kuna käsiraamatud sisaldavad sellisel juhul turbe seisukohast olulist infot, tuleb neid hoida volitamata isikute juurdepääsu eest kaitstuna. Volitatud administraatoritele peaks juurdepääs sellistele käsiraamatutele olema seevastu võimalikult lihtne. Käsiraamatutes loetletud soovitused võiksid olla vaid üldsõnalised, kuna süsteemi turvalisuse tagamine sõltub ka kohapealsetest oludest. Seetõttu tuleb vastavad süsteemi turvalist käitust tagavad poliitikad, mis arvestaksid kohapealsete oludega, koostada juba siis, kui tegeletakse alles kataloogiteenuse puustruktuuri planeerimisega. Sõltuvalt konkreetsetest tingimustest võib ette tulla olukordi, kus teatud mehhanisme ei õnnestugi optimaalselt konfigureerida. Sellised olukorrad võivad tekkida nt siis, kui on tarvis edasi käitada „vanu“ rakendusi, mis on varustatud kas ainult nõrga autentimismehhanismiga või millel puudub see üldse. Sellistel juhtudel tuleb sobiva turvalisuse saavutamiseks rakendada alternatiivseid vastumeetmeid mõnes muus kohas, nt organisatoorse töö tasandil.

Potentsiaalseid turvaauke on suutelised tuvastama ainult kompetentsed administraatorid. Seetõttu moodustab ühe olulise kaitsemeetme ka süsteemihaldajate koolitus ja nende täiendõpe (vt M 3.62 Kataloogiteenuste administreerimise koolitus). Lisaks on tarvis turbeaspektide vallas koolitada ka tavakasutajaid (vt M 3.63 Kasutajate koolitus autentimiseks kataloogiteenuste abil), et neile oleksid teada potentsiaalsed ohud ning et kasutajad suudaksid olemasolevaid turvamehhanisme õigesti rakendada.

Täiendavad kontrollküsimused:

- Kas kõik käitamisprotseduurid on dokumenteeritud?
- Kas *System* -logisid kontrollitakse regulaarselt?
- Kas tavakasutajatele on tõkestatud juurdepääs kõikidele administraatorite tööriistadele?

M 4.312 Kataloogiteenuste monitooring

Algatamise eest vastutavad: IT-juht, IT-turbespetsialist
Rakendamise eest vastutavad: IT-juht, administraator, audiitor

Süsteemi turvaseisundi mõistmiseks on hädavajalik rakendada pidevat seiret. Selleks tuleks muuhulgas regulaarselt kontrollida ka serveri turvaseadistusi ja serveri logiandmeid. Niisuguse seire eesmärgiks on tuvastada kehtivate turvaeeskirjade rikkumised, avastada võimalikud olemasolevad turvaaugud ja tuvastada turvaauke tekitavad väärkonfiguratsioonid. Vajaminevat seirekontseptsiooni tuleb siinkohal käsitleda turvakontseptsiooni ühe osana. Keerukamate süsteemide nagu nt kataloogiteenuste puhul ei ole mõeldav, et seirega tegelevad vaid mõned üksikud administraatorid, st seire peab toimuma automatiseeritud kujul vastavate süsteemikomponentide või kolmandate tootjate toodete poolt. Siinkohal tuleb arvestada, et seoses süsteemis asetleidvate muudatustega tuleb vastavalt kohandada ka seiresüsteemi.

Kataloogiteenuse süsteemiseireks tuleks rakendada sobivaid tarkvaratööriistu. Klient-server-ühenduse puhul peab juurdepääs seiretööriistadele olema kaitstud sobivate autentimismehhanismidega. Juurdepääsu loojal peab olema võimalik andmetele ligi pääseda alles pärast seda, kui ta on edukalt läbinud autentimise, ning tal tohib olla võimalik kasutada vaid selliseid õigusi, mis on tema jaoks konfigureeritud. Tavakasutajatele peab juurdepääs kõikidele administraatorite tööriistadele olema tõkestatud. Vastavaid juurdepääse tuleks üldjuhul kasutada ainult koos sideühenduse piisava krüpteeringuga. Sõltuvalt kataloogiteenusest ja rakendatavatest tööriistadest on võimalik eraldi logifailidesse salvestada kõiki kataloogiteenuse raames asetleidvaid sündmusi. Eraldi salvestatud logiandmete põhjal saab sündmusi palju paremini tuvastada ja analüüsida võrreldes sellega, kui logiandmed salvestatakse operatsioonisüsteemi globaalsesse logifaili. Seire puhul tuleb arvestada järgnevate aspektidega:

- Planeerimisfaasi tuleks võimalikult varakult kaasata ka andmekaitsespetsialist ja töötajate esindus, kuna süsteemiseire käigus puututakse tavaliselt kokku ka isikuandmetega.
- Täielikuma pildi saamiseks süsteemis asetleidvate protsesside kohta tuleks lisaks konkreetselt kataloogiteenusega seotud sündmustele jälgida ja logida ka operatsioonisüsteemi sündmusi. Soovitusi ja juhtnööre operatsioonisüsteemi sündmuste logimiseks leiate vastavatest teemakohastest moodulitest.
- Logifailide ühte kesksesse kohta kokkukogumiseks ja automaatseks analüüsimiseks on võimalik kasutada kolmandate tootjate lahendusi. Juhul kui kasutatakse võrgu- ja süsteemihalduse tööriista (vt moodul B 4.2 Võrgu- ja süsteemihaldus), on võimalik sõltuvalt tootest erinevad kataloogiteenust kajastavad logid integreerida otse vastava tööriista alla.
- Seire käigus toodetakse sõltuvalt konfiguratsioonist suuri andmemahte. Neid pole tarvis mitte ainult regulaarselt analüüsida, vaid salvestusruumi pii-

ratuse tõttu ka kustutada või teistele andmekandjatele ümber salvestada ja hoiule panna. Intensiivne seire võib vähendada süsteemi jõudlust. Mõnikord võib juhtuda, et server koormatakse seirega nii üle, et tavapärane töö muutub lausa võimatuks. Sel põhjusel tuleb juba proovikäitamise raames välja selgitada optimaalsed seireparameetrid ning neid vajadusel ka kohandada. Parameetrite kohandamine võib avaldada mõju tervele seirekontseptsioonile, kuna võib selguda, et teatud liiki seireülesandeid ei ole võimalik ellu rakendada. Eriti võib seda esineda siis, kui rakendatakse täiendavaid tooteid, mis seavad kõrgeid nõudeid logitavatele sündmustele. Näitena võib siinkohal esile tuua programmid, mille puhul põhineb logiandmete automaatne analüüs käitumises esinevate anomaaliate tuvastamisel nagu nt võimalike rünnete tuvastamisel.

Süsteemifunktsioonide seire raames on lisaks soovitatav regulaarselt kontrollida kataloogiteenusest loodavaid replikatsioone, mis edastatakse konfiguratsioonis aseleidnud muudatuste tõttu. Replikatsioonides esinevad vead viivad enamasti selleni, et konfiguratsioonis asetleidnud muudatusi ei rakendata järjepidevalt, mille tagajärjel võib nt mõni kasutaja saada liiga palju õigusi.

Täiendavad kontrollküsimused:

- Kas on koostatud ja ellu rakendatud vajadustest lähtuv seirekontseptsioon? Kas protsessidesse on kaasatud ka andmekaitsespetsialist ja töötajate esindus?
- Kas olulisi süsteemis asetleidnud sündmusi logitakse ning kas vastavaid logisid analüüsitakse regulaarselt?
- Kas seireparameetreid kontrollitakse proovikäitamise raames ning kas neid kohandatakse regulaarselt vastavalt vajadusele?
- Kas kohandamise käigus arvestatakse sellega, et pärast muudatuste tegemist oleks jätkuvalt võimalik kõiki seireülesandeid ka reaalselt täita?

M 4.313 Turvaliste domeenikontrollerite kasutuse võimaldamine

Algatamise eest vastutavad: IT-juht, IT-turbespetsialist, vastutav spetsialist
Rakendamise eest vastutavad: administraator

Kuna domeenikontrolleritele on salvestatud Active-Directory infrastruktuur, peavad need olema konfigureeritud piisavalt turvaliselt. Järgnevad turbealased soovitused peaksid aitama teil minimeerida riske, mis on seotud turvaliste domeenikontrollerite kasutuse võimaldamisega.

Domeenikontrollerite turvaline käitamine

Üldjuhul tuleks domeenikontrollereid käitada turvalises keskkonnas nagu nt arvutuskeskuses või ruumides, kuhu on õigus siseneda ainult usaldusväärsel personalil. Sellel lisaks on neid tarvis täiendavalt kaitsta turvalise infrastruktuuriga, nt marsruuterite, kommutaatorite jms abil. Operatsioonisüsteemi installeerimine tuleks läbi viia vastavalt IT etalonturbe kataloogides toodud moodulite kihile nr 3, mis käsitleb erinevaid Windows-serverite operatsioonisüsteeme.

Ennustatav ja korduv kasutuse võimaldamine

Võimalike konfiguratsioonigade vältimiseks ja ühtse turbeastme tagamiseks tuleks domeenikontrollerite jaoks luua etaloninstallatsioon. Seejärel tuleks ühtlustada ka turvaseadistuste tegemine domeenikontrollerite aluskonfiguratsiooni raames. See tuleks saavutada rakendades ennustatavat ja kergesti korratavat võimaldamisprotseduuri.

See sisaldab:

- Regulaarset kiirparanduste (Hotfix 'ide) ja remondipakettide (Service Pack'ide) paigaldamist - Värskeid kiirparandusi ja remondipakette tuleks paigaldada regulaarselt. Nende võimalikke mõjusid tuleks aga eelnevalt domeenikontrolleri etalonist tehtud kujutise (image) peal põhjalikult testida.
- Piisavalt tugevate paroolide jagamist - Active Directory kasutajakontod tuleb varustada piisavalt tugevate paroolidega. Sellega tuleb tagada, et keegi ei saaks endale vargsi luua volitamata juurdepääsu. Piisavalt tugevate paroolide rakendamise kohta leiate infot M 2.11 Paroolide kasutamise reeglid . Keerukate paroolide kasutuselevõtmise kõrval on tarvis tagada, et ka paroolide edastamine asjaga seotud isikutele toimuks turvaliselt. Lisaks peaksid kasutajakontod olema, eriti nende esmakordsel sisseseadmisel, varustatud individuaalsete paroolidega.
- Automaatsete niinimetatud 8.3-failinimede genereerimise desaktiveerimist NTFS-is - Automaatne 8.3-failinimede (st kaheksast tähemärgist koosnevate ja kolme tähemärgiga lõppevate failinimede) genereerimine tuleks desaktiveerida, et vältida võimalikke viiruseid ja ründeid, mis on suunatud spetsiaalselt 8.3-ühilduvate failinimede vastu. Kui 16-bitiseid rakendusi enam ei kasutata, pole antud funktsioon enam tingimata vajalik. Lisaks sellele kasvab vastavast funktsioonist loobumise korral ka kataloogide kuvamise jõudlus. Selleks tuleb HKLM\SYSTEM\CurrentControlSet\Control\FileSystem all teha järgnev sissekanne:

Sissekande nimi = NtfsDisable8dot3NameCreation;Andmetüüp = REG_DWORD;Väärtus = 1.Registrivõtmes tehtavaid muudatusi tuleks esmalt

testimiskeskkonnas uurida, et kontrollida nende ühildumisvõimet ja tuvastada nende võimalikke mõjusid.

- Installeeritud tarkvara tervikluse tagamist - Juhul kui domeenikontrollereid hoitakse kasutusvalmis kujul kusagil mujal asukohas, tuleks nende transportimiseks kasutada signatuure, et kindlustada niimoodi installatsioonide terviklus.

Piirdumine vajalike teenustega

Domeenikontrollerite võimaliku ründepinna minimeerimiseks tuleks võimalike teenuste hulgast välja valida ja kasutusse võtta ainult sellised, mis on käitamiseks hädavajalikud.

Käitusfailide volitused

Kaitsmaks pärast domeenikontrollerite funktsioonide laiendamist salvestuskohtade tüvikatalooge andmekandjatele suunatud rünnete vastu, tuleks kasutajagrupilt „All“ ära võtta volitused „Read and Execute“. Täisvolitustega juurdepääse tuleks jagada ainult administraatoritele.

Teiste operatsioonisüsteemide süsteemikäivituse takistamine

Mõne teise operatsioonisüsteemi käivitamine domeenikontrollerites võib suuta kõrvaldada NTFS-juurdepääsudele kehtestatud piirangud ning luua seeläbi juurdepääsu kriitilise tähtsusega andmetele. Seetõttu on tarvis lisaks juba eelpool mainutud serverite käitamisruumi turvalisuse tagamisele kasutusele võtta ka veel asjakohased organisatsioonilised meetmed. Süsteemikäivitusel tuleks ette näha, et selle käigus desaktiveeritaks kaugpääsul põhinevad võrgukäivitused ning koos sellega ka kaugpöördusel töötavate võrguinstallatsioonide, nt RISi (Remote Installation Services) või BOOTP (Bootstrap Protocol'i) kasutamine samamoodi, nagu keelatakse ära BIOS-paroolide rakendamine.

Taaskäivituse vastane kaitse SYSKEY abil

Süsteemivõtme (SYSKEY) kasutamine kaitseb Windowsi turvaandmeid offline -rünnete eest. Kaitse tagamiseks salvestatakse Active Directory andmebaasi ja lokaalse turvaautoriteedi (LSA) paroolid krüpteeritud kujul domeenikontrollerite alla. Pärast SYSKEY aktiveerimist on domeenikontrolleri taaskäivitamiseks tarvis kas kasutajatunnust või süsteemivõtit sisaldavat andmekandjat, st nende puudumisel pole arvutit võimalik käivitada. Iga kasutuskorra järel on hädavajalik, et süsteemivõtit sisaldavad andmekandjad eemaldatakse domeenikontrolleritest ja pandaks hoiule turvalisse kohta. Lisaks peaks olema tagatud, et vastavast andmekandjast oleks loodud ka töökoopia.

Kontrollküsimused:

- Kas domeenikontrollereid käitatakse turvalises keskkonnas?
- Kas domeenikontrollerite platvormiks olev Windows-Serveroperatsioonisüsteem on installeeritud ja konfigureeritud turvaliselt?
- Kas igas domeenikontrollerist on loodud kujutis (image)?

- Kas kiirparandusi (Hotfix ’e) ja remondipakette (Service Pack’e) paigaldatakse regulaarselt? Kas kiirparanduste (Hotfix ’ide) ja remondipaketteide (Service Pack ’ide) võimalikke mõjusid kontrollitakse enne paigaldamist testimiskeskkonnas?
- Kas kasutajakontod varustatakse piisavalt tugevate paroolidega?
- Kas 8.3-failinimede genereerimine desaktiveeriti?
- Kas ühildumine varasemate versioonidega desaktiveeriti?
- Kas vastavatel domeenikontrolleritel sisse seatud teenuste puhul piirdutakse ainult hädavajalikega?
- Kas kasutajagrupi „All“ volitusi on piiratud?
- Kas domeenikontrollerid on kaitstud volitamata taaskäivitamise vastu ning kas hädavajalik võrguturve on tagatud?

M 4.314 Domeenide ja domeenikontrollerite turvaliste poliitikaseadistuste loomine

Algatamise eest vastutavad: IT-juht, IT-turbespetsialist

Rakendamise eest vastutavad: administraator

Active Directory 'ga töötaval Windowsi serveril on nii domeeni kui ka domeenikontrollerite jaoks omad standardsed turvapoliitikate seadistused. Domeenide ja domeenikontrollerite turvalisuse tõstmiseks on siiski soovitatav turvapoliitikate standardseid turvaseadistusi muuta, rakendades selleks järgmisi abinõusid:

- Turvalised kasutajatunnusepoliitikate seadistused - Juurdepääs domeenikontrolleritele peab olema kaitstud tugevate turvamehhanismidega. Täpsemat infot kasutajatunnusepoliitikate vajalike seadistuste kohta leiate spetsiaalsetest Microsofti tooteid käsitlevatest moodulitest.
- Kontosulgemispoliitikad - Sisselogimiskatsed peaksid kajastuma logis selliselt, et sinna kogutava info põhjal oleks võimalik tuvastada ründeid (vt M 4.316 Active Directory infrastruktuuri monitooring). Näiteks võib suur hulk ebaõnnestunud paroolisisestusi ühe sisselogimiskatse kohta viidata selle, et tegemist võib olla Brute-Force -ründega. Konto reaalne sulgemine tuleb aga defineerida mõistete konto blokeerimise kestvus, konto sulgemislävi ja konto blokeerimisloenduri nullimine, mille kirjeldused leiate meetmest M 2.231 Windowsi grupipoliitika planeerimine .
- Kerberos-poliitikate seadistused - Kerberos protokolli näol kasutatav autentimisteenus edastab kliendile ressurssidele juurdepääsemiseks vajalikud autentimisandmed. Võrguressurssidele võimaldatakse juurdepääs vastavate seansipiletite (Ticket 'ite) abil. Selleks väljastab domeenikontroller kliendile eelnevalt nn piletiandmise pileti TGT (Ticket-Granting-Ticket'i). Kui klient püüab ligi pääseda mõnele soovitud ressursile, edastab klient oma TGT pileti domeenikontrollerile, kes peab seda kontrollima. Pärast edukalt läbitud kontrolli loob domeenikontroller omakorda kliendi jaoks seansipileti, mis võimaldab tal teatud piiratud aja jooksul ressurssidele ligi pääseda. Kerberospoliitikate kohandamisega on võimalik kohandada domeeni kasutajakontodele väljastatavaid Kerberose Ticket 'eid, nt nende kestust. Kerberospoliitikate kohandamiseks vajalikke juhtnööre leiate IT etalonturbe abimaterjalid hulgast, vt Active Directory 't käsitlevate abimaterjalide alt Kerberospoliitikate seadistamine.

Domeenikontrollerite poliitikate turvaliste seadistuste saavutamiseks soovitame lisaks ka veel järgnevaid meetmeid:

Kasutajaõigusi tuleks jagada piirangutega, kuid selliselt, et kasutajatel oleks võimalik domeenis või domeenikontrollerites täita oma tööga või administreerimisega seotud ülesandeid. Kasutajate juurdepääsuvõimalusi tuleks piirata selliselt, et kasutajatel ei oleks võimalik ohustada domeenikontrollerite turvalisust (vt lisaks meedet M 2.229 Active Directory planeerimine). Domeenikontrollerite seirepoliitikatele seadistuste kehtestamisega luuakse võimalus tõestada, kes on teostanud tundlikke kataloogioperatsioone nagu nt viinud sisse muudatusi haldamisse või teinud muudatusi konfiguratsioonis. Seire peaks kajastama andmeid sisselogimiskatsete, kontohaldamiste, Active- Directory -juurdepääsude, objektidele suunatud juurdepääsukatsete, poliitikate muutmise, volituste kasutamise, protsessi jälgimise ja süsteemis toimunud sündmuste kohta. Olulisi Active

Directory -objekte nagu nt kataloogidest tehtud partitsioone tuleb kaitsta sobivate poliitikaseadistuste abil. Selleks tuleb sisse lülitada kataloogi partitsioonide seire (Active Directory -andmebaasi loogiliste osade seire).

Antud teemast puudutatud partitsioonid kannavad nimetust „Skeem“, „Konfiguratsioon“ ja „Domeen“. Eelnevalt toodud soovitused poliitikatele seadistuste kehtestamiseks viivad selleni, et turvalogile eelseadistusega määratud maksimaalset suurust on tarvis tõsta, et suurenenud sündmuste hulk sinna ka reaalselt ära mahuks. Logisid tuleb analüüsida võimalikult kiiresti. Lisaks peab olema loodud selgelt sõnastatud protseduur logide regulaarseks ja õigeaegseks arhiveerimiseks ning turvasündmusi ja süsteemisündmusi kajastavate logide varundamiseks, mille käigus ei tohi ükski sündmus kaduma minna ega tohi ühtegi sündmust üle kirjutada.

Kui lisaks eelnevale on tarvis toetada domeenide koostööd erinevate tervikstruktuuride vahel, nt rakenduste ühiskasutust või piiratud ühiskasutust erinevate tervikstruktuuride vahel ühe institutsiooni piires, tuleks kehtestada välised usaldussuhted. Väliste usaldussuhte kehtestamisega kaasneb aga potentsiaalne turvarisk, kuna sellega ületatakse turvapiire. Seetõttu peaksid domeenikontrollerid usaldusväärsetes domeenides filtreerima kasutajate autoriseerimisandmeid ja nende turvatunnuseid (Security ID 'sid, SID-sid) ning eemaldama need, mis ei ole seotud kasutajakonto domeeniga. Põhjaliku kirjelduse laiaulatuslike volituste hõivamise kohta, mis saavutatakse võltsitud SID-de abil, ning SID-filtreerimisel põhinevate vastuabinõude kohta leiate Microsoft Knowledge Base artiklitest nr 289243 ja 289246. Domeenikontrollerite turvavalikute poliitikate seadistused mõjutavad Windowsi serverite operatsioonisüsteemide turvalisusega seotud konfiguratsiooniseadeid ning seetõttu tuleks nende konfigureerimisel olla võimalikult kohusetundlik. Antud nõue ei kehti mitte ainult Active Directory'ga seonduvate konfiguratsioonide puhul, vaid ka Windows Server operatsioonisüsteemide teistele komponentidele (nt võrgu, failisüsteemi ja kasutajate sisselogimise turvakonfiguratsioonide seadistustele).

Kontrollküsimused:

- Kas olulisemaid Active Directory objekte ja nendega seotud sündmusi jälgitakse ja logitakse?
- Kas turvalisust kajastavate logidele kehtestud andmemahust piisab, et suurt hulka erinevaid sündmusi piisavalt kaua logida?
- Kas logisid analüüsitakse ja varundatakse regulaarselt ja õigeaegselt?
- Kas on kehtestatud välised usaldussuhted ning kas nende raames filtreeritakse ja muudetakse kasutajate autoriseerimisandmeid anonüümseks?

M 4.315 Active Directory töökindluse tagamine

Algatamise eest vastutavad: IT-juht, IT-turbespetsialist, vastutav spetsialist
Rakendamise eest vastutavad: administraator

Administraatorid peavad suutma tagada töökeskkonnas rakendatavate domeenikontrollerite ettenähtud turbeastme ning kõrgenenud nõudmiste korral neid ka vastavalt kohandada. Süsteemides tehtavate muudatuste jaoks, mis tulenevad muuhulgas regulaarsetest hooldamistöödest, tuleb juba eelnevalt koostada kirjalikult fikseeritud poliitikad. Domeenikontrollerite turvalise käitamise tagamiseks on ilmtingimata tarvis regulaarselt läbi viia viirusekontrolle, mille puhul tuleb järgida ka teatud eripärasid (vt M 2.414 Domeenikontrollerite kaitse arvutiviiruste eest , alalõiku *Domeenikontrollerite kriitilise tähtsusega failid*).

Jooksvad värskendused *Hotfix* 'ide ja *Service Pack* 'ide näol
Domeenikontrollereid tuleks regulaarsete ajavahemike tagant kaitsta uute potentsiaalsete ohtude vastu, kasutades selleks sobivaid meetmeid nagu *Windows Update* 'i, *Service Pack* 'e ja *Hotfix* 'e. Ka neil juhtudel, kus nimetatud värskendused suudavad kõrvaldada turvaauke ja neid tuleks seetõttu paigaldada olemasoleva struktuuri alla võimalikult operatiivselt, tuleb vastavaid värskendusi ajasurvele vaatamata eelnevalt testimiskeskkonnas testida, kuna vastasel korral ei tuvastata õigeaegselt kasutuskeskkonnas ilmnevaid võimalikke negatiivseid mõjusid.

Teenustega seotud administraatorikontode turvalisus
Kataloogiteenuse juhtimise, konfigureerimise ja käitamisega seotud vastutust tohiks anda ainult usaldusväärsete isikute kanda. Vastav isikute ring peab tundma institutsiooni kehtivaid turvapoliitikaid ning nad peavad näitama üles omapoolset valmisolekut vastavate poliitikate järjepidevaks rakendamiseks. Teenuseid haldavate administraatorite pääsuõigused peaksid olema piiratud vajaliku miinimumini ning neid tuleks kasutada vaid selliste tööülesannete täitmiseks, mis eeldavad laiendatud volituste kasutamist. Vajalike minimaalsete volituste jagamiseks teenuste haldamisega seotud administraatoritele tuleb pääsuõigusi regulaarselt kontrollida ja neid vajadusel kohandada. Ka administraatorikontode arv tuleks hoida võimalikult väike, piirdudes hädavajaliku miinimumiga. Administraatorikontode puhul on ilmtingimata vajalik, et nende puhul kasutataks piisavalt tugevaid paroole. Kaaluda tuleks tugeva autentimisprotseduuri rakendamist nagu nt täiendavate kiipkaartide kasutamist operatsioonisüsteemi sisselogimisel.

Lähteinfo värskuse tagamine
Mõiste alla lähteinfo koondatakse kõik *Active Directory* olulisemad konfiguratsiooniparameetrid. Lähteinfo peaks sisaldama vähemalt järgnevaid punkte:

- Seirepoliitikad
- Grupipoliitika objektid ja nende jaotumine
- Olemasolevad usaldussuhted

- Domeenikontrollerite ja teenuseadministraatorite organisatoorne turvalisus
- Käitamisega seotud *Master* -funktsioonide omanikud
- Replikeerimise topoloogia
- Andmebaasiomadused
- Domeenikontrolleritele ja administraatorite tööjaamadele paigaldatud *Service Pack*'id ja *Hotfix*'id ja nende värske süsteemiseisund
- Olemasolevad andmevarunduseks mõeldud andmekandjad
- Andmevarunduse andmekandjate kontroll
- Teenuseadministraatorite hetkel vajalike volituste kontroll

Dokumenteeritud lähteinfo alusel on võimalik tuvastada ja kontrollida *Active Directory*'s tehtud muudatusi. Kõikide domeenikontrollerite lähteinfo tuleks kokku koguda ühtsesse lähteandmebaasi. Vastav andmebaas võimaldab lisaks muule saada ülevaadet hetkel kasutuses olevatest komponentidest. Lähteinfoga tegelemiseks tuleb määrata vastutav töötaja.

Täiendavad kontrollküsimused:

- Kas kiirparandusi (*Hotfix*'e) ja remondipakette (*Service Pack*'e) paigaldatakse regulaarselt?
- Kas kiirparanduste (*Hotfix*'ide) ja remondipakettide (*Service Pack* 'ide) võimalikke mõjusid kontrollitakse enne paigaldamist testimiskeskkonnas?
- Kas teenuseadministraatorite õigused on piiratud nende tööks vajaliku miinimumini? Kas seda kontrollitakse regulaarselt?
- Kas lähteinfos kajastatakse kõiki vajalikke parameetreid?

M 4.316 Active Directory infrastruktuuri monitooring

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: administraator

Active Directory infrastruktuuri turbeseisundit kontrollitakse ja hinnatakse süsteemis asetleidvate sündmuste logimise abil. Logide põhjalikkust tuleb kohandada vastavalt konkreetsetele vajadustele ning seda tuleks pidevalt jälgida. Logiandmeid tuleb analüüsida regulaarselt. Lisaks tuleks neid analüüsi käigus võrrelda etalonväärtustega, mida on võimalik tuletada nt varasemate andmete põhjal.

Active Directory

Seire raames koostatud logiandmeid võib analüüsida sõltuvalt tekitatud andmemahust kas käsitsi või spetsiaalse seiretarkvara abil. Suurte Active Directory-struktuuride puhul ei pruugi seireandmete käsitsi analüüsimine siiski enam kõne alla tulla. Turvalisust kajastava seire tulemused tuleks kokku võtta regulaarselt koostatavatesse aruannetesse ning need tuleks läbi analüüsida, et määrava tähtsusega turvaprobleeme oleks võimalik varakult tuvastada ja likvideerida. Logimisel võib esineda turvahoiatusi, millele tuleb kohe reageerida, lähtudes seejuures ettevõtte või asutuse avariiplaanist (vt M 6.106z Kataloogiteenuse hädaolukorraks valmisoleku plaani koostamine). Domeenikontrolleri või Active Directory turvalisust puudutavate konfiguratsiooniparameetrite muudatuste tuvastamiseks on võimalik rakendada kahte erinevat meetodit. Üheks võimaluseks on sündmusest teavitamine, teiseks trendianalüüsid. Sündmusest teavitamise puhul määratletakse Active Directory 's või domeenikontrolleris endas konfiguratsiooniparameetrite muudatuste piirväärtused. Kui konfiguratsiooniparameetri muudatusega kaasneb eeldefineeritud piirväärtuse ületamine, kajastab operatsioonisüsteem seda oma logis. Trendianalüüsi raames toimub pikema aja jooksul regulaarsete ajavahemike tagant ja eelnevalt määratud parameetrite alusel kogutud andmete analüüsimine.

Kui nende andmete analüüsimisel tuvastatakse ekstreemseid muudatusi, võib see olla märk võimalike turvaintsidentide leidumisest. Näiteks kui kõvaketta vaba ruumi kontrollitakse regulaarsete ajavahemike tagant (nt iga 5 min järel) ja märgatakse tarbitud kettamahu järsku tõusu, võib see viidata domeenikontrolleri vastu suunatud Denial-of-Service ründele (DoS-ründele).

Muudatused domeenikontrolleri seisundis

Domeenikontrolleri muutmine võib ohustada Active Directory turvalisust. Seega peaks seiresüsteem kajastama vähemalt selliseid domeenikontrolleri valdkondi nagu käideldavus ja süsteemiressursid:

- Domeenikontrollerite käideldavuse seireks on erinevaid võimalusi. Kasutada saab nt eriotstarbelist seiretarkvara. Alternatiivina võib domeenikontrollerile saata ka regulaarseid LDAP-päringuid. See meetod võimaldab selgitada, kas vastav domeenikontroller on aktiivne (test-klient saab vastuse), lisaks saab vastuse laekumisele kuluva aja põhjal teha järeldusi ka domeenikontrolleri süsteemikoormuse üle.
- Samuti tuleb tagada, et märkamata ei jääks domeenikontrolleri taaskäivitamised, kuna domeenikontrollerite volitamata taaskäivitamine võib olla märk

võimalikust ründest. Seetõttu tuleb kontrollida asutuses kõikide domeenikontrollerite süsteemisündmuste logisid, et teha kindlaks, kas süsteemides on esinenud volitamata taaskäivitamist või mitte.
- Lisaks domeenikontrollerite enda käideldavusele tuleks seires kajastada ka domeenikontrollerite süsteemiressursse. Süsteemiressursside muutumine ei tähenda alati ilmtingimata rünnet. Põhjus võib olla ka tehniline, nt kas vale konfiguratsioon või vananenud riistvara kasutamine üha kasvavate Active-Directory- struktuuridega.

Asutuses tuleks jälgida kõikidel domeenikontrolleritel järgnevaid süsteemiressursse ja ebatavaliste väärtuste puhul võtta tarvitusele sobivad vastumeetmed:

- Protsessori protsentuaalne koormus (ülemine piirväärtus: 80%)
- Active Directory andmebaasi sisaldava andmekandja vaba salvestimaht protsentides (alumine piirväärtus: 25%)
- Vaba töömälu protsentides (alumine piirväärtus: 10%)
- LDAP-ühenduste kestus (silmatorkavaks võib lugeda ühenduse kestuse ebatavaliselt tugevat tõusu)
- Edukate LDAP-ühenduste arv sekundis (silmatorkavaks võib lugeda LDA-Pühenduste arvu ebatavaliselt tugeva tõusu. Vastav piirväärtus sõltub seejuures organisatsioonisiseste LDAP-ühenduste poolt tekitatavast andmehulgast).

Muudatused Active Directory's

Kui muudatusi tehakse domeeni tasandil, mõjutavad need tavaliselt kõiki domeenikontrollereid, süsteemi kuuluvaid servereid, kasutajaid ja tööjaamu.

Selles kontekstis on mõeldavad alljärgnevad muudatused:

- Domeeniülese käitamisega seotud master -funktsiooni muutmine - Domeeniülese käitamisega seotud master -funktsiooni muudatused mõjutavad kogu domeeni. Domeeniülese käitamisega seotud master -funktsioonide alla kuulub muuhulgas peamise domeenikontrolleri (PDC) emuleerimis-master. See võib vale konfiguratsiooni korral mõjutada negatiivselt domeeni üldstruktuuri ja tekitada võrgus ulatuslikke probleeme. Käitamisega seotud master-funktsioonide muutmist on seega vaja hoolikalt planeerida.
- Usaldussuhete muutmine - Organisatsiooni või ametiasutuse erinevate domeenide vahel saab sisse seada usaldussuhteid. Usaldussuhete muudatusi tuleb kindlasti jälgida, kuna eriti just usaldussuhete lisamine ja seega domeenikasutaja võimalik volituste laienemine on olukorrad, mis vajavad kiiret tuvastamist.
- AdminSDHolder 'i muutmine - AdminSDHolder -objekti kasutatakse peamises domeenikontrolleris (PDC), et kaitsta teenuseadministraatorite gruppide kasutajaid ja teenuseadministraatorite gruppi ennast volituste loata muutmise eest. Seega peaks peamine domeenikontroller (PDC) kord tunnis

kontrollima, kas eelnevalt nimetatud kasutajakontode puhul kattuvad kasutajate endi määratavad pääsuloendid (DACLid, Discretionary Access Control Lists) vastava AdminSDHolder -objekti DACLiga. Kui DACLid erinevad üksteisest, tuleb kasutajakontode DACLid kohandada AdminSDHolder -objekti seadistusele vastavaks.

- Grupipoliitika objektide ja nende seoste muutmine - Grupipoliitika muudatused, nt domeenikasutajate paroolisuuniste muudatused mõjutavad domeeni ja seega kõiki vastava domeeni domeenikontrollereid, mistõttu tuleb neid jälgida. Lisaks sellele tuleb seire all hoida ka grupipoliitika objektide määramist domeenikonteineritele, samuti grupipoliitika objektide määramist organisatsiooniüksusele „Domeenide-kontroller“.
- Eeldefineeritud teenuseadministraatorite gruppide liikmelisuse muutmine - Kasutajate loata lisamine või kasutajate eemaldamine eeldefineeritud teenuseadministraatorite gruppidesse, nt gruppi administraatorid või varunduse operaatorid, võib olla märk ründest. Seetõttu tuleb teenuseadministraatorite gruppide liikmelisuses asetleidvaid muudatusi jälgida.
- Domeeni seirepoliitika muutmine - Seirepoliitika loata muutmine võib seireprotsessi häirida või selle täielikult desaktiveerida. Seire desaktiveerimise tuvastamiseks peavad seires olema kajastatud ka seirepoliitikad.

Kui tehakse muudatusi, mis mõjutavad kogu Active Directory struktuuri, nt organisatsiooni või ametiasutuse kõiki defineeritud domeene, on tegu tervikstruktuuri muudatustega.

Tervikstruktuuri muudatused hõlmavad alljärgnevaid sündmusi:

- Muudatused domeenikontrollerite liigituses - Kui domeenikontrollerit liigutatakse hierarhias üles või alla, on tegu domeenikontrolleri liigituse muutmisega.
- Muudatused Active Directory skeemis - Kataloogiteenuse andmebaasi struktuuri muutmine, nt objektiklasside või atribuutide muutmine Active Director's, toob endaga kaasa muudatused ka Active Directory skeemis.
- Muudatused LDAP-poliitikates - LDAP-poliitikate abil saab piirata LDAPpäringuid ja seega ka LDAP kaudu toimivat juurdepääsu Active Directory andmetele.
- Muudatused domeenikontrollerite vahel asetleidva replikeerimise topoloogias - Replikeerimise topoloogia muudatuste all mõistetakse Active Directory asukohtade, asukohtade otseteede ja alamvõrkude loomist, kustutamist ja muutmist.
- dSHeuristic -atribuudi muutmine - dSHeuristic -atribuut juhib Active Directory käitumist, selle kaudu saab näiteks aktiveerida või desaktiveerida objektide loendit.
- Tervikstruktuuri hõlmavad käitamisega seotud master -funktsioonide muudatused - Tervikstruktuuri hõlmavaid, käitamisega seotud master -funktsioonide muudatusi nimetatakse ka Flexible Single Master Operation'iteks (FSMOdeks). FSMOde alla kuulub skeemi ja domeeni master -funktsioon.

Kõiki eelnimetatud muudatusi kajastavaid sündmusi tuleb niihästi üksiku domeeni kui ka tervikstruktuuri tasandil kõikidel domeenikontrolleritel jälgida ning vastava seire tulemusi tuleb pidevalt analüüsida. Kui domeenikontrolleri turvaseire logi analüüsimisel tuvastatakse volitamata muudatus, tuleb rakendada vastavaid avariimeetmeid (vt M 6.106z Kataloogiteenuse hädaolukorraks valmisoleku plaani koostamine). Teatud sündmuste puhul ei ole logifailidest näha, milliseid objekte või atribuute on muudetud. Seega tuleb Active Directory skeem ilmtingimata dokumenteerida, et muudatusi saaks hiljem käsitsi võrreldes tuvastada ja tühistada.

Kui kõikide Active Directory volitamata muudatuste täielikku tühistamist pole võimalik tagada, tasub kaaluda tervikstruktuuri taastamist.

Grupis „Teenuseadministraatorid“ tuleb jälgida kasutajakontode loomist, kustutamist ja muutmist. Lisaks tuleb jälgida administraatorite tööjaamade lisamist või kustutamist organisatsiooni allüksuses „Teenuseadministraatorid“. Kui Active Directory andmebaasi salvestimaht domeenikontrolleril on otsas, ei saa Active Directory ’sse enam uusi objekte lisada. Seega tuleks Active Directory objektide poolt kasutatavat salvestimahtu pidevalt jälgida.

Selline seire võimaldab lisaks Active Directory andmebaasi otsasaava salvestimahu märkamisele ära tunda ka massilise objekt-ülekoormamise abil tehtavaid ründeid, mille puhul salvesti vaba maht lühikese aja jooksul järsult väheneb. Tagamaks kiiret reageerimist massilise objekt-ülekoormamise ründele, võib domeenikontrollerile paigaldada suvalises suurusega abifaili. Salvestimahu ründamise puhul saab vastaval domeenikontrolleril abifaili kustutada, et tekitada kiirelt juurde vaba ruumi ja tagada seeläbi normaalse töö jätkumine. Järgmise sammuna tuleb leida ja eemaldada Active Directory ’s soovimatud ründega seotud objektid.

Kriitilise tähtsusega failide muudatused

Nii domeenikontrolleritele kui ka administraatorite töökohtadele tuleks paigaldada seiresüsteem, mis tuvastaks kriitilise tähtsusega failide muutmise. Seejuures tuleks hoida seire all vähemalt neid faile, mida kasutatakse operatsioonisüsteemi või paigaldatud rakenduste konfigureerimiseks. Lisaks sellele tuleks muudatuste seire all hoida ka olulisi käitusfaile, nt administraatorite tarkvaratööriistu administraatorite töökohtadel. Süsteemikonfiguratsiooni seire jaoks tuleb esmalt valida sobilik tarkvara. Seejärel tuleks koostada seire alla kuuluvate operatsioonisüsteemide usaldusvääne aluskonfiguratsioon.

Seiretarkvara abil luuakse selle aluskonfiguratsiooni põhjal võrdluspilt, mida kasutatakse edasiste kontrollide alusmaterjalina. Regulaarselt tuleb kontrollida, kas domeenikontrolleris või administraatorite töökohtades hetkel kehtiv konfigu-

ratsioon on aluskonfiguratsiooniga võrreldes muutunud. Muudatuste tuvastamisel tuleb võimalikult ruttu taastada süsteemi esialgne seisund.

Kontrollküsimused:

- Kas Active Directory infrastruktuurile rakendatakse seiremeetmeid?
- Kas turvaseire tulemusi analüüsitakse regulaarselt?
- Kas domeenikontrolleri käideldavust ja süsteemiressursse jälgitakse? Kas seire suudab tuvastada nt domeenikontrolleri volitamata taaskäivitamised, protsessori kõrge koormuse, täis andmekandjad ja vaba töömälu nii pikaajaliste trendide kui ka nende lühiajaliste esinemiste lõikes?
- Kas muudatusi domeeni tasandil ja Active Directory tervikstruktuuris logitakse ja analüüsitakse?

M 4.317z Windowsi kataloogiteenuste turvaline migratsioon

Algatamise eest vastutavad: IT-juht, IT-turbespetsialist

Rakendamise eest vastutavad: administraator

Paremate funktsioonide, suurema turvalisuse, suurema ühilduvuse ja tootjate toe vaatepunktist on soovitatav kasutatavad Windowsi operatsioonisüsteemid ajakohastada.

Enne üleviimist tuleb planeerimisfaasis selgeks teha:

- Milliseid servereid/teenuseid saab konsolideerida?
- Kas kasutatud (siht-)riistvara on piisava jõudlusega ja vastab suurenevatele süsteeminõuetele?
- Kas võrgukeskkonnas vajalikud teenused ühilduvad uuema tarkvaraga (logid, õigused jne)?

Vanemate operatsioonisüsteemide all juba olemasolevad funktsioonid, nt DNS ja Active Directory, muutuvad üleviimisega uuematele süsteemidele veelgi täiuslikumaks. Enamasti tuleks üleviimist katsetada esmalt testimiskeskkonnas, et tagada seeläbi saadud tulemuste abil võimalikult optimaalne tootmissüsteemi üleviimine.

DNSi kasutamine

Tuleb jälgida, et Active Directory funktsioonide kasutuselevõtuga toimuks võrgusisene nimeteisendus DNSi abil. Sellest tuleneb nõue varustada üleviidud võrk DNS-teenusega. Lisainfot selle kohta leiab tootja artiklist Deploying Domain Name System, mis asub Microsofti TechNetis (http://technet.microsoft.com).

Grupipoliitikad

Windowsi serveri all saab kasutada grupipoliitika täiendust, mis võimaldab objekte Active Directory struktuuris põhjalikumalt hallata.

Üleviimise piirangud

Peamise domeenikontrolleri (PDC) üleviimise ajal ei saa seda kasutada, seega peavad kliendipoolsed sisselogimised ja ressursside poole pöördumised toimuma varu-domeenikontrolleri (Backup Domain Controller 'i, BDC) kaudu. Üleviimise ajal ei saa teha domeeni puudutavaid muudatusi, nt vahetada paroole või luua kasutajakontosid.

Upgrade 'i kontroll

Järgmise sammuna enne olemasoleva operatsioonisüsteemi struktuuri väljalülitamist tuleb testida ja hinnata Upgrade-protsessi edukust. Kontrollitavate komponentide detailse info, mis puudutab õiget konfiguratsiooni ja funktsioone, leiate IT etalonturbe abimaterjalide hulgast (vt Active Directory't käsitlevate abimaterjalide alt Üleviidud kataloogiteenuseandmebaasi kontrollimine), (sks Prüfung der migrierten Verzeichnisdienst).

Planeerimise käigus määratakse serverirollid, näiteks süsteemi kuuluv server või täiendav domeenikontroller, mida tuleb samuti pärast nende sisseseadmist põhjalikult testida.

Serverikeskkonna värskendamine

Laiendatud funktsioonivaliku kasutamiseks, eriti just Windowsi serveri haldamiseks Active Directory abil, tuleks viimase sammuna värskendada serverikeskkonda. Seejuures tuleb eriti arvestada sellega, et pärast süsteemi värskendamist ei toetata enam käesolevast süsteemist vanemaid versioone.

Kontrollküsimused:

- Kas pärast üleviimist värskendati serverikeskkonda?
- Kas pärast üleviimist testiti kõikide andmete ja seadistuste õiget ülevõtmist ja funktsioneerimist?

M 4.318 Active Directory turvaliste haldusmeetodite rakendamine

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: administraator

Domeeni administreerimiseks jaotatakse vastutusalad ja ülesanded alamgruppidesse. Kuna kasutajakontod, mis on seotud haldusgruppidega „Teenuseadministraatorid“ (vastutavad tööde eest, mis on vajalikud kataloogiteenuse tööshoidmiseks) ja „Andmeadministraatorid“ (vastutavad Active Director'sse salvestatava või Active Directory poolt kaitstud sisu haldamise eest) omavad eriti laiaulatuslikke pääsuõigusi, tuleb selliste kasutajakontode kaitseks võtta tarvitusele sobilikud meetmed:

Teenuseadministraatorite kontod

Igas tervikstruktuuri domeenis luuakse installeerimisel standardne konto „Administraator“. Standardse kontona on see kasutajakonto väga suurel määral rünnetele avatud. Kuna administraatorikontot ei saa desaktiveerida ega kustutada, tuleks see kaitsmise eesmärgil ümber nimetada. Ümbernimetamisel tuleb jälgida, et muudetud saaks ka administraatorikonto kirjeldus. Pärast konto ümbernimetamist tuleks luua nime „Administraator“ alla privileegideta konto, mida ei tohi igapäevases kasutada. Logiandmete analüüsimisel saab seeläbi tuvastada, kas sellesse privileegideta kasutajakontosse tehtud sisselogimiskatsed on osutunud edukateks või ebaõnnestunud. See oleks märk võimalikest rünnetest.

Teenuse- ja andmeadministraatorite kontode arv tuleks hoida võimalikult minimaalne. Rutiinseid administreerimis- ja haldusülesandeid, mis ei puuduta Active Directory konfiguratsiooni ennast, nt domeenikasutajate haldamine, ei peaks täitma mitte teenuseadministraatorid, vaid sellised ülesanded tuleks delegeerida andmeadministraatoritele. Administraatorikontosid tuleks kasutada võimalikult säästlikult. Administraatoriõigustega asjatut sisselogimist domeeni tuleks vältida. Seega peaksid asutuse administraatorid kasutama igapäevaste, mitteadministratiivsete ülesannete jaoks (nt info otsimiseks Internetist) privileegideta kasutajakontosid. Teenuseadministraatorite kontosid võivad hallata ainult teenuseadministraatorite grupi liikmed. Eriti just vähemate privileegidega kasutajad, näiteks andmeadministraatorid, ei tohi muuta teenuseadministraatorite kontosid, kuna sellega saaksid vähemate privileegidega kasutajad oma õigusi oluliselt laiendada. Seega tuleks teenuseadministraatorite kontode haldamiseks luua Active Directory kasutajahaldusesse eraldi organisatsiooni allüksus, näiteks teenuseadministraatorid.

Selle alamstruktuuri volitused tuleb valida järgnevalt:

- Desaktiveerida hierarhias kõrgemalasuvate objektide volituste pärimine
- Anda pääsuõigused sisseseatava organisatsiooni allüksuse jaoks (kaasaarvatud hierarhias allpool asuvad objektid)
- Administraatorid: täielik juurdepääs
- Organisatsiooni administraatorid: täielik juurdepääs
- Domeeni administraatorid: täielik juurdepääs

- Varasemate versioonidega ühilduvad kasutajaobjektide pääsuõigused (kui vajalik)
- Sisu loetlemine
- Kõikide omaduste lugemine
- Volituste lugemine

Teenuseadministraatorite grupid (domeeniadministraatorid, organisatsiooniadministraatorid ja skeemiadministraatorid) tõstetakse lõpuks uude alamstruktuuri. Lisaks tuleb domeeniadministraatorite administratiivsed kasutajakontod teisaldada organisatsiooni allüksusesse „Kasutajad ja grupid“ ja tööjaamade kontod uue alamstruktuuri organisatsioonistruktuuri alla „Administraatorite tööjaamad“. Seejuures tuleb arvestada asjaoluga, et domeenikontrolleri kontosid ei tohi ümber tõsta. Lisaks tuleks seire abil jälgida nii muudatuste logimist, teenuseadministraatorite kontode ja tööjaamade kustutamist ja loomist kui ka poliitika muutmist. Kuna mõningaid juba eelnevalt määratletud teenuseadministraatorite kontosid ei saa uude alamstruktuuri teisaldada, tuleb neid kontosid eriti hoolikalt kaitsta.

Active Directory's kontrollitakse kaitstud teenuseadministraatorite kontosid regulaarselt. Seejuures kirjutatakse kaitstud kontode turvaseadistused üle AdminSDHolder-objekti turvasätetega (süsteemikonteineris “CN= AdminSDHolder, CN=süsteem, DC=domeeni nimi”). Vastav protsess, millega ülekirjutamist algatatakse, käivitub kindlalt etteantud intervallide alusel (15 minutit pärast süsteemi käivitamist ja seejärel iga poole tunni järel).

Teenuseadministraatorite gruppi kuuluvad isikud peavad olema usaldusväärsed ja omama piisavaid teadmisi Active Directory administreerimise kohta. Tagamaks asutuses kehtivate turvapoliitikate järjepidevat rakendamist, peavad teenuseadministraatorid tundma vastavaid poliitikaid. Teenuseadministraatorite grupi liikmete nimekiri peab eranditult koosnema asutusesisese Active Directory tervikstruktuuri kasutajatest. Kui usaldatakse eemalasuva domeeni teenuseadministraatoreid, usaldab asutus automaatselt ka eemalasuva asutuse turvameetmeid. Kuna vastavaid turvameetmeid ei saa tavaliselt mõjutada, tuleb asutusevälistе kasutajate jaoks luua asutusesiseses tervikstruktuuris eraldi kasutajakonto. See võimaldab juurdepääsu asutuse domeenile paremini reguleerida ja kasutajad ei pääse ligi domeenidele, mille õigused pole automaatsete usaldussuhete tõttu teada.

Ulatuslike volituste tõttu on teenuseadministraatorite kontod eelistatud ründesihid. Seega on kõrgendatud turvanõuete puhul soovitatav keelata privileegideta kasutajate jaoks kõikide teenuseadministraatori gruppide kuuluvusinfo nägemine. Seejuures tuleb siiski arvestada, et teatud serverirakendused vajavad tõrkevaba töö tagamiseks lugemisõigusega juurdepääsu teenuseadministraatorite liikmete nimekirjale. Seega tuleb esimese sammuna tuvastada, kas asutuses kasutatakse selliseid serverirakendusi või mitte. Kasutajakontod, mille all tuvastatud serveriprotsesse käivitatakse, tuleb koondada eraldi gruppi, nt gruppi nimega Serverira-

kendused.

Seejärel määratakse sellele grupile AdminSDHolder -objekti pääsuloendis järgnevad volitused:

- Sisu loetlemin
- Kõikide omaduste lugemine
- Volituste lugemine

Juurdepääsu saab seeläbi piirata autenditud kasutajatega, kellel peab olema liikmete nimekirja lugemisõigus. Kuna teenuseadministraatorite gruppide grupikuuluvuste varjamine võib mõjutada käitamist, on tungivalt soovitatav ülalkirjeldatud AdminSDHolder -objekti sisseviidavaid muudatusi eelnevalt võimalike mõjude suhtes kontrollida.

Active Directory grupi „Varunduse operaatorid“ liikmeid tuleb põhimõtteliselt käsitleda teenuseadministraatoritena, kuna nad saavad taastada domeenikontrolleri süsteemifaile. Nende kasutajagruppide liikmete arv peaks olema võimalikult väike. Seega ei tohi administraatoreid, kes vastutavad Active Directory piires rakendusserverite varundamise ja taastamise eest, kanda Active Directory gruppi „Varunduse operaatorid“. Selle asemel tuleb vastavad kasutajakontod paigaldada rakendusserverite lokaalsetesse gruppidesse „Varunduse operaatorid“. Active Directory gruppi „Kontode operaatorid“ ei tohiks kasutada andmete haldamiseks, nt kontode haldamiseks, kuna selle liikmed saavad oma õigusi ise laiendada. Sel põhjusel ei tohiks grupis „Kontode operaatorid“ olla mitte ühtegi liiget. Sama kehtib Active Directory grupi „Skeemiadministraatorid“ kohta. Kuna muudatused Active Directory skeemis on üldjuhul väga haruldased, tuleks usaldusväärseid administraatoreid hoida grupis „Skeemiadministraatorid“ ainult seni, kuni neil vastavaid volitusi tegelikult vaja läheb. Niipea kui skeemimuudatused on tehtud, tuleks liikmed taas grupist eemaldada.

Asutuse Active Directory tervikstruktuuri tüvidomeeni gruppide „Organisatsiooniadministraatorid“ ja „Domeeniadministraatorid“ kasutajakontod vajavad oma laiaulatuslike volituste tõttu eriti tugevat kaitset. Seega peaks iga sellise konto jaoks määrama kaks administraatorit ja parooli nende vahel pooleks jagama. Kahest administraatorist tohib kumbki teada vaid poolt parooli, et kasutajakontos saaks töötada ainult nelja silma põhimõtte alusel. See aitab vältida tüvidomeeni teenuseadministraatorite kontode märkamatut kasutamist Active Directory tervikstruktuuris. Nelja silma põhimõtte kehtestamiseks on võimalik kasutada ka muid meetodeid, nt kiipkaarti, mille puhul üks kasutaja teab PINi ja teine omab kiipkaarti.

Lisaks teenuse- ja andmeadministraatori kontode kaitsmisele vajavad järgnevat kaitset ka administraatorite töökohad:

- Administraatorite kasutajakontod tuleb luua selliselt, et kontosid saaks kasutada ainult konkreetsetes töökohtades. Kompromiteeritud administraatorikontosid saab niimoodi kasutada ainult kindlates tööjaamades.
- Kui kasutaja on 5 minutit passiivne, peab aktiveeruma automaatne tõkestus. Seejuures tuleb jälgida, et konsoolitõkke tühistamiseks ei saaks kasutada vahemälu andmeid; selle asemel tuleb ennast uuesti domeenikontrolleris autentida.
- Administraatorite tööjaamades tuleb kasutada viirusetõrjetarkvara.
- Rakendusi ei tohiks käivitada administraatoriõigustega. Uue tööjaama lisamisel domeeni tuleb jälgida, et domeeniadministraatoreid ei lisataks automaatselt tööjaama administraatorite lokaalsesse gruppi.
- Protsesse ei tohiks käivitada domeeniadministraatorite volitustega. Selle asemel tuleks kasutada vastava tööjaama lokaalse administraatorigrupi turvakonteksti.
- Administraatorite tööjaamade ja domeenikontrollerite vaheline andmeside peab olema vastavalt turvatud. Selleks tuleks aktiveerida LDAP-pakettsignatuurid (selleks tuleb Windowsi registris registrivõtme LDAPClientIntegrity väärtuseks asukohas HKLM\System\CurrentControlSet\Services\LDAP\ määrata “2”).

Domeenikontrollerite kaugadministreerimiseks tuleks eranditult kasutada andmeside krüpteerimist võimaldavaid protokolle.

Andmeadministraatorite kontod

Andmeadministraatori kontode struktuurid ja volitused sõltuvad üldjuhul oluliselt neid kasutava asutuse struktuurist. Järgnevalt loetletud aspektide puhul tuleb kindlaks teha, kas neid on võimalik ühildada organisatsiooni nõuetega.

Andmehaldamise delegeerimine toimub gruppide kaudu, millele anti vastavad kasutajaõigused.

Nende gruppide liikmetele rakendatakse grupipoliitika seadistusi.

Nende sammude järel piisab delegeerimiseks kasutajakontode lisamisest loodud gruppidesse. See tagab suurima võimaliku turvalisuse ja administraatorid saavad oma ülekantud ülesandeid jätkuvalt täita. Juurdepääs grupipoliitikale peab piirduma usaldusväärsete isikutega. Kasutajad, kelle kontod võimaldavad grupipoliitika seadistusi luua ja muuta, saavad nende poliitikate kaudu määrata teistele kontodele suuremaid volitusi ning seetõttu peavad need isikud olema usaldusväärsed.

Andmeadministraatorid on objektide loojatena samaaegselt ka nende omanikud.

Tuleb tagada, et grupid „Administraatorid“ või „Domeeniadministraatorid“ oleksid üksikutes domeenides vastava domeenipartitsiooni domeeni tüviobjekti omanikud. Nende partitsioonide omanikud saavad päritavate pääsusissekannete

(Access Control Entries, ACE'de) kaudu muuta kõikide teiste selle partitsiooni objektide turvaseadistusi. Tuleb tagada, et kontode haldamise ülesannete planeerimisel muudaks grupikuuluvust delegeeritud alas kas ainult üks kindel andmeadministraator või et ülesande täitmine toimuks väheste andmeadministraatorite kooskõlastamisel. Kui replikeerimise raames tuvastatakse erinevate domeenikontrollerite poolt tehtud grupikuuluvuse kaks samaaegset muudatust, jääb kehtima värskeim kontomuudatus. Serveri replikeerimiseni kehtib vastavas serveris tehtud muudatus.

Globaalses kataloogis replikeeritavate objektiatribuutide lugemisõiguste juhtimiseks tuleks vältida domeeni lokaalgruppide kasutamist, kuna seejuures võidakse kogemata objektijuurdepääse keelata või lubada. Globaalse kataloogi andmete juurdepääsude juhtimiseks tuleks selle asemel kasutada globaalseid või universaalseid gruppe.

Kontrollküsimused:

- Kas teenuseadministraatorite ja andmeadministraatorite kasutajakontod on piisavalt kaitstud?
- Kas nende gruppide liikmeteks on võimalikult väike arv usaldusväärseid isikuid?
- Kas standardne konto „Administraator" nimetati ümber ja loodi privileegideta konto nimega „Administraator"?
- Kas rutiinsed administreerimis- ja haldusülesanded delegeeriti teenuseadministraatoritelt andmeadministraatoritele?
- Kas igapäevaseid, mitteadministratiivseid ülesandeid tehakse privileegideta kasutajakontode alt ning kas asjatuid administratiivsete õigustega domeeni sisselogimisi välditakse?
- Kas on tuvastatud, millised serverirakenduste kasutajakontod vajavad lugemisõigust teenuseadministraatorite liikmete nimekirjale ja kas kõikide privileegideta kasutajate puhul on juurdepääs sellele infole keelatud? Kas lugemisõigusega kasutajakontod on koondatud ühte kasutajagruppi?
- Kas grupi „Varunduse operaatorid" liikmete arv on viidud miinimumini?
- Kas grupp „Kontode operaatorid" on tühjaks jäetud?
- Kas grupi „Skeemiadministraatorid" alla kuuluvad administraatorid määratakse ainult ajutiselt skeemimuudatuste ajaks?
- Kas tüvidomeeni administreerimisel rakendatakse gruppide „Organisatsiooniadministraatorid" ja „Domeeniadministraatorid" puhul nelja silma põhimõtet?
- Kas administraatorite töökohad on piisavalt kaitstud?
- Kas domeenikontrollerite kaugadministreerimisel asetleidev andmeside krüpteeritakse?
- Kas tagatakse, et grupid „Administraatorid" või „Domeeniadministraatorid" on ka vastava domeeni tüviobjekti omanikud?
- Kas objektiatribuutide lugemisõiguse juhtimisel välditakse domeeni lokaalgruppide kasutamist?

M 4.319 VPNi lõppseadmete turvaline installeerimine

Algatamise eest vastutavad: IT-turvaspetsialist, IT-juht

Rakendamise eest vastutavad: administraator

VPNi ülesehitamisega võib alustada kohe kui vajalikud komponendid on olemas (vt M 2.419 Sobivate VPN-toodete valimine). VPNi turvalise käitamise eelduseks on kõikide komponentide kohusetundlik paigaldamine ja konfigureerimine ja asjaolu, et väljavalitud VPN-tooted suudaksid vajalikke turvafunktsioone ka reaalselt täita. Lisaks tuleb tagada ka nende IT-süsteemide turvalisus, milles VPN-komponente kasutama hakatakse. See puudutab eriti neid IT-süsteeme, millele on paigaldatud standardne operatsioonisüsteem ja mida käitatakse VPNlõpp-punktina (näide: VPN-toega Linux-süsteem). Seega tuleb esmalt rakendada iga sellise operatsioonisüsteemi kohta kehtivaid üldisi turvameetmeid, lähtudes IT etalonturbe kataloogide vastavate moodulite kirjeldusest. Leidub ka selliseid VPN-komponente, mille puhul on platvormi konfiguratsioon tootja poolt määratud ning seda ei saa muuta (eraldiseisvad VPN-seadmed). Selliste VPN-seadmete kasutamine säästab ühest küljest aega ja erinevalt individuaalsest lahendusest nõuab see IT-personalilt vähem erialaseid teadmisi, nt vähem teadmisi operatsioonisüsteemi konfigureerimise kohta. Teisest küljest tuleb eraldiseisvate seadmete kasutamisel usaldada tootjate andmeid.

VPNi paigaldamise raames tuleks lisaks arvestada ka järgnevate punktidega:

- Installeerimisfaasi käigus ei tohiks ei kasutajatel ega ka kolmandatel isikutel olla juurdepääsu VPNile ega ka selle osadele. Selles faasis ei tohi olla ühendusi teiste võrkudega.
- Tuleb tagada, et kõikide VPN-komponentide installeerimisega tegeleks kvalifitseeritud personal. See võib eriti keeruliseks osutuda siis, kui ühendatavad asukohad asuvad üksteisest geograafiliselt kaugel. Näiteks tuleb selgitada, kas VPNi paigaldamiseks vajalikud personaliressursid on ka teistes riikides olemas. Ka mobiilsete infosüsteemide VPN-lõpp-punkte, nt töölähetuses olevate töötajate sülearvuteid, tohivad installeerida ainult kvalifitseeritud IT-töötajad.
- VPN-komponentide installeerimine ja konfigureerimine tuleb dokumenteerida. Selleks võib kasutada eraldiseisvat installeerimisdokumentatsiooni või ka kinnitust, et installeerimine kattub planeerimisfaasis väljatöötatud andmetega. Eelnevalt kindlaksmääratud süsteemiarhitektuurist kõrvalekaldumine (näiteks täiendavate ühenduste lisamine) tuleb seejuures põhjendada ja dokumenteerida. Dokumentatsiooni kvaliteet on VPNi pideva täiustamise vaatepunktist ülimalt oluline.
- Kontrollida tuleb iga üksiku komponendi õiget funktsioneerimist (nt viia läbi funktsioonitestimisi, st eneseteste (self tests) või koormuste).
- Toodetele tuleb enne kasutuselevõtmist paigaldada kõik turvalisuse seisukohalt olulised paigad ja püsivara värskendused.
- Igal turvalisuse seisukohalt olulise seadistuse puhul tuleb testida selle turvamehhanismide funktsioone. Näiteks tuleks võrguanalüüsi tööriista abil kontrollida ühenduse krüpteerimist, samuti kasutatud autentimisfunktsioone (vt

lisaks M 5.76w Sobivate tunneldusprotokollide kasutamine VPN-süsteemis).

- Enne kui süsteem võetakse igapäevaselt kasutusse, tuleb see üles seada tootmisvõrgust eraldatud keskkonnas ja vastavalt testida. Samuti on soovitatav juba testkeskkonnas mõõta jõudlust ja teha võtmete jaotamise proov.

Pärast installeerimise lõpuleviimist tuleb kontrollida, kas terviksüsteem töötab korrektselt (installatsiooni vastuvõtt ja kinnitamine). Kõikide tehtud testide käigus tuleb jälgida, et VPNile pääseksid ligi ainult testide tegemiseks volitatud isikud.

Kui peamised installeerimistööd on lõpule viidud, saab hakata looma meetmes M 4.320 VPNi turvaline konfigureerimine kirjeldatud konfiguratsiooni. See peab viima süsteemi turvalisse tööseisundisse, et seejärel võiks alustada igapäevast kasutamist. VPNi tõrgeteta käitamise jaoks on olulised meetmes M 4.321 VPNi turvaline käitamine loetletud sammud. Seejuures saadud teadmised ja korrigeerimisel abistavad meetmed tuleb vastavalt dokumenteerida ja lisada detailsesse kontseptsiooni.

Näide:

Järgnevalt on toodud näiteid olulisemate punktide kohta VPN-süsteemi installeerimisel. Kuna konkreetsed konfiguratsioonid sõltuvad tootjast, on siinkohal tegemist vaid üldise tutvustusega, mis ei ole kindlasti täielik.

Kaugpöörduseks rakendatava VPN-kliendi puhul tuleb installeerimisel arvestada järgnevate punktidega:

- VPN-teenuse serverifunktsioonid tuleb desaktiveerida. See tuleneb nõudest, et kõikides seadmetes, mida saab kaugpöörduse jaoks kasutada (nt modemites, ISDN-kaartides, VPN-adapterites), oleks lubatud ainult väljuvad kõned.
- VPN-kliendi puhul võib kasutada ainult kaugpöörduse jaoks heakskiidetud protokolle.
- VPN-turvakontseptsioonis määratletud parameetrid, mis puudutavad terviklust, autentsust ja konfidentsiaalsust, tuleb konfigureerida vastavalt vajadustele.

Kaugpöörduse VPN-serveri puhul tuleb arvestada järgnevate punktidega:

- VPN-teenuse klientfunktsioonid tuleb desaktiveerida. See realiseeritakse nii, et kõikidel kaugpöörduse jaoks kasutatavates seadmetes lubatakse ainult sisenevaid kõnesid.
- VPN-serveri puhul tuleks lubada kasutada ainult kaugpöörduseks lubatud protokolle.
- VPN-turvakontseptsioonis määratletud parameetrid, mis puudutavad terviklust, autentsust ja konfidentsiaalsust, tuleb konfigureerida vastavalt vajadustele.

- Sissevalimine peaks olema lubatud ainult volitatud kasutajatele.

Kontrollküsimused:

- Kui eraldiseisvaid seadmeid ei kasutata: kas VPN-platvormi aluseks olev operatsioonisüsteem on konfigureeritud turvaliseks?
- Kas VPN-komponentide installeerimisega tegeles kvalifitseeritud personal?
- Kas VPN-komponentide installeerimine ja konfigureerimine, samuti võimalik kõrvalekaldumine planeerimisel koostatud ettekirjutustest on dokumenteeritud?
- Kas VPN-komponentidele paigaldati kõik uuemad saadaolevad paigad ja värskendused?
- Kas VPN-komponentide funktsioone ja turvamehhanisme testiti?

M 4.320 VPNi turvaline konfigureerimine

Algatamise eest vastutavad: IT-juht, IT-turbespetsialist
Rakendamise eest vastutavad: administraator

Kõiki VPN-komponente tuleb hoolikat konfigureerida, kuna VPN-komponentide ebasobiv konfiguratsioon võib põhjustada olukorra, kus võrk või selle üksikosad kaotavad oma käideldavuse. Samuti on võimalik info konfidentsiaalsuse või andmetetervikluse kaotsiminek. Sõltumata sellest, kas VPN-komponentide puhul on tegu eraldiseisval riistvaral (*appliances*) või tarkvaral põhinevate süsteemidega, on komponentide õige konfigureerimine ülimalt oluline. Kuna VPN koosneb mitmest komponendist ja nende konfiguratsioonidest, on tervikkonfiguratsioon selle võrra keerulisem. Mõne komponendi konfiguratsiooniparameetri muutmine võib koostöös teiste komponentidega põhjustada turvaauke, tõrkeid ja/või avariisid. Kuna VPN-süsteemi konfiguratsioon muutub pidevalt (nt personali muudatuste, uute kasutusotstarvete lisandumise või süsteemi laiendamise tõttu), ei saa lähtuda sellest, et on olemas ainult üks turvaline (ja muutumatu) konfiguratsioon, mida tuleb vaid üks kord seadistada ja siis mitte kunagi enam muuta. Konfiguratsioon vajab reeglina pidevat muutmist. VPNi eest vastutavate administraatorite ülesandeks on tagada, et loodaks ainult turvalisi süsteemikonfiguratsiooni versioone ja et süsteem viidaks ühest turvalisest konfiguratsioonist üle järgmisele turvalisele konfiguratsioonile. Kõik muudatused ja hetkel kehtivad seadistused peavad olema selgelt dokumenteeritud.

Algseadistused

Turvaline konfigureerimine

VPN-komponentide tootjate või edasimüüjate poolt tehtud algseadistused ei lähtu ilmtingimata turvalisusest, vaid toote lihtsast paigaldamisest ja kasutuselevõtust. Algseadistuse puhul peab olema esimeseks sammuks selle kontrollimine ja kohandamine turvapoliitika nõuetega vastavaks. Standardsed paroolid tuleb asendada asutuse enda piisavalt keeruliste paroolidega.

Serveri konfiguratsioon

VPN-serveri tarkvara turvaline konfiguratsioon nõuab, et tarkvara poolt pakutavad ja kasutusotstarbe jaoks mõistlikud turvaseadistused peavad olema ka tegelikult aktiveeritud ja kasutuses. Mõningate turvaseadistuste kasutamine eeldab, et ka VPNi teised komponendid on vastavad funktsioonid või on vastavalt seadistatavad. Näiteks tuleb telefoninumbri edastamisel (*Calling Line Identification Protocol* - CLIP) tagada, et see oleks valitud ühenduse jaoks ka aktiveeritud. Selleks, et kasutajate identifitseerimine saaks Interneti kaudu toimuva juurdepääsu korral toimuda X.509-sertifikaatide alusel, peab VPN tundma kasutajate sertifikaatide salvestuskohta. Selleks peab VPN-tarkvara toetama välist autentimisserverit või pakkuma omapoolset sertifikaatide haldamist. Seega tuleks eelnevalt kontrollida, kas kõiki pakutavaid turvamehhanisme saab ka reaalselt kasutada või kas selleks läheb tarvis teistsugust ehk täiendavat riist- või tarkvara. Töö käigus tuleb regulaarselt kontrollida seadistuste korrektsust.

Kliendi konfiguratsioon

VPN-klienttarkvara turvalise konfigureerimise puhul kehtivad sarnased nõuded nagu servertarkvara puhul. Turvalise kommunikatsiooni võimaldamiseks kliendi ja serveri vahel tuleb tagada asjassepuutuvate komponentide ühtne konfiguratsioon

(nt kommunikatsiooni turvamiseks kasutatud protseduuride puhul). Lisaks tuleb jälgida, et tarkvara ei salvestaks VPN-juurdepääsuks vajalikke paroole, isegi kui seda võimalust korduvalt pakutakse. Kui salvestamist ei saa tehniliselt takistada, tuleb see kõikidele kasutajatele selgesõnaliselt ära keelata. Kasutajatele tuleb selgitada salvestatud paroolidega kaasnevaid turvaprobleeme.

Standardsete IT-süsteemide sisseseadmine

Kliendi ja serveri turvalist konfigureerimist saab toetada sellega, et VPN-kliendi (riist- ja tarkvara) standardne konfiguratsioon määratakse kindlaks VPN-kontseptsiooni poolt ja viiakse ellu organisatoorsete meetmete abil. Seeläbi saavutatakse olukord, kus kasutatakse ainult kindlat arvu erinevaid klientkonfiguratsioone.

Juurdepääsuvõrkude sisseseadmine

Lisaks VPNide konfigureerimisele saab juurdepääsude juhtimiseks jaotada ühendatud võrgud alamvõrkudesse. IT-turbe põhjustel võib siin olla vajalik sisse seada nn juurdepääsuvõrgud (*Access-Networks*) (vt M 5.77 Alamvõrkude rajamine).

Marsruutimisseadistused

Võrguliiklust tuleks piirata VPN-süsteemi jaoks kasutatavate võrguühenduse elementide marsruutimisseadistuste abil. Moodsad võrguühenduse elemendid võimaldavad pakette lubatud võrguühenduste piires (paketifiltri funktsioon) valikuliselt edasi saata. Sel moel võib näiteks saavutada olukorra, et serveri HTTP-teenusele edastatakse ainult ühenduspäringud. VPN-klientidele tohiksid ligi pääseda ainult volitatud kasutajad. VPNi juurdepääsude piiramine on eriti oluline just mobiilsete arvutite puhul. Vastasel juhul saavad mobiilse arvuti varguse korral volitamata isikud ennast VPNi sisse valida. Seetõttu peavad kasutajad kehtestatud reeglitest täpselt kinni pidama (nt turvaline autentimine ja vargusevastane kaitse, vt lisaks moodulit B 3.203 Sülearvuti). Mobiilseid VPN-kliente tuleks seadistada selliselt, et VPN-klienttarkvara käivitamise järel toimuks kogu andmeside ainult VPN-ühenduse kaudu. VPN-ühendusest möödaminev, teistesse võrkudesse suunatud andmeside tuleks keelata. Paljudel VPN-klient-toodetel on see seadistusvõimalus olemas.

Juurdepääsuõigused

Tuleb jälgida, et võimalikud testimisotstarbelised (nt installeerimise ajal testimiseks loodud) juurdepääsud ja kasutajatunnused eemaldataks. Lisaks tuleb antud pääsuõigusi regulaarselt kontrollida, et tagada vajalike funktsioonide kasutamine ja vältida valesti antud pääsuõiguste kuritarvitamist.

Kaugpöörduse juurdepääs

Hoolduse eesmärgil pakuvad aktiivsed võrgukomponendid tavaliselt kaugpöörduse võimalust. Administreerimiseks võib kaugpöördusi lubada ainult siis, kui on tagatud, et kasutajanime ja parooli ei edastata loetava teksti kujul (nagu nt Telneti puhul). Kui esineb võimalus lokaalse konfiguratsiooni loomiseks, tuleks eelistada seda ja kaugpöördus desaktiveerida.

Sisselogimisteade

VPN-komponentidesse sisselogimisel näidatakse sageli üsna põhjalikku sisselogimisteadet. Sisselogimisteade võib mõnikord sisaldada infot (nt mudeli või versiooni numbrit ja tarkvara versiooni), mida potentsiaalne ründaja saab kurjasti ära kasutada. Standardne sisselogimisteade tuleks võimaluse korral asendada kohandatud versiooniga, mis ei sisalda sellist infot. Sisselogimisteade ei tohiks turvalisuse põhjustel mingil juhul reeta seadme mudeli ja versiooni numbrit ega ka operatsioonisüsteemi versiooni.

Liidesed

VPN-komponentide mittekasutatavad liidesed on standardse seadistuse põhjal sageli aktiveeritud. Esmakordse installeerimise ja konfigureerimise käigus tuleb need seetõttu desaktiveerida, et vähendada ründevõimalusi.

Logimine

VPN-komponendid pakuvad tavaliselt logimisvõimalust, mis peab olema igal juhul aktiveeritud ja hoolikalt sisse seatud. Vastava logiinfo analüüsimine võimaldab hinnata seadme töökindlust ja tuvastada ründekatseid. Logimisinfo võimaldab sageli tuvastada ka ründe liiki, aidates niiviisi kohandada konfiguratsiooni. Logimisfunktsioonid vajavad hoolikat konfigureerimist, kuna suurest andmehulgast saab vajaliku info kätte ainult mõistliku filtreerimisega. Pärast info sobivat salvestamist tuleb tagada saadud andmete võimalikult kiire analüüsimine (vt M 4.321 VPNi turvaline käitamine). Arvestada tuleb andmekaitset puudutavate ettekirjutustega.

Dokumentatsioon

Tuleks dokumenteerida, milliseid VPN-komponentide seadistusi aluskonfiguratsiooni raames kontrolliti, samuti seda, kas ja kuidas neid muudeti. Dokumentatsioon peab olema selline, et peale tegeliku administraatori suudaks ka mõni teine isik, kes vastavat süsteemi ei tunne, aru saada, mida on tehtud. Tõrke korral peaks süsteemi taastamine olema võimalik ainult dokumentatsiooni põhjal. Seejuures tuleb arvestada ka moodulis M 4.78 Konfiguratsioonimuudatuste hoolikas teostamine kirjeldatud protseduuriga.

Asukohapõhine autentimine

Site-to-Site - või *End-to-Site* -VPNi autentimine võib lisaks kasutajapõhisele meetodile toimuda ka asukohapõhiselt. Seejuures peab olema tagatud vastaspoole selge tuvastamine. See eeldab, et kogu ametiasutuses või ettevõttes on olemas tsentraalne asukoha haldus. VPN tugineb vaid sellel. Asutuse sisevõrku suunatud kaugpöörduste korral tuleb arvestada infoga (vt M 4.113 Autentimisserveri kasutamine kaugpöördussüsteemis *)*.

Muudatuste haldus

VPN-süsteemikonfiguratsiooni muudatused peaksid kuuluma organisatoorse protseduuri alla, mis tagab, et VPN aktiveeritakse ainult kontrollitud konfiguratsiooni puhul. Kõik muudatused tuleb dokumenteerida ja kinnitada. VPN-kasutajatunnuste lisamine või kustutamine ei nõua tavaliselt VPN-süsteemikonfiguratsiooni muutmist, kuna need muudatused toimuvad sageli operatsioonisüsteemi või autentimisserveri (nt RADIUS, TACACS+) kasutajate halduse kaudu.

VPN-konfiguratsiooni regulaarne kontrollimine

Kõikide VPN-komponentide konfiguratsiooni tuleks regulaarselt kontrollida. Seejuures tuleb veenduda, et kõik VPN-turvapoliitika nõuded on ellu rakendatud ja et seadistustes pole kitsaskohti. VPN-konfiguratsiooni puhul on tegu VPN-turvapoliitika tegeliku realiseerimisega. Kõik turvapoliitikas VPNi jaoks määratletud turvanõuded tuleb sobival moel ellu viia. Siin loetletud valdkondi tuleb VPN-süsteemiplaneerimise ja VPNi käitamise raames täpsustada, täiendada ja kohandada. Üldjoontes sõltub komponentide konfiguratsioon alati kohalikest oludest või nõuetest. Üldkehtivat juhendit ei saa siinkohal anda, kuna vastavaid komponente tuleb vaadelda ettevõtte kontekstis.

Täiendavad kontrollküsimused:

- Kas kõikide VPN-komponentide algseadistusi kontrollitakse ja kohandatakse vastavalt turvapoliitika nõuetega?

- Kas kõikide VPN-komponentide standardsed paroolid on asendatud asutuse enda piisavalt keeruliste paroolidega?
- Kas VPN-serveri pakutavad turvamehhanismid, mida on edaspidises kasutusvaldkonnas mõttekas rakendada, on aktiveeritud ja leiavad kasutust?
- Kas VPN-serveri turvaseadistuste korrektsust kontrollitakse regulaarselt?
- Kas on tagatud VPN-serveri ja VPN-kliendi ühtne konfigureerimine?
- Kas tehniliselt või organisatoorselt on tagatud, et VPN-juurdepääsu kasutajaparoole ei salvestata?
- Kas VPNi jaoks kasutatavate võrguühenduselementide marsruutimisseadistused on konfigureeritud piisavalt suurte piirangutega?
- Kas kõik mobiilsed VPN-kliendid on konfigureeritud selliselt, et kogu andmeside toimub ainult VPN-ühenduse kaudu?
- Kas kõik olemasolevad testimisjuurdepääsud ja -kontod on VPN-komponentidest eemaldatud?
- Kui administreerimise jaoks on tarvis rakendada kaugpöördust, kas on tagatud, et kasutajanime ja parooli ei edastataks loetava teksti kujul?
- Kui sisselogimisteadet saab muuta: kas sisselogimisteade on koostatud selliselt, et see ei edastaks seadme mudeli ega versiooni numbrit ega ka operatsioonisüsteemi versiooni?
- Kas kõik VPN-komponentide mittekasutatavad liidesed on desaktiveeritud?
- Kas logimine on VPNis aktiveeritud ja õigesti konfigureeritud?
- Kas VPN-logisid analüüsitakse regulaarselt ja õigeaegselt?
- Kas VPN-süsteem on dokumenteeritud selliselt, et erialaselt pädev kolmas osapool oleks suuteline selle põhjal süsteemi uuesti üles ehitama?
- Kas kõik VPN-konfiguratsiooni muudatused on kinnitatud ja dokumenteeritud? Kas kõikide VPN-komponentide kohta on olemas aktuaalsed ja selgesti mõistetavad konfiguratsioonikirjeldused?

M 4.321 VPNi turvaline käitamine

Algatamise eest vastutavad: IT-juht, IT-turbespetsialist

Rakendamise eest vastutavad: administraator

Kuna VPNid edastatavad andmeid, on need ründajatele atraktiivsed sihtmärgid ning seetõttu tuleb neid võimalikult turvaliselt käidelda. Selle eelduseks on vastavate riist- ja tarkvarakomponentide turvaline installeerimine (vt M 4.319 VPNi lõppseadmete turvaline installeerimine ja M 4.320 VPNi turvaline konfigureerimine). Lisaks tuleb määratleda ja ellu viia kõik organisatsioonilised protseduurid (nt teatamisprotseduurid ja vastutusalad). Siinkohal tuleb arvestada infoga meetmes M 2.418 VPNi kasutamise turvapoliitika koostamine .

Käitamiskontseptsiooni koostamine

Üha sagedamini on vajalik, et asutuste VPN-ühendused oleksid igal ajahetkel stabiilselt tööks valmis. Paljudes asutustes peavad need olema ööpäevaringselt käideldavad (24/7-käitamine). VPNi sujuva käitamise tuleb luua käitamiskontseptsioon ja ka vastav avariikontseptsioon (vt M 6.109 Virtuaalse privaatvõrgu (VPN) hädaolukorraks valmisoleku plaan). Käitamiskontseptsiooni koostamisel tuleb arvestada eriti just järgnevate aspektidega.

Seire

Antud juhul tähendab seire kvaliteedihaldust. VPNi teenuse kvaliteeti tuleb pidevalt jälgida. Saadud andmed tuleb koondada haldusraportitesse ja esitada regulaarselt (näiteks kord kuus või kvartalis) IT-haldusosakonnale. Mõõdetud väärtused on mõeldud VPNi kvaliteedi ja ribalaiuse jaotuse jooksva peenhäälestamise jaoks. Sel moel saab aegsasti tuvastada kitsaskohti ning võimalikke probleeme tarkvaras ja riistvaras. Seejuures tuleb ka mõelda, kas VPNi käideldavust tuleks tagada vastavate teenusetasemelepetega SLAdega (Service Level Agreement 'idega) või käitamislepingutega ehk OLAdega (Operational Level Agreement 'idega).

Vaatamata regulaarselt koostatavatele aruannetele tuleb võimalikest kõrvalekalletest teada anda kohe, et probleeme saaks kiiresti lahendada.

Seirekontseptsioon

Erinevalt mainitud teenusekvaliteedi seirest on seirekontseptsioonis esikohal VPNi turvalisus. Saadud logiandmeid tuleb kontrollida turvapoliitikast lähtuvalt (nt juurdepääsupiiranguid), analüüsida ning vajadusel õiguslikel põhjustel ka arhiveerida. Seire raames saadud infot peab regulaarselt kontrollima vastavaid erialaseid teadmisi omav administraator. Parimat tulemust aitab saavutada logiandmete analüüsiks rakendatav spetsiaalne tarkvara. Oluline on järgida andmekaitset puudutavaid ettekirjutusi (vt M 2.110 Andmeprivaatsuse suunised logimisprotseduurides).

Hoiatamine

Hoiatamise kontseptsioon peab tagama, et kriitilise olukorra esinemisel teavitatakse sellest kohe mõnda vastutavat isikut. Sealjuures tuleb võtta tarvitusele eelnevalt määratletud meetmed ja vahejuhtumid vastavalt dokumenteerida (vt B

1.8 Turvaintsidentide käsitlus). Seejärel võib avariide kõrvaldamiseks rakendada meetme M 6.109 Virtuaalse privaatvõrgu (VPN) hädaolukorraks valmisoleku plaan põhjal koostatud avariikontseptsiooni.

Hooldus

Kui vähegi võimalik, ei tohiks VPNi hooldustöid teha tavatöö režiimis, st sel ajal, kui kasutajad saavad sellele juurde pääseda. Hooldustööde tegemisel tuleb olla hoolikas. Süsteemide hooldustööde või muudatuste tegemiseks tuleb eelnevalt määrata vastutusalad. Hooldustöödeks ja muudatuste tegemiseks tuleb kindlaks määrata vajalikud hooldusajad ja need tööprotsessidesse sisse planeerida. Hooldustööde liigist, mahust, ajast ja kestusest tuleb teatada õigeaegselt, samuti tuleb täpsustada, milliseid teenuseid see puudutab. Iga hooldustöö või muudatuse lõpus tuleb tehtud muudatused dokumenteerida ja need ka üle kontrollida.

Autoriseerimine kaugpöördus-VPNide puhul

Kaugpöördus-VPNide kirjeldavaks omaduseks on asjaolu, et VPNi ei pea ennast sisse valima mitte ainult mõned, vaid paljud VPN-vastaspooled. Tavaliselt on tegu kasutajatega, kelle paroolid võivad regulaarselt muutuda. Võimaldamaks kaugpöörduse korral kasutajate reguleeritud autentimist (nt RADIUS, TACACS, TACACS+ abil), peab olema tagatud autentimisandmete ühtsus. See võib toimuda andmete tsentraalse haldamisega (autentimisserveri abil) või perioodilise võrdlemisega.

Kaugpöördus-VPNide kasutamine sissevalimistega ühenduste kaudu

Sõltuvalt rakendatavast VPN-variandist võib sissevalimine toimuda ka andmevõrkude või sissevalimisel toimivate ühenduste, nt ISDNi või GSMi kaudu.

Sissevalimistega ühendused vajavad spetsiaalseid kaitsemeetmeid:

- Iga ühenduse loomise puhul tuleb kasutaja autentida valitud mehhanismi kaudu. CLIP-mehhanism (telefoninumbri edastamine) üksinda ei ole autentimiseks mitte mingil juhul piisav.
- Iga ühenduse jaoks tuleks side turvata VPNi turvakontseptsioonis heakskiidetud protseduuriga, et tagada andmete piisavalt turvaline edastamine.

Ühendus mobiiltelefoni vahendusel

- Kasutada tuleks juurdepääsutehnoloogia poolt pakutavaid täiendavaid turvamehhanisme (telefoninumbri edastamist, eelnevalt seadistatud telefoninumbril tagasihelistamist mittemobiilsetele või mobiili kaudu ühendatud VPN-klientidele).
- Kaasaskantava IT-süsteemi saab LANiga ühendada mobiilsidevõrgu, GSMi kaudu (vt M 5.81 Turvaline andmeedastus mobiiltelefoni kaudu). Kasutades VPNi mobiilivõrkude vahendusel, tuleb jälgida, et CLIP-mehhanism (telefoninumbri edastamine) sobib tavaliselt ainult täiendavaks autentimistunnuseks, kuna telefoninumbri kaudu tuvastatud mobiiltelefone saab väga kergesti varastada.
- WLANi kaudu sissevalimisel tuleb arvestada soovitustega moodulis B 4.6 Traadita kohtvõrgud .

Koolitamine ja ohtudest teavitamine

VPNi kasutajatele tuleb õpetada VPNi turvamehhanismide kasutamist. Selleks tuleb neile anda ülevaade tüüpilistest VPNi ohtudest ja vajalikest turvameetmetest.

Kuid VPNi turvalahenduste kasutamist peavad piisaval määral tundma ka administraatorid ja tõrgete kõrvaldamise meeskonna liikmed. Üldised juhised selle kohta leiate meetmest M 2.198 Personali teadvustamine infoturbe küsimustes.

Kaugpöördus-VPNide kliendid

Sageli soovitakse, et üksikutel kasutajatel oleks võimalik ennast ettevõtte või asutuse LANi sisse valida ebaturvaliste võrkude kaudu. Selle näiteks on kaugtöö tegijad või kasutajad, kes valivad ennast sisse mõne avaliku WLANi või siis mobiiltelefoni kaudu. Seejuures kasutatakse tavaliselt standardseid IT-süsteeme, millele installeeritakse rakendus kaugpöördus-VPNi sissevalimiseks. Kuna kaugpöördduse VPN-kliente käitatakse sageli ainult osaliselt kontrollitavates keskkondades, tuleb sel puhul kasutada spetsiaalseid mehhanisme, protseduure ja meetmeid, mis tagaksid kliendi piisava turvalisuse. Eriti ohustatud on siinkohal just mobiilsed VPN-kliendid, kuna neid on füüsiliselt lihtne rünnata (nt varastada, manipuleerida). Kompromiteeritud VPN-klient võib ohustada LANi turvalisust.

Mobiilsete VPN-klientide turvaliseks käitamiseks tuleb lisaks meetmes M 5.122 Sülearvuti turvaline ühendamine kohtvõrguga loetletud soovitustele arvestada järgnevate aspektidega:

- Tuleb tagada mobiilse IT-süsteemi turvalisus (vt B 3.203 Sülearvuti , B 3.404 Mobiiltelefon , B 4.3 Modem ja B 5.8 Kaugtöö).
- Kuna mobiilseid VPN-kliente ohustavad suuremad riskid kui statsionaarseid VPN-kliente, tuleks neid kaitsta täiendavate meetmetega. Selleks saab kasutata kõvaketta krüpteerimist, mis tagab, et kaotatud seadmetest ei saa ei andmeid lugeda ega luua volitama VPN-ühendust.
- Eriti just internetiühenduste kaudu toimuva VPN-juurdepääsu korral on oluline paigaldada kõikidele kaugpöördusklientidele viirusetõrjetarkvara (vt B 1.6 Viirusetõrje kontseptsioon).

Mobiilsete VPN-klientide kaasamine süsteemihaldusesse Süsteemihaldusesse tuleks võimalusel kaasata ka mobiilsed VPN-kliendid. Ühelt poolt võimaldab see klienti käitamise raames jälgida. Teiselt poolt jällegi võimaldab see lihtsalt ja reguleeritud moel paigaldada tarkvaravärskendusi (viiruseandmebaase, rakendusprogramme). Kaugemalasuvad arvutid esitavad süsteemihaldusele kõrgendatud nõudmisi, kuna need pole pidevalt võrku ühendatud, mistõttu tuleb arvuteid regulaarselt kontrollida, kas neis esineb (loata) konfiguratsioonimuudatusi. Seejuures tuleb arvestada, et vastava info kogumine koormab VPN-klienti ja et andmeid tuleb edastada VPN-ühenduse kaudu. Väikese ribalaiusega VPN-ühenduste puhul (nt mobiiltelefoni kaudu) võib see põhjustada kasutaja jaoks vastuvõetamatult pikki reaktsiooniaegu.

Sideühendused

VPNi turvalise töö jaoks tuleb kõik edastatavad andmed krüpteerida. Lisaks tuleb täielikult tagada edastatavate andmete autentsus ja terviklus. Selle saavutamiseks võib näiteks kasutada meetmes M 5.148 Turvaline välisvõrguühendus OpenVPN-i abil ja M 5.149 Turvaline välisvõrguühendus IPSec-i abil kirjeldatud protseduure.

Trusted -VPNid

VPNe käitatakse väga harva oma kontrolli all olevate võrgu infrastruktuuride kaudu. Sageli kasutatakse VPNe selleks, et realiseerida turvalist ühendust võõraste võrkude, nt Interneti või välise teenusepakkuja pakutud eraldiseisva liini kaudu. Eriti just viimase puhul tuleb hoolikalt jälgida ühendust ennast, ühenduse kvaliteeti ja teenusepakkuja valimisel määratletud turvaaspektidest kinnipidamist (vt M 2.420 Trusted VPN teenusepakkuja valimine).

Kontrollküsimused:

- Kas on tagatud, et VPN-ühenduste kvaliteedipuudused tuvastatakse õigeaegselt?
- Kas kõiki logiandmeid kontrollitakse regulaarselt ja analüüsitakse spetsialistide poolt?
- Kas VPNi seire puhul peetakse kinni andmekaitsenõuetest?
- Kas VPN-komponentide hoolduse, muudatuste ja revisjoni jaoks on määratletud süstemaatilised protseduurid?
- Kas on kindlaks määratud, mida tuleb teha VPNi vigade ja tõrgete puhul?
- Kas on tagatud, et VPNi käitamises esinevate kriitiliste olukordade puhul teavitatakse sellest viivitamata vastutavaid isikuid?
- Kas VPNi kasutajad ja administraatorid on läbinud piisava koolituse ja neile on selgitatud VPNi turvaaspekte?
- Kas puudutatud IT-süsteemide baasturvalisus on tagatud?

M 4.322 Mittevajalike VPN-pääsude blokeerimine

Algatamise eest vastutavad: IT-juht, IT-turbespetsialist

Rakendamise eest vastutavad: administraator

VPN-juurdepääse tuleb turvata selliselt, et neid saaksid kasutada ainult volitatud kasutajad ja IT-süsteemid. Selleks tuleb VPN-lõpp-punktides rakendada pääsukontrolli protseduure, mis kontrollivad, kas saatja on volitatud side alustamiseks adressaadiga. Vastava protseduuri nõuetekohast töötamist ja konfiguratsiooni tuleb regulaarselt kontrollida. Unustatud juurdepääsud või juba lahkunud töötajate või eemaldatud IT-süsteemide kasutajatunnused kujutavad endast ohtlikke turvaauke ja seetõttu tuleb need võimalikult ruttu sulgeda. Ka tarnijate, partnerite või klientide ebavajalikud VPN-juurdepääsud tuleb võimalikult ruttu desaktiveerida. Pärast juurdepääsu kustutamist tuleb kontrollida, et neid tõesti ei saaks enam võrgujuurdepääsu loomiseks kasutada. Kui on eelnevalt teada, et mõned VPNi kasutajad viibivad kas pikemat aega eemal või ei kasuta VPNi mõnel muul põhjusel (nt puhkuse, haiguse või muude ülesannete tõttu), tuleks kaaluda nende kasutajatunnuse sulgemist VPN-serveris selleks ajaks nii, et nende kasutajatunnuste kaudu ei saaks ajutiselt enam tööd teha. Võimalusel peaks iga kasutaja võrguadministraatorile õigeaegselt teatama, kui tal tuleb pikemat aega eemal viibida. Kui välised kliendid või tarnijad vajavad VPN-juurdepääsu ainult teatud kindlatel aegadel, tuleks neile anda pääsuõigused ka ainult vastavateks hetkedeks.

Kasutusele tuleks võtta volitusega kasutajate ja IT-süsteemide tõhus haldamine, mis toimub näiteks sertifikaatide alusel, ning seda haldust tuleks regulaarselt kontrollida ja kohandada. Pääsuandmeid ja vastavaid teenuseid tuleb kaitsta volitamata juurdepääsu eest.

Täiendavad kontrollküsimused:

- Kas regulaarselt kontrollitakse, et VPNi kasutamine oleks võimaldatud ainult volitatud IT-süsteemidele ja isikutele?
- Kas on tagatud, et ebavajalikud VPN-juurdepääsud desaktiveeritakse ilma viivituseta?
- Kas VPNi kasutajate jaoks on loodud süstemaatiline haldus?
- Kas VPNi pääsuandmed ja vastavad teenused on volitamata juurdepääsu eest kaitstud?

M 4.323z Sünkroniseerimine turvapaikade ja muudatuste halduse raames

Algatamise eest vastutavad: IT-juht, IT turbespetsialist

Rakendamise eest vastutavad: muudatuste haldur, administraator

Enamikes ametiasutustes ja ettevõtetes muudetakse IT infrastruktuuri sageli. Paikade ja muudatuste haldusprotsess peab suutma nendele muudatustele reageerida. Seejuures tuleb tagada, et vastavad paigad ja muudatused paigaldataks kõikidele puudutatud IT-süsteemidele võimalikult operatiivselt ja korraga.

Mobiilsete lõppseadmete puhul või ka võrgutehnoloogia ülekoormuse puhul võib juhtuda, et IT-süsteemid pole riist- või tarkvaramuudatuste jaotamisel enam kättesaadavad. Sellise olukorra jaoks tuleb luua mehhanismid, mis tagavad, et süsteemid saavad võrku logida alles siis, kui sobivad värskendused on paigaldatud. On erinevaid tööriistu, mis kontrollivad enne tootmisvõrku pöördumist, kas turvaprogrammid ja turvapaigad on uuendatud ja keelavad turvapuuduste esinemisel juurdepääsu sisevõrku. Tavaliselt kasutatakse selliseid tööriistu enneköike süsteemide tarkvaraseisundi tuvastamiseks ja seejärel nimekirja loomiseks uuendamist vajava tarkvara kohta. Olenevalt paikade ja muudatuste protsessi liigist saab neid seejärel kas automaatselt või pärast eelnevat kinnitust vastavatesse süsteemidesse laiali jaotada ja installeerida. Süsteemi taaskäivitamist nõudvad muudatused tuleks paigaldada viimasena või alles IT-süsteemi väljalülitamise käigus. Olenevalt tehnilisest toest ja protsessi teostamisest saab esmalt paigaldada uuendused ja sellele järgnev vajalik taaskäivitamine võib toimuda pärast eraldi kinnitust.

Kontrollküsimused:

- Kas paikade ja muudatuste halduse tagamisel arvestatakse uute ja kättesaamatute IT-süsteemidega
- Kas kõik protsessi faasid viiakse sünkroniseerimise raames läbi ka vahepeal kättesaamatuna olnud süsteemide peal?
- Kas IT infrastruktuuri muudatustele reageeritakse ka paikade ja muudatuste haldamise protsessis?

M 4.324 Automaatsete uuendusmehhanismide konfiguratsioon turvapaikade ja muudatuste haldamisel

Algatamise eest vastutavad: muudatuste haldur

Rakendamise eest vastutavad: administraator

Paljudel toodetel on automaatsed uuendusmehhanismid (autoupdate), mis teavitavad kasutajat saadaolevatest paikadest või värskendustest. Sageli pakuvad need ka võimalust värskendusi otse internetist alla laadida ja installeerida. Üldjuhul sisaldavad selliseid mehhanisme kõik tänapäevased operatsioonisüsteemid ja tarkvarapaketid. Uuendusmehhanismi tööviis sõltub selle versioonist, installeerimisrežiimist ja tootjast. Tavaliselt otsivad automaatse uuenduse funktsiooniga varustatud IT-tooted avalikust uuenduste serverist uusi versioone või tarkvarapakette igal süsteemikäivitusel või internetti sisenemisel. Tooted pakuvad automaatsete uuendusmehhanismide konfigureerimiseks erinevaid võimalusi. Uute IT-komponentide kasutussevõtul tuleks alati kontrollida, kas ja millised uuendusmehhanismid neil on ja kuidas neid konfigureerida. Seejuures tuleks kontrollida, milliseid andmeid automaatuuenduste mehhanism tootjale edastab. Esmalt tuleks selgitada, mida nende mehhanismidega teha. Seejärel tuleks kindlaks määrata, kuidas uuendusfunktsioone konkreetselt erinevates toodetes konfigureerida.

Alljärgnevalt antakse ülevaade nende mehhanismide erinevatest variantidest.

Täielik keeld

Mitte iga tarkvara ei paku täieliku desaktiveerimise võimalust. Kui asutus soovib takistada IT-komponentide ja asutusevälise punkti kontrollimatut ühendust, tuleb paigaldada paketifiltrid.

Ümbersuunamine

Kui avalikku värskendusserverisse suunatud päringuid ei taheta lubada, saab mitmes tarkvaratootes asendada tootja sihtaadressi mõne muu, nt asutuse enda aadressiga.

Värskendusserverite käitamine asutuses endas

Osad tootjad pakuvad tarkvara värskendusserverite või värskenduste peegelserverite asutusesiseseks käitamiseks, seejuures paigaldatakse täiendiserver asutusse lokaalselt (nt WSUS, Windows Server Update Services). Värskendusserver suhtleb siis otse tootjaga ja laadib soovitud värskendusi otse tootjalt. Selle lahenduse eeliseks on asjaolu, et värskendustest puudutatud asutuse IT-süsteemid ei suhtle vahetult tootja värskendusserveriga, vaid asutusse lokaalselt installeeritud serveriga. See võimaldab vähendada väljapoole suunatud andmesidet miinimumini.

Paljude värskendusserverite toodete puhul saab vajalikke seadistusi teha mugavalt graafilise kasutajaliidese (GUI) kaudu. On ka tooteid, mille puhul on

kohalike värskendusserverite kasutamise või avaliku värskendusserveri päringu keelamise jaoks vajalikud seadistused varjatud või võimalikud ainult paketifiltri või tulemüüri abil. Avalike värskendusserverite kasutamisel tuleb esmalt kontrollida värskendusserveri autentsust, vt M 4.177 Tarkvarapakettide tervikluse ja autentsuse tagamine . Lisaks tuleks kontrollida, kas täiendite päringute ajaintervalle või käivitussündmusi saab seadistada. Seadistusi tuleb teha muudatuste strateegia alusel. Tuleks kontrollida, kuidas saaks viia värskendusserveritega suhtlemist miinimumini. Lisaks tuleb otsustada, kas otseühendus tootjaga jääb ainukeseks alternatiiviks või käitatakse seda paralleelselt sisemise kommunikatsiooniga (paralleelkonfiguratsioon).

Paralleelkonfiguratsioon on sageli kasulik mobiilsete kasutajate jaoks, kes ei saa ennast alati ühendada ametiasutuse või ettevõtte sisevõrguga. Mobiilsete IT-süsteemide puhul võib teel olles olla olulisem mõne paiga kiire installeerimine, kui see sulgeb ohtliku turvaaugu, ilma et peaks ootama muudatuste halduri kinnitust. Siiski on võimalik ka variant, mille puhul toimuvad kõik tarkvaramuudatused eranditult asutusesisese tarkvaraosakonna kinnituste alusel.

Automaatsete uuendusmehhanismide puhul tuleb lisaks mõelda, kas laadida tootja pakutud muudatused asutusesisesele IT-süsteemile ja jätta muudatuste paigaldamine kasutajate hooleks või paigaldada muudatused pärast allalaadimist automaatselt. Lisaks tuleb otsustada, mida teha muudatuste paigaldamise järel vajalike taaskäivitustega, nt kas need peaksid toimuma alles süsteemi väljalülitamise käigus.

Kontrollküsimused:

- Kas asutuse paikade ja muudatuste haldusstrateegia koostamisel määratleti ka automaatsete värskendusmehhanismide strateegia?
- Kas uusi komponente kontrollitakse, kas ja millised automaatsed värskendusmehhanismid neil on?
- Kas automaatsete värskendusmehhanismide turvalisuse tagamise meetod on kindlaks määratud?

M 4.325 Likvideerimisele kuuluvate failide kustutamine

Algatamise eest vastutavad: infoturbe spetsialist, IT-juht

Rakendamise eest vastutavad: administraator, kasutaja

Tänapäevased operatsioonisüsteemid toetavad virtuaalmälu. Selleks, et kasutajad saaksid (virtuaalselt) kasutada rohkem põhimälu kui arvutisse paigaldatud, suunatakse töömälu hetkel mittekasutatav osa kõvakettale (swap-alasse). Vastavad saalefailid sisaldavad osaliselt ka infot, mida kasutajad töö ajal kasutasid. Siia hulka võivad kuuluda ka tundlikud andmed, nagu paroolid või krüptograafilised võtmed. Failid jäävad kasutaja väljalogimise või süsteemi väljalülitamise korral alles, st neid ei kustutata. Seega saab ründaja kasutada saalefaile konfidentsiaalsete andmete lugemiseks. Saalefailide lugemise takistamiseks tuleb saalimisala ajutiselt või püsivalt desaktiveerida või enne väljalülitamist alati turvaliselt kustutada.

Uuemaid Windowsi operatsioonisüsteeme saab konfigureerida selliselt, et arvuti buutimisel või väljalülitamisel kirjutatakse saalefail üle. Saalefail (Windows Paging File, pagefile.sys) kirjutatakse sarnaselt säästurežiimi failile (Hibernation File, hiberfil.sys) süsteemi väljalülitamisel nullidega üle juhul, kui on määratud seadistus „Shut down: Clear virtual memory pagefile". Olenevalt suurusest võib saalefaili ülekirjutamine võtta palju aega. Siiski tuleks klientide puhul, eriti sülearvutites, seda võimalust kindlasti kasutada. Väga suurte saalefailidega serverite puhul, millele ei ole kehtestatud kõrgendatud kaitsevajadust, tuleks kaaluda, kas selline meetod on vajalik või mitte. Kõrgema kaitsevajaduse puhul tuleks saalefail aga kindlasti alati automaatselt kustutada. Saalefaili saab süsteemi käivitamisel EFS-i abil krüpteerida. See on märksa tõhusam ja alati kasulik olukordades, kus saalefail pole krüpteeritud täieliku kõvakettakrüpteeringu, näiteks BitLocker Drive Encryptioni abil.

Kõrgendatud kaitsevajaduse korral tuleb saalefaili lugemise takistamiseks võtta kasutusele täiendavad meetmed. Selleks saab näiteks kasutada tarkvaratööriistu, mis kustutavad saalimisala iga kord enne väljalülitamist. Probleemi vältimiseks võib kasutada krüptograafilisi failisüsteeme, millega krüpteeritakse kogu kõvaketta sisu. See välistab ka juurdepääsu saalefailile. Saalimisala väljalülitamine või kustutamine sobib juhtumipõhiste lahenduste jaoks, kuid pole püsiv alternatiiv. Kõrgema kaitsevajaduse puhul on kõvaketaste täielik krüpteerimine parem lahendus. Unix-süsteemides hoitakse saalefaile swap-failisüsteemis. Tegu on eraldi partitsiooniga, mida saab krüpteerida. Enne swap-partitsiooni krüpteerimist tuleb kontrollida, kas arvuti võimsus on selleks piisav. Saalimisala ärakasutamise vältimise turvaline meede on kogu andmekandja krüpteerimine ja võimaluse korral tuleks seda kasutada.

Kontrollküsimus:

- Kas IT-süsteemide juurdepääs saalimisalale on kindlalt takistatud?

M 4.326 NTFS funktsioonide tagamine Samba failiserveril

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator

Windowsil põhinevad failisüsteemid on teatud valdkondades Unixi failisüsteemidest väga erinevad. Näiteks failisüsteemi objektide kopeerimine ja ümberpaigutamine väljapoole süsteemi piire, võib endaga kaasa tuua andmekao, juhul, kui administraatorid pole vastavatest efektidest teadlikud ja on konfigureerinud Samba valesti. Selle näite puhul on konkreetselt puudutatud info, mille salvestuskohtadeks võivad olla New Technology File System (NTFS), Access Control Lists (ACL) ning NTFS Alternate Data Streams (ADS).

1. NTFS Access Control Lists

Samba 3 kasutab NTFS ACL-ide kopeerimiseks Portable Operating System Interface (POSIX) ACL-e. See mehhanism on standardina sisse lülitatud järgmistel juhtudel:

- kui failisüsteem toetab Samba ühiskasutust POSIX ACLs,
- kui samba on kompileeritud ACL-i toega (configure skripti parameetriga -with-acl-support) ning
- kui konfiguratsioonifaili smb.conf konfigureerimisparameetri „ nt acl support ” väärtuseks pole määratud „ no ”.

Sellisel juhul on tegu NTFS ACL-ide otseste koopiatega POSIX ACL-ide kujul. Täpsemat infot selle kohta, kuidas ja milliste piirangutega Samba NTFS ACL-e failisüsteemi ümber kopeerib, leiate meetmest M 4.332 Samba serveri pääsuõiguste turvaline konfiguratsioon . Enne seda, kui failisüsteemi objekte hakatakse süsteemi piiridest väljapoole ümber paigutama, peab olema tagatud, et nendega poleks seotud ühtegi sellist NTFS ACL-i, mida Samba ei suuda kopeerida. Seda asjaolu tuleks arvestada muuhulgas juba üleorganisatsioonilise, erinevate failisüsteemide tarbeks koostatava pääsuõiguste kontseptsiooni väljatöötamisel. Loobuda tuleks selliste NTFS ACL-ide sissekandekombinatsioonide kasutamisest, mida Samba ei suuda otse kopeerida.

2. NTFS Alternate Data Streams

Samba versioonis 3.0.x puudub võimalus NTFS ADS-ide kopeerimiseks. Samba versioonis 3.2.x ja sellest uuemates versioonides saab NTFS ADS-e kopeerida otse POSIX Extended Attributes (xattr) abil. Juhul, kui kasutusel on Samba versioon, mis NTFS ADS-e kopeerida ei suuda, tuleb enne süsteemi piiridest väljapoole kopeerimist ja ümberpaigutamist tagada, et failisüsteemide objektid ei sisaldaks olulist infot kandvaid ADS-e.

3. Windowsi ja Unixi failisüsteemide täiendavad erinevused

Windowsi ja Unixi failisüsteemide vahel leidub veel ka täiendavaid erinevusi nagu nt väike- ja suurtähtede eristamine Unixis ning kataloogide eraldusmärgid. Neid erinevusi suudab Samba arusaadaval moel kompenseerida ning need endast info kaotsimineku ohtu ei kujuta.

Täiendavad kontrollküsimused:

- Kas administraatorid tunnevad Unixi ja Windowsi failisüsteemitehnoloogiate erinevusi?
- Kas enne objektide ümberpaigutamist süsteemi piiridest väljapoole tagatakse, et failisüsteemide objektidega pole liidetud ühtki sellist NTFS ACL-i, mida Samba ei suuda kopeerida?

- Kas enne objektide ümberpaigutamist süsteemi piiridest väljapoole tagatakse, et failisüsteemide objektid ei sisalda olulist infot kandvaid ADS-e, mida kasutatav Samba versioon ei suuda kopeerida?

M 4.327 Samba tarkvarapakettide ja lähtetekstide tervikluse ja autentsuse kontroll

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator

Pärast seda, kui Samba kasutuselevõtu planeerimise käigus (vt M 2.437 Samba-serveri kasutuselevõtu plaanimine) on otsustatud, kas Samba installeeritakse lähteteksti paketina või binaarpaketina, tuleb kontrollida nende allikate autentsust (vt M 4.177 Tarkvarapakettide tervikluse ja autentsuse tagamine). Installeeritava tarkvara päritolu tuleks samamoodi dokumenteerida nagu seda tehakse tarkvara tervikluse kontrollimise protsessi puhul.

1. Installeerimine lähtetekstipaketist

Lähtetekstipakettide turvamiseks kasutavad Samba arendajad programmiga GnuPG koostatud digitaalseid allkirju (vt M 5.63 GnuPG või PGP kasutamine) . Digitaalne allkiri asub alati eraldi failis, mis kannab sama nime nagu pakett ise, kuid sellele on lisatud veel ka järelliide „.asc". Näiteks paketi samba-3.0.28a.tar.gz digitaalne allkiri asub failis samba-3.0.28a.tar.asc. Avaliku võtme, mida Samba arendajad allkirjastamiseks kasutavad, User-ID on „ Samba Distribution Verification Key ". Võti kehtib reeglina üks kuni kaks aastat. Seejärel võetakse kasutusele uus võti koos uue sõrmejäljega (ingl: Fingerprint). Avaliku võtme saab hankida järgmistest allikatest:

- Samba projekti veebiserver. Fail aadressil http://www.samba.org/samba/ftp/samba-pubkey.asc sisaldab Samba arendajate poolt lähtekoodi allkirjastamiseks kasutatavat avalikku GPG-võtit.
- Keyserver.

Enne lähtetekstipaketi kontrollimist tuleb see gzip-d samba-.tar.gz lahti pakkida.

2. Installeerimine distro binaarpakettidest

Juhtudel, kus Samba installeeritakse vabavara versiooni ametlikest installeerimisallikatest, milleks kasutatakse vastavaid paketihaldureid (kas yum-i või rpm-i), kontrollivad pakettide autentsust ja terviklust reeglina vastavad paketihaldurid.

3. Installeerimine võõraste allikate binaarpakettidest

Juhtudel, kus binaarpaketid hangitakse installeerimisallikatest, mis ei kuulu kasutatava vabavara versiooni hulka, tuleb kindlasti veenduda, et tegemist oleks usaldusväärse pakkujaga. Binaarpakettide tervikluse ja autentsuse kontrollimine toimub sel juhul nii, nagu on kirjeldatud alalõigus „Installeerimine lähtetekstipaketist" või alalõigus „Installeerimine distro binaarpakettidest".

Täiendavad kontrollküsimused:

- Kas installatsioonipakettide autentsust ja terviklust on kontrollitud?
- Kas installatsioonipakettide päritolu ning tervikluse kontrollimise protseduur on dokumenteeritud?

M 4.328 Samba serveri turvaline aluskonfiguratsioon

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator

Pärast Samba serveri installeerimist tuleb teenuste jaoks sisse seada turvaline aluskonfiguratsioon. See puudutab muuhulgas juurdepääsukontrolli reguleerivaid seadistusi, kuid ka selliseid seadistusi, mis mõjutavad serveri jõudlusnäitajaid. eskset rolli mängib siinkohal Samba konfigureerimisfail smb.conf, mis asub reeglina kataloogis /etc/samba/. Nimetatud konfiguratsioonifailis tehakse vahet ühe globaalse ja mitmete, ühiskasutust puudutavate konfigureerimislõikude vahel.

Ühiskasutusse puutuvaid konfigureerimislõikusid on võimalik ära tunda selle järgi, et need lõigud algavad enamasti mõne markeeringuga, mille nimes ei kajastu mõiste „[global]”. Parameetrid, mis kajastuvad globaalses lõigus, kehtivad kõige kohta. Ühiskasutuse eripärasid kajastavate lõikude parameetrid kehtivad seevastu ainult sellele ühiskasutusele, millega need on seotud. Kõikide smb.conf faili konfiguratsiooniparameetrite kirjeldused leiate dokumentatsioonist, täpsemalt man pages hulgast. Järgnevalt kirjeldatakse olulisemaid konfigureerimisseadeid.

Turvarežiimid

Kasutajate autentimisel on üheks olulisemaks parameetriks „ security ”. Server Message Block (SMB)-protokoll eristab kahte turvaastet (Security Levels):

- user-level,
- share-level.

Turvaastmes share-level reguleeritakse juurdepääsusid ühiskasutuse tasandil. Ühiskasutust kaitstakse selles turvaastmes vaid parooliga. Ükskõik millisel kasutajal on võimalik ühiskasutuse funktsioonidele ligi pääseda juhul, kui ta teab parooli. Turvaastmes user-level reguleeritakse juurdepääsu seevastu hoopis kasutajate tasandil. See tähendab, et iga kasutaja kohta on võimalik individuaalselt määratleda, millised õigused talle ühiskasutuse funktsioonide tarbimiseks antakse. Enne ühiskastutuse funktsioonidele ligipääsemist peab kasutaja ennast autentima. Sambas rakendatakse kaht eelnimetatud turvaastet viiel erineval moel, mida nimetatakse turvarežiimideks (Security Modes). Turvaastet user-level on rakendatud neljal moel (režiimidena User , Server , Domain ja ads Security Mode), turvaaste share-level töötab seevastu vaid ühtmoodi, töörežiimis Share Security Mode. Turvarežiim nimega Share on ainuke režiim, mille puhul toimib juurdepääsude juhtimine ühiskasutuse tasandil. Kõikides teistes turvarežiimides toimib juurdepääsude juhtimine kasutaja tasandil.

Järgnevalt kirjeldatakse erinevaid turvarežiime veidi lähemalt.

- Share - Selle turvarežiimi kasutamisest tuleks loobuda, kuna see ei võimalda kasutajaid teineteisest ükshaaval eristada. Iga ühiskasutus seotakse mõne parooliga.
- Server - Selle turvarežiimi asendamiseks töötati välja turvarežiim nimega domain ning seetõttu tuleks selle kasutamisest enamatel juhtudel loobuda.

Selle turvarežiimi puhul delegeerib Samba autentimise mõnele välisele IT-süsteemile, toimides seejuures nõnda, nagu teeks seda IT-süsteem, kuhu on installeeritud kas Windows 95 või Windows 98. Sellega kaasnevad paljud puudused, näiteks enam ei saa kasutada Winbindi, kontosid on võimalik sulgeda ilma järelevalveta ja Samba ei suuda kontrollida selle serveri identiteeti, millele autentimine delegeeritakse.

Alles turvarežiimis domain delegeerib Samba autentimise edasi mõnele DC-le.

- User - Samba tüüpseadistus. Selle seadistuse puhul rakendatakse autentimisel kasutajaid ja paroole.
- domain - Selles turvarežiimis edastab Samba autentimise mõnele välisele süsteemile. Kasutajate haldamiseks võetakse kasutusele nn Remote Procedure Call (RPC).
- Ads - Microsoft kasutab Active Directoryt. Viimane rakendab autentimisel eelistatult Kerberost ning võimaldab kasutajate haldamiseks kasutada Lightweight Directory Access Protocol (LDAP)-kausta. Turvarežiimis „ads" edastab Samba autentimise mõnele välisele süsteemile. See turvarežiim on paljudes valdkondades sarnane turvarežiimiga domain , kuid selle erinevusega, et Samba võimaldab kliendi autentimismeetodina kasutada ainult Kerberost.

Turvarežiimid domain ja ads on teineteisele väga sarnased. Ühe või teise režiimi kasuks otsustamisel tuleks arvestada järgmiste aspektidega. Turvarežiimis domain on iga Active Directory suuteline Samba teenuseid endaga liitma, kajastades neid liikmetena. See ei kehti mitte ainult nn Mixed Mode režiimi domeenidele. IT-kooslusele kehtivad turvapoliitikad võivad nõuda, et kasutataks Kerberost. Kerberost peetakse enamikel juhtudel märgatavalt turvalisemaks kui NTLM-i (NT LAN Manageri), kuigi versioonil NTLMv2 on samuti täiesti vastuvõetav turvstandard. Autentimiseks kasutab Samba standardina kas NTLM või NTLMv2 protseduuri. Selleks, et Samba kasutaks ainult versiooni NTLMv2, tuleb konfiguratsioonifailis smb.conf määratleda parameeter „ntlm auth = no". Kerberose üheks eeliseks NTLM-i ees on DC väiksem koormus ja madalam võrgukoormus. Kerberose piletid kehtivad seevastu aga teatud aja ning on iseseisvad. Juhtudel, kui kasutajal õnnestub end kehtiva piletiga mõne Samba teenuse suhtes autentida, pole täiendav autentimine DC-s enam vajalik. Domeenikontrollerite väiksem töökoormus ja madalam võrgukoormus on saavutatav ka siis, kui võtta kasutusele Winbind (vt M 4.333 Winbindi turvaline konfigureerimine Samba keskkonnas). LDAP-d kasutades kuvatakse loetelus kõik kasutajad. Kasutajate ülesloetlemine on operatsioon, mida tuleks vältida, kuna suurte domeenide puhul võib selline protsess kujuneda väga ajamahukaks. Juhtudel, kus kasutajate loetelu koostamine on vältimatu, tuleks valida turvarežiim „ads". Active Directory s on kasutusel nn asukohtade kontseptsioon (Sites). Iga DC ja iga liikmeks olev arvuti on seotud konkreetse asukohaga. Juhul, kui mõni liikmesarvuti soovib luua ühenduse mõne DC-ga, peaks see toimuma vaid ettenähtud asukoha piires. Vastavaid mehhanisme võimaldab Samba kasutada ainult turvarežiimis ads Security Mode.

Turvarežiim „ads” on väga kriitiline aja sünkroniseerimise ja korrektselt toimiva DNS-i (Domain Name System) suhtes. Olukorras, kus Samba otsib mõnd DC-d, toimub see turvarežiimis ads Security Mode DNS-i, mitte Network Basic Input/Output System (NetBIOS)-nimeteisenduse kaudu. Autentimise eest hoolitseb Kerberos. Kerberose turvalisus põhineb osaliselt sellel, et kõikide võrgus olevate arvutite kellaajad on sünkroonsed. Kui ajad ei ole sünkroonsed, siis Kerberosega autentimine ebaõnnestub. Juhtudel, kus kasutatakse turvarežiimi Security Mode ads, tuleks kaaluda, kas oleks mõttekas kasutada üht Windows-DNS-serverit nimeserverina ja üht Samba-teenuse jaoks ajaserverina. Samba-teenuses on selle jaoks tarvis teha vastav sissekanne failidesse /etc/resolv.conf ja /etc/ntp.conf. Vanemad Kerberose teegid põhjustavad Active Directory s kasutatavatele algoritmidele tihti suuri probleeme. Mõningatel juhtudel puudub neil üleüldse vajamineva räsifunktsiooni HMAC-MD5 tugi või on nende juurutused vigased. Selle tagajärjel võib Kerberosest tingituna tekkida arvuti töös isegi avarii. Kohati liiga vanu Kerberose teeke panevad oma toodetega kaasa eriti just Unixi operatsioonisüsteemide tootjad.

Turvarežiim ads on võrreldes turvarežiimiga domain märgatavalt progressiivsem.

Kuna Samba installeerimine ja konfigureerimine turvarežiimis Security Mode ads võib osutuda tavapärasest keerulisemaks, soovitatakse väikestes domeenides, kus on ainult üks asukoht ehk LAN, kasutada turvarežiimi Security Mode domain. Juhtudel, kus on tarvis kasutada Winbindi koos ID-Mapping-Backend ads -iga (vt M 4.333 Winbindi turvaline konfigureerimine Samba keskkonnas), tuleb Samba tööle rakendada turvarežiimis Security Mode ads.

Kasutajal põhinev kaitse

Ühenduse loomine Samba-teenusega peaks reeglina olema lubatud ainult valitud kasutajatele ja kasutajagruppidele. Sel põhjusel tuleks juurdepääsu piirata konfiguratsioonifailis smb.conf funktsiooniga „ valid users ”. Siinkohal on oluline, et see funktsioon rakendataks tööle konfiguratsioonifaili smb.conf alalõigus [global]. Sama parameetrit on võimalik kasutada ka konfiguratsioonifaili selles alalõigus, mis reguleerib ühiskasutust ning sellisel juhul piirab see seadistus vaid juurdepääsu konkreetsele ühiskasutusele.

Näide võiks olla järgmine:

valid users = @smbusers Administrator

Eelnev seadistuse näide määrab kindlaks, et juurdepääsu võimaldatakse ainult serveri kasutajagrupile „smbusers” ja kasutajale „Administrator”. Standardina on see valik sisse lülitamata. Sellisel juhul on serverisse võimalik sisse logida igal kasutajal, kellel on kehtiv kasutajakonto. Juhul, kui sama kasutaja on sisse kantud nii loendisse valid users kui ka loendisse invalid users , siis selle kasutaja juurdepääs tõkestatakse.

Grupi nimedes sisalduvaid viitemärke tõlgendatakse järgnevalt.

- @ Nimi tõlgendatakse esmalt Network Information Service (NIS) Netgroupina. Juhul kui NIS Netgroup i ei leita, lähtutakse sellest, et tegu on Unixi grupiga.

- + Nimi tõlgendatakse Unixi grupina.
- & Nimi tõlgendatakse NIS-i grupina.

Viitemärke + ja & võib nimeteisenduse jaoks soovitud järjekorra tekitamiseks kombineerida suvalisel moel.

Hostil põhinev kaitse Samba aktsepteerib standardina kõikide hostide ühendusi. Seetõttu tuleks Samba konfigureerida nõnda, et see aktsepteeriks vaid turvaliseks peetavate hostide ja võrkude ühendusi. Samba võimaldab selle jaoks kasutada enda „tcpwrapper”-juurutust.

Selle töölerakendamiseks on konfiguratsioonifailis smb.conf valikud „ hosts allow ” ja „ hosts deny ”. Näiteks:

- hosts allow = 127.0.0.1 192.168.2.0/24
- hosts deny = 0.0.0.0/0

Ülemise näite puhul lubatakse ühendusi vaid localhost -ist (127.0.0.1) ja sellistest IT-süsteemidest, mille IP-aadress (Internet Protocol Address) jääb vahemikku 192.168.2.1 ja 192.168.2.255. Kõik ülejäänud ühenduse loomise katsed tõrjub Samba tagasi, väljastades teate „ not listening on called name ”.

Võrguaadressi 127.0.0.1 tuleb lubada, kuna see on vajalik järgmiste Samba rakenduste korrektseks toimimiseks:

- smbpasswd

smbpasswd ühendab end kui SMB-Client standardina aadressiga 127.0.0.1 selleks, et vahetada kasutaja parooli.

- swat

Samba veebipõhise konfigureerimisprogrammi olekulehekülg swat ühendab enda nmbd ja smbd-ga aadressil 127.0.0.1, et kontrollida, kas need töötavad. Juhul kui swat -il ei õnnestu nende protsessidega ühendust saada, pole võimalik Samba seisundit korrektselt kuvada ning seetõttu ei saa ka Sambat usaldusväärselt käivitada, peatada ega ka taaskäivitada.

Võrguliidesed

Samba ühendab end standardseadistuse kohaselt kõikide süsteemis saadaolevate võrguaadressidega. Samba tuleks konfigureerida selliselt, et see seoks ennast vaid turvaliseks peetavate võrguaadressidega. Sellisel juhul jäetakse ebasoovitud paketid Samba protsessidele edasi saatmata. Selle ellurakendamiseks on konfiguratsioonifailis smb.conf valikud „ interfaces ” ja „ bind interfaces only ”.

Näiteks:

- interfaces = lo eth0
- bind interfaces only = yes

Ülemises näites ühendab Samba end vaid võrguliideste aadressidega lo ja eth0. Olukorras, kus keegi üritab Samba-teenusega ühendust saada näiteks võrguseadme ppp0 kaudu, keeldutakse juba operatsioonisüsteemi tasandil TCPühenduse (Transmission Control Protocol ühenduse) loomisest. Sellisel juhul saab klient teate, et TCP-ühenduse loomise soov on tagasi lükatud. Sellist infot võivad aga oma tarbeks ära kasutada rünnete toimepanijad. Seetõttu tuleks täiendavalt rakendada ka meetmes M 4.331 Samba serveri operatsioonisüsteemi turvaline konfiguratsioon toodud soovitused lokaalse paketifiltri konfigureerimise kohta. Paketifiltriga on võimalik saavutada seda, et sissetulevaid ebasoovitud pakette ignoreeritakse. Aadressilt 127.0.0.1 (Interface lo) laekuvaid pakette tuleks lubada, et Sambakeskkonna programmid saaksid korralikult toimida.

Ühiskasutused

Parameeter „ follow symlinks ” juhib seda, kas Sambal on võimalik järgneda sümbolilisele lingile Unix-failisüsteemis või saab kasutaja hoopis veateate. Standardseadistuses on selle parameetri väärtuseks määratud „ yes ”. Selle parameetri standardseadistust tuleks säilitada muutmata kujul, ka siis, kui smdb peaks kataloogidel kuvamisel veidi aeglasemalt töötama. Parameeter „ wide links ” juhib seda, kas kasutajal on võimalik järgneda sümbolilisele lingile Unix-failisüsteemis, mille sihtkoht asub väljaspool ühiskasutusse lubatud kataloogipuud. Siia alla kuuluvad linkide teises otsas asuvad failid ja kataloogid, juhul, kui nende jaoks on olemas failisüsteemi volitused. Selle parameetri standardse seadistuse väärtus on „yes”. Seda parameetrit ignoreeritakse juhul, kui on määratud seadistus „follow symlinks = no ”. Seadistuse korral „ wide links = no ”, võib juhtuda, et smbd töötab märgatavalt aeglasemalt, kuna iga link on tarvis üle kontrollida.

Juhul, kui parameetri väärtuseks valitakse „ yes ”, on sellega võimalik takistada kasutaja juurdepääsu sümbolilise lingi kaudu näiteks infole, mis asub kaustas /etc/. Olukorras, kus turvapoliitikad nõuavad, et kasutajatel ei tohi olla ligipääsu väljaspool ühiskasutuse piire asuvale infole, on soovitav kasutada seadistust „wide links = no”. Juhtudel, kus seatakse kõrgeid nõudmisi jõudlusele ning kus on tarvis sellele vaatamata takistada juurdepääsu andmetele, mis asuvad väljaspool ühiskasutuse piire, pakub Samba veel ka üht täiendavat võimalust, millega kaasneb aga kahjuks suurem administreerimistööde maht. Parameeter „ root directory ” määrab ära, millisesse kataloogi Samba pärast lähtestamist ümber lülitub. Selleks kasutatakse chroot() süsteemikutset. Standardina kehtib „ root directory = / ”. Juhul, kui see parameeter seadistatakse väärtusele „root directory = /var/fileserver /”, ei saa mitte ükski Samba käivitatud protsess tulevikus ligi pääseda andmetele väljaspool asukohta „ /var/fileserver/ ”. See puudutab ka mõningaid faile, mida on tarvis Samba korrektseks tööshoidmiseks.

Sellistel juhtudel tuleb tagada, et asukohas /var/fileserver/ oleksid Samba jaoks kättesaadavad järgmised failid:

- Fail nimega etc/passwd.
- Juhtudel, kus kasutatakse Samba printimisfunktsioone, läheb printimisfunktsiooni kasutamiseks tarvis kõiki binaarfaile või konfiguratsioonifaile.

Lisaks võib juhtuda, et asukohas /var/fileserver/ tuleb Samba jaoks kättesaadavaks teha veel ka täiendavaid faile. See sõltub kasutatavast operatsioonisüsteemist.

[netlogon] ühiskasutus

Ühiskasutusega [netlogon] saab Samba klientide jaoks kättesaadavaks teha operatsioonisüsteemiga ühilduvaid poliitikaid või sisselogimisskripte. Juhul, kui konfigureeritakse ühiskasutus [netlogon], tuleb tagada, et volitamata isikutel ei oleks mitte mingil juhul võimalik muuta selle ühiskasutuse alla kuuluvaid faile. Seda on võimalik saavutada näiteks ühiskasutust kajastava parameetriga „ read only = yes ”.

Kasutajaandmebaasid

Samba ei suuda kasutajate autentimiseks rakendada Unixoperatsioonisüsteemi mehhanisme. Samba peab Windowsi maailmas kasutatavad kasutajaparoolide räsiväärtused (LAN Manager (LM) ja/või NTLM-Hashes) eraldi salvestama. Räsiväärtuste salvestamiseks kasutab Samba niinimetatud Backend -e. Lisaks räsiväärtustele võib Samba, sõltuvalt kasutatavast Backend-ist, kasutajate kohta ka veel täiendavat infot salvestada. Backend -lahendusena saab kasutada tavalist tekstifaili, andmebaasi, või LDAP-kataloogiteenust, mida pakub nt OpenLDAP. Versioonides Samba 3.0.0 kuni 3.0.23 sai kasutada mitut Backend -i korraga. Varasemad ja ka hilisemad Samba versioonid seda võimalust enam, ei paku.

Backend -ide alla kuuluvad:

- smbpasswd - Selle Backend -i puhul salvestatakse kontoandmed tavalisse tekstifaili. Vastupidiselt Backend -idele tdbsam ja ldapsam ei suuda see Backend salvestada 200x SAM-i (Security Account Manager i) andmeid. Seetõttu pole soovitav seda Backend -i kasutada uue installatsiooni loomisel.
- tdbsam - Seda Backend -i on soovitav kasutada Backend -i smbpasswd asemel, vaatamata sellele, et tegu ei ole veel standardse seadistusega. Kontoandmed salvestatakse Trivial Database (TDB) faili.
- ldapsam - Selle Backend -i puhul salvestatakse kontoandmed LDAPkataloogi. See tagaprogramm sobib ennekõike suurtesse võrkudesse, eriti neil juhtudel, kus kasutatakse Samba Primary Domain Controller /BDCSetup-i.

Tuleb tagada, et kasutajal ei õnnestuks tagaprogrammist räsiväärtusi välja lugeda. Seetõttu peaks tagaprogrammide smbpasswd ja tdbsam puhul olema failidele, kuhu salvestatakse kasutajate andmeid, lugemis- ja kirjutusõigusega juurdepääs ainult „ root ”-kasutajal. Kõikidel teistel kasutajatel ei tohiks seda tüüpi failidele olla mitte mingisugust juurdepääsu. Juhul, kui kasutatakse tagaprogrammi ldapsam, tuleks pääsuõiguseid kehtestada sarnasel moel, kasutades Access Control List -e (ACL-e). Kuna Windowsi keskkonnas on räsiväärtused sama tähendusega nagu loetava teksti kujul paroolid, ei tohiks kasutajad neile ligi pääseda. Selle väite tagajärgede selgitamiseks tutvustame järgnevalt lühidalt Windowsi NTLM- ja NTLMv2-autentimisprotseduuri. Protseduur, millega Windows-arvutid krüpteeritud

autentimist võimaldavad, põhineb sümmeetrilisel krüpteerimisalgoritmil ning see viiakse ellu Challenge-Response protseduuriga.

Suuresti üldistades toimib protseduur järgmiselt:

1. Enne seda, kui SMB-Client loob ühenduse serveriga, peab kasutaja sisestama oma kasutajanime ja parooli. Seejärel rakendab klient sisestatud parooli suhtes räsifunktsiooni ning salvestab sellest tekkiva räsiväärtuse.
2. Klient loob ühenduse serveriga ja saab vastuseks juhusliku arvu, mida nimetatakse ka väljakutseks (Challenge).
3. Klient krüpteerib väljakutse sümmeetrilise krüpteerimisalgoritmiga ja rakendab seejuures kasutaja parooli räsiväärtust kui võtit.
4. Klient edastab serverile kasutajanime ja krüpteeritud väljakutse (Response).
5. Server loeb oma kasutajate andmebaasist kasutaja parooli sisaldavalt andmeväljalt välja kasutaja räsiväärtuse. Windowsi keskkonnas ei salvestata kasutajate andmebaasi mitte kasutajate loetaval kujul esinevad paroole, vaid ainult paroolide räsiväärtuseid. Seejärel kasutab server välja loetud räsiväärtust selleks, et dekrüpteerida kliendi käest laekunud vastus (Response). Juhul, kui tulemus langeb kokku juhusliku arvuga, mille server edastas kliendile sammus nr 2, on autentimine osutunud edukaks. Vastasel korral autentimine ebaõnnestub.

Juhul, kui ründe toimepanija pääseb ligi isiku kasutajanimele ja räsiväärtusele, võib ta toimida järgnevalt: olukorras, kus SMB-kliendile edastatakse parooli kujul kasutajanimi ja räsiväärtus, rakendab SMB-klient sisestatud parooli suhtes tavaliselt veel üks kord räsifunktsiooni ning saadab alles seejärel vastuse edasi serverisse. Sellises olukorras autentimine ebaõnnestub. Kui aga ründaja rakendab hoopis SMB-klienti (nt mõnda smbclient-i mugandatud versiooni), mis edastab sisestatud kasutajanime ja parooli serverile ilma eelnevalt räsifunktsiooni rakendamata, võib ta ennast edukalt autentida. Sel põhjusel on loetaval kujul paroolide räsiväärtused Windowsi keskkonnas sama tähtsad nagu loetaval kujul paroolid.

Kontrollküsimused:

- Kas ühiskasutuse [netlogon] juurdepääsudel on kirjutamisõigus takistatud?
- Kas on tagatud, et turvarežiimi share ei kasutata?
- Kas on tagatud, et turvarežiimi server ei kasutata?
- Kas Samba kasutab autentimiseks eranditult Kerberost, juhul, kui ITkooslu-se turvapoliitikad seda ette näevad?
- Kas Samba rakendab autentimisel eranditult NTLM-protseduuri versiooni nr 2 (NTLMv2)?
- Kas Sambat käitatakse turvarežiimis ads , juhul, kui IT-koosluses rakendatakse asukohtade kontseptsiooni?
- Kas Samba teenusele on juurdepääs ainult valitud kasutajatel ja kasutajagruppidel?
- Kas Samba on konfigureeritud selliselt, et see aktsepteeriks vaid turvaliseks peetavate hostide ja võrkude ühendusi?

- Kas Samba on konfigureeritud selliselt, et see ühendaks ennast vaid turvaliseks peetavate võrguaadressidega?
- Kas kasutajate juurdepääsu infole väljaspool ühiselt kasutatavaid ressursse takistatakse, juhul, kui IT-kooslusele kehtivad turvapoliitikad seda nõuavad?
- Kas smbpasswd-tagaprogrammi kasutamisest on loobutud?
- Kas on tagatud, et kasutajatel ei õnnestuks rakendatavast tagaprogrammist kasutajaparoolide räsiväärtuseid volitamata välja lugeda?

M 4.329 Sideprotokollide turvaline kasutamine Samba serveri kasutamisel

Algatamise eest vastutavad:infospetsialist, IT-juht
Rakendamise eest vastutavad: administraator

Sideprotokollide seadistuste vale konfiguratsioon võib pärssida Samba serveri poolt pakutavate teenuste käideldavust ja turvalisust. Rakendatavate sideprotokollide turvalise kasutamise tagamiseks on seetõttu soovitav kasutusele võtta järgnevad meetmed.

NetBIOS

Samba suudab ainukesena kasutada Network Basic Input/Output süsteemi (NetBIOS-t) Transmission Control protokolli (TCP)/Internet protokolli (IP) kaudu. Usaldusväärselt töötava võrgu jaoks on ülimalt oluline, et Windowsi klientidel kasutataks ainult neid protokolle, mida ka reaalselt vaja läheb. Kui Windows kasutab näiteks lisaks TCP/IP-le veel ka võib-olla NetBEUI-d (NetBIOS Extended User Interface'i), pole üheselt kindel, kas Windowsi võrgukeskkond kasutab NetBEUI-d või TCP/IP-d. Tänapäeval läheb tavaliselt ainult TCP/IP-d tarvis . Internetwork Packet Exchange (IPX) võib olla veel vajalik, kui Netware-süsteemid peavad ligi pääsema Samba serverile.

Krüpteerimine

Server Message Block (SMB) protokoll ei toeta andmepakettide krüpteerimist. Meetmes M 4.334 SMB Message Signing ja Samba kirjeldatud meetmega saab kaitsta ainult edastatavate andmepakettide terviklust. Edastatud info kõrgema kaitsevajaduse korral tuleks seetõttu edastatud info krüpteerimine tagada täiendatavate meetmete abil. Hea võimalus on kasutada Internet Protocol Securityt (IPSec-i) . IPSec võimaldab kaitsta kõiki IP-põhiseid sideühendusi, mis klienti sisenevad või kliendist väljuvad. Seejuures on võimalik autentida kommunikatsiooni lõpppunkte ja edastada andmepakette allkirjastatult ja krüpteeritult nõnda, et tagatakse kõrgendatud turbenõuetega kaasnev andmete terviklikkus ja konfidentsiaalsus. IPSec-infrastruktuuri osakontseptsioon peaks arvestama kasvava administreerimistööde mahuga ja see eeldab testkeskkonnas teostatavat asjaosaliste süsteemide ühilduvuse kontrolli. Enamatel juhtudel tuleb kindlasti arvestada ka IPSeci kasutamisest tuleneva suureneva arvutusvõimsusega ja selle võimaliku pärssiva mõjuga serveri koormuskäitumisele.

Täiendavad kontrollküsimused:

- Kas Windowsi klientsüsteemides kasutatakse ainult reaalselt vajaminevaid protokolle?
- Kas võrgu kaudu edastatava info kõrgendatud turbevajaduste korral tagatakse selle info krüpteerimine täiendavate meetmete abil?

M 4.330 Samba serveri turvaline installeerimine

Algatamise eest vastutavad:infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator

Samba-serveri installeerimisel tuleb arvestada mitme asjaoluga, mis mõjutavad otseselt selle turvalisust. Operatsioonisüsteem, mille keskkonnas Samba teenust käitatakse, tuleb installeerida ja konfigureerida, arvestades paljude erinevate turvaaspektidega. Selleks tuleb kasutada vastavaid IT etalonturbe mooduleid. Lisainfot selle kohta, millised on täiendavalt vajalikud sammud serveril, mis Samba teenust käivitab, leiate meetmest M 4.331 Samba serveri operatsioonisüsteemi turvaline konfiguratsioon . Samba teenuse installeerimise oluliseks aspektiks on installeeritava tarkvara terviklus (vt M 4.327 Samba tarkvarapakettide ja lähtetekstide tervikluse ja autentsuse kontroll). Sambateenusega kaasasolev dokumentatsioon on väga detailne ja kirjeldab põhjalikult installeerimiseks vajalikke samme. Mitte ükski etalonturbe meede ei asenda kaasasolevat dokumentatsiooni, vaid juhib ainult tähelepanu punktidele, mis vajavad erilist hoolt. See puudutab Samba-serveri installeerimist kompileeritud lähteteksti alusel. Operatsioonisüsteemi tootjate või levitajate binaarpaketid võivad sellest erineda.

Lähtetekstist kompileerimine ja installeerimine

Kui lähteteksti paketi terviklust ja autentsust on Pretty Good Privacy (PGP) signatuuri alusel kontrollitud, tuleks pakett mõne privileegideta kasutajakonto all lahti pakkida, konfigureerida (skriptiga configure) ja tõlkida (programmiga make). Alles viimane samm, tõlgitud programmi tegelik installeerimine (make install) võib vajada kõrgemaid privileege. Kuid olukorras, kus privileegideta kasutajakontol on olemas kõikide installeerimise sihtkataloogide jaoks kirjutamisõiguseid, on isegi see viimane samm teostatav ilma root volitusteta. Sambat ei soovitata installeerida kontrollimatult, make install abil, serveri juur-failisüsteemi. Sellisel juhul tuleb Samba-teenuse täielikuks deinstalleerimiseks väga palju käsitsi vaeva näha. Installeerimise viimase sammu juures (make install avamine) on mõeldav mõne abivahendi (nt CheckInstall) kasutamine. CheckInstall on programm, mis loob tõlgitud lähteteksti alusel automaatselt pakette erinevate paketihaldussüsteemide jaoks (nt RPM Package Manageri (RPM) või Debiani jaoks). Loodud pakette saab seejärel kasutatud operatsioonisüsteemi paketihaldussüsteemide kaudu installeerida ja vajadusel täielikult deinstalleerida. Kui administraatoril on juba kogemusi, kuidas kasutatava paketihaldussüsteemi jaoks pakette luua, on soovitav Samba versiooni jaoks paketid ise luua. Kui Samba-server tõlgitakse lähtetekstist, tuleb valitud parameetrid täpselt dokumenteerida. Oluline on see, et kompileerimise protseduur oleks vastava dokumentatsiooni alusel alati selgelt mõistetav ja korratav. Lisaks tuleks koostada konfigureerimise ja tõlkimise protseduuri logi (nt suunates väljundinfo edasi mõnda faili) ja see säilitada.

Kõik installeerimissammud tuleb dokumenteerida, et konfigureerimine oleks vajadusel kiiresti korratav. See puudutab lisaks kompileerimise seadistustele ka installeerimise sihtkohti, õiguseid, konfiguratsioonifaili smb.conf muudatusi ja muud sarnast infot. Samba serveri käivitamine peaks üldjuhul toimuma operatsioonisüsteemi Startup-skripti abil. Nii on Samba server ka serveri taaskäivitamisel kohe kasutatav.

Kontrollküsimused:

- Kas tarkvara terviklust kontrolliti enne installeerimist?
- Kas installeerimine ja konfiguratsioon on piisavalt dokumenteeritud?
- Kas lähteteksti pakett pakiti lahti, konfigureeriti ja tõlgiti privileegideta kasutajakonto all?
- Kas Samba installeerimine serveri juur-failisüsteemi toimus kontrollitult?
- Kas on dokumenteeritud, milliste parameetritega kompileerimine käivitati?
- Kas konfiguratsiooni- ja kompilatsiooniprotseduuri väljundinfost on koostatud logi?

M 4.331 Samba serveri operatsioonisüsteemi turvaline konfiguratsioon

Algatamise eest vastutavad: administraator, infoturbespetsialist

Rakendamise eest vastutavad: administraator

Samba serveri operatsioonisüsteemi tuleks turvalise käitamise tagamiseks konfigureerida alljärgneval moel.

ReiserFS ja TDB-formaadis andmebaasid

Samba salvestab mitmesse kataloogi Trivial Database (TDB) formaadis andmebaase. Katalooge, millesse Samba neid andmebaase salvestab, kirjeldatakse meetme M 6.135 Samba serveri tähtsate süsteemikomponentide regulaarne varundamine lõigus „TDB-failid (Konfiguratsiooniandmed ja seisundiinfo)“. Nende kataloogide failid on Samba veatu töö tagamiseks ülimalt olulised. Kõik TBD-formaadis andmebaasid tuleks salvestada partitsioonile, mille failisüsteemiks ei ole ReiserFS (vt G 4.72 Triviaalse andmebaasi vormingus andmebaaside ebakõlad Samba keskkonnas).

Failisüsteemide sidumine

Mõned vajalikud meetmed moodulis B 5.17 Samba eeldavad seda, et failisüsteem, millel Samba ressursse pakub, peab toetama pääsuloendeid (ACL-e). Sambat käitava serveri kernel peab seega toetama pääsuloendeid seoses rakendatava failisüsteemiga. Lisaks tuleb tagada, et failisüsteem ühendataks töösse sobiva parameetriga (mount -prorammi parameeteriga acl), et pääsuloendite tuge oleks võimalik ka aktiveerida. Sama kehtib ka laiendatud atribuutide (Extended Attributes , xattr) puhul, kui neid kasutatakse seoses Sambaga.

Paketifilter

Samba kasutab järgnevalt loetletud Transmission Control protokolli (TCP) ja User Datagram protokolli (UDP) porte:

- port 137/UDP (kasutajaks on protsess nmbd): Network Basic Input/Output System (NetBIOS) Name Service
- port 138/UDP (kasutajaks on protsess nmbd): NetBIOS Datagram Service
- port 139/TCP (kasutajaks on protsess smbd): NetBIOS Session Service . Faili- ja printeriteenused, juhul kui NetBIOSi kaudu kasutatakse Server Message Blocki (SMB).
- port 445/TCP (kasutajaks on protsess smbd): faili- ja printeriteenused, juhul kui TCP/IP kaudu kasutatakse SMB-d.

Lisaks meetmes M 4.328 Samba serveri turvaline aluskonfiguratsioon kirjeldatud meetmetele konfiguratsiooniparameetrite interfaces ja bind interfaces only kohta, tuleks blokeerida kõik mitteloetletud pordid lokaalse paketifiltri liidestes ja Internet Protocol (IP)-aadressid, mille kaudu pole tarvis Sambale ligi pääseda (vt M 4.238 Lokaalse paketifiltri rakendamine).

Täiendavad kontrollküsimused:

- Kas lokaalses paketifiltris on vabad ainult need TCP ja UDP pordid, mida läheb tarvis Samba serveri töö jaoks?

- Kas TDB-formaadis andmebaase salvestatakse eranditult partitsioonidele, mis ei kasuta ReiserFS failisüsteemi?
- Kas Sambat käitava operatsioonisüsteemi kernel toetab pääsuloendeid seoses kasutatava failisüsteemiga?
- Kas vajalike parameetritega failisüsteem on ühendatud?
- Vajadusel: kas Sambat käitava operatsioonisüsteemi kernel toetab xattr-i seoses kasutatava failisüsteemiga?

M 4.332 Samba serveri pääsuõiguste turvaline konfiguratsioon

Algatamise eest vastutavad: infoturbespetsialist, IT-juht
Rakendamise eest vastutavad: administraator

Failisüsteemi keskkonnas jätab Samba pääsuõiguste juhtimise operatsioonisüsteemi kerneli hooleks. Sel põhjusel vajab iga kasutaja Samba serveris nii Windowsi kui ka Unixi kasutajakontot. See tähendab, et iga domeenikasutaja peab eksisteerima Unixi operatsioonisüsteemis kõikide oma grupikuuluvustega. Põhjuseid, miks Samba kasutamisega kaasneb keerukas pääsuõiguste juhtimine, on kaks.

Esiteks ei suuda Samba Windowsi õigustemudelit otse Unixisse üle võtta ja teiseks analüüsib Samba olukorras, kus failisüsteemi poole pöördutakse, järgnevaid kihte:

- Unixi failivolitused
- Samba Share Definitions
- Samba Share pääsuloendid (ACLs)

Unixi failivolitused

Kui kasutaja tahab ligi pääseda Samba serveri ressursile, peab ta end kõigepealt Samba teenusesse sisse logima. Seejärel kontrollib Samba, kas sisselogitud kasutajal on olemas Unixi failisüsteemis juurdepääsuks vajalikud õigused. Samba loob Unixi failisüsteemis Windowsi õigustemudeli struktuuri järgnevalt: standardsest Unixi kolmikust „kasutaja” / „grupp” / „teised kasutajad” (user/group/others) luuakse kolme elemendiga NT ACL. Unixi õigustebitid kantakse seejuures NT-volitustele üle alljärgneva tabeli alusel. „Teiste kasutajate” õigustebitid kannab Samba üle grupile „kõik”. Pääsuloenditesse ei saa teha sissekandeid, mis keelaksid mõne kasutaja puhul teatud NT-volitusi.

NT õigus

	File Attribute Flag
Täielik juurdepääs	#
Kausta läbiotsimine / faili käivitamine	x
Kaustaloetelu koostamine / faili lugemine	r
Atribuutide lugemine	r
Laiendatud atribuutide lugemine	r
Failide koostamine / andmete kirjutamine	w
Kaustade loomine / andmete lisamine	w
Atribuutide kirjutamine	w
Laiendatud atribuutide kirjutamine	w
Alamkaustade ja failide kustutamine	w
Kustutamine	#

Volituste lugemine	vt teksti
Volituste muutmine	#
Omandiõiguste ülevõtmine	#

Tabel: õigustemudeli ülekandmine Unixi failisüsteemidele

Märk „#” tähendab, et seda tingimust määratakse failile või kataloogile ainult kahel tingimusel: Windowsi administraator aktiveerib volituse „täielik juurdepääs”, või kui kasutaja või tema grupp omab Unixi failisüsteemis selle faili jaoks volitusi „lugemine”, „kirjutamine” ja „käivitamine”. NT-õigus „õiguste lugemine” määratakse kasutajale alati, kui kasutajale antakse vähemalt veel mõni teine NT-õigus. Kui Windows NT4 määrab õiguseid, mida selles tabelis pole, ignoreerib Samba neid. Võimalikud olemasolevad Portable Operating System Interface (POSIX) pääsuloendite sissekanded kannab Samba NT-õigustemudelile üle samal viisil. POSIX-i ACL-e kasutab Samba ainult selleks, et määrata õiguseid kasutajatele ja gruppidele juhtudel, kus nad pole faili või kataloogi omanikud.

Samba tunneb DOS-i atribuutide näitamiseks mitut võimalust. Need atribuudid on failide omadused, mida sellisel kujul Unixi keskkonnas ei ole. Samas eeldavad mitmed võrguketta poole pöörduvad rakendused õigeid DOS-i atribuute.

DOS tunneb nelja atribuuti, mida on võimalik failidele anda:

- Read-Only (kirjutuskaitse) - Sellise faili sisu saab ainult lugeda, kuid mitte kirjutada. Faili ei saa kustutada. Kuna aga DOS-i all saab DOS-i atribuute määrata iga kasutaja oma äranägemise järgi, ei ole selle atribuudi puhul tegu tõhusa kirjutuskaitsega. Kirjutuskaitsebitt on ainult abistav meede juhusliku vale kasutamise ärahoidmiseks.
- System (süsteem) - See fail on mõeldud operatsioonisüsteemi tööülesannete jaoks.
- Hidden (peidetud) - Seda faili kasutajale ei näidata (näiteks kui ta kasutab Windows Explorerit või käsuviiba käsku „dir”).
- Archive (arhiiv) - Arhiivibitt määratakse igal kirjutaval pöördumisel. Varundusprogrammidel on õigus see bitt nullida. See võimaldab inkrementaalset varundamist.

Samba kannab DOS-i atribuudid standardina üle Unixi bittidele:

Atribuut	Unixi õigus	Mask	Parameeter	Standardväärtus
Kirjutuskaitse	w-omanik	200	*map read only*	*yes*
Arhiiv	x-omanik	100	*map archive*	*yes*
Süsteem	x-grupp	010	*map system*	*no*

Peidetud	x-teised	001	*map hidden*	*no*

Tabel: DOS-i atribuutide ülekandmine Unixi failisüsteemidele

Kuna õigust „käivitamine” DOS-i all ei ole, saab vastavat bitti kasutada selleks, et näidata DOS-i atribuute Unixi failisüsteemis. DOS-is leiduval kirjutuskaitse bitil on Unixis olemas ligilähedane vaste failiomaniku kirjutamisõiguse näol. Samba peab Unixi õigustest looma Windowsi failiomaduste dialoogakna jaoks failidele sobivad atribuudid. Lisaks peab Samba määrama uutele failidele Unixi õigused. Uue faili loomisel edastab klient serverile soovitud DOS-i atribuudid. Sellest kliendi soovist moodustab Samba Unixi pääsuõiguste kogumi. Neid õiguseid piirab parameeter „create mask ”. Standardseadistus „ create mask ” parameetri jaoks on 744, mis vastab maskile rwxr–r–. Failiomanikul on kirjutamis- ja lugemisõigused, kõigil teistel on ainult lugemisõigused.

Samba piirab õiguseid sellega, et ühendab soovitud õiguste kogumi loogilise JA-operatsiooni abil create mask- iga. Uues loodavas failis võivad esineda ainult need õigused, mis on „ create mask ” parameetris määratud. Sellele järgneva sammuga määrab Samba selgelt soovitud pääsuõigused, lähtudes parameetrist „force create mode”, mille standardväärtuseks on 000. Selleks ühendatakse selle väärtusega liides VÕI. Kui uue faili lugemisõigust tohivad omada ainult faili omanikud ja lugemisõiguste grupp ning ülejäänud ei tohi faili lugeda, määratakse „ create mask ” parameetri väärtuseks 740. See välistab ülejäänud maailma lugemisõiguse.

Kui lisaks sellele peab omanike grupp omama kirjutamisõigust, saab selleks kasutada seadet „ force create mode = 020 ”. Tabel näitab protseduuri:

Ülesanne			rw-r–r–
create mask	740	JA	rw-r——
			rw-r——
force create mode	020	VÕI	—-w—-
tulemus			rw-rw—-

Olukorras, kus failis smb.conf on seadistus „ map read only = yes ”, käitub Samba järgnevalt: kui määratakse DOS-i atribuut „kirjutuskaitse”, seab Samba failisüsteemi objekti omanikud/grupp/teised „w”-biti väärtusele „0”. Samba ignoreerib pääsuloendite „w”-bitte. Kui aga DOS-i atribuut „kirjutamiskaitse” eemaldatakse, siis seab Samba ainult failisüsteemi objekti omaniku „w”-biti väärtusele „1”.

Grupi/teised „w”-bitid jäävad väärtusele „0”. Lisaks on veel parameeter „ map read only = Permissions ”. Selle parameetri kohta leiate lisainfot smb.conf dokumentatsioonist man pages. Tuleb arvestada, et Samba parameetrid „ create mask ” ja „ directory mask ” võivad takistada Unixi õigustebiti määramist, mille tagajärjel ei võeta DOS-i atribuute üle. Tulbas „ Mask ” antakse minimaalselt vajalikud

väärtused parameetritele „ create mask ” ja „ directory mask ”, mida läheb tarvis, et Samba saaks määrata kõik vajalikud Unixi õigustebitid. Teatud tingimustel võib Unixi õiguste vahel esineda konflikte, mis tulenevad DOS-i atribuutidest ja Unixi volitustest, mis omakorda tulenevad Windowsi pääsuloendist. Neid Samba poolt standardina kasutatavaid parameetreid DOSi- atribuutide ülekandmiseks Unixi failisüsteemile ei tohiks kasutada. Selle asemel tuleks Sambat seadistada selliselt, et DOS-i atribuudid salvestataks parameetri „ Extended Attributes ” alla.

Selleks tuleb konfiguratsioonifailis smb.conf teha järgnevad seadistused:

- store dos attributes = yes
- map archive = no
- map read only = no

Samba Share Definitions

Administraator saab erinevate konfiguratsiooniparameetrite abil konfiguratsioonifailis smb.conf mõjutada juurdepääsude juhtimist ressursside kasutamisele ja käitumist, mis määrab, millal kasutajad ressurssidega suhtlevad. Kasutaja- ja grupipõhised konfiguratsiooniparameetrid kirjutavad Unixi failisüsteemis kehtivad kasutajate või gruppide juurdepääsuõigused üle.

Kasutada saab järgnevaid konfiguratsiooniparameetreid:

- admin users
- force group
- force user
- guest ok
- invalid users
- only user
- read list
- username
- valid users
- write list

Järgnevad konfiguratsiooniparameetrid kontrollivad ressursside käitumist failideja kaustadega seotud operatsioonides. Enne mõne sellise parameetri muutmist tuleks vaadelda konfiguratsioonifaili smb.conf dokumentatsiooni (man pages):

- create mask
- directory mask
- dos filemode
- force create mode
- force directory mode
- force directory security mode
- force security mode
- hide unreadable

- hide unwriteable files
- nt acl support
- security mask

Lisaks on veel mitmeid seadistusi, mis mõjutavad ressursside käitumist erinevatel viisidel. Enne mõne sellise parameetri muutmist tuleks vaadelda konfiguratsioonifaili smb.conf dokumentatsiooni (man pages):

- case sensitive, default case ja short preserve case
- csc policy
- dont descend
- dos filetime resolution
- dos filetimes
- fake oplocks
- hide dot files, hide files ja veto files
- read only ja selle vastupidised sünonüümid writeable ja writable
- veto files

Kõikide konfiguratsiooniparameetrite põhjaliku kirjelduse leiate konfiguratsioonifaili smb.conf dokumentatsioonist („man smb.conf").

Samba Share pääsuloendid
Sambaga saab, sarnaselt Windowsiga, luua iga ressursi jaoks pääsuloendi. Standardina pole ükski piirang aktiivne. See tähendab, et kasutajal „igaüks" on volitused „täielik kontroll". Samba salvestab ressursside pääsuloendid faili share_info.tdb. Kuid Samba ise ei paku programmi nende pääsuloendite administreerimiseks. Seega on administraator sunnitud kasutama Windowsi.

Windowsi all saab administraator kasutada järgmiseid võimalusi:

- Windowsi avatud failihalduris tuleb toimida järgnevalt: tehke parempoolne hiireklõps ühiskasutusse antud kaustal. Omadused | Turvalisus. Selles aknas saab administreerida ressursi pääsuloendi sissekandeid.
- Et kasutada Computer Management Snap-In- i MMC jaoks, tuleb toimida järgnevalt. Esmalt laetakse MMC Computer Management Snap-In- iga: System Control / Management / Computer managemen t. Seejärel Action | Connect to another computer. Sisestage Samba-serveri hosti nimi. Selleks, et luua ühendust arvutiga, läheb kasutajal domeenis tarvis administraatori priviileege.

Kui Samba-serveriga on ühendus edukalt loodud, saab teha järgnevat:
valige System | Shared Folders | Shares. Seejärel tehke paremas aknas paremklõps ressursile, mida tahetakse administreerida | valige registrikaart „ Security ". Selles aknas saab administreerida ressursi pääsuloendit.

Kui kasutajalt „igaüks" võetakse ära kõik õigused, ilma teda ressursi pääsuloendist täielikult kustutamata, pole ühelgi kasutajal sellele ressursile enam pääsuõigust.

Selle põhjuseks on asjaolu, et kasutaja õiguseid vähendavatel pääsuloendi sissekannetel on prioriteet selliste pääsuloendite sissekannete ees, mis kasutaja õiguseid suurendavad.

Kontrollküsimused:

- Kas DOS-i atribuutide näitamiseks Unixi failisüsteemis kasutatakse laiendatud atribuute (Extended Attributes)?
- Kas administraatoritel on selge, kuidas loob Samba Windowsi õigustemudelit Unixi failisüsteemis?
- Kas administraatorid teavad, millistel põhimõtetel saavad uued, loodud failid endale Unixi õigused?
- Kas administraatorid mõistavad, kuidas mõjutab DOS-i atribuudi „kirjutuskaitse” eemaldamine Unixi õiguseid?
- Kas administraatorid teavad, et kasutaja- ja grupipõhised konfiguratsiooniparameetrid kirjutavad Unixi failisüsteemis kehtivad kasutajate või gruppide juurdepääsuõigused üle?

M 4.333 Winbindi turvaline konfigureerimine Samba keskkonnas

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator

Kui Sambat kasutatakse „ domain ”- või „ ads ”- turvarežiimis (vt M 4.328 Samba serveri turvaline aluskonfiguratsioon), on Winbindi turvaline konfiguratsioon ülimalt oluline. Sel juhul tuleb arvestada terve rea soovitustega. Domeeni liitumisel suudab smbd kasutajat domeenikontrolleris (DC) autentida. Sõltuvalt turvarežiimist ja kliendist toimub see Kerberos-pileti analüüsimisega või päringu esitamisega domeenikontrollerile. Eriti just viimane meetod on küllaltki töömahukas, kuna smbd peab esmalt leidma domeenikontrolleri ja end sinna sisse logima, alles seejärel saab ta hakata kasutajat autentima. See tekitab vähemalt 30 võrgupaketti, millest ainult kaks on autentimiseks olulised. Windows töötab teisiti. Local Security Authority (LSA) loob domeeniliikme käivitamisel ühenduse domeenikontrolleriga ja autendib end masinana. Kõik kasutaja autentimised toimuvad seejärel ainult selle ühenduse kaudu. Seda põhimõtet ei saa ellu viia ainult smbd abil, kuna iga kliendi jaoks on eraldi smbd-protsess ja mitu protsessi ei saa võrguühendusi samaaegselt kasutada. Seega saab domeenikontrolleriga ühendamisel proksina kasutada Winbindi. Sellel on sarnane funktsioon nagu LSA-l Windowsi all. Üheks eriomaduseks on see, et ta hoiab ühenduse domeenikontrolleriga avatuna ja pakub oma teenuseid kõikidele süsteemi protsessidele, kasutades Unixi domeeni soklit (Unix Domain Socket) asukohas /tmp/winbindd/pipe. Smbd-protsessid püüavad autentimisel end esmalt selle sokliga ühendada. Alles siis, kui need ebaõnnestuvad, loovad protsessid ise ühenduse mõne domeenikontrolleriga.

Lisaks edukale autentimisele vajab Samba täiendavat infot kasutaja kohta.

Samba-serveril peab iga kasutaja jaoks olema üks Windowsi ja üks Unixi konto.

Unixi kasutajakontot läheb muuhulgas vaja selleks, et Samba saaks failisüsteemi juurdepääsukontrolli jätta Kerneli hooleks (vt M 4.332 Samba serveri pääsuõiguste turvaline konfiguratsioon). See tähendab, et iga domeenikasutaja peab eksisteerima Unixi operatsioonisüsteemis kõikide oma grupikuuluvustega. Teoreetiliselt on võimalik kõiki domeenikasutajaid Unixi all uuendada ka käsitsi. Seda ei tasuks siiski teha, selle asemel tuleks kasutada Winbindi. Juhul, kui neid veel pole, suudab Winbind Windowsi kasutajatele ja gruppidele vastavaid Unixi kasutajaid ja gruppe luua dünaamiliselt. Seejuures kasutatakse „nss_winbind”-moodulit, mida saab ühendada sissekandega faili /etc/nsswitch.conf.

See võib olla näiteks järgnev:

- passwd: files winbind
- group: files winbind

Selle seadistusega otsib operatsioonisüsteem kasutajanimesid esmalt failis /etc/passwd. Kui sealt sobivat kasutajat ei leita, võetakse ühendust Winbindiga.

Selleks et Winbind suudaks kasutajanime jaoks kõik vajalikud Unixi kasutajaatribuudid (nt kasutaja ID, isikliku kataloogi või Login-Shell -i) dünaamiliselt luua, peab deemon läbima kaks sammu. Esmalt küsib Winbind DC-lt kasutajanime turva-ID-d (Security Identifier , SID). Seejärel peab Winbind, kuna DC tavaliselt ei tunne kasutaja Unixi kasutaja-ID-d, iseseisvalt leidma SID-ga sobiva Unixi kasutaja-ID.

Winbindi tegutsemine sõltub konfigureeritud ID-vastenduse tagaprogrammist:

- tdb - Tegu on standardseadistusega. Kui mõni kasutaja, kellele pole veel Unixi kasutaja-ID-d määratud, logib sisse, siis määrab Win-bind kasutajale eelnevalt seadistatud alast järgmise vaba Unixi kasutaja-ID ja salvestab ID-vastenduse lokaalselt tdb-faili. ID-vastendused salvestatakse faili winbindd_idmap.tdb. Selle faili kaotamisega kaasneb kõikide failisüsteemis välja jagatud õiguste kaotamine. Selle tagajärjeks võivad olla tõsised turvaaugud nagu järgnevas näites. Kasutaja „Kasutaja1” logib end Windowsi kasutajanimega BERLIN\kasutaja1 esimest korda Samba-serverisse. Kasutajal BERLIN\kasutaja1 on Windowsi domeenis SID S-1-5-12-7623811015-3361044348-030300820-1013. Windbind reserveerib vaba Unixi kasutaja-ID ja seob SID-lga Unixi kasutaja-ID 2000. See vastendus salvestatakse faili winbindd_idmap.tdb. Pärast edukat sisselogimist salvestab kasutaja BERLIN\kasutaja1 Samba-serverisse mõned failid. Need salvestatakse Unixi kasutaja-ID 2000 alla. Pärast faili winbindd_idmap.tdb ebaõnnestunud varundamist lähevad mõned sinna salvestatud vastendused kaduma. Mõni aeg hiljem logib kasutaja „Kasutaja2” oma Windowsi kasutajanimega BERLIN\kasutaja2 Samba-serverisse. Kasutajal BERLIN\kasutaja2 on Windowsi domeenis SID S-1-5-12-7623811015-3361044348-030300820-1017. Kuna Unixi kasutaja-ID 2000 määramine läks andmekao tõttu kaduma, seob Winbind selle nüüd Kasutaja2 SID-ga. „Kasutaja2” saab nüüd avada kõiki faile, mida „Kasutaja1” esialgu Unixi kasutaja-ID 2000 alla salvestas. Seetõttu tuleb faili winbindd_idmap.tdb regulaarselt varundada. Lisaks meetmes M 6.135 Samba serveri tähtsate süsteemikomponentide regulaarne varundamine leiduvatele selgitustele ja soovitustele saab ID-vastendust varundada ka järgnevalt. Käsk „ net idmap dump ” juhatab loetavas tekstivormis faili juurde, mida saab vajadusel „net idmap restore” abil taastada.
- rid - See Backend kasutab Unixi kasutaja-ID algoritmilise arvutamise jaoks Relative Identifier- it (RID), Windowsi SID-i viimase sidekriipsu taga asuvaid märke. Selle tagaprogrammi puhul ei vajata andmebaasi, kuna vastendus toimub deterministlikult.
- ad - Seda tagaprogrammi saab kasutada, kui Active Directory -s on juurutatud Services For Unix (SFU) täiendused ja Sambat käitatakse „ads”-turvarežiimis. Selle täienduse raames saab administraator Active Directorys eraldi Unixi kasutaja-ID-sid määrata. Winbind peab selle tagaprogrammi puhul ID-vastendusi ainult lugema. ID-vastenduste täiendamise või muutmisega Winbind ei tegele. Lisaks on selle tagaprogrammi puhul tegu ainukese Backend -iga, mida Winbind saab kasutada, et hankida täiendavaid Unixi kasutajaatribuute (nt kasutaja isiklikku kataloogi või Login-Shell -i). Kõikide teiste tagaprogrammide puhul tuleb selleks kasutada teisi mehhanisme, nt konfiguratsiooniparameetreid „ template shell ” ja „ template homedir ” kon-

figuratsioonifailis smb.conf.

- ldap - See tagaprogramm salvestab enda valitud ID-vastendused Lightweight Directory Access Protocol (LDAP) kataloogi.
- nss - See tagaprogramm ei kasuta SID-del põhinevat vastendamist, vaid eeldab, et domeenikontroller ja domeeniliige suudavad /etc/passwd infot muude vahenditega sünkroniseerida, nt nss_ldap abil. Kui mõni süsteem küsib siiski Winbindilt vastendamist, tagastab ta selle nimepõhiselt. See tähendab, et ta muudab esmalt SID-i vastavaks kasutajanimeks ja otsib nime /etc/passwd alt. See tagaprogramm vabastab Winbindi parameetri „ winbind trusted domains only ".

Lisainfot ID-vastenduse erinevate tagaprogrammide kohta leiate nende juhistest man pages alt. Need on nimetatud põhimõttel „idmap_". Sisestus „man idmap_nss" pakub lisainfot nss-tagaprogrammi kohta. Igal ID-vastenduse tagaprogrammil on individuaalsed konfiguratsiooniparameetrid. Veaanalüüsiks tuleks kasutada programmi „wbinfo". Lisaks Unixi kasutaja-ID-le peab Winbind tavaliselt iga kasutajaga siduma ka täiendavaid Unixi kasutajaatribuute, nt isikliku kataloogi. Seda saab suunata parameetriga „template homedir" või „template shell". Ainult ID-vastenduse tagaprogrammi „ad" puhul on, nagu juba selgitatud, kasutada ka üks teine mehhanism. Kui domeeni liikmeks on ainult üks Samba-server ja Unixi kasutaja-ID-sid pole tarvis kogu serveri ulatuses sünkroniseerida, võib kasutada ID-vastenduse tagaprogrammi tdb. Kui domeeni liikmeks on mitu Samba-serverit ja seega tuleb Unixi kasutaja-ID-sid kõikide serverite ulatuses sünkroniseerida, tuleb kasutada mõnd muud ID-vastenduse tagaprogrammi. Kui IT-kogumi domeenide vahel on olemas usaldussuhe, tuleb ellu viia lõigu „Domeenidevahelised usaldussuhted" soovitused.

Domeenidevahelised usaldussuhted

Usaldussuhe on suhe domeenide vahel, mille abil saab autentida domeeni kasutajaid sellise domeenikontrolleri abil, mis asub teises domeenis. Ka siis, kui IT-kogumi domeenide vahel ei ole veel usaldussuhteid, on tulevikku arvestades mõistlik selle lõigu meetmed ellu viia.

Unixi kasutaja-ID-d

Windows määrab igale kasutajale ja igale grupile ainulaadse ID, ehk SID (Security Identifier). SID sisaldab üht 96-bitist domeenisektsiooni ja üht, domeenis ainulaadset, RID-d (Relative Identifier). Seni, kuni IT-kogumis on ainult üks domeen, saab Unix kasutada RID-d, et arvutada ainulaadseid Unixi kasutaja-ID-sid. Kui IT-kogumis on mitu domeeni, mis usaldavad üksteist, ei saa seda meetodit enam kasutada. Kui domeen, milles Samba-server on liikmeks, usaldab teist domeeni, pole RID enam ainulaadne. RID „500" tähistab administraatorit, RID „513" on määratud domeenikasutajate grupile ja 1000-st ülespoole annab iga domeen järjestikku RID-sid. Alates Samba versioonist 3.0.25 on olemas parameeter „idmap domains". See parameeter võimaldab konfigureerida ID-vastendust domeeni nimest olenemata.

```
[global]
idmap domains = BONN BERLIN
idmap config BONN:backend = rid
idmap config BONN:range = 10000 - 49999
idmap config BERLIN:backend = rid
```

idmap config BERLIN:range = 50000 – 99999

Eelpool olevas näites määrataks kasutajale BONN\administraator Unixi kasutaja-ID 10500, samal ajal saaks kasutaja BERLIN\administraator Winbindi poolt Unixi kasutaja-ID 50500.

Kui IT-kogumi domeenide vahel on olemas usaldussuhted, siis tuleb kasutada üht alljärgnevaist ID-vastenduse tagaprogrammist:

- tagaprogramm rid koos idmap domeenikonfiguratsiooniga
- tagaprogramm ldap koos idmap domeenikonfiguratsiooniga
- tagaprogramm ad
- tagaprogramm nss

Unixi isiklik kataloog

Kasutaja domeen tuleks lisada tema isikliku kataloogi asukohta. See meede aitab vältida usaldussuhete puhul esineda võivat nimekonflikti. Kasutaja „Kasutaja1" peab domeenis BERLIN saama teistsuguse isikliku kataloogi kui kasutaja „Kasutaja1" domeenis BONN. Seda saab teha järgneva sissekandega konfiguratsioonifailis smb.conf:

template homedir = /home/%D/%u

Selle asemel on võimalik kasutajate isiklikke katalooge hooldada ka Active Directory (AD) abil, kui Winbind kasutab ID-vastenduse tagaprogrammi „ad".

Ülemises näites määrataks kasutajale BERLIN\kasutaja1 Unixi isiklik kataloog /home/BERLIN/kasutaja1. Winbind ei loo isiklikke katalooge automaatselt. Kui Samba-serverit kasutataks näiteks failiserverina, poleks see ka mõistlik.

Unixi kasutajanimi

Kasutajanimede ainulaadsuse tagamiseks tuleb Windowsi kasutajanimed järgneval viisil Unixi kasutajanimedeks ümber muuta. Windowsi kasutaja BONN\kasutaja1 kasutajanimi Unixis on BONNkasutaja1. Standardina on parameetri „ winbind separator " eelseadistuses kasutusel märk „\". Kui eelseadistatud märk tekitab Unixi süsteemides probleeme, näiteks kui märgil „\" on Unixi sisestuste jaoks eriline tähendus, saab konfiguratsioonifailis smb.conf määrata mõne muu märgi. Parameetri „ winbind separator " muutmise korral tuleb eelnevalt kontrollida, millistes kohtades on domeenikasutajad ja -grupid määratud (nt konfiguratsioonifailis smb.conf). Kõiki neid kohti tuleb pärast parameetri muutmist vastavalt muuta.

Kontrollküsimused:

- Kas Winbind on konfigureeritud selliselt, et Unixi kasutaja-ID-d ei satuks omavahel konflikti?
- Kas Winbind on konfigureeritud selliselt, et usaldussuhetega domeenide isiklike kataloogide nimed ei satuks omavahel konflikti?
- Kas Winbind muudab Windowsi kasutajanimed ainulaadseteks Unixi kasutajanimedeks?
- Kas ID-vastendusest tehakse regulaarselt varukoopiaid?

M 4.334 SMB Message Signing ja Samba

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator

Samba 3 versioon toetab Server Message Block -i (SMB) Message Signingut. SMB Message Signingu puhul lisatakse igale paketile allkiri. Nii teab klient, et pakett pärineb õigest serverist ja server, et pakett pärineb õigelt kliendilt. SMB Message Signingu puudumisel ohustavad SMB-protokolli Man-in-the-Middle -rünnakud. Microsoft toetab SMB Message Signingut. Konfiguratsiooniparameeter client signing on seatud auto peale, kuid server signing on seatud disabled peale. Need eelseadistused failis smb.conf kattuvad suuremalt jaolt Microsofti operatsioonisüsteemide omadega (lisainfot Microsoft Knowledge Base artiklist #887429).

Microsoft aktiveeris SMB Message Signing -u standardina ainult domeenikontrollerites, kuna SMB Message Signing pärsib märkimisväärselt jõudlust. Väiksemate andmehulkade ülekandmisel võib jõudluseprobleeme tavaliselt eirata. Suurte andmehulkade puhul võib jõudlus mõnes olukorras kuni poole võrra väheneda. Soovitav oleks järgida Microsofti seadistusi, muidugi juhul, kui need ei ole vastuolus IT-koosluse olemasoleva turvapoliitikaga. Kui Sambat kasutatakse domeenikontrollerina, siis peaks konfiguratsioonifailis smb.conf all olema seadistus server signing = yes. Kui Sambat kasutatakse ainult failiserverina, tuleks kasutada standardseadistust.

Kontrollküsimused:

- Kas SMB Message Signingu seadistus on Sambas kooskõlas IT-koosluse kehtiva turvapoliitikaga?
- Kas SMB Message Signingut kasutatakse, juhul, kui Sambat kasutatakse domeenikontrollerina?

M 4.335 Samba serveri turvaline kasutamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator

Samba-serveri turvalisuse tagamiseks selle käitamise ajal ei piisa ainuüksi turvalise algkonfiguratsiooni loomisest. Täiendavalt tuleb regulaarselt kasutada mitmeid meetmeid, et tuvastada võimalikke probleeme juba varakult. Samba serveri käitamisel tuleb arvestada ennekõike järgmiste aspektidega:

- Konfiguratsioonis tehtavad muudatused tuleb hoolikalt dokumenteerida, et igal ajal oleks võimalik kontrollida, kes ja mis põhjusel muudatusi tegi ja mida muudeti. Konfiguratsioonifailide muudatuste jaoks oleks mõistlik kasutada revisjoniprogramme (nt git, mercurial või RCS). Nii saab igal ajal taastada varasema konfiguratsiooni seisundi, samuti on alati näha, kes mida ja mis põhjusel muutis.
- Pärast iga failis smb.conf tehtud muudatust tuleb esmalt programmiga testparm kontrollida, kas konfiguratsioonifaili süntaks on õige. Konfiguratsioonifaili süntaksivigade tagajärjeks võib olla serveri taaskäivitamise takistamine või turvaaukude teke.
- Samba kasutusõiguseid tuleb regulaarselt kontrollida (vt M 4.332 Samba serveri pääsuõiguste turvaline konfiguratsioon). Eriti tuleb seda teha pärast tarkvara uuendamist või konfiguratsiooni muutmist. Serveri enda failidest (nt serveriprogrammist smbd või konfiguratsioonifailist smb.conf) tuleb luua kontrollsummad ja neid regulaarselt kontrollida.
- Administraatorid peavad ennast kasutatud tarkvaras avastatud turvaaukude suhtes võimalikult varakult kurssi viima (vt M 2.35 Teabe hankimine turvaaukude kohta). Uute leitud turvaaukude infot avaldab Samba meeskond alati samba-teavitusmeilide nimekirja kaudu (http://lists.samba.org/archive/samba-announce/). Ülevaadet kõikide seniavastatud turvalisust puudutavate paikade kohta pakub lisaks http://www.samba.org/samba/security/.
- Meetmes M 2.64 Logifailide kontroll kirjeldatud meetmed tuleb ellu viia ka Samba kontekstis. Tavaliselt salvestavad rakendused nmbd, smbd ja winbind oma logiandmed kataloogi /var/log/samba/.
- Turvalise kasutamise juurde kuuluvad ka regulaarsed andmevarunduse ja avariiolukorraks ettevalmistamise meetmed (vt M 6.135 Samba serveri tähtsate süsteemikomponentide regulaarne varundamine).

Täiendavad kontrollküsimused:

- Kas konfiguratsioonis tehtavad muudatused dokumenteeritakse hoolikalt, et igal ajal oleks võimalik kontrollida, kes muutis mida ja millisel põhjusel?
- Kas pärast iga konfiguratsioonifaili smb.conf muudatust kontrollitakse programmiga testparm, kas süntaks on jätkuvalt õige?
- Kas Samba-serveri aktiivseid juurdepääsuõiguseid kontrollitakse regulaarselt?
- Kas administraatorid kontrollivad regulaarselt, kas Sambas on avastatud uusi turvaaukusid?

- Kas Samba-serveri logifaile kontrollitakse regulaarselt?
- Kas andmevarunduse ja avariiolukorraks ettevalmistamise meetmeid rakendatakse regulaarselt?

M 4.336 Hulgilitsentslepinguga Windowsi süsteemide aktiveerimine alates Windows Server 2008-st

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: administraator, IT-juht

Hulgilitsentslepingu Windows 7 või Windows Server 2008 litsentside aktiveerimine kannab ka nime Volume Activation 2.0 (seisuga sügis 2007).

Sobiva aktiveerimise valimine

Eristatakse alljärgnevaid aktiveerimisvõimalusi:

- MAK-proksiaktiveerimine (Multi Activation Key, mitmekordse aktiveerimise võti),
- MAK-ist sõltumatu aktiveerimine
- KMS-aktiveerimine (Key Management Service, võtmehaldusteenus).

Nende aktiveerimismeetodite piires on veel täiendavaid jaotuseid, mida iseloomustavad erinevad suhtluskanalid, mida kasutatakse Microsoftiga litsentsiinfo vahetamiseks.

Toetatakse interneti ja telefoni kasutamist. Litsentsiinfost moodustab ühe osa võtmematerjal, mis sisestatakse aktiveerimise käigus aktiveeritavasse klienti või abitööriistadesse ja abiprogrammidesse automaatselt või käsitsi.

Tuleb valida õige aktiveerimismeetod. Valikukriteeriumite hulka kuulub aktiveeritavate klientide arv, samuti kliendi ühenduse olemasolu LAN-i ja internetiga. Järgnevalt on ära toodud võimalikud sobivate aktiveerimismeetodite kriteeriumid ja iga aktiveerimismeetodi olulisemad omadused.

Sobivate aktiveerimismeetodite valikukriteeriumid

„Volume Activation 2.0" on ülikeerukas protseduur, mida saab käesolevas tekstis tutvustada vaid pealiskaudselt. Lisainformatsiooni leiate Microsofti dokumentatsioonist.

Alljärgnev tabel aitab valida võimalike aktiveerimismeetodite vahel, tuginedes võimalikele kriteeriumitele, nt aktiveeritavate klientide arvule ja kasutatavatele sideühendustele. Pärast tabelit tutvustatakse neid aktiveerimismeetodeid lähtuvalt valitud omadustest. Sellele järgneb üldine info.

Sihtsüsteem	Aktiviseerimismeetod	Kirjeldus

Windows Server 2012 või Windows 8, mõlemad vähemalt kord 180 päeva jooksul võrguühenduses Active Directory'ga	Aktiveerimine Active Directory kaudu	Kui on olemas turvalise ühendusega asukoht tuumvõrguga, saab Windows Server 2012 või Windows 8 keskkonnas olevatel süsteemidel kasutada aktiveerimist Active Directory kaudu.
Windowsi versioonid enne Windows Server 2012 ja Windows 8, mis on vähemalt kord 180 päeva jooksul võrguühenduses, KMS-aktiveerimise piirväärtus ületatakse.	KMS	Kui on olemas turvalise võrguühendusega asukoht, saab võrgu kaudu aktiveerimiseks kasutada KMS-i.
Ilma võrguühenduseta või isoleeritud võrkudega arvutid või Windowsi versioonid enne Windows Server 2012 ja Windows 8, mille puhul ei saavutata KMS-i aktiveerimise piirväärtust.	MAK	Sõltumatu MAK-aktiveerimine telefoni või interneti kaudu arvuti jaoks, millel luuakse harva või ei looda kunagi ühendust tuumvõrguga.

1. Aktiveeritavate klientide juurdepääs firma LAN-ile
2. Multi-Activation-Key -proksi (MAK-proksi) internetijuurdepääs firma LANis, olukord nr 1 tarbeks.
3. Aktiveeritava kliendi internetijuurdepääs
4. Key Management serveri (KMS) internetijuurdepääs firma LAN-is

Aktiveerimismeetodite valitud omadused

Olukord 1, MAK-proksiaktiveerimine LAN-i ja interneti kaudu

- Administraator installeerib ühe korra LAN-i IT-süsteemile VAMT-i (Volume Activation Management Tool). VAMT-i rakendatakse MAK proksina ja hulgilitsentside haldamiseks.
- Litsentsiinfo vahetamiseks suhtleb iga klient LAN-is MAK-proksiga ja MAK-proksi suhtleb Microsoftiga interneti kaudu.
- Igale kliendile paigaldatakse vajalik litsentsiinfo (MAK-litsentsivõti) automaatselt.
- Aktiveerimist pole tarvis uuendada.
- Aktiveerimise alguses tuleb määrata võimalike aktiveerimiste arv. Vajadusel saab litsentse juurde osta.

Olukord 2a, MAK-ist sõltumatu aktiveerimine interneti kaudu

- Administraator peab iga kliendi ükshaaval aktiveerima.
- Litsentsiinfo vahetamiseks suhtleb iga klient Microsoftiga interneti kaudu.
- MAK-litsentsivõti installeeritakse igale kliendile automaatselt.
- Aktiveerimist pole tarvis uuendada.
- Aktiveerimise alguses tuleb määrata võimalike aktiveerimiste arv. Vajadusel saab litsentse juurde osta.

Olukord 2b, MAK-ist sõltumatu aktiveerimine telefoni kaudu

- Administraator peab iga kliendi ükshaaval aktiveerima.
- Litsentsiinfo vahetamiseks suhtleb administraator Microsoftiga telefoni kaudu.
- MAK-litsentsivõti tuleb igas kliendis käsitsi sisestada.
- Aktiveerimist pole tarvis uuendada.
- Aktiveerimise alguses tuleb määrata võimalike aktiveerimiste arv. Vajadusel saab litsentse juurde osta.

Olukord 3a, KMS-aktiveerimine LAN-i ja interneti kaudu

- Administraator installeerib KMS-i ühe korra mõnesse LAN-is asuvasse IT-süsteemi.

KMS toetab serverioperatsioonisüsteemi Windows Server 2008.

Olukord 3b, KMS-aktiveerimine telefoni ja LAN-i kaudu

- Sarnane olukorrale 3a, ainult et KMS ja Microsoft ei suhtle interneti kaudu.

Selle asemel helistab administraator litsentsiinfo vahetamiseks Microsofti. Seejärel sisestab administraator Microsofti käest telefoni teel saadud litsentsiinfo ühekordse toiminguna KMS-i.

Lisainfo

- Aktiveerimismeetodeid saab sõltuvalt vajadustest ja võrgu omadustest suvaliselt kombineerida.MAK-aktiveerimine (olukorrad 1, 2a ja 2b) eeldab administraatori õiguste olemasolu. Vajadusel saab aktiveerida ka standardkasutaja, kui talle antakse vastav registrivõti.

Kontrollküsimused:

- Kas sobiv aktiveerimismeetod on valitud?
- Kas aktiveerimise tehnilised eeldused on täidetud?
- Kas tehnilised eeldused, eriti just KMS-aktiveerimise puhul, on täidetud?

M 4.337z BitLockeri Drive Encryption kasutamine

Algatamise eest vastutavad: IT-juht,

Rakendamise eest vastutavad: administraator, kasutaja, IT-juht, infoturbe, turvaspetsialist

Lisaks kõvaketta krüpteerimisele kasutatakse BitLocker Drive Encryption it (BDE-d) ka süsteemitervikluse tagamiseks buutimise ajal. See eeldab, et Windowsi arvutil on olemas TPM (Trusted Platform Module). BitLocker on kasutusel alates Windows Server 2008 versioonidest Enterprise ja Ultimate. BitLockeri peamine turbe-eesmärk on tagada andmete konfidentsiaalsus ajal, mil süsteem on välja lülitatud. Windowsi käivitamisel laadib BitLocker endasse krüpteeritud kõvakettapartitsioonide võtmed ning hoiab neid enda sees kogu selle aja vältel, mil klient on sisse lülitatud. Seega ajal, mil süsteem töötab, ei kaitse BitLocker konfidentsiaalsust mitte mingil määral. Kõikide Windowsiga töötava kliendi andmete konfidentsiaalsust tuleks kaitsta BDE-ga. See kehtib eriti kaasaskantavate klientsüsteemide kohta, mille puhul on kaotamise ja varguse ohvriks langemise oht tavapärasest suurem ning mille riistvara ei paku ühtki samaväärse toimega ajamikrüpteeringut ega autentimist. Krüptograafilise võtmematerjali konfidentsiaalsust ja käideldavust puudutav turbeaste tuleb hinnata vähemalt sama suureks nagu krüpteeritavate andmete oma. Kui BitLockerit soovitakse kasutada korraga mitmes süsteemis, tuleb juba varem planeerida ka asjakohane võtmehaldus, mida saab BitLockeri puhul teha näiteks Active Directoryga. BitLockeri kasutamisel mitmes süsteemis korraga tuleks järgida ka moodulit B 1.7 Krüptokontseptsioon .

BitLockeri kasutuselevõtu ettevalmistamine

BDE kasutamiseks peaks Windows arvutil olema TPM. BitLocker toetab TPMi alates versioonist 1.2 (kaasa arvatud). TPM on turvakiip, mille on määratlenud Trusted Computing Group (TCG). Lihtsustatult võib TPM-i ette kujutada emaplaadile külge joodetud Smartcard -ina. Kui Windowsi arvutil on olemas Trusted Platform Module (TPM), saab BitLocker kasutada seda võtme salvestamiseks, võtme kontrollimiseks ja süsteemitervikluse tagamiseks buutimise ajal. TPM-ita võib BitLocker kasutada võtmesalvestina ka USB-andmekandjat, kuid tervikluse kaitse pole sel juhul enam tagatud. BitLocker krüpteerib nn lihtköiteid (simple volumes).

Lihtköide koosneb täpselt ühest partitsioonist (muus olukorras võib köide koosneda ka mitmest partitsioonist). Mõisted „köide", „lihtköide" ja „partitsioon" (volume, simple volume, partition) on antud juhul sünonüümid.

Kui Service Pack 1 pole installeeritud, tuleb BitLockeri jaoks kasutusele võtta vähemalt kaks köidet:

- Üks köide operatsioonisüsteemi jaoks (tavaliselt C-ketas). Seda köidet nimetatakse edaspidi buutimispartitsiooniks. Buutimispartitsioon peab olema formaaditud NTFS-failisüsteemiga. BitLocker krüpteerib buutimispartitsiooni täielikult, erandiks on buutimissektor ja ala, mis sisaldab BitLockeri metaandmeid.

- Süsteemipartitsioon peab olema formaaditud NTFS-failisüsteemiga. Süsteemipartitsiooni suurus peab olema vähemalt 1,5 GB Windows 7 ja Windows Server 2008 puhul vähemalt 100MB.

Kui Windowsiga töötavas süsteemis seni käivituspartitsioon (start partition) puudus, siis alates Windows 7-st luuakse selline partitsioon BitLockeri installimise või aktiveerimise käigus automaatselt. BitLockeri aktiveerimine ja taustprotsessina töötav krüpteerimine võivad põhjustada ebakõlasid installitud tarkvaraga. Nende õigeaegseks avastamiseks tuleb BitLocker aktiveerida pärast Windowsi installimist ja enne täiendava tarkvara installimist. Kui käivituspartitsiooni hakatakse looma alles hiljem, tuleks töötavast terviksüsteemist teha kõigepealt varukoopia.

BitLockeri aktiveerimise protsessi saab BitLockeri käsuviibatööriistaga ka automaatseks muuta. Selleks ei tohi automatiseerimisskriptid sisaldada taastamisparoole. Selle asemel tuleks BitLockeri jaoks juba varem planeerida ja kasutusele võtta tsentraalselt toimiv võtmehaldus, nt Active Directory baasil. Ülejäänud partitsioonid, nt andmepartitsioon, tuleks krüpteerida tavapärasest suuremate turbevajaduste korral, välja arvatud juhul, kui see peaks tekitama teatud rakendustega ühildumise probleeme. Kasutada tuleks eranditult NTFS-partitsioone.

Grupipoliitikate planeerimine

Kui BitLockerit kasutatakse korraga mitmes süsteemis, tuleks krüpteerimisseadistuste juhtimiseks ja seadistuste järgimise tagamiseks rakendada grupipoliitikaid. Kui tsentraalne võtmehaldus on üles ehitatud Active Directoryga, ei pääse grupipoliitikate planeerimisest ei üle ega ümber. Järgmistes lõikudes kirjeldatakse Windowsi grupipoliitika Computer Configuration | Administrative Templates | Windows Components | BitLocker Drive Encryption olulisemaid seadistusi.

Kasutajale sobiva autentimismeetodi valimine

BitLockeri edukaks käivitamiseks saab administraator konfigureerida mitmeid erinevaid meetodeid kasutaja autentimiseks:

- „Autentimine puudub” - See eeldab, et Windows arvutil on olemas TPM. BitLocker käivitub kasutaja jaoks märkamatult.
- Autentimine USB-pulgaga ehk „omand” - See variant on võimalik Windows arvutis sõltumatult TPM-i olemasolust. TPM-i puudumisel salvestatakse krüpteerimiseks vajalik BitLockeri võtmematerjal USB-pulgale. TPM-i olemasolul jaotatakse see võtmematerjal TPM-ile ja USB-pulgale.
- Autentimine PIN-iga ehk „teadmine” - See eeldab, et Windows arvutil on olemas TPM. TPM kontrollib sisestatud PIN-i.
- Mitmefaktoriline autentimine USB-pulga ja PIN-iga - See eeldab, et Windows arvutil on olemas TPM. TPM on teatud osa võtmematerjali salvesti ja kontrollib PIN-i.

Kasutaja autentimiseks BitLockeriga tuleb valida sobiv meetod. Siinkohal tuleb arvestada järgnevate punktidega ja neid omavahel võrrelda:

- „Autentimine puudub” võib olla sobilik valik juhul, kui kasutajad ei aktsepteeri peale lokaalsele sisselogimisele arvutis või domeenis ühtki teist sisse-

logimismeetodit ega ka nendega seotud autentimismeetodeid nagu PIN-e ja/või USB-pulkasid. Kuna seadistus „Autentimine puudub” pakub kõige vähem kaitset, tuleks seda kasutada ainult erijuhul.

- „Autentimine puudub” koos TPM-iga soodustab tuntud ründemeetodeid, mille abil saab volitusteta kasutaja BitLockeri krüpteeringust jagu. Seadistusega „Autentimine puudub” laetakse buutimisel BitLockeri võtmematerjal automaatselt TPM-ist Windowsi arvuti töömälusse (RAM , Random Access Memory). See toimub enne kasutaja sisselogimist. Ründemeetodid võimaldavad volitamata kasutajal võtmematerjalile ligi pääseda, kuid selle eelduseks on füüsiline juurdepääs Windowsi arvutile. Selline ründemeetod nõuab eritööriistu ja ründajalt vastavat kõrget kvalifikatsiooni. Taoliste ründemeetodite vältimiseks soovitatakse autentimisvahenditena kasutada PIN-i ja/või USB-pulka.
- Erinevalt USB-pulgaga autentimisest ohustab PIN-iga autentimist klahvinuhi (keylogger) olemasolu. Klahvinuhke on nii tark- kui riistvaralisi. Klahvinuhid salvestavad kasutaja klahvisisestused ja muudavad need volitamata kolmandatele isikutele väärkasutuseks kättesaadavaks. Tarkvarapõhine klahvinuhk peab ületama Windowsi süsteemiterviklust kaitsvad kaitsemehhanismid. Teine PIN-iga seonduv oht esineb siis, kui PIN-i sisestamiseks kasutatakse juhtmeta klaviatuuri. Seda ülekannet on võimalik pealt kuulata. Seega, kui juhtmeta andmeedastuseks ei kasutata krüpteeringut või kui rakendatav krüpteering on nõrk, ei tohiks PIN-i sisestamiseks kasutada juhtmeta klaviatuuri.
- USB-pulgaga autentiminst pole soovitatav rakendada kaasaskantavas arvutis, kuna USB-pulka hoitakse sageli arvutiga samas kohas (nt sülearvuti kotis).
- Kõrgendatud turvanõuete puhul võib autentimisvahenditena kasutada USB-pulka ja PIN-i. Selline mitmefaktoriline autentimine on võimalik alles alates Windows Server 2008st ja samuti Windows 7s ja Server 2008 R2s.

Kõiki siin tutvustatud nelja autentimismeetodit võib kasutada ka kogude (pool) puhul, kui ühel kaasaskantaval Windowsi arvutil on mitu kasutajat. Kõikidel kasutajatel peab sel juhul olema sama PIN ja/või sama võtmematerjal USB-pulgal. Alternatiivse lahendusena saab kasutusele võtta TPM-i ja individuaalsed autentimisvõtmed, mis salvestatakse igale USB-pulgale (võimalik ainult käsuviibaga). Alates Windows 7-st tuleks aktiveerida komplekssete PIN-koodide grupipoliitika (Operating System Drives | Enhanced PINs for Startup). Osa riistvara- ja buutimiskonfiguratsioonid, nt vanemat tüüpi PXE buutimiskeskkonnad, seda ei toeta, mistõttu tuleks sellistest konfiguratsioonidest loobuda.

Krüpteeritud Windowsi süsteemide taastamine hädaolukorras

Taastamisparoolid ja -võtmed võimaldavad administraatoril hädaolukorras, st kui TPM-is on defekt või kui kasutaja on enda käivitamis-PIN-koodi või USB-pulga ära kaotanud, krüpteeritud andmeid taastada. Lisaks võimaldavad need jätkata Windowsi käivitusprotsessiga olukorras, kus BitLocker on tuvastanud kas BIOS-is või mõnes muus BitLockeriga kaitstavas buutimiskomponendis manipuleerimise. Windowsi turvalise režiimi käivitamiseks, nt hooldamiseks või vigade kõrvaldamiseks, läheb samuti tarvis taastamisparooli või -võtit. Kõvakettapartitsioonide krüpteerimisel tuleb administraatoril valida 48-kohaline taastamisparool. Selleks koostatakse standardina juhuparool. See tuleks kas välja printida või tekstifailina

kuhugi turvalisse kohta salvestada. Taastamisparooli säilitamine tuleb meetme M 2.22z Paroolide deponeerimine kohaselt täpselt dokumenteerida. Taastamisparoolid peavad olema sama konfidentsiaalsed ja nendega tuleb sama hoolikalt ümber käia nagu käivitamis-PIN-koodi ja smartcard 'iga. Kooskõlas meetmega M 4.86 Krüptomoodulite kindel rollijaotus ja konfigureerimine tuleb kindlaks määrata, kas ja kuidas taastamisparoole ja -võtmeid tsentraalselt deponeeritakse ning kes tohivad nendele andmete taastamise eesmärgil juurde pääseda. Et tagada sellise info parem kaitse ja kiirendada andmete taastamist hädaolukorras, on soovitatav need andmed ilma kasutaja sekkumata automaatselt Active Directorysse salvestada ning muudel juhtudel peaks süsteem tagama, et BitLockeri krüpteerimisfunktsiooni ei rakendata (grupipoliitika „Choose how BitLocker-protected operating system drives can be recovered"). Detsentraliseeritud võtmehalduse korral tuleks kaaluda, kas taastamisparoolist ja -võtmest peaks looma varukoopiad ning kas neid peaks hoidma kusagil sobivas kohas eraldi. Kõikidel juhtudel tuleb täpselt dokumenteerida, millised on taastamiseks vajalikud tööetapid, kes tohib andmeid taastada ja mis ressursse tohib selleks kasutada (mooduli B 1.7 Krüptokontseptsioon. Kui taastamisparool valitakse käsitsi või kui seda muudetakse tagantjärele, tuleb kindlasti vältida lihtlabaseid järjestusi (vt M 2.11 Paroolide kasutamise reeglid). Kui on kahtlus, et PIN-kood, USB-pulk, taastamisparool või -võti on kompromiteeritud, tuleb määrata uus võti. Selleks saab kasutada käsuviibatööriistu manage-bde.wsf (Server 2008) või manage-bde.exe (alates Windows 7-st, Server 2008 R2-st) ning asjakohast taastamisparooli või -võtit. Sel moel saab tõkestada ja uuesti koostada ka kaduma läinud või rikkis USB-pulki ja/või PIN-koode. Grupipoliitikaga saab kehtestada ka nõude, et iga krüpteeritud andmekandja jaoks koostatakse 256-bitine taastamisvõti. Taastamisvõti võimaldab andmekandja sisule juurde pääseda ka näiteks siis, kui algsed autentimisvahendid ei ole enam kättesaadavad.

Taastamisvõtit ei saa välja printida ning seda ei saa suuliselt, nt telefonis edasi öelda. Nii suureneb küll andmete konfidentsiaalsus, kuid hädaolukorras kulub andmete taastamiseks palju rohkem aega. Taastamisvõtmeid võib salvestada kas üksnes mõnele USB-mälupulgale või failidena Active Directorysse. Seevastu süsteemide puhul, milles töödeldakse väga suurte konfidentsiaalsusnõuetega andmeid, tohib lubada üksnes taastamisvõtmeid, kuid taastamisparoolidest tuleb loobuda.

Alates versioonidest Windows 7 ja Server 2008 R2 saab administraator lisameetmena installida andmetaastusviisardi (Group Policy snap-in | Computer Configuration | Windows Settings | Security Settings | Public Key Policies | BitLocker). See on universaalse taastamisvõtme avalik osa ja see installitakse ühtmoodi kõikidesse BitLockeri klientidesse. Selle juurde kuuluva privaatvõtmega saab krüpteeritud andmekandja sisu dekrüpteerida. Privaatvõti ei tohiks olla administraatori valduses. Andmetaastusviisardite rakendamine eeldab väga tugevaid meetmeid, mis välistaksid nende väärkasutuse. Viisardi väljavahetamine on kompromiteerimise korral väga töömahukas. Seega ei suuda andmetaastusviisard asendada ei taastamisparoole ega -võtmeid, vaid pakub üksnes andmekadudevastast lisakait-

set sellistele kasutajatele, kes ei ole liidetud tsentraalselt toimivasse võtmehaldusse.

Võtmematerjali hävitamine

Niipea kui krüpteeritud andmekandja eemaldatakse kasutuselt või kui see on kaotsi läinud, tuleb kõik sellega seotud võtmed ja paroolid viivitamatult hävitada. Tsentraalselt salvestatud võtmete korral, juhul kui võtmega krüpteeritud andmete konfidentsiaalsusnõuded on tavapärasest suuremad, tuleks võtmete hävitamist kajastada revisjonikindlas protokollis.

BitLockeri hooldusrežiimi seire

Hooldustööde ajaks, nt BIOS-i värskendamiseks, peab administraator BitLockeri krüpteerimisfunktsiooni ajutiselt desaktiveerima. Hooldusrežiimis saavad ründajad ja kahjurvara kerge vaevaga BitLockerisse salvestatud võtmematerjali välja nuhkida. Seetõttu tuleks süsteemi seisundit pidevalt jälgida ning eriti hoolikalt tuleb pöörata tähelepanu võimalikele BitLocker Driveri tüüpi teadetele. Kui logides kajastuvad kas ebaootuspäraselt pikad hooldusfaasid, krüpteerimis- ja/või dekrüpteerimisprotsessid või kui sündmuste kuvas esineb lünki, tuleks olukorrast teavitada infoturbespetsialisti. Turvaintsidendi avastamisel tuleb klient täielikult uuesti krüpteerida. Võtmete ja taastamisparoolide muutmisest sellisel juhul ei piisa (vt G 3.97 Konfidentsiaalsuse kadu vaatamata draivide krüpteerimisele BitLockeriga).

Kasutajate koolitamine

Kasutajatele tuleb selgitada, kuidas BitLockeriga ümber käia ning milliseid kõvaketta partitsioone BitLocker krüpteerib ja milliseid mitte. Lisaks tuleb kasutajatele õpetada, kuidas toimida õigesti ning milliste kontaktisikute poole pöörduda olukorras, kus käivitus-PIN-kood, USB-võti või smartcard on kaotsi läinud.

BitLocker ja energiasäästurežiimid

Windowsi arvuti, mida hetkel ei kasutata ja mis pole välja lülitatud, võib töötada energiasäästurežiimis. Windowsi süsteemides on olemas energiasäästurežiimid Standby , Hibernate ja Hybrid Sleep. Standby režiimis jääb BitLockeri võtmematerjal Windowsi arvuti töömällu (RAM-i). Seetõttu ohustab BitLockeriga krüpteeritud andmete konfidentsiaalsust RAM-is asuv BitLockeri võtme ründemeetod. Selle ründemeetodi vältimiseks soovitatakse Standby režiimis töötavat Windowsi arvutit mitte kunagi järelevalveta jätta. Alternatiivideks on Hibernate ja väljalülitamine. Standby režiim on kaasaskantavate arvutite puhul tavaline energiasäästumeetod. RAM-is asuva BitLockeri võtme ründemeetod ei mõju Hibernate režiimi puhul, kuna võtmematerjal kirjutatakse krüpteeritult kõvakettale ega jää töömälusse.

Hybrid Sleep on Windows kasutusele võetud uuendus. See režiim kombineerib omavahel Standby ja Hibernate režiimid. Sarnaselt Standby režiimile ohustab RAM-is asuva BitLockeri võtme ründemeetod ka Hybrid Sleep režiimi. Seega tuleks vältida Hybrid Sleep režiimi kasutamist, kui BitLocker peab kaitsma kõrge konfidentsiaalsusega andmeid ja Windowsi arvuti jääb järelevalveta. Kõikidel juhtudel peab Standby režiimist, Hibernate režiimist või Hybrid Sleep režiimist väljumine olema võimalik alles pärast seda, kui parool on uuesti sisestatud. Selleks tuleb aktiveerida vastavas grupipoliitika objektis User Configuration \ Administra-

tive Templates \ System \ Power Management seadistus Prompt for password on resume from hibernate / suspend.

BitLocker väga suurte turbenõuete korral

Kasutada tuleks grupipoliitikat „Deny write access to fixed drives not protected by BitLocker" asukohas BitLocker Drive Encryption | Fixed Data Drives. See tõkestab kirjutavad juurdepääsud nii tagantjärele loodud andmepartitsioonidele kui ka kõikidele lisaks loodud sisemistele kõvaketastele. Kõik tavalised andmepartitsioonide tuleb sel juhul siiski krüpteerida. Krüpteerimistugevuse saab 128-bitise AES Diffuserilt suurendada 256-bitise AES Diffuserini (grupipoliitika - Choose drive encryption method and cipher strength). Kuna sellise seadistuse korral koormab krüpteerimisprotsess CPU-d varasemast palju rohkem, tuleks seadistuse töövõimet enne kasutuselevõttu kindlasti katsetada (eelkõige nõrgamate näitajatega sülearvutites). Grupipoliitikaga „Configure TPM platform validation profile" saab aktiveerida täiendavaid integreeritud riistvararühmi, et suurendada rootkit 'ide turvet manipulatsioonide suhtes. Virtuaalsete andmekandjate krüpteerimine BitLocker To Go-ga kõvaketastel, mis on ise juba BitLockeriga krüpteeritud (topeltkrüpteerimine), on küll põhimõtteliselt võimalik, kuid kasutu, sest mõlemas krüpteerimisprotsessis kasutatakse ühte ja sama krüpteerimisalgoritmi, st dekrüpteerimistarkvara suhtes suuremat kaitset ei saavutata. Seevastu võtmehalduse kompleksus ja vastuvõtlikkus vigadele suurenevad ning süsteemi töökiirus väheneb. Seetõttu tuleks BitLockeri puhul topeltkrüpteerimist vältida.

BitLockeri tööriistad

Microsoft pakub tööriistu BitLockeri ettevalmistamiseks, konfigureerimiseks, administreerimiseks ja avariiolukordadega toimetulekuks:

- TCG BIOS DOS Test Tool (tcgbios.exe) on mõeldud BitLockeri jaoks olulise BIOS-e funktsiooni testimiseks (vt Microsoft Developer Network – MSDN).
- BitLockeri kettaseadme ettevalmistamistööriist (Drive Preparation Tool) valmistab kõvaketta ette kaht köidet eeldava BitLockeri kasutamiseks (vt Knowledge Base , artikkel 930063).
- Graafiline kasutajaliides BitLocker Control Panel GUI on mõeldud BitLockeri haldamiseks. Eelduseks on TPM-i olemasolu.
- Käsuviiba tööriist manage-bde.wsf on mõeldud BitLockeri haldamiseks. TPM pole hädavajalik.
- Recovery Password Viewer on mõeldud Active Directory taastamisparoolide haldamiseks (vt Knowledge Base , artikkel 928202).
- Repair Tool on mõeldud andmete varundamiseks kahjustatud köidetest, mis on krüpteeritud BitLockeriga (vt Knowledge Base , artikkel 928201).

BitLockeri sobivuse piirid

Kui Windowsis on tarvis käivitada ka veel mõnda muud operatsioonisüsteemi (multiboot- süsteem), tuleks kõvaketta krüpteerimiseks kasutada programmi, mis suudab iga operatsioonisüsteemi süsteemipartitsiooni dekrüpteerida ükshaaval ja teistest partitsioonidest sõltumatult. BDE ei sobi kasutamiseks multiboot - süsteemides. BitLockeri asemel saab kasutada ka EFS-i (Encrypting File System), mis krüpteerib partitsioonide asemel hoopis ühekaupa faile (vt M 4.147z EFS-i turvaline kasutamine Windows 'i keskkonnas). EFS-i kasutamine on mõistlik ka

siis, kui kaasaskantavas arvutis hoitavad andmed peavad olema krüpteeringuga kaitstud ka sel ajal, kui Windowsiga töötav arvuti on sisse lülitatud. Sisselülitatud arvuti korral ei kaitse BitLockeri krüpteering andmete konfidentsiaalsust mitte mingil moel. Sellise konfiguratsiooni saavutamiseks EFS-i kasutamata saab virtuaalajameid alates versioonidest Windows 7 ja Windows Server 2008 R2 krüpteerida BitLocker To Go-ga. Virtuaalajamid on andmekandjatest tehtud kujutisfailid, mida saab töötavas süsteemis protsessidesse liita ja nendest eemaldada. Administraatoriõigusteta kasutajad saavad virtuaalajameid tavakasutaja režiimis kolmandate tootjate tarkvaraga ise luua ja nagu USB-pulki ajutiselt süsteemiga liita.

M 4.338 Windows 7 failide ja registri virtualiseerimise kasutamine

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: administraator, infoturbespetsialist, IT-juht

Windowsi pärandrakendused (legacy applications) on rakendused, mis loodi kunagi vanemate Windowsi versioonide jaoks, kuid neid tuleks kasutada ka uuemas Windowsi versioonis, nt Windows 7s. Sageli on standardkasutajate jaoks arendatud pärandrakendused teatud turvapuudujääkidega: pärandrakendused vajavad kirjutamisõigust kriitilise tähtsusega failikaustadele või registri võtmetele. Kriitilise tähtsusega failikaustad on näiteks kaust %ProgramFiles% (tüüpinstallatsiooni puhul C:\Programs) või %SystemRoot% (tüüpinstallatsiooni korral C:\Windows). Kirjutamine nendesse kriitilise tähtsusega aladesse nõuab administratiivseid volitusi. Selle tulemusel, et oleks võimalik kasutada kirjeldatud tüüpi pärandrakendusi, peab standardkasutaja end sisse logima administraatorikonto alt. See ohustab Windowsisüsteemi terviklust kahjulike programmide läbi, mis võivad hakata kasutama sisselogimise konto, antud juhul administraatorikonto, privileege. Windows 7 kasutavad pärandrakenduste turvaliseks kasutamiseks File Virtualization -i ja Registry Virtualization -i meetodit.

Sellega seotud mehhanismid võimaldavad pärandrakendusi käitada standardkasutaja konto alt, st ilma administraatori õigusteta. See takistab tegeliku, mittevirtualiseeritud Windowsisüsteemi tervikluse ohustamist. File Virtualization -i ja Registry Virtualization-i puhul juhib Windows kõik vastava rakenduse kirjutamispöördumised ja vajadusel ka lugemispöördumised ümber, juhul, kui selliste pöördumiste sihiks on kriitilise tähtsusega kataloogi või registri alad, millele juurdepääsuks rakendusel õigust pole. Ümberjuhtimise sihtkohtadeks on spetsiaalsed alad, mis kehtivad ainult sisselogitud kasutaja jaoks. Nende alade tervikluse kahjustamine ei ohusta tegeliku Windowsisüsteemi terviklust, kuid vastava, kasutaja jaoks nähtava, „virtualiseeritud“ süsteemi terviklus seevastu on kaitseta.

Enamatel juhtudel ei tohiks standardkasutajad rakendada selliseid pärandrakendusi, mis töötasid enne Windows 7-t ainult administraatoriõigustega. Sellele vaatamata võib esineda ka olukordi, kus mõne niisuguse pärandrakenduse kasutamine on mõne kas ülesande või äriprotseduuri lõpuleviimiseks vältimatu.

Sellisel juhul võib kaaluda pärandrakenduse kasutamist Windows 7 keskkonnas. Windows 7 on käsuviiba tööriista reg.exe täiendatud käsuga FLAGS. Selle abil saab administraator registri võtmes \HKLM\Software all määrata, kas Registry Virtualization funktsiooni toetatakse või mitte. Kriitilise pilguga tuleb kontrollida, kas kirjeldatud tüüpi pärandrakenduste kasutamine on üldse vajalik. Registry Virtualization toega registrivõtmete arvu oleks mõistlik hoida miinimumis, lähtudes pärandrakenduste vajadustest. Selleks võib kasutada käsuviiba tööriista reg.exe.

Pikemas perspektiivis tuleb siiski kaaluda võimalust, kuidas asendada kirjeldatud ohtusid sisaldavaid pärandrakendusi mõne turvalise rakendusega. Turvalised tavakasutaja rakendused ei vaja kirjutamisvolitustega pöördumisi kriitilise tähtsusega kataloogi ja/või registri aladesse. Turvaliste rakenduste peale üleminek on soovitav veel ka seetõttu, et ka Microsofti enda jaoks on File Virtualization-i ja Registry Virtualization-i meetodid ainult üleminekulahendused seni ebaturvaliste pärandrakenduste jaoks.

Kontrollküsimused:

- Kas kirjeldatud ohtusid sisaldavate pärandrakenduste kasutamise vajadust on kriitiliselt analüüsitud?
- Kas Registry Virtualization piirdub hädavajalike võtmetega?
- Kas on olemas turvalistele rakendustele ülemineku strateegia?

M 4.339 Vahetavate andmekandjate volitamata kasutamise tõkestamine Windows 7-s

Algatamise eest vastutavad: infoturbespetsialist

Rakendamise eest vastutavad: administraator, kasutaja

Windows 7 pakuvad mehhanisme, mis aitavad kontrollida juurdepääsu vahetatavatele andmekandjatele. Vahetatavad andmekandjad on näiteks salvestuskaardid, USB-pulgad, kaasaskantavad kõvakettad, digikaamerad, disketid, CD-d või DVD-d. Neid kasutatakse andmete mobiilseks salvestamiseks ja andmete vahetamiseks IT-süsteemide vahel. Windows 7 süsteemi abil saab andmeid vahetatavalt andmekandjalt lugeda ja sellele salvestada. Ka rakendusi saab vahetatavatelt andmekandjatelt käivitada. Vahetatavate andmekandjate kasutamise alla käib ka vajalike draiverite installeerimine või uuendamine. Windows 7 abil saab grupipoliitikate abil teha seadistusi, mis kontrollivad vahetatavate andmekandjate installeerimist ja kasutamist.

Vahetatavate andmekandjate kasutamisnõuete tuvastamine

Esmalt tuleb tuvastada vahetatavate andmekandjate kasutamisnõuded. Selleks tuleb vaadelda tööalaseid ülesandeid, mille täitmiseks võib teatud kasutajatel tarvis minna vahetavaid andmekandjaid. Nõnda saab selgitada, milliseid vahetatavaid andmekandjaid tuleks lubada ja/või keelata ning millised peaksid olema nende kasutusvõimalused. Windows 7-s on Microsoft kasutusele võtnud funktsioonid AutoRun ja AutoPlay. Funktsiooniga AutoRun käivitatakse automaatselt programme ja laiendatud sisu (nt meediafaile) olukorras, kus andmekandja asetatakse kas lugerisse või ühendatakse süsteemiga. Funktsiooniga AutoPlay saab kindlaks määrata, millist programmi tuleb erineva sisu käivitamisel kasutada. Nii saab näiteks audio-CD-de jaoks kehtestada reegli, et need käivitatakse MediaPlayeriga. Sellisel juhul käivitatakse audio-CD lugerisse asetamisel automaatselt.

Soovitame tungivalt funktsioonid AutoPlay ja AutoRun desaktiveerida. Nõuded, mille elluviimist tuleks kaaluda, on järgnevad:

- Vahetatavate andmekandjate AutoRun-funktsiooni desaktiveerimine. Vastav grupipoliitika objekt: Turn off Autoplay poliitikas Computer Configuration | Administrative Templates | Windows Components | Autoplay Policies
- Vahetatavate andmekandjate kasutamise piiramine, lubades seda ainult lokaalsetele kasutajatele. Vastavad grupipoliitika objektid: CD-ROM-lugejatele juurdepääsu piiramine lokaalselt sisselokitud kasutajatele poliitikas Computer Configuration | Windows Settings | Security Settings | Local Policies / Security Options | Devices ja All Removable Storage: Deny all access in remote sessions poliitikas Computer Configuration | Administrative Templates | System | Removable Storage Access

Eriti tuleb siin arvestada USB-pulkadega, kuna neid võidakse kasutada ka autentimiseks Windows 7 BitLockeri suhtes. Selleks vajalikud lugemis- ja kirjutamisjuurdepääsud peavad olema lubatud. Windows 7-s saab automaatse taasesituse ära keelata ka asukohas Control Panel | Hardware and Sound | Autoplay. Siin on võimalik täpsustada ka süsteemi käitumist eri tüüpi andmekandjate

korral ning üldist reageerimist vahetatavatele andmekandjatele.

Seadistus „Use AutoPlay for all media and devices” tuleb desaktiveerida.

Vahetatavate andmekandjate kasutusnõuete elluviimine

Vahetatavate andmekandjate kohta väljaselgitatud vajalikud kasutusnõuded tuleb ka ellu viia. Esmajoones tuleks seda teha tehnilisel tasandil, rakendades vastavaid grupipoliitikaid.

Alternatiivina või täiendusena on võimalik kasutada ka töökorralduslikke meetmeid. Grupipoliitikate konfiguratsiooniseadistusi tuleb eelnevalt testida, veendumaks, kas need töötavad korrektselt ja alles seejärel võib neid igapäevatöös kasutama hakata. Vahetatavate andmekandjate rakendamise kohta vastu võetud reeglid tuleb kindlasti teatavaks teha ka töötajatele.

Kontrollküsimused:

- Kas vahetatavate andmekandjate kasutamise nõuded on välja selgitatud?
- Kas vahetatavate andmekandjate kasutamise nõuded on ellu viidud?
- Kas tehnilise teostuse õigsust on testitud?
- Kas kasutajad on vahetatavate andmekandjate kasutamise reeglitest informeeritud?

M 4.340 Windows kasutajakonto haldamise (UAC) kasutamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator, IT-turvaspetsialist

Kasutajakontode haldamine (UAC, User Account Control) on üks Windowsi uusimatest turvaomadustest. See kasutab Least-Privileged User Account printsiipi, et piirata administratiivsete privileegide kuritarvitamise võimalust (vt M 2.32z Piiratud kasutajakeskkonna loomine). Kui kasutajakontode haldamine on sisse lülitatud, töötavad kõik kasutajad standardkasutajatena. Ka administraatorid täidavad oma ülesandeid esmalt standardkasutajatena.

Kasutajakontode haldamine (UAC) tuvastab, kas kasutaja tegevus eeldab tavapärasest suuremaid õigusi, ja annab need talle või keeldub sellest (olenevalt konfiguratsioonist). UAC toimib eranditult vaid lokaalsetele kasutajaseanssidele (ka Remote Desktopi seanssidele). Kui kasutatakse domeenikontosid, siis teistest arvutitest võrgu kaudu ennast sisselogivatele kasutajatele (nt ühiskasutusse antud failidele tehtavad pöördused) see mõju ei avalda. Kui UAC on sisse lülitatud, ei ühildu lokaalsed kontod sugugi mitte kõikide võrgupõhiste haldusteenustega, nt võrgu kaudu IT-süsteemi WMIliidesele (Windows Management Interface) juurde ei pääse. Seetõttu tuleks haldusteenuste ja -tööde jaoks alati kasutada domeenikontosid.

Mõningad tegevused nõuavad siiski lokaalse seansi raames suuremaid õigusi, mida standardkasutajatel pole. Nende tegevuste alla kuuluvad näiteks rakenduste installimine, kirjutav juurdepääs süsteemikataloogidele, juurdepääs vanemat tüüpi töörakendustele, samuti teatud operatsioonisüsteemi programmide ja haldusskriptide käivitamine. Tuleb arvestada, et ka kahjurvara kasutab enda huvides ära tavapärasest suuremaid õigusi. Kui IT-süsteemis kasutatakse administraatoriõigustega kontosid, peaks UAC olema alati sisse lülitatud. Windows Server 2008-s on see tagatud juba standardseadistusega. Seevastu Windows 7-s ja Windows Server 2008 R2-s on UAC tööle seadistatud nõrgendatud kujul. Administraatorikontod saavad piiramatute volitustega edasi töötada, ilma et töölaua kuva peatataks. Selleks, et UAC kaitsefunktsioonid saaksid kahjurvara suhtes toimida, peab olema tööle lülitatud valik „Teavita alati” („Always notify”) asukohas Control Panel | User Accounts | Change User Account Control settings.

Mõju kasutajakeskkonnale

Enne seda, kui tavakasutaja saab käivitada mõne suuremaid õigusi eeldava protsessi, ilmub ekraanile kaitsefunktsioonidega turvatud sisselogimisaken, kuhu kästakse sisestada administraatori autentimise andmed. Selline olukord võib tavakasutajas tekitada ebakindlust ja viia väärkasutuseni. Teisalt jällegi võib see põhjustada nn üle-õla-piilumist, st olukordi, kus hooldustöötaja peab kasutaja juuresolekul korduvalt sisestama enda parooli. Tagajärjeks võib olla parooli juhuslik kompromiteerimine.

Lokaalne turbesuvand „User Account Control:

Behavior of the elevation prompt for standard users” tuleks seadistada väär-

tusele „Automatically deny elevation requests” (asukohas gpedit.msc | Security Settings | Local Policies | Security Options). Alates versioonidest Windows 7/ Windows Server 2008 R2 on selle turbesuvandi nimi „User Account Control: Behavior of the elevation prompt for standard users”. Selle rakendamisel kuvatakse tavakasutajale üksnes tavaline veateade. Kui administraatoritel on tarvis mõne protsessi jaoks tavapärasest suuremaid õigusi, saavad nad jätkuvalt kasutada käsku run as. Kui arvuteid kasutatakse kas suurte või väga suurte turbenõuetega keskkondades, tuleks see suvand alati sisse lülitada. Enne seda, kui administraatorite kasutajagrupi liige saab käivitada protsessi, mis eeldab tavapärasest suuremaid õigusi, kuvatakse talle UAC tavaline kinnitusaken. Teisi autentimisandmeid sisestada ei ole tarvis ning seda selles aknas ei saagi teha. Ainukese erandi moodustab versioonis Windows Server 2008 kasutatav eeldefineeritud konto Administrator, mida kasutajakontode halduse funktsioon ei piira. Kinnitusaken võib siiski administraatori regulaarset tööd ka liigselt pärssida, sest aina korduv andmesisestus muudab vajalikud tööprotsessid pikemaks. Kui erinevaid halduskonsoole on tarvis kasutada sageli, tuleks need koondada üheks MMC-konsooliks (mmc.exe, Microsoft Management Console), et vältida tüütuid korduvaid andmesisestusi.

Administraatori tööülesandeid saab koondada veel ka ülesannete planeerimisega, kolmandate tootjate haldustööriistade ja käsuviiba akendega (PowerShell koos suurendatud volitustega, DOS Box jt). Lisaetappide tagajärgede ja tööprotsesside kokkukoondamise üle tuleks nõu pidada asjaomaste administraatoritega. Kui kinnitusaken takistab administraatoreid efektiivselt töötamast, võib selle ka välja lülitada. Selleks tuleb kasutada GPO-poliitikat „User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode” ja valida seadistus „Elevate without prompting”. Selle tulemusel suurendab UAC administraatori õigusi taustal, st ilma administraatori sekkumiseta. Enne mainitud seadistuse kasutuselevõttu tuleb hoolikalt läbi kaaluda käsitsemismugavust ja turbeastet puudutavad aspektid ning tulemused dokumenteerida. Sellise seadistuse kõige sagedasem kasutusnäide on töökohaarvutid, kus tehakse tööd piiratud kasutajakeskkonnas. Kui administraator peab sellise arvutiga tegema hooldustöid, logib ta end vaid lühikeseks ajaks arvutisse ja püüab hooldustöödega võimalikult kiiresti valmis jõuda. Oma töös ei kasuta ta tavapäraseid kasutajarakendusi kas üldse või kasutab neid väga vähe. Vastupidine näide, st näide olukorrast, kus sellist seadistust kindlasti kasutada ei tohi, on tavakasutajatele mõeldud halduskontod, olenevalt olukorrast ka teisesed kontod, mida kasutatakse regulaarselt või mis tehakse kättesaadavaks kaasaskantavates arvutites.

Administraatorite tööjaamade puhul tuleks asjakohase turvapoliitikaga (vt M 2.325 Windows 7 turvapoliitika kavandamine) kindlaks määrata, kas osa administreerimistöid tuleb teha piiratud kasutajakeskkonnas. Otsuse langetamisel tuleks lähtuda eelkõige tööülesannetest, kasutatavast haldustarkvarast ja kehtivast turbeastmest. Kui piiratud kasutajakeskkonna rakendamine on ette nähtud, tuleks selles turvapoliitikas kindlaks määrata, et turvaline töölaud ja sisselogimise kinnitusfunktsioon jäetakse desaktiveerimata. Kui administraatoritööde valdkonna

jaoks piiratud kasutajakeskkonda ette ei nähta, on soovitatav UAC täielikult välja lülitada. Nõrgendatud seadistusega UAC muudaks kaitsetoime peaaegu olematuks. Samuti jäävad nii alles ka UAC ühilduvusprobleemid, nt seoses WMI-skriptidega. Olenemata UAC konfiguratsioonist tuleb kõik administraatoriõigustega kontod kindlasti dokumenteerida. Regulaarselt tuleb kontrollida administraatoritele antud õiguste vajalikkust ja neid vastavalt kohandada (kui tarvis, tuleb need õigused ka tagasi võtta) (vt M 2.8 IT-rakendustele ja andmetele pääsuõiguste andmine).

Turvaline töölaud (Secure Desktop)

UAC kinnitusteated ja täiendavad sisselogimisaknad on ründajate ja kahjurvara eest kaitstud seni, kuni neid kuvatakse turvalisel töölaual. Eelnimetatud grupipoliitika sisaldab mitmeid lisaseadistusvõimalusi, millega saab turvalisest töölauast mööda hiilida ja seda ka desaktiveerida. Turvalisest töölauast aga ei tohi mööda hiilida ja seda ei tohi ka desaktiveerida.

Internet Exploreri kaitstud režiim (Protected Mode)

Internet Explorer 7 kaitstud režiimi kasutamiseks peab olema sisse lülitatud kasutajakontode haldamine (UAC), mis on Windows 7 puhul standardne konfiguratsioon. Kui kasutajakontode haldamine desaktiveeritakse, lülitab Internet Explorer 7 kaitstud režiimi kohe välja (operatsioonisüsteem asjakohast hoiatusteadet ei kuva).

Kontrollküsimused:

- Kas kasutajakontode haldamine (UAC, User Account Control) on aktiveeritud?
- Kas GPO-poliitika User Account Control: Behavior of the elevation prompt for standard users konfiguratsioonis on valitud seadistus Automatically deny elevation requests ?
- Kas administraatoritele on GPO-poliitika User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode konfigureeritud nõnda, et see lähtub praktilise kasutamise põhimõttest ja vajaliku turbeastme saavutamisest?
- Kas kõik administraatoriõigustega kontod on dokumenteeritud?
- Kas administraatoritele antud õiguste vajalikkus kontrollitakse regulaarselt, kas neid kohandatakse vastavalt oludele ja kas neid võetakse vajadusel ka ära?

M 4.341 Tervikluse kaitse

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: administraator, IT-juht

Microsoft on kasutusele võtnud mitmed uued turvamehhanismid kriitiliste süsteemiressursside tervikluse ja kasutajate andmete tervikluse kaitseks. Nende turvameetmete hulka kuuluvad Windows Integrity Mechanism (WIM), Internet Exploreri Kaitstud režiim (Protected Mode), Windows Ressource Protection (WRP), Trusted Installer ja Windowsi ressursside kontroll (sfc.exe).

Windows Integrity Mechanism (WIM) ja tervikluse tasandid

WIM kaitseb koos kasutajakontode haldamisega süsteemi terviklust ja kasutajate andmeid märkamatuks jäävate, kahjuliku tarkvara poolt põhjustatud tervikluskadude eest. WIM tugineb tehniliselt nn tervikluse tasanditel (Integrity Level, IL), mis on seostatud operatsioonisüsteemi teatud objektidega, nn turvatavate objektidega (Securable Objects). Turvatavad objektid on kasutajakontod, grupikontod, failid, kaustad, protsessid ja registri võtmed.

Operatsioonisüsteemi objektidel on olemas alljärgnevad tervikluse tasandid (loetelu on langevas tähtsuse järjekorras, lähtuvalt terviksüsteemi terviklusest):

- System
- High
- Medium
- Low
- Untrusted

Erinevate terviklusastmetega 0peratsioonisüsteemi objektide omavaheliseks suhtlemiseks saab kehtestada kolm reeglit:

- No write up (nw) - Operatsioonisüsteemi objekt ei saa muuta endast kõrgemal tervikluse tasandil asuvaid objekte, isegi mitte siis, kui nt pääsuloendid (ACL-id) seda lubaksid.
- No read up (nr) - Operatsioonisüsteemi objekt ei saa lugeda endast kõrgemal tervikluse tasandil asuvate objektide andmeid (nt paroole, mida mõni protsess mälus hoiab).
- No execute up (nx) - Operatsioonisüsteemi objekt (nt mõni protsess) ei saa käivitada endast kõrgemal tervikluse tasandil asuvaid protsesse.

Standardina on ainult nw -reegel aktiivne, nr -reegel ja nx -reegel on desaktiveeritud.

Kõige kõrgem tasand protsessidele, mida standardkasutaja saab käivitada ja objektidele, mida standardkasutaja saab luua, on tervikluse tasand Medium. Administraatorite puhul kannab vastavate tegevuste kõrgeim võimalik tervikluse tasand nimetust High. Tervikluse tasand System on mõeldud süsteemiteenuste jaoks. Kui objektile pole selgelt tervikluse tasandit määratud, kehtib

standardtasandina Medium. Tervikluse tasandeid pärandatakse sarnaselt ACL-i sissekannetele.

Operatsioonisüsteemi objektide vaheliseks suhtlemiseks nw -, nr - või nx-reeglitega kehtestatud piirangute rakendamine operatsioonisüsteemi poolt ei sõltu vastavate objektide pääsuloenditest. Näiteks töötab administraator aktiivse kasutajakontode haldamise ja veel mittetoimunud õiguste suurendamise puhul standardkasutajana tervikluse tasandil Medium. Nw -reegli kohaselt ei saa administraator tervikluse tasandi High objektidele kirjutavat juurdepääsu isegi siis, kui tal on objektile pääsuloendi kohaselt omanikuna täielik juurdepääsuõigus. Kirjutavaks juurdepääsuks objektile, mille tervikluse tasand on High , vajab administraator (antud näite puhul tegutseva operatsioonisüsteemi objektina) tervikluse tasandit High. See tasand määratakse administraatorile alles pärast õiguste suurendamist kasutajakontode haldamise poolt. Standardkonfiguratsioonis nõuab selline õiguste suurendamine administraatori selget nõusolekut. Sellele vaatamata pole administraatoril kirjutavat juurdepääsu süsteemiprotsessidele, kuna need töötavad kõrgemal tervikluse tasemel kui High , nimelt tasandil System.

Kaitstud režiim ja Internet Explorer 7 (IE7)

Kaitstud režiimi (Protected Mode) all mõistab Microsoft tervikluse tasandi Low määramist protsessidele, selle asemel et kasutada standardset tasandit Medium. Internet Explorer 7 (IE7) töötab Windows Server 2008-s standardina kaitstud režiimis, ehk siis tervikluse tasandil Low. IE7-e kaitstud režiimi jaoks peab aktiivne olema kasutajakontode haldamine. Kasutajakontode haldamise desaktiveerimisel kaotab IE7 kohe (ja ilma operatsioonisüsteemi poolse hoiatuseta) oma kaitstud režiimi. IE7 poolt allalaetud andmed, nt käivitatav programmikood, saab salvestada ainult sellistesse kataloogidesse, mille tervikluse tasandiks on Low , kuna IE7 puhul kehtib tervikluse tasand Low. Need andmed asuvad seejärel ka ise tasandil Low. Nw -reegli tõttu ei saa allalaetud programmikood endale märkamatult hankida kirjutavat juurdepääsu kasutaja andmetele (mis asuvad tavaliselt tervikluse tasandil Medium) või operatsioonisüsteemi andmetele (tasandil High või System). Kaitstud režiim raskendab seetõttu programmikoodi märkamatut allalaadimist IE7-ga ja selle koodi käivitamist. IE7 toetab vajadusel ka andmete allalaadimist ja salvestamist tervikluse tasandil Medium. See on vajalik näiteks siis, kui tegu on rakendusega, millega kasutaja soovib hiljem oma andmeid (tasandil Medium) töödelda: selleks töötab Internet Exploreri protsessiga paralleelselt nn User Broker protsess (IEUser.exe). Seda protsessi saab kasutada andmete salvestamiseks terviklustasandiga Medium , kuid ainult kasutaja selgesõnalisel nõustumisel. Internet Exploreril on laiendusi (kannavad ka nime Extensions või Add-Ons), mis ei ühildu kaitstud režiimiga , kuna nad peavad allalaetud andmeid kirjutama failisüsteemi aladesse või registrisse, mille tervikluse tasandiks on Medium. Nende laienduste rakendamiseks kasutab IE7 failisüsteemi ja registri virtualiseerimist. Antud kontekstis tähendab virtualiseerimine, et IE7 suunab nende laienduste kirjutavad juurdepääsud edasi vajalike alade koopiatesse. Need duplikeeritud (virtualiseeritud) alad asuvad tervikluse tasandil Low. Nõnda ei ole virtualiseeritud kasutajaandmete terviklus ohustatud. Sarnast meetodit kasutab Server 2008 ebaturvaliste Alt-rakenduste turvaliseks käivitamiseks (vt M 4.338 Windows 7 failide ja registri virtualiseerimise kasutamine).

IE7-s saab standardkasutaja kaitstud režiimi iga nelja turvatsooni jaoks eraldi aktiveerida ja desaktiveerida. Tuleb arvestada, et standardse konfiguratsiooni puhul on kaitstud režiim turvatsoonis usaldusväärsed leheküljed (Trusted Sites) desaktiveeritud! Kaitstud režiim (Protected Mode) on aktiveeritud vaid ülejäänud kolmes turvatsoonis: Internet , Local Intranet ja Restricted Sites. Kolme turvatsooni Internet, Local Intranet ja Restricted Sites puhul ei tohiks standardkasutajal olla võimalik kaitstud režiimi välja lülitada. Selleks tuleb iga kolme turvatsooni puhul grupipoliitika objekti Computer Configuration \ Administrative Templates \ Windows Components \ Internet Explorer \ Internet Control Panel \ Security Page \ Locked Down < tsooni nimi > jaoks aktiveerida poliitika Enable Protected Mode.

Kui tõendatult usaldusväärne veebileht ei pruugi kaitstud režiimiga ühilduda, siis tuleks ta määrata turvatsooni Usaldusväärsed leheküljed (Trusted Sites). Selle turvatsooni jaoks peab kaitstud režiim jääma desaktiveerituks. Sellega kaasnevat programmikoodi märkamatu allalaadimise ja käivitamise riski IE7-e poolt tuleb võrrelda vastava veebilehe kättesaadavuse olulisusega.

Windows Resource Protection ja Trusted Installer

Lisaks WIM-ile, tervikluse tasanditele ja kaitstud režiimile on Windows Resource Protection (WRP) täiendav Windows 2008 turvamehhanism, mis aitab kaitsta kriitiliste süsteemiressursside terviklust. WRP on uus nimi varasemates Windowsi versioonides Windows File Protectioni (WFP) nime kandnud turvamehhanismi jaoks. Kriitiliste süsteemiressursside alla kuuluvad seejuures teatud registrivõtmed, kataloogid ja failid. Failideks on kõik.dll,.exe,.ocx, ja.sys failid, samuti erinevat tüüpi, teatud kriitilise tähtsusega failid (kokku u 90). WRP tsentraalseks komponendiks on Trusted Installer. Trusted Installer tähistab süsteemiteenust kriitiliste süsteemiressursside nõuetekohaseks modifitseerimiseks ja lisaks sellele ka veel kasutajate gruppi, mille liikmed on kriitilise tähtsusega süsteemiressursside omanikud. Täielik juurdepääsuõigus kriitilistele süsteemiressurssidele piirdub Trusted Installeri omanikega. Kontodel Süsteem ja Administraator on kriitilise tähtsusega süsteemiressurssidele ainult piiratud juurdepääsuõigus, ja ei mingit kirjutusõigust. Seeläbi takistatakse kriitilise tähtsusega süsteemiressursside tervikluse juhuslikku rikkumist, nt administraatori poolt. Siiski on võimalik, et administraator määrab end omanikuks ja määrab seeläbi endale täieliku juurdepääsuõiguse. Seega on tahtlikud tervikluse rikkumised selle toeal ainult raskendatud, kuid mitte võimatuks muudetud.

Kriitilise tähtsusega süsteemiressursside muudatused, nt Service Pack -ide või Hotfix -ide paigaldamine toimub eranditult WRP ja Trusted Installeri kaudu (TrustedInstaller süsteemiteenuse kujul). Kriitilise tähtsusega süsteemifailide käsitsi kontrollimiseks saab administraator kasutada käsuviiba tööriista Windowsi ressursikontrollija sfc.exe. Seeläbi saab tuvastatud tervikluse rikkumise korral vastavad failid käsitsi rikkumata versioonide vastu välja vahetada.

Kontrollküsimused:

- Kas kasutajakontode haldus on aktiveeritud?
- Kas on defineeritud, milliste tsoonide puhul peab interneti turvaseadistuste all kehtima kaitstud režiim (Protected Mode)?
- Kas kaitstud režiim on vajalike tsoonide jaoks interneti turvaseadistuste alt domineerivalt sisse lülitatud?
- Kas kasutajaid õpetati kaitstud režiimi kasutama nii, et nad ei annaks allalaetud failidele/programmidele ilma eelneva kontrollita mingeid volitusi?

M 4.342z Last Access ajatempli aktiveerimine

Algatamise eest vastutavad: infoturbespetsialist

Rakendamise eest vastutavad: administraator

NTFS-failisüsteem haldab failisüsteemi muudatuste tuvastamiseks kolme ajatemplit. Neid ajatempleid nimetatakse ka MAC-ajatempliteks.

Mõiste MAC-Time tähendab Windowsi NTFS-failisüsteemis teatud faili Modification- , Access - ja Creation -aega.

- **Modification Time** (viimase muutmise aeg) on faili viimase kirjutamise aeg. Seda ajatemplit uuendatakse faili sisu muutmise korral.
- **Last Access Time** (viimase pöördumise aeg) on faili viimase lugemise või käivitamise aeg. Seda ajatemplit uuendatakse metaandmete või failide sisu kuvamisel. Seejuures pole oluline, kas fail ka salvestati või kas seda kuidagi muudeti. Kõik juhtumid, mil fail avati, selle poole pöörduti või seda mingil muul moel vaadati ,kajastuvad ajatemplis.
- **Creation Time** (loomise aeg) on faili loomise aeg, mis tekib kas uue faili loomise või mõne faili kopeerimisega.

Kui turvaintsidendi uurimisel (vt B 1.8 Turvaintsidentide käsitlus) analüüsitakse NTFS-andmekandjat, aitab MAC-aja analüüs tuvastada, milliseid faile oletatava kuritarvitamise ajal loeti, kirjutati, käivitati või muudeti. See aitab tuvastada, milliseid konfiguratsioonifaile või süsteemifaile näiteks süsteemi tagaukse paigaldamiseks muudeti. Lisaks saab analüüsida rünnaku oletatava toimumisaja jooksul muudetud faile ja võib-olla tuvastada ka meetodi, mida kasutati süsteemi sissemurdmiseks.

Niinimetatud ajakavade koostamisega saab üsna täpselt kindlaks teha, millal fail süsteemi kopeeriti, kas seda on seejärel vaadatud või kas selle poole on pöördutud.

Windows 7 ja Windows 2008 on Last Access ajatempli

uuendamine registris standardina desaktiveeritud, kuna ebasobiva failisüsteemi struktuuri puhul võib sellega kaasneda jõudluse langus. Kui kuritarvitamise analüüsiks on olemas teised sobivad meetmed, võib funktsiooni aktiveerimisest loobuda. Last Access ajatempli aktiveerimiseks tuleb registri võti HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate seada väärtusele „0”.

M 4.343z Hulgilitsentsilepinguga Windowsi süsteemide reaktiveerimine alates Windows Server 2008-st

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: administraator, kasutaja, infoturvaspetsialist, IT-juht

Windows 7 ilmumisega tühistas Microsoft RFM-funktsiooni. RFM-i asemel näitab Windows 7 ja Windows Server 2008 vastavaid hoiatusteateid.

Mõlemal juhul tuleb vastav klient reaktiveerida, et normaalne töö saaks jätkuda. Tuleks kaaluda võimalust testida Windows kliendi plaanipäraseid muudatusi testkeskkonnas, kuna need muudatused võivad tekitada vajaduse reaktiveerimise järele. Eriti just Windows klientsüsteemi riistvara muutmisel tuleks pöörduda Microsofti tugiteenuse poole, et saada lähemat infot vajalikuks osutuda võiva reaktiveerimise kohta.

Eriinfo KMS-aktiveerimise kohta

Selleks, et Windows kliente saaks reaktiveerida maksimaalse lubatud tähtaja jooksul (210 päeva pärast viimast aktiveerimist), peavad need olema võimelised suhtlema Key Management Service 'iga (KMS). Kättesaadavuse tagamiseks peaksid klientide ja KMSi vahelised ühendused toimuma regulaarselt ja oluliselt lühemate intervallidega. See vähendab ohtu, et maksimaalset 210-päevast ajalimiiti võidaks ületada. KMS peab omalt poolt LANi kaudu ligi pääsema vähemalt 25-le Windows kliendile, et klientsüsteemi reaktiveerida. Reaktiveerimise jaoks määratud ajaks peab KMS kasutatav olema. Vajadusel võib kaaluda ka teise KMSi käitamist.

Kontrollküsimused:

- Kas, aktiveerimise tüübist sõltumatult, kontrollitakse muudatusi eelnevalt testkeskkonnas, et kontrollida reaktiveerimise vajaduse tekkimist?
- Kas, aktiveerimise tüübist sõltumatult, on teada, millised asjaolud tekitavad vajaduse reaktiveerimise järele?
- Kas KMS-reaktiveerimise otstarbeks on tagatud, et Windows kliendid saaksid KMS-iga suhelda 210 päeva jooksul alates viimasest aktiveerimisest?
- Kas KMS-reaktiveerimise puhul on tagatud, et KMS pääseks võrgu kaudu ligi vähemalt 25-le Windows kliendile, kui tekib vajadus Windows klienti reaktiveerida?
- Kas KMS-reaktiveerimise puhul on tagatud, et KMS on reaktiveerimiseks määratud ajal kättesaadav?

M 4.344 Windows 7 ja Windows Server 2008 süsteemi seire

Algatamise eest vastutavad: infoturvaspetsialist, IT-juht

Rakendamise eest vastutavad: administraator, revident

Arvutisüsteemide turvalisuse ja tervikluse tagamiseks tuleb süsteeme jälgida. Ainult nii on võimalik tuvastada võimalikke turvaaukusid, kehtivate turvapoliitikate rikkumisi ja organisatsiooni seest või väljast alguse saanud ründeid ning nende vastu sobivaid vastumeetmeid käiku lasta. Windows 7 ja Windows Server 2008 süsteemi seirevajadustega tuleb arvestada juba planeerimisfaasis, et olulised parameetrid oleksid määratletud vastavalt vajadustele. Selleks, et Windows 7-s oleks seire võimalik, tuleb see esmalt aktiveerida kas grupipoliitikate või lokaalsete seadistuste kaudu. Eriti kehtib see failide ja Registry seire kohta. Microsoft Windows 7 või Windows Server 2008 eristab sündmuste kuvamisel „Windowsi logisid" ning „Rakenduste ja teenuste logisid".

Windowsi logidega salvestatakse järgmiste sündmuste info:

- Rakenduste logi: sisaldab rakendustest tulenevaid sündmusi. Milliseid sündmuseid logida saab, määravad rakenduse arendajad.
- Turvalogi: sisaldab sündmuseid, mille Microsoft on turvalisuse jaoks olulisteks liigitanud. Seirepoliitika konfigureerimise abil saab administraator määrata, mida täpselt logida tuleks.
- Installeerimislogi: sisaldab rakenduste installeerimisel esinevaid sündmusi.
- Süsteemilogi: sisaldab Microsoft Windowsi süsteemikomponentidest lähtuvaid sündmusi.
- Edasisuunatud sündmused: ainult siis, kui klient on selgelt konfigureeritud teiste arvutite (remote clients) sündmuste kogumiseks, näidatakse Microsoft Windowsi kliendil „edasisuunatud sündmuseid". Seejuures on tegu eelnevalt nimetatud logide sündmustega. Ka kaugkliendid vajavad nende sündmuste kuvadele juurdepääsu lubamiseks konfigureerimist.

Microsoft Windowsis kasutatakse rakenduste ja teenuste logisid. Nendes logides ei salvestata kogu süsteemi sündmuseid, vaid sündmuseid, mis puudutavad ükskuid rakendusi või komponente. Järgnevates tabelites on ära toodud soovitused sündmuste kuvamiseks Event viewer -is. Sündmused tekitavad turvalogis vastavaid teateid. Järgnevate tabelite pealkirjad näitavad grupipoliitika asukohti (Group Policy Objects , GPOd). Neid saab konfigureerida lokaalselt või Active Directory all (vt M 2.326 Windows 7 grupeerimissuuniste planeerimine).

Asukoht „ Computer Configuration | Windows Settings | Security Settings | Local Policies | Audit Policy "

Parameeter	Soovitus
Protsessi jälgimise seire	Protsessi seire ei ole üldjuhul mõttekas ning see tuleks sisse lülitada vaid Debugging eesmärgil.
Õiguste kasutamise seire	Ebaõnnestunud juurdepääsukatseid tuleks jälgida.
Poliitikate muudatuste seire	Poliitikaseadistuste (GPO-de) muutmine on turvalisuse seisukohalt kriitilise tähtsusega tegevus ning seda tuleks jälgida.

Süsteemi kajastavate sündmuste seire	Süsteemisündmuseid tuleks jälgida.
Sisselogimisega seotud sündmuste seire	Sisselogimisega seotud sündmuste seire peaks lokaalsete arvutite (nt töökohaarvutite) puhul olema sisse lülitatud.
Sisselogimiskatsete seire	Sisselogimiskatsete logimine peaks olema aktiivne.
Kontode haldamise seire	Kontode seadistustes tehtavad muudatused on turvalisuse seisukohast olulised sündmused ning neid tuleks jälgida.
Objektidele tehtud pöörduste seire	Objektijuurdepääsusid tuleks jälgida, kuna see logib ka juurdepääse nt failidele ja registrivõtmetele. Kuna sündmuste arv on suur, tuleks objektidele tehtud edukate pöörduste kajastamine aktiveerida üksnes väikse arvu oluliste objektide puhul.
Kataloogiteenuste tehtud pöörduste seire	Kataloogiteenusele tehtud pöördusi tuleks jälgida. Salvestada tuleks vähemalt pöörduste käigus tekkinud ja registreeritud ebakõlad (vead).

Microsoft Windows 7 või Windows Server2008 all on lisaks eelpool nimetatutele võimalik teha täiendavaid seireseadistusi.

Alljärgnevad tabelid annavad soovitusi järgmisteks konfiguratsioonideks:

- Sündmuste kuvale ligipääsu omavate kasutajate määramine,
- Sündmuste logi seadistused, 1. osa,
- Sündmuste logi seadistused, 2. osa
- Turvavalikud

Need aitavad korraldada seiret Microsoft Windows 7 ja Windows Server 2008 süsteemides. Alljärgnevalt kirjeldatakse seadistusi, mis puudutavad vahetult logide loomist ja annavad konfigureerimissoovitusi.

Asukoht „Computer Configuration | Windows Settings | Security Settings | Local Policies | User Rights Assignment”

Parameeter	Soovitus

Seire- ja turvalogide haldamine	Nimetatud õigus võimaldab: - konfigureerida auditeerimisseadistusi üksikute objektide (failide, Registry , Active Directory) lõikes, - vaadata ja kustutada turvalogi. Millisele kasutajagrupile (või gruppidele) sellist õigust anda, sõltub suuresti seirekontseptsioonist. Reeglina tuleks selle õiguse andmisel olla mõõdukas, näiteks anda see ainult administraatorite grupile. Samas tuleks arvestada ka järgnevaga: - juurdepääs turvalogile võib olla hädavajalik ka selliste probleemide diagnostikaks ja lahendamiseks, mis ei ole seotud turvalisusega; - administraatorid suudavad selle õiguse enese jaoks taastada ka juhul, kui see neilt ära võetakse. Seega tuleks vastav protseduur logida (valik Computer Policies / Local Policies / Audit Policy | Audit privilege use).

Asukoht „ Computer Configuration | Administrative Templates | Windows Components | Eventlog Service | ”

Parameeter	Soovitus
- Logi maksimaalne suurus (rakenduse logi) - Logi maksimaalne suurus (installeerimislogi) - Logi maksimaalne suurus (turvalogi) - Maksimaalne suurus (süsteemilogi)	Suurus tuleb valida selline, et sõltuvalt säilitamiseks valitud meetodist oleks alati piisavalt ruumi ka keskmisest suurema süsteemisündmuste arvu kajastamiseks. Eriti oluline on see turvaprotokolli jaoks, kuna vastasel korral võib süsteemi turvalisuse seires tekkida ajaline lünk. Siin tehtavate seadistuste soovitused leiate meetmest M 2.326 Windows Vista ja Windows 7 grupeerimissuuniste planeerimine või meetmest M 4.244 Windowsi klientoperatsioonisüsteemide turvaline süsteemikonfiguratsioon . Viimased tuleb aga kindlasti viia vastavusse reaalsete tingimustega (testida proovikäituse raames).

Vanade sündmuste säilitamine	Kui see poliitika pole aktiivne ja logifail on jõudnud maksimaalse suuruseni, asendatakse vanimate sündmuste sissekanded uute sündmuste sissekannetega. Nende vanemate sündmuste info läheb kaduma. Kui see poliitika on aktiivne ja logifail maksimaalse suurusega, ei logita logifaili enam uusi sündmuseid. Uute sündmuste info läheb kaduma. Poliitika „Vanade sündmuste säilitamine” tuleks aktiveerida. Kui logide automaatseks arhiveerimiseks tahetakse kasutada poliitikat „Kogu logi automaatne varundamine” (vt allpoolt), peab poliitika „Vanade sündmuste säilitamine” olema aktiivne.
Kogu logi automaatne varundamine	Kui aktiivsed on see logi ja logi „Vanade sündmuste säilitamine”, suletakse logifail maksimaalse suuruseni jõudmisel automaatselt. Samuti antakse sellele uus nimi. See poliitika peaks olema aktiivne.

Järgneva tabeli seadistusi saab konfigureerida ainult Active Directory alt, kohalikku grupipoliitikat ei saa selleks kasutada.

Asukoht „ Computer Configuration | Windows Settings | Security Settings | Local Policies | Event Log ”

Parameeter	Soovitus

- Rakenduslogi säilitusmeetod - Turvalogi säilitusmeetod - Installeerimislogi säilitusmeetod - Süsteemilogi säilitusmeetod	Sõltuvalt logimiskontseptsioonist saab valida - sündmuste ülekirjutamise päevade kaupa, - sündmuste ülekirjutamise vastavalt vajadusele ja - sündmuste ülekirjutamise keelamine (logi puhastamine käsitsi). Kui logimine pole vajalik või kui logisid ei analüüsita, võib valida valiku „sündmuste ülekirjutamine vastavalt vajadusele”. Teistel juhtudel võib kasutada valikut „sündmuste ülekirjutamine päevade kaupa” või „sündmuste ülekirjutamise keelamine (logi puhastamine käsitsi)”. Seejuures tuleb tähele panna, et valik „sündmuste ülekirjutamine päevade kaupa” nõuab poliitika „ säilitada” konfigureerimist koos vastava arvu päevadega. Lisainfot selle kohta näete ka järgmise konfiguratsiooniseadistuse alt. Valiku „sündmuste ülekirjutamise keelamine (logi puhastamine käsitsi)” puhul tuleb tagada, et logisid kustutataks käsitsi. Kui neid ei kustutata, siis uusi sündmuseid logi maksimaalse suuruseni jõudmisel enam ei logita.
- Rakenduste logi säilitamine - Turvalogi säilitamine - Installeerimislogi säilitamine - Süsteemilogi säilitamine	Selle poliitikaga saab määrata logi säilitamise aja. See seadistus on oluline siis, kui logi säilitamise meetodiks valiti „sündmuste ülekirjutamine päevade kaupa”. Määratud päevade arv sõltub süsteemikeskkonnast ja peab olema piisavalt suur, et võimaldada logiandmete varundamist. Lisaks peab „logi maksimaalne suurus” olema piisavalt suur, et vältida selle ülekirjutamist. Vt ka tabelit „Sündmuste logi seadistused, 1. osa”. Logide arhiveerimiseks peab administraator või kasutaja omama õigust „Seire- ja turvalogide haldamine”. Vt ka tabelit „Sündmuste kuvale ligipääsu omavate kasutajate määramine”.

- Lokaalse külaliskonto alt installeerimislogile juurdepääsemise tõkestamine - Lokaalse külaliskonto alt rakenduslogile juurdepääsemise tõkestamine - Lokaalse külaliskonto alt turvalogile juurdepääsemise tõkestamine - Lokaalse külaliskonto alt süsteemilogile juurdepääsemise tõkestamine	Külaliskonto juurdepääsude piirangud peaksid olema sisse lülitatud.

Asukoht „ Computer Configuration | Windows Settings | Security Settings | Local Policies | Security Options ”

Parameeter	Soovitus
Seire: kui turvakontrolle ei saa enam logida, lülitatakse süsteem kohe välja	Käideldavuse tagamiseks tuleks see valik välja lülitada. See valik tuleks aktiveerida vaid kõrge turbevajaduse korral, kuna seal on tõendamine käideldavusest olulisem. Aktiveerimine nõuab töö normaalse kulgemise tagamiseks täiendavaid meetmeid.

Lokaalselt saab sündmuste kuvas iga logi puhul määrata eraldi logi suuruse ja käitumise olukorras, kus sündmuste logi maksimaalne suurus peaks täituma.

DirectAccessi kasutamisel alates Windows 7-st tuleks kliendis juurutada tunneli ühendusprotsesside logimine (vt M 5.123 Võrgusuhtluse kaitse Windowsis). Selleks tuleb muu hulgas hankida perfmon.exe jõudlusnäitajad (counters) ja koostada kogumiskomplektid (collection sets). Kogumiskomplektide salvestuskohaks tuleks valida mõni turvaline süsteemikataloog nagu %systemdrive % \perflogs \System \Diagnostics. Logifailide suurus tuleb kohandada optimaalseks, lähtudes IT-koosluse seisundi regulaarsetest kontrollidest. Võimalike väärfunktsioonide ja ründemustrite tuvastamiseks tuleb ühenduseandmeid kajastada vähemalt ühe nädala võrra tagasiulatuvalt.

Seire raames tuleb reeglina arvestada lisaks ka järgmiste aspektidega:

- Andmekaitsespetsialist ja töötajate esindus tuleb kaasata seire kavandamisse võimalikult varajases faasis. Seire käigus kogutakse tavaliselt ka isikuid puudutavat infot, et lihtsustada turvaintsidendi põhjustaja tuvastamist.

- Selleks, et seirekomponendid genereeriksid logisissekandeid, tuleb sisse lülitada asjakohaste grupipoliitikate seirefunktsioonid.
- Microsoft Windows 7 ja Windows Server 2008 pakub seireks täiendavat logimisfunktsiooni „Rakenduste ja teenuste logid". Vanemates Microsoft Windowsi versioonides leiduvaid Windowsi logisid on täiendatud „rajamise" ja „edasisuunatud sündmustega". Lokaalselt saab kõikide logide jaoks logimise aktiveerida või desaktiveerida. Lisaks saab konfigureerida logi suurust ja käitumist olukorras, kus logi jõuab oma maksimaalse suuruseni.
- Logifailide tsentraalse kogumiskoha loomiseks ning failide automaatseks analüüsimiseks võib kasutada Microsofti, või kolmandate tootjate lahendusi. Juhul, kui võrgu ja süsteemi haldamiseks kasutatakse mõnd tööriista (vt B 4.2 Võrgu- ja süsteemihaldus), on võimalik sõltuvalt toote eripäradest importida Windowsi logid otse vastava tööriista alla.
- Microsoft Windowsi seirepoliitika abil saab turvalogisse salvestada pöördumisi, muuhulgas failidele või registrivõtmetele. Selleks tuleb Windowsi logis „Forwarded events" jaoks konfigureerida vastavad abonemendid (Subscriptions).
- Abonemendis konfigureeritakse see, milliseid sündmuseid tuleks koguda. Tüüpinstalleerimisel edastatakse edasisuunatud sündmuse andmed http kaudu. Andmetransport https-i kaudu on samuti võimalik ja seda tuleks ka kasutada.
- Microsofti Windows klientsüsteeme tuleb konfigureerida, et nad võimaldaksid juurdepääsu vastavatele andmetele. Seda saab teha tööriistaga winrm.
- Microsoft Windows klientsüsteemis, kus analüüsimine toimub, tuleb sisse seada abonemendid. Seda saab teha Forwarded events | Properties | Subscriptions alt.
- Üksikuid seirepoliitikaid saab Microsoft Windows konfigureerida grupipoliitika abil. Et seire täiendaks grupipoliitikat, tuleb seiret täpsemalt seadistada. Seda saab teha tööriistaga auditpol.exe.
- Seire käigus toodetakse sõltuvalt konfiguratsioonist suuri andmemahtusid. Lisaks võib intensiivne seire vähendada jõudlust. Äärmuslikel juhtudel võidakse süsteem seirega nii üle koormata, et tavapärane töö muutub võimatuks. Sel põhjusel tuleb juba proovikäitamise raames välja selgitada optimaalsed seireparameetrid ning neid vajadusel ka kohandada. Siinkohal tuleb arvestada, et parameetrite kohandamine võib avaldada mõju kogu seirekontseptsioonile, kuna võib selguda, et teatud liiki seireülesandeid pole enam võimalik rakendada. Eriti võib seda esineda siis, kui rakendatakse täiendavaid tooteid, mis seavad logitavatele sündmustele täiendavaid kõrgeid nõudeid. Näitena võib siinkohal nimetada programme, mille läbi viidav logiandmete automaatne analüüs põhineb käitumises aset leidvate anomaaliate, näiteks võimalike rünnete, tuvastamisel.
- Süsteemifunktsioonide seire raames tuleks regulaarselt kontrollida ka AD-replikeerimist, mille abil jaotatakse konfiguratsioonimuudatusi domeeni domeenikontrolleritele. Selleks võib kasutada niihästi AD-tööriistu kui ka kontrollida ADS-logi (Active Directory Service) ja FRS-logi (File Replication Service) veateadete esinemise osas. Replikeerimisel toimunud vigade tagajärjeks on reeglina see, et konfiguratsioonis tehtud muudatusi ei ole võimalik kõikjal üheselt rakendada. Sellega kaasneb oht, et mõnele kasutajale võidakse anda kas ebasobivad või liiga laialdased volitused.

Süsteemi seires ja logitud andmete analüüsimises mängib tähtsat rolli süsteemiaeg. Eriti neil juhtudel, kus seiresse on kaasatud mitmeid süsteeme, tuleb süsteemiaeg kõikides arvutites kindlasti sünkroniseerida. Windowsi sisemise kella teenus vastutab aja sünkroniseerimise eest ja seega ei tohi seda desaktiveerida.

Active-Directory -keskkonnas saab domeeni liikmete kellana kasutada domeenikontrollerit. Windowsi ajateenuse hierarhiline ülesehitus on võimaldatud.

Domeenikontrollerid kasutavad aja jaoks peamise domeenikontrolleri (PDC) Operations master -it või hierarhias kõrgemal asetseva domeeni domeenikontrollerit.

PDC Operation master -id kasutavad kellana kõrgemalasetseva domeeni PDC Operation master -it. Tüvidomeeni PDC on autoriseeriv kell.

Domeenikontrollerit saab käsuga

net time /setsntp:

seadistada selliselt, et sünkroniseerimiseks kasutatakse mõnd välist kella. Väline kell võib asuda nii oma võrgu sees kui ka sellest väljas, kuid eelistada tuleks võrgusisest kella. Juhul, kui kasutatakse väljaspool võrku asuvat kella, peab selle usaldusväärsus olema tagatud.

Klient-arvutid, mis ei ole domeeni liikmed, kasutavad standardina Microsofti ajaserverit time.windows.com. Neid on aga võimalik ka ümber konfigureerida käsuga „net time” selliselt, et need kasutaksid mõnd muud kella.

Kontrollküsimused:

- Kas grupipoliitikates või kohalikes seadistustes on seire aktiveeritud?
- Kas vajadustest lähtuv seirekontseptsioon on koostatud ja kas seda on rakendatud?
- Kas olulisi süsteemisündmusi logitakse?
- Kas logifailid varundatakse maksimaalse suuruse saavutamisel?
- Kas oluliste süsteemifailide ja Registry sissekannete seireseadistusi on konfigureeritud?
- Kas süsteemiaja sünkroonsus tagatakse usaldusväärse kella abil?

M 4.345z Kaitse soovimatu infoäravoolu eest

Algatamise eest vastutavad: IT-juht, infoturbespetsialist

Rakendamise eest vastutavad: administraator

Konfidentsiaalne info ei tohi sattuda valedesse kätesse. Selle takistamiseks saab kasutada mitmeid töökorralduslikke või tehnilisi meetmeid. Paljude selliste meetmetega kaasnevad probleemid. Nad kas takistavad oluliselt tööprotseduure või kaitsevaid info väljavoolu eest küll teatud liideseid, aga siiski mitte kõiki. Üks lahendus konfidentsiaalse info paremaks juhtimiseks on tööriistad, mis kontrollivad andmevoogu võrgus ja/või lõppseadmetes. Need peaksid ära tundma sellised olukorrad, kus konfidentsiaalne info liigub ebaturvalisi kanaleid pidi või satub valedesse kätesse, ja võimaluse korral peaksid need isegi sekkuma. Sellised tööriistad kontrollivad näiteks, kas teatud infot tuleks edastada e-posti teel, andmevahetusel või interneti kaudu või kirjutada lausa CD-le või kopeerida USB mälupulgale.

Selliste tööriistade puhul kasutatakse erinevaid mõisteid: lekketõrje (data loss prevention, DLP), infolekketõrje (information leakage prevention, ILP) või ka väljaviimise tõrje (extrusion prevention), kuid nende eesmärgid ja mehhanismid on sarnased. Sellised süsteemid eristavad konfidentsiaalset ja väheolulist infot. Väheoluliste failide saatmine meili teel võib olla lubatud, kuid konfidentsiaalsete failide saatmine e-posti teel või nende kopeerimine mobiilsetele andmekandjatele (nt USB mälupulkadele) võib olla tõkestatud. Teatud DLP-tööriistad suudavad isegi takistada seda, et faili sisust teatud osasid teise faili kopeeritaks. Hetkel on DLP-tööriistade jaoks kaks erinevat tehnilist lähtepunkti. Ühed püüavad seadme või eraldiseisva seadme abil võrgu andmevoos konfidentsiaalset infot tuvastada ja vastavalt reageerida. Teised vajavad kõikides asjassepuutuvates lõppseadmetes agenti, kes kontrolliks tundlike failide liigutamist ja töötlemist. Sarnaselt sissetungi tuvastamisele on ka DLP puhul tegu hostidel ja võrkudel põhineva lähenemisega.

Võrgupõhine lähenemine

Võrgupõhise DLP-tööriista puhul paigaldatakse teatud kohtadesse võrgus andurid või agendid. Kuna lisatarkvara tuleb paigaldada vaid vähestesse kohtadesse, on sisseseadmine ja käitamine lihtsam kui toodete puhul, mis tuleb installeerida igasse puudutatud lõppseadmesse. Seejuures kontrollitakse ainult neid andmevoogusid, mis liiguvad võrgus nende andurite/agentide kaudu, kuid mitte neid andmevoogusid, mis liiguvad detsentraalsete liideste või mobiilsete andmekandjate (nt USB mälupulkade) kaudu. Täiendav probleem on ka krüpteeritud info kontrollimine.

Hostidel põhinev lähenemine

Hostidel põhinevate DLP-tööriistade puhul tuleb agendid või andurid installeerida igasse IT-süsteemi, mida tahetakse kasutada andmevoo kontrollimiseks. Selle tulemuseks on suurem töömaht installeerimisel ja käitamisel. Eeliseks on, et DLP-tööriist saab kontrollida kasutaja kõiki tegevusi, mis võivad põhjustada andmete väljavoolu.

Kontseptuaalne meetod

Täielik kaitse info soovimatu väljavoolu eest on saavutatav ainult siis, kui tehnilised meetmed käivad käsikäes töökorralduslike ja personalialaste meetmetega ja on juurutatud turvahalduse protseduuri. DLP-protseduuride oluliseks aluseks on kogu tegevuse jaoks olulise info liigitamine turbevajaduse järgi (vt M 2.217 Teabe, rakenduste ja süsteemide hoolikas liigitamine ja käitlus). Sellele tuginedes tuleb täpsustada, kes ja millistel tingimustel tohib seda infot töödelda, salvestada ja edasi saata ning kuidas seejuures infot kaitsta. DLP-tööriistade kasutamine ei eelda iga üksiku faili eraldi klassifitseerimist.

Tööriista saab tavaliselt konfigureerida selliselt, et faili turbevajadus lähtuks selle salvestuskohast (kontekstipõhine), teatud struktuuriomadustest või sisust, ehk siis tuletataks see eelnevalt määratud võtmesõnade abil. Kontekstipõhise lähenemise puhul tuleb kasutada struktureeritud andmehaldust, mille puhul eraldatakse kõrgema turbevajadusega failid väiksema konfidentsiaalsusastmega failidest näiteks kataloogistruktuuride abil (vt M 2.138 Struktureeritud andmetalletus). Enne DLP-tööriista soetamist tuleb selle kasutusotstarve täpselt kindlaks määrata. Enne DLP-tööriista kasutuselevõtmist tuleb luua poliitika selle kasutamise kohta, samuti määrata tööriista kontrollimise reeglistik. Kasutamist ja reeglistikku tuleb hoolikalt planeerida ja institutsiooni oludega sobivaks kohandada. Sellesse tuleb kaasata töötajate esindus ja andmekaitsespetsialist. Väljatöötatud reeglistik tuleks kirja panna tööleppesse. Oluline on mitte liiale minna. Pärast DLP-tööriistade esimesi teste on vastutavad isikud tavaliselt testi käigus välja tulnud arvukate potentsiaalsete nõrkade kohtade üle kohkunud, kuid reeglid ei tohi olla nii piiravad, et nad segaksid normaalset tööprotseduuri.

Töötajaid tuleb informeerida DLP-tööriistade kasutamisest, st sellest, mida need tööriistad kontrollivad ja millised on reeglistiku rikkumise tagajärjed.

Reeglite rikkumise puhul pakuvad DLP-tööriistad erineva tugevusastmega reageerimisvõimalusi:

- kasutajale kuvatakse teade, et planeeritav tegevus rikub reegleid
- kasutajalt nõutakse sõnaselget nõustumist
- tegevus tõkestatakse
- logimine
- kolmanda osapoole, nt administraatori või ülemuse informeerimine.

Kogemus näitab, et hoiatusteadete kuvamine on ülimalt tõhus, harjutamaks kasutajaid konfidentsiaalse infoga vastutustundlikult ümber käima. Liiga tugevad piirangud või DLP-tööriistade kontrollid võivad mõjuda töötajate motivatsioonile negatiivselt. DLP-tööriista konfiguratsiooni tuleb kontrollida regulaarselt ning optimeerida ja kohandada institutsiooni, tööprotseduuride ja IT vajadustele vastavaks.

Kontrollküsimused:

- Kas soovimatu infoäravoolu vältimise meetmed on integreeritud turvahalduse protseduuri?

- Kas soovimatu infoäravoolu meetmed on kooskõlastatud töötajate esinduse ja andmekaitsespetsialistiga?
- Kas on tagatud, et soovimatu infoäravoolu meetmed on kooskõlas töötajate tööprotseduuridega?
- Kas töötajad on teadlikud soovimatu infoäravoolu kaitse kasutamise, regulatsioonide ja võimalike sanktsioonide olemasolust?

M 4.346 Virtuaalsete IT-süsteemide turvaline konfigureerimine

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: administraator

Virtuaalsed IT-süsteemid (aegajalt nimetatakse neid ka virtuaalmasinateks) on esmajoones ikkagi IT-süsteemid. Seega tuleb neid käsitleda ja modelleerida nagu füüsilisi IT-süsteeme (vt M 2.392 Virtualiseerimisserverite ja virtuaalsete IT-süsteemide modelleerimine).Virtuaalsetele IT-süsteemidele kehtivad mõningad erisused, mida tuleb jälgida.

Tihti tuleb virtuaalsetele IT-süsteemidele võimaldada ligipääs virtualiseerimisserveriga ühendatud seadmetele, näiteks CD ja DVD ajamid, USB-tongel, SCSI ja teised välisseadmed. Seejuures võivad seadmed, mille kasutamist virtualiseerimisserver virtuaalsetel IT-süsteemidel võimaldab, tihtipeale juhtida virtuaalse masina tööriistadega. Näiteks saab sel moel desaktiveerida võrgukaardi või laadida andmekandjaid füüsilisest CD/DVD ajamist või disketiajamist virtuaalsesse ajamisse. Mõnede virtualiseerimissüsteemide juures on veel lisaks võimalus kas põhimälu või kõvakettaruumi üle täita. Seejuures räägitakse ressursside „ülebroneerimisest", kui virtuaalse IT-süsteemi käsutusse on võimalik anda rohkem ressursse kui füüsiliselt üleüldse olemas on. Ressurssidega seotud kitsaskohtade ennetamiseks saab virtuaalsetes IT-süsteemides olevate tööriistadega kasutusele võtta funktsioone, et juhtida sellist ülebroneerimisfunktsiooni. Näiteks on firma VMware (VMware Tools) tööriistadel olemas funktsioon põhimälu hõivamiseks, et see siis anda teiste virtuaalsete IT-süsteemide käsutusse. Nende tööriistadega saab ette valmistada ka virtuaalse kõvaketta konteineri vähendamise. Selleks nihutatakse kõik virtuaalse kõvaketta hõivatud blokid konteineri algusesse ja vabaks jäänud blokid kirjutatakse nulliga üle, et virtualiseerimiskiht tunneks nad ära kui vabad blokid.

Seepärast tuleb virtuaalse IT-süsteemi kasutusele võtmisel jälgida peale füüsilise serverikäituse meetmete lisaks veel järgmisi aspekte:

- Kerneli, rakenduste ja süsteemiraamatukogu binaarsete failide muudatused mõjuvad operatsioonisüsteemi virtualiseerimisele vastupidiselt serveri virtualiseerimisele, kõigile virtuaalsetele IT-süsteemidele, mida virtualiseerimisserveril käitatakse ja ka virtualiseerimisserverile endale. Andmeid tuleb kontrollida muudatuste suhtes, eelkõige seetõttu, et kompromiteerimise korral on sellistel failidel suur kahjupotentsiaal. Vaata ka M 4.93z Regulaarne tervikluse kontroll .
- Tööriistad võivad virtuaalse IT-süsteemi kasutajal võimaldada ligipääsu virtualiseerimisserveri disketi- või CD/DVD ajamis paiknevatele andmekandjatele.

Ka mehaanilised tegevused nagu näiteks füüsilise ajami ajamisahtli kaane avamine ja sulgemine on selle kaudu juhitavad. Seetõttu esineb võimalus, et pääsetakse volitamata ligi füüsilises ajamis olevatele andmekandjatele või andmekandja eemaldatakse virtuaalsest IT-süsteemist seeläbi, et ajam avatakse mõne teise

virtuaalse süsteemi kaudu. Virtuaalsed IT-süsteemid ja virtualiseerimisserver tuleb konfigureerida nii, et selline võimalus oleks üldjuhul välistatud. Kõige lihtsam meetod selle teostamiseks on, kui virtuaalsetele IT-süsteemidele antakse vastavad seadmed kasutada ainult siis, kui neid vaja on.

Kui neid seadmeid ei vajata, tuleks ühendus nendega katkestada. Kui on võimalik CD või DVD andmekandjad anda kasutusse kujutisfailina (ISO Image), tuleks seda ka teha.

- Funktsioonid, mis võimaldavad põhimälu või kõvakettaruumi ülebroneerimise tuleb desaktiveerida virtuaalsete IT-süsteemide juures, millel on kõrged jõudlusnõuded või mille andmeterviklus on erilise tähtsusega. Üldjuhul vähendavad ressurssidega seotud kitsaskohad olulisel määral virtualiseerimisserveri põhimälust mõjutatud virtuaalsete IT-süsteemide jõudlust. Kui kõvakettaruum broneeritakse üle ja kui füüsiliselt olemasolevast ruumist enam ei piisa, keelab virtualiseerimisserver tavaliselt kõik kirjutavad ligipääsud vastavale ülebroneeritud salvestuskohale. Seeläbi tekivad virtuaalsetes IT-süsteemides kõvakettavead, mis võivad viia salvestatud failide leketeni.
- Virtuaalse kõvaketta ettevalmistamine tema füüsilise konteineri suuruse vähendamiseks tähendab virtualiseerimisserverite massmäludele suur koormust. See võib viia kõigi virtualiseerimisserveril paiknevate virtuaalsete IT-süsteemide jõudluse piiramiseni. Kui mitu virtualiseerimisserverit tahab juurdepääsu ühele salvestusvõrgule, võivad sellest olla teatud juhtudel mõjutatud kõik virtualiseerimisserverid. Seetõttu tuleks see funktsioon, kui seda ei vajata, desaktiveerida.
- Seadmete nagu võrgukaardi desaktiveerimine tööriista kaudu on samaväärne lahendus võrgukaabli lahtiühendamisele füüsilise IT-süsteemi küljest. Kuna see on virtualiseeritud keskkonnas tihti võimalik ka ilma ligipääsuta sellele süsteemile, tuleks see funktsioon desaktiveerida. See tuleks aktiveerida ainult siis, kui seda vajatakse.

Mõningad ülalkirjeldatud funktsioonid on juhitavad või võimaldatud virtuaalsetes IT-süsteemides installeeritud tööriistade kaudu. Seepärast tuleb luua regulatsioonid virtuaalsete IT-süsteemide tööriistade kasutamiseks.

Kontrollküsimused:

- Kas virtualiseeritud operatsioonisüsteemiga keskkonnas on tagatud operatsioonisüsteemi andmete, süsteemiraamatukogu ja ühiskasutuses olevate rakenduste terviklikkus?
- Kas tööriistade kasutamiseks virtuaalsetes IT-süsteemides on loodud ja realiseeritud vastavad reeglid?
- Kas virtuaalse IT-süsteemiga ühendatakse seadmed nagu CD ajam ainult siis,kui neid vastaval IT-süsteemil vaja läheb?
- Kas virtuaalsete IT-süsteemide korral, millel on kindlaks määratud kõrge jõudlusnõue või kõrge turbevajadus tervikluse suhtes, on põhimälu või kõvakettaruumi ülekirjutamisfunktsioon desaktiveeritud?
- Kas funktsioon, millega on võimalik tööriista abiga seadmeid nagu näiteks võrgukaarte ja CD/DVD ajameid sisse ja välja lülitada, on standardis välja lülitatud?

M 4.347z Virtuaalsete IT-süsteemide snapshot'ide desaktiveerimine

Algatamise eest vastutavad: asutuse/ettevõtte juhtkond, IT-turvaosakond

Rakendamise eest vastutavad: infoturbespetsialist, IT-juht

Võimalust virtuaalse IT-süsteemi olekut kindlal ajahetkel külmutada ja selle olekus nii kaua kui vaja hoida, näiteks see oleks salvestatakse kõvakettale, on virtuaalsete IT-süsteemide tehniline eripära. Kui see olek on võimalik salvestada ja süsteemi seejärel jätkata, esineb võimalus süsteem salvestatud olekusse tagasi viia. Sellist olekut nimetatakse enamiku virtualiseerimistoodete puhul snapshot'iks. Seda meetodit saab kasutada mitmekülgse haldustegevuse jaoks. Näiteks on võimalik sedasi pärast ebaõnnestunud uuendust taastada vana versioon. Ka virtuaalse taristu elementaarsed võimalused nagu külalissüsteemide teisaldamine virtualiseerimissüsteemide vahel Live Migation i, vMotion i või XenMotion i kaudu, põhinevad võimel luua snapshot'e. See hõlmab järgnevalt ka sinna külge ühendatud kõrgkäideldavuse mehhanisme.

Seepärast tuleb snapshot'ide kasutamisel arvestada järgmiste aspektidega:

- Konfidentsiaalsuse ja tervikluse kaitse ohustatud külaliste korral - Virtuaalses taristus võib teatud IT-süsteemidel olla konfidentsiaalsuse ja tervikluse suhtes kõrge või väga kõrge turbevajadus.

Ühe protsessi andmeid töödeldakse tihtipeale põhimälu üksteisest eraldatud alades, nii et teised IT-süsteemi protsessid ei pääse neile ligi ja ei saa neid andmeid lugeda ega muuta. Seeläbi jääb andmete töötlemisel (virtuaalse) IT-süsteemi põhimälus nende konfidentsiaalsus ja terviklus puutumata. Kui nüüd külmutatakse virtuaalse IT-süsteemi suvaline olek, et süsteemi hilisemal ajahetkel uuesti samasse olekusse seada, salvestatakse põhimälu andmed virtualiseerimisserveri massmällu. Ründaja saab nüüd ligipääsukaitsest, mida virtuaalse IT-süsteemi operatsioonisüsteem erinevate protsesside failidele tagab, põhimälu sisu sisaldavat faili analüüsides mööda hiilida. Näitlikustamiseks võib tuua järgmise näite: Tagamaks salvestatud andmete konfidentsiaalsust ja terviklust, on virtuaalne IT-süsteem varustatud kõvaketta krüpteeringuga. Kuna virtuaalse masina põhimälu sisu loeti snapshot'i tegemisel välja ja salvestati virtualiseerimisserveri kõvakettale, võib juhtuda, et kõvaketta krüpteerimistarkvara krüptograafilised võtmed kirjutatakse krüpteerimata kujul kõvakettale. Sama juhtub ka siis, kui süsteem virtualiseerimistarkvara kaudu ainult peatatakse ja olek kirjutatakse käituse hilisemaks jätkamiseks kõvakettale. Failist, kuhu salvestati põhimälu sisu, on siis teatud juhtudel võimalik välja lugeda kõvaketta dekrüpteerimise võti. See näitab, et füüsiliste IT-süsteemide konfidentsiaalsuse ja tervikluse tagamise meetmetel on virtuaalsete IT-süsteemide korral tihtipeale vähendatud mõju. Nendest on võimalik virtualiseerimisserveri enda vahenditega mööda hiilida. Raskendamaks virtuaalse IT-süsteemi snapshot'i Offline analüüsi, tuleks mõelda variandile selliste süsteemidel snapshot'ide tegemine ja süsteemi külmutamine deaktiveerida.

Selljuhul tuleb kontrollida, kas kasutatud snapshot'idel põhinevad andmevarundusmeetmed ikka veel töötavad.

- Andmemuudatuste püsivus - Virtuaalsete IT-süsteemide snapshot'id sisaldavad IT-süsteemi tervikliku olekut, kaasaarvatud kõiki andmeid mis selle loomisel virtuaalsel IT-süsteemil paiknesid. Kui virtuaalne IT-süsteem viiakse snapshot'iga tagasi varasemale tasemele, saab seeläbi tühistada ka andmetes tehtud muudatusi. Sellekohased näited on failiserveri andmed või kataloogiteenuse nagu Active Directory struktuur ja sisu. Virtuaalse IT-süsteemi jaoks, mida ei tohi mitte mingil juhul varasemasse olekusse tagasi viia, tuleb snapshot'ide tegemise võimalus samuti desaktiveerida. Kui snapshot'idest ei ole võimalik loobuda, tuleks piirata nende mahtu. Näiteks võiks snapshot sisaldada ainult teatud ajameid või töösamme enne ja pärast snapshot'ti loomist või taastamist. Näiteks kui eelnevasse olekusse viiakse tagasi Active Directory domeenikontroller, tuleb kasutusele võtta meetmed Active Directory andmebaasi taastamiseks, kuna vastasel juhul sisaldaks see ebatäpseid andmeid. Piiratud snapshot'i maht ja vajalikud töösammud tuleb dokumenteerida.

Kontrollküsimused:

- Kas on kindlustatud, et kõikidele desaktiveerimata snapshot'i funktsiooniga virtuaalsetele IT-süsteemidele on hinnatud ja dokumenteeritud snapshot'ide maht ja selleks vajalikud töösammud?
- Kas võimalus snapshot'te luua või süsteemi külmutada on virtuaalsete IT-süsteemide korral, mille tervikluse ja konfidentsiaalsuse ohustamisel oleksid raskekaalulised tagajärjed, desaktiveeritud.

M 4.348 Aja sünkroniseerimine virtuaalsetes IT-süsteemides

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: administraator

Paljud rakendused vajavad veatuks töötamiseks täpset süsteemiaega. Algab see juba failiserveriga, et see saaks endal salvestatud failid varustada ajatempliga. Teised süsteemid kasutavad süsteemiaega erineval moel. Teatud autentimissüsteemid nagu Kerberos või tokenil põhinevad süsteemid vajavad tõrgeteta tööks korrektset süsteemiaega. Monitooringusüsteemid nagu näiteks *mrtg* kasutavad süsteemiaega tavaliselt indeksina andmebaasi salvestatud salvestiste jaoks. Seepärast tuleb jälgida, et ka virtuaalsete IT-süsteemide süsteemiaeg oleks alati täpne. Virtualiseerimistoodetel, mis põhinevad serveri täielikul virtualiseerimisel, ei ole see tihtipeale ilma lisameetmeteta kindlustatud.

Süsteemiaja arvutamine taktilugemise kaudu

Kaasaegsed operatsioonisüsteemid ei tuvasta süsteemiaega süsteemikella pideva lugemisega, vaid seeläbi, et loetakse protsessori tsükleid ja võrreldakse neid tsükleid välise ajaallikaga. Selleks väliseks ajanäitajaks võib olla nii ajaserver kui ka riistvarakell. Sellist esmapilgul tüütut ajatuvastusmeetodit kasutatakse, kuna kaasaegsed protsessorid vajavad ajanäitajat, millel on kõrgem resolutsioon kui enamikel tavalistel kelladel. Resolutsioon peab olema kaasaegse protsessori taktialas. Pideva võrdlusega protsessoritsüklite ja usaldusväärse ajanäitaja pideva võrdlemise teel luuakse ümberarvutustegur, mis võimaldab protsessoritsükleid ajaks ümber arvutada. Kindlate ajavahemike tagant korrigeeritakse seda ümberarvutustegurit eelnevate tsüklite võrdlemisel ajaallikaga, et likvideerida arvestuses esinevad võimalikud ebakorrapärasused. Enamik serveri virtualiseerimistooteid jagavad virtuaalsetele IT-süsteemidele ning sellega ka virtuaalsetele protsessoritele sõltuvalt nende koormusest dünaamilised protsessoritsüklid. Sellest tulenevalt jookseb protsessoritsüklite lugeja virtuaalse masina vaatenurgast vaadelduna erinevate kiirustega. Aja väljaselgitamise algoritm annab iga kord erinevad tulemused, mis viib selleni, et ka süsteemiaeg virtuaalses IT-süsteemis käib näiliselt erineva kiirusega. Sellest lähtuvalt võib juhtuda, et ajaline erinevus virtuaalsetes IT-süsteemides võib olla kuni mõni minut, nii et ekstreemsetel juhtudel korrigeeritakse ajalugejaid üle ning virtuaalse IT-süsteemi aeg jookseb osaliselt näiliselt tagurpidi. Tavaliselt jookseb süsteemikell ühtlase protsessorikoormusega virtuaalsetes IT-süsteemides piisava täpsusega. Siinkohal ei ole oluline, kas koormus on suur või väike, vaid küsimus on selles, kas koormus on ühtlane. Süsteemides, milles on ajutiselt kõrge ja ajutiselt madal koormus, tekivad eelpool kirjeldatud efektid. Siinkohal käituvad operatsioonisüsteemid sõltuvalt oma konfiguratsioonist väga erinevalt.

Parandusmeetodid ja nende piirid

Enamikel virtualiseerimistoodetel on mehhanism virtuaalse IT-süsteemi süsteemiaja korrigeerimiseks. Seda realiseeritakse tihtipeale vastava tööriista funktsiooni kaudu. Näiteks sisaldavad firmade Citrix ja VMware tooted funktsiooni virtuaalsete IT-süsteemide süsteemiaja sünkroniseerimiseks virtualiseerimisserveri süsteemiajaga. Need mehhanismid ei ole aga mitte alati virtuaalses IT-süsteemis käitatavatele rakendustele piisavad, kuna nad ei mõju tavaliselt kõigile operatsioonisüsteemi taimeritele, vaid ainult nn *Time of Day Clock'ile.* Peale selle ei toimu sünkroniseerimine pidevalt, vaid kindla aja tagant. Need vahed jäävad küll enamasti sekundi murdosa piiresse, on aga täpse aja määramiseks tihtipeale ikkagi liiga suured. Seda aspekti tuleb jälgida rakenduste käitamisel virtuaalses IT-süsteemis.

Rakendused peavad toime tulema kas ebaühtlaselt käiva süsteemikellaga või tuleb ette võtta konfiguratsioonimuudatused virtualiseerimisserveris või virtuaalses IT-süsteemis, mis muudavad virtuaalsete IT-süsteemide süsteemikella täpsemaks. Sellised konfiguratsioonimuudatused seisnevad selles, et välise ajanäitaja päring viiakse läbi standardis ettenähtust tihedamini. See võib toimuda vastava tööriista kaudu, kui see toetab vastavat konfiguratsioonivõimalust. Vastavat virtuaalset IT-süsteemi on võimalik seadistada ka nii, et see saadaks tihedamini päringuid NTP-serverile ning korrigeeriks seeläbi oma süsteemikella. Seeläbi muutuvad intervallid, mille jooksul käib kell vale kiirusega, väiksemaks ja protsessoritsükli ümberarvutustegur ühtlustatakse kiiremini. Reeglina ei ole mõttekas neid kahte võimalust omavahel kombineerida, kuna vastasel juhul tuleb arvestada minimaalse jõudluskaoga. Unixi operatsioonisüsteemide jaoks tuleb tihtipeale kasutada virtualiseerimisega kalibreeritud kerneleid. Siin tuleb sõltuvalt Unixi derivaadist, näiteks buudilaaduris, seadistada vastavad parameetrid. Teatud juhtudel tuleb selline kernel luua püsivalt (ise koostatud).

Põhimõtteliselt tuleks luua tegutsemisviis, mis kindlustab, et probleemid süsteemiaja sünkroonsusega avastatakse ja kõrvaldatakse enne virtuaalsete süsteemide käikulaskmist. Uue virtuaalse IT-süsteemi alguskäituses tuleb süsteemi süsteemiaega hoolsamini jälgida. Seejuures tuleb välja selgitada, kas virtuaalse IT-süsteemi sisemine kell kaldub tegelikust ajast kõrvale. Sel juhul tuleb kontrollida, kas see mõjub virtuaalsel IT-süsteemil käitatavatele rakendustele negatiivselt ning vajadusel võtta kasutusele korrigeerivad meetmed. Korrigeerivate meetmete efektiivsust tuleb kontrollida nii katsekäituses kui ka edasises tootmises.

Täiendavad kontrollküsimused:

- Kas jälgiti piisavalt kindla IT-süsteemi või kindla rakenduse virtualiseerimise mõju süsteemiajale?
- Kas virtuaalsete IT-süsteemide rakendusi kontrolliti ebaühtlaselt jooksvate süsteemiaegadega seotud probleemide suhtes?
- Kas loodi üldkontseptsioon virtuaalsete IT-süsteemide piisava süsteemiaja sünkroonsuse tagamiseks?

M 4.349 Virtuaalse taristu turvaline kasutamine

Algatamise eest vastutavad: IT-juht, infoturbespetsialist

Rakendamise eest vastutavad: administraator

Ühel virtualiseerimisserveril käitatakse tavaliselt mitut virtuaalset IT-süsteemi. Kuna kõik üksikud virtuaalsed IT-süsteemid sõltuvad sellest taristust, võib viga taristusüsteemis, näiteks virtualiseerimisserveril, mõjutada kõiki selles süsteemis käitatavaid virtuaalseid IT-süsteeme. Järgnevalt antakse mõningad näpunäited selle kohta, kuidas virtualiseerimisserverit või virtuaalset taristut turvaliselt kasutada.

Soovitusi virtualiseerimisserveri enda kohta, mis ei puuduta virtualiseerimise aspekti, vaid serveri töö põhimõtteid, leiate moodulist B 3.101 Server .

Haldusligipääs

Virtualiseerimisserverid sisaldavad funktsioone neil käitatavate virtuaalsete IT-süsteemide juhtimiseks, hooldamiseks ja monitooringuks. Neid haldusfunktsioone saab kasutada kas lokaalselt virtualiseerimisserveril endal või administraatori töökeskusest võrgu kaudu. Selleks kasutatakse kas virtualiseerimisserveril paiknevat veebipõhist haldusliidest või spetsiaalset haldustarkvara„ näiteks VMware vSphere Client.Lisaks veel on mõningate virtualiseerimislahenduste korral võimalik hallata mitut virtualiseerimisserverit ja sellel käitatavaid virtuaalseid IT-süsteeme ühe keskse süsteemi kaudu (näiteks Citrix XenCenter, Microsoft System Center Virtual Machine Manager, SUN Management Center, VMware vCenter). Virtualiseerimisserverite või keskse haldussüsteemi vastavad võrguliidesed võimaldavad täieliku ligipääsu virtualiseerimisserveritele ja virtuaalsetele IT-süsteemidele. Sellest lähtuvalt tuleb haldusliideseid turvata. Siinjuures tuleb arvestada meetmega M 5.154 Virtuaalse taristu võrgu turvaline konfiguratsioon .

Monitooring ja käitusolek

Virtuaalse taristu administraatorid peaksid kindla aja tagant vastavalt infoturbedirektiivile (vt M 1.74z Virtuaalse taristu planeerimine) teostama monitooringut.

Siia hulka kuuluvad:

- snapshot'ide loomine ja kustutamine.
- Virtualiseerimisserveri ja virtuaalsete IT-süsteemide käitusoleku monitooring.
- ressursside koormuse kontroll.
- kontroll, kas on olemas piisavalt protsessoriressursse, et rahuldada virtuaalsete IT-süsteemide jõudlusvajadus.
- kontroll, kas esineb põhimälukitsaskohti, mis ohustavad virtuaalsete IT-süsteemide käideldavust.
- kontroll, kas on kasutada piisavalt massmälu (kõvakettaruum või salvestusvõrgu jaotatud ja kogu maht).
- võrgu ribalaiuse kitsaskohtade kontroll.
- füüsiliste võrkude ühenduskohtade kontroll.

- Virtualiseerimisserveri ja virtuaalsete IT-süsteemide konfiguratsiooni tervikluse kontroll (vt M 2.448 Virtuaalsete taristute funktsiooni ja konfiguratsiooni kontroll , M 2.449z Konsooli kaudu virtuaalsetele IT-süsteemidele juurdepääsu minimaalne kasutamine , M 4.93z Regulaarne tervikluse kontroll ja M 5.8 Võrgu regulaarne turvakontroll)

Eeskätt olukorras, kus kasutatakse mõningate virtualiseerimistoodete poolt pakutud põhimälu või kõvakettaruumi ülebroneerimise võimalust, tuleb kehtestada pidev protsess ressursside monitooringuks. Vastasel juhul võivad liigse ülebroneerimise tõttu tekkida suured jõudluskaod. Kui kõvakettaruumi jääb puudu, võivad kõik sellest mõjutatud IT-süsteemid korraga rivist välja langeda. Kui kasutatakse snapshot'e, tuleks ka massmälu koormust hoolega jälgida, kuna snapshot'i failid kasvavad reeglina dünaamiliselt. Regulaarselt läbiviidavat monitooringut on võimalik automatiseerida (näiteks meiliteated jne).

Konfiguratsioonimuudatuste testid

Virtualiseerimisserveri konfiguratsioonimuudatustest võivad mõjutatud olla paljud IT-süsteemid. Vead võivad viia selleni, et sellel virtualiseerimisserveril paiknevaid IT-süsteeme ei ole enam võimalik käivitada või katkeb ühendus süsteemide jaoks vajalike ressurssidega. Kui virtualiseerimisserveri konfiguratsiooni muudetakse, tuleb enne aktiveerimist kontrollida selle tehnilist töövalmidust. See võib toimuda näiteks testkeskkonnas või nelja silma põhimõttel.

Kontrollküsimused:

- Kas virtuaalse taristu haldusliidesed on kaitstud?
- Kas virtuaalse taristu korral viiakse regulaarselt läbi monitooringuid?
- Kas virtualiseerimistaristu konfiguratsioonimuudatusi kontrollitakse enne realiseerimist?

M 4.350 DNS-serveri turvaline aluskonfiguratsioon

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

DNS-serverid on ründajatele meelepärased sihtmärgid. DNS-serveri manipuleerimisega saab mõjutada kõiki DNS-i kasutavaid teenuseid. Näiteks saab domeeniinfo muutmisega mõjutada veebiserverit, meiliserverit, kaughaldusrakendusi jms. Sel põhjusel on DNS-serveri hoolikas konfigureerimine ülimalt vajalik.

Õiguste piiramine

DNS-serveri protsessil peavad olema ainult hädavajalikud õigused, et õnnestunud ründe korral oleksid tagajärjed võimalikult väikesed. Kui tehniliselt võimalik, tuleks DNS-serveri protsessile määrata eraldi kasutaja ja eraldi grupp. Kasutaja saab ainult vajalike failide õigused. Kui DNS-server käivitatakse süsteemi käivitamisel automaatselt, peab automaatne käivitamine olema seadistatud selliselt, et DNS-serveri protsess käivituks talle määratud kasutaja ja grupiga.

DNS-serveri versioon

DNS-serveritoote versioon võib pakkuda ründajale väärtuslikku infot. Näiteks aadressil http://www.isc.org/sw/bind/bind-security.php on kirjas kõik DNS-serveritoote BIND seni avalikustatud puudujäägid. Sel põhjusel tuleb versiooni numbrit varjata. Selle võib näiteks asendada kirjega „tundmatu” (*unknown*). See meede ei tõsta küll otseselt DNS-serveri turbeastet, kuid muudab ründajale info kogumise raskemaks.

Päringud

Vahemälu mürgitavate rünnete oht suureneb siis, kui DNS-serverid võtavad päringuid vastu tingimusteta. Seetõttu on oluline kindlaks määrata, milliseid päringuid võib vastu võtta. Resolvingu DNS-serverid tegelevad võrgu või institutsiooni Resolverite päringutega ja tavaliselt on need rekursiivsed päringud. See tähendab, et Resolvingu DNS-serverid peavad vastu võtma sisevõrgust laekuvaid rekursiivseid päringuid. Internetist tulevaid päringuid ei tohi need vastu võtta, sest selle ülesandega tegeleb Advertisingu DNS-server. Internetist tulevaid päringuid tuleb alati töödelda iteratiivselt, sest seeläbi pakub Advertisingu DNS-server infot ainult oma hallatavate tsoonide kohta ega saa saata võltsitud vastuseid. Resolvingu DNS-serverite turbeastme tõstmiseks tuleks kasutada mõnd lisamehhanismi. Nagu juba mainitud, peavad Resolvingu DNS-serverid vastu võtma institutsioonisiseste IT-süsteemide päringuid. Resolvingu DNS-serverid on seega sunnitud teisendama nimesid, mille suhtes nad ei ole ise autoriteetsed. Ründaja saaks siinkohal sisestada valesid vastuseid. Vastuste ja päringute seostamine toimub järgmiselt:

- IP-aadress,
- päringu ID (juhuarv),
- päringu *source port*.

Kuna IP-aadress ja ID pakuvad liiga vähe kaitset, tuleks päringute saatmisel kasutada lisaks juhuslikke *source port* 'e. Tänapäeval minnakse üle ka meetodile, mille kohaselt konfigureeritakse Resolvingu DNS-serverile mitu IP-aadressi ja muudetakse need juhuslikuks.

Tsooniedastused

Tsooniedastuste põhjus ja eesmärk on primaarse DNS-serveri ja sekundaarse DNS-serveri sünkroniseerimine. Primaarne DNS-server loeb domeeniinfot tsoonifailidest ja sünkroniseerimiseks saadetakse see tsooniedastusega sekundaarse(te)sse DNS-serveri(te)sse. Tsooniedastused peavad olema võimalikud ainult primaarse DNS-serveri ja domeeni sekundaarse DNS-serveri vahel, vt M 4.351 Tsooniedastuse turve .

Teatud DNS-serverite välistamine

Kui valet domeeniinfot edastavad DNS-serverid on teada, ei tohi lasta oma Resolvingu DNS-serveritel neile päringuid saata. Kui institutsioon ei kasuta privaatseid IP-võrkusid, nt 10/8, 172.16/12 ja 192.168/16, tuleb turvalisuse põhjustel nendest võrkudest tulevaid päringuid eirata.

Täiendavad kontrollküsimused:

- Kas DNS-serveri protsessi õigused on piiratud vajaliku miinimumini?
- Kas rekursiivseid DNS-päringuid tohivad esitada ainult õigustega hostid?
- Kas tsooniedastused on võimalikud ainult primaarse ja sekundaarse DNS-serveri vahel?

M 4.351 Tsooniedastuse turve

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

Tsooniedastus sünkroniseerib primaarse DNS-serveri ja ühe või mitme sekundaarse DNS-serveri vahelise domeeniinfo. Primaarne DNS-server loeb ülemfailidest (master files) domeeniinfot ja tsooniedastusega jõuavad need ühte või mitmesse sekundaarsesse DNS-serverisse.

Tsooniedastuse puhul tuleb arvestada kahe turvaaspektiga:

- tuleb tagada, et tsooniedastus primaarse ja sekundaarse DNS-serveri vahel ka reaalselt töötaks;
- välistada loata tsooniedastused.

Tsooniedastuse funktsiooni toimimise tagamiseks tuleb iga kord, kui tsooniedastuse seadistusi muudetakse, kontrollida, ega funktsiooni toimimine selle tõttu vähimalgi määral ei kannatanud. Selleks võib näiteks käivitada tsooniedastuse. Seejärel tuleb logifailide alusel kontrollida, kas esines vigu. Kui tsoonid ei ole ülemäära suured, on võimalik primaarse DNS-serveri hallatavat domeeniinfot võrrelda sekundaarse DNS-serveri domeeniinfoga ka käsitsi. Et volitamata isikutel ei oleks võimalik tsooniedastust käivitada ja et nad ei saaks seeläbi enda valdusesse mõne tsooni kogu domeeniinfot, tuleb tsooniedastused konfigureerida selliselt, et need oleksid võimalikud ainult primaarsete ja sekundaarsete DNS-serverite vahel.

Selleks peab piirama vähemalt DNS-serveri IP-aadresse, veelgi kindlam on kasutada ülekandesignatuure (Transaction Signatures, TSIG). IP-aadresside piiramiseks tuleb primaarses DNS-serveris iga tsooni jaoks konfigureerida sellega kokkukuuluvad sekundaarsed DNS-serverid. Selleks määratakse üks või mitu IPaadressi.

Tsooni sekundaarse(te)s DNS-serveri(te)s tuleb konfigureerida vastav primaarne DNS-server.

Tugevama kaitse saab, kui kasutada tsooniedastuse turvamiseks ülekandesignatuure (TSIG). TSIG-ide jaoks defineeritakse primaarses DNS-serveris ja sekundaarse(te)s serveri(te)s sümmeetrilised võtmed. Tsooniedastuse käivitamisel koostab ülekandesignatuur päringu binaarandmetest, kasutades sümmeetrilist võtit ja räsifunktsiooni (hash), räsisõnumi autentimiskoodi (Hash Message Authentication Code, HMAC). HMAC lisatakse päringule. Sekundaarne DNS-server, mis võtit samuti tunneb, arvutab HMAC iseseisvalt. Kui saadetud ja arvutatud HMAC-d ühtivad, toimub tsooniedastus, kui ei ühti, ei toimu. Erinevalt IP-aadressidel põhinevast turbest kaitseb see meetod ka IP-võltsimise eest. Ülekandesignatuuride puhul tuleb siiski arvestada seda, et kõikides DNS-serveritoodetes ei pruugi seda funktsiooni olla või on see juurutatud viisil, mis erineb standardist.

Kontrollküsimused:

- Kas DNS-i tsooniedastused töötavad korralikult?

- Kas DNS-i tsooniedastused on lubatud ainult primaarse serveri ja sekundaarse(te) DNS-serveri(te) vahel?

M 4.352 DNS-i dünaamiliste värskenduste turve

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

Dünaamiliste värskenduste turvaliseks kasutamiseks tuleb tagada, et domeeniinfot saavad muuta ainult legitiimsed IT-süsteemid. Lisaks tuleb määrata, millist domeeniinfot IT-süsteemid muuta tohivad. Selleks, et volitamata IT-süsteemid ei saaks dünaamiliste värskenduste abil domeeniinfot manipuleerida, võib kasutada kahte võimalust:

- volitatud hostide piiramine IP-aadressidega;
- volitatud hostide piiramine ülekandesignatuuridega (TSIG).

IP-aadresside piiramisel tähistatakse IP-aadressiga dünaamiliste värskenduste allikas. Ülekandesignatuuride puhul kasutatakse dünaamiliste värskenduste allika tuvastamiseks sümmeetrilist krüpteerimist, vt M 4.351 Tsooniedastuse turve . Peale IP-võltsimise ohu kaasneb IP-aadressidega veel üks probleem. Sekundaarsed DNS-serverid saab sisse seada dünaamiliste värskenduste edasisaatjatena (*forwarder*) ja primaarset DNS-serverit saab konfigureerida selliselt, et see võtab vastu ainult sekundaarsetelt DNS-serveritelt tulevaid värskendusi. Kuna seda, millistelt IT-süsteemidelt värskendusi vastu võetakse, konfigureeritakse ainult sekundaarsetes DNS-serverites, jääb primaarsele DNS-serverile värskenduste allikas nähtamatuks. Seega pole DNS-i dünaamilisi värskendusi tegevaid hoste võimalik piirata originaalallika alusel.

Allika tuvastamise kõrval tuleb konfigureerida ka seda, millist domeeniinfot lubatakse muuta. Reeglid peavad olema seatud nii, et need tagaksid dünaamiliste värskenduste veatu kasutamise. Näiteks vajab DHCP-server volitust domeeninimede ja IP-aadresside seoste muutmiseks, kuid pole mingit põhjust võimaldada DHCP-serveril muuta tsooni eest vastutavat DNS-serverit.

Täiendavad kontrollküsimused:

- Kas DNS-i dünaamilised värskendused on piiratud volitatud hostidega?
- Kas on kindlaks määratud, millistel konkreetsetel juhtudel tohivad volitatud hostid muuta domeeniinfot?

M 4.353z DNSSEC kasutamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

DNS-protokolli kontseptsiooni puudujääkidele ja DNS-tarkvara turvaaukudele vaatamata ei ole DNSSEC (DNS Security Extensions) kasutamine veel eriti levinud. Näiteks sai see taas kord selgeks 2008. aasta suvel, mil ilmnesid DNS-protokolli disainiprobleemid. Disainiviga muudab vahemälu mürgitamise (ja seetõttu ka teiste rünnete toimepaneku) oluliselt kergemaks. Lühikeseks ajaks saab selle disainiprobleemi lahendada, kasutades päringute puhul ID-dena krüptograafiliselt tugevaid juhuarve ja juhuslikku source port 'i. Pikemas perspektiivis saab selliseid probleeme ja kriise lahendada ainult DNSSEC-ga. DNSSEC on loodud DNS-i kaitsmiseks mitmete rünnete, muu hulgas ka vahemälu mürgitamise rünnete eest. Selleks kasutatakse asümmeetrilist krüptograafiat, mistõttu tuleb koos selle meetmega kasutada ka meedet M 2.46 Krüpteerimise õige korraldus .

DNSSEC puhul allkirjastatakse kogu tsooniinfo privaatvõtmega. Neid allkirju saab kontrollida vastava avaliku võtmega. Võtmepaari nimetatakse tsooni allkirjavõtmeks (Zone-Signing-Key, ZSK). Kui DNSSEC-d toetav Resolver saadab päringu DNS-serverile, milles on konfigureeritud DNSSEC, saadab server päringule vastuseks domeeniinfo koos allkirjadega. See võimaldab Resolveril allkirja ja avaliku võtmega kontrollida domeeniinfo õigsust. Tsooni allkirjavõtme (ZSK) autentsuse tagamiseks allkirjastatakse see võtme allkirjavõtmetega (Key-Signing-Keys, KSK). Võtme allkirjavõtmete avaliku osa räsiväärtus edastatakse ülemdomeenile. Ülemdomeen allkirjastab oma võtmega räsiväärtuse ja kinnitab räsiväärtuse autentsust. Sellega tekib usaldusahel (Chain-of-Trust). Kui ülemdomeen DNSSEC-d ei kasuta, puudub tal võti ja ta ei saa luua allkirja, mis kinnitaks võtme allkirjavõtmete autentimist. DNS-serveritele saab siiski anda korralduse usaldada oma võtmeid, luues vastavad usaldussaared (Island-of-Trust). DNSSEC levides muutvad need usaldussaared suuremaks ja paraneb ka turvalisus. DNSSEC-l on järgmised turvamehhanismid:

- DNS-info allika autentimine;
- tagatakse domeeniinfo terviklus; domeeniinfot ei saa enam manipuleerida, sest allkiri muudab manipuleerimise nähtavaks. Kliendid võivad näiteks kindlad olla, et nad suhtlevad õige veebiserveri, meiliserveri või muuga;
- domeeninime puudumisel saadetakse autenditud veateade.

Tsooni allkirjavõtmeid (ZSK) ja võtme allkirjavõtmeid (KSK) tuleb hoolikalt hallata ja neid tuleb regulaarselt vahetada. Kuna tsooni allkirjavõtmetega allkirjastatakse rohkem andmeid, tuleb neid vahetada sagedamini. Olenevalt allkirjastatud tsoonide suurusest tagab piisava turvalisuse see, kui võtmeid vahetatakse ühe kuni kolme kuu möödudes. Võtme allkirjavõtmeid tuleks vahetada vähemalt kord aastas. Kui võtme allkirjavõti või tsooni allkirjavõti tuleb avalikuks, on vaja võtmed kohe välja vahetada. DNSSEC ja sellega seotud vajalike krüptograafiliste operatsioonide kasutamisel tuleb suurendada DNS-serverite jõudlust, eriti oluline võib olla arvutusvõimsuse suurendamine. Tuleb tagada, et ka suure koormusega hetkedel oleks vastuse laekumise aeg lühike.

Täiendavad kontrollküsimused:

- Kas on tagatud, et DNSSEC võtme allkirjavõtmeid (KSK) ja tsooni allkirjavõtit (ZSK) vahetatakse regulaarselt?

- Kas DNS-serveri jõudlust on võrreldes DNS-serveriga, millel puudub DNSSEC, suurendatud?

M 4.354 DNS-serveri seire

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

DNS-serveri turvalise käitamise tagamiseks ei saa lootma jääda ainult hoolikale planeerimisele ja esmasele konfigureerimisele. Tuleb võtta erinevaid meetmeid, mis tuvastaksid võimalikud probleemid ja turvaaugud. Võimsusnõuded tuleb kindlaks määrata juba planeerimisfaasis.

Kuna võimsusnõuded sõltuvad näiteks:

- tsooni(de) suurusest,
- päringute arvust,
- rekursiivsete päringute arvust,
- tsooniedastuste arvust,
- dünaamiliste värskenduste arvust,

on raske vajalikku võimsust täpselt planeerida. Seega tuleb DNS-serverit pidevalt koormuse kontrollimiseks jälgida, et vajaduse korral kohandada riistvara võimsust. Lisaks võib suurem koormus olla märk ründest. Konfiguratsiooni muudatused tuleb hoolikalt dokumenteerida, nii et igal ajal saaks kontrollida, kes, mida ja mis põhjusel muutis. Konfiguratsioonifailide muudatuste jaoks võib kasutada revisjoniprogrammi, mis kergendab dokumenteerimist ja võimaldab taastada varasemaid konfiguratsioone (vt M 2.25 Süsteemi konfiguratsiooni dokumenteerimine). Lisaks tuleb failisüsteemis regulaarselt kontrollida DNS-serveri pääsuõiguseid. Eriti tuleb seda teha pärast tarkvara värskendamist või konfiguratsiooni muutmist.

Administraatorid peavad kasutatud tarkvaras avastatud turvaaukudega end võimalikult kiiresti kurssi viima (vt M 2.35 Teabe hankimine turvaaukude kohta). DNS-serveri logifaile ja operatsioonisüsteemi logifaile tuleb regulaarselt kontrollida ja analüüsida.

Logifailide ebaregulaarsused, mis võivad viidata võimalikele probleemidele, on näiteks järgmised:

- teatud allikatest tehtud päringute sagenemine;
- (ebaõnnestunud) tsooniedastuste sagenemine;
- kindlate domeeninimedega seotud päringute sagenemine;
- olematute domeeninimedega seotud päringute sagenemine;
- loata rekursiivsete päringute sagenemine. Ebaregulaarsused ei ole ilmtingimata märk serveri kompromiteerimisest. Sageli võivad põhjuseks olla valed seadistused.

Turvalise käitamise juurde kuuluvad ka regulaarsed hädaolukorraks valmisoleku meetmed (vt M 6.139 DNS-serveri avariiplaani koostamine).

Kontrollküsimused:

- Kas DNS-serveri koormust kontrollitakse regulaarselt?
- Kas muudatused DNS-serveri konfiguratsioonis dokumenteeritakse (automaatselt)?
- Kas DNS-serveri pääsuõigusi kontrollitakse regulaarselt?
- Kas administraatorid on DNS-serveri tarkvara aktuaalsetest turvaaukudest teadlikud?
- Kas DNS-serveri logifaile analüüsitakse regulaarselt?

M 4.355 Kasutajahaldus rühmatarkvarasüsteemide puhul

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator

Rühmatarkvarasüsteemis töödeldavate äriandmete turve sõltub suuresti kasutajatele ja administraatoritele antud pääsuõigustest – need määravad kindlaks, milliseid andmeid vaadata või muuta saab. Seetõttu kujutavad konfigureeritud pääsuõigused ja nende haldamine endast väga olulist süsteemiturbe komponenti. Pääsuõigusi (eelkõige privilegeeritud õigusi) tuleb regulaarselt pääsuõiguste kontseptsiooni suhtes kontrollida ning ülesannete muutumisel õigel ajal kohandada. Pääsuõiguste kontseptsioon peab vastama kaitsevajadusele ning hõlmama kõiki rühmatarkvarakomponente. Pääsuõiguste haldamisel tuleb silmas pidada järgmisi soovitusi. N imekirja tuleb kohalike vajaduste järgi kohandada ja täiendada.

Pääsuõiguste andmine

Põhimõtteliselt tuleb pääsuõigusi jaotada võimalikult piiratult. See kehtib eelkõige rühmatarkvara administraatorite puhul - iga administraator peab saama ainult oma ülesannete täitmiseks vajalikud õigused. Igasugune pääsuõiguste andmine tuleb dokumenteerida. Operatsioonisüsteemi ja rühmatarkvara tasemel on soovitatav administratiivsed toimingud üksteisest võimalikult suures ulatuses lahutada, pidades siiski silmas, et piiramatult pole see võimalik: mõnede ülesannete puhul vajavad rühmatarkvara a dministraatorid ka kohalikke a dministraatoriõigusi (näiteks teenuste alustamiseks ja peatamiseks).

Koolitus

Kasutajatunnuste, rollide, profiilide või pääsuõiguste eest vastutavad administraatorid peavad tingimata saama koolituse õiguste kontseptsiooni ja haldamise (protsessid, tööriistad, õige kasutamine) kohta või tõestama vastavate teadmiste olemasolu . Ainult nii saavutatakse õiguste asjakohane haldamine (vt M 3.74 Rühmatarkvarasüsteemide süsteemiarhitektuuri ja turbe koolitus administraatoritele).

Rollide lahutamine administreerimise puhul

Halduskontseptsioon tuleb üles ehitada nii, et vastutusvaldkonnad oleksid võimalikult palju üksteisest eraldatud. Silmas tuleb pidada tuleb järgmist:

- Tuleb määrata kasutajaadministraator, kes annab ja muudab k asutajatunnuseid ning määrab rolle. Süsteemiadministraatorile ei tohi rollide või profiilide määramine ja muutmine lubatud olla.
- Tuleb määrata profiiliadministraator, kes võib olemasolevate rollide jaoks luua profiile, mis ei sisalda privilegeeritud süsteemiõigusi.

Eraldamise abil (kui see on tehniliselt õigesti teostatud) saavutatakse see, et administraatorid ei saa ise pääsuõigusi anda, vaid ainult määratud ülesandeid täita. Väiksemates ettevõtetes või asutustes ei pruugi personali vähesuse tõttu selline eraldamine võimalik olla – siis täidab kõiki ülesandeid üks ja sama isik . Sel juhul saab administraator kõiki rühmatarkvarasüsteemi andmeid märkamatult vaadata ja muuta. Üldiselt peetakse seda turbe seisukohalt ohtlikuks ning siis on vaja lisakontrolli . Sama kehtib üldiselt ka isikuandmete töötlemise puhul, kus vastavad funktsioonid tuleb üksteisest lahutada. Kui see pole võimalik, tuleb sobivad kontrollmeetmed asutuse tasemel kindlaks määrata ja nende rakendamine tuleb taga-

da. Rühmatarkvara poolt etteantud ja eraldatud rolle tuleb hoolikalt oma nõuetega võrrelda ja vastavalt kohandada.

Täiendavad kontrollküsimused:

- Kas kasutatavate rühmatarkvarakomponentide puhul on olemas sobiv pääsuõiguste kontseptsioon ?
- Kas rühmatarkvara administraatorid on saanud koolituse pääsuõiguste haldamise kohta ?

M 4.356 Rühmatarkvarasüsteemide turvaline installeerimine

Algatamise eest vastutavad: IT-turvaspetsialist, IT-juht.

Rakendamise eest vastutab: administraator.

Rühmatarkvarasüsteemi installimisel tuleb arvestada allkirjeldatud asjaoludega, sest süsteemi turvalisusele pannakse oluline alus juba installimisfaasis.

Operatsioonisüsteemide turve

Rühmatarkvarasüsteemi komponendid installitakse IT-süsteemidesse, näiteks serveritesse ja klientsüsteemidesse rakendusprogrammidena ning neid käitatakse protsessidena. Seetõttu on kasutatava operatsioonisüsteemi turve oluline ka rühmatarkvarasüsteemi turvalisuse tagamiseks. Sel põhjusel tuleb kasutatavate IT-süsteemide seisukohast oluliste IT etalonturbe kataloogide moodulitega arvestada ja neid rakendada juba süsteemi modelleerimisel. Rühmatarkvarasüsteem koosneb sageli paljudest eri osadest. Kõikvõimalikud komponendid, mida ei kasutata, võivad aga muutuda turvariskideks, sest tihti unustatakse need ära ja seetõttu jäävad nende konfiguratsioonid kohandamata. Seetõttu tuleks komponendid, mida ei kasutata, võimaluse korral üldse installimata jätta või hiljem välja lülitada.

Olulised autentimisandmed tuleb seadistada juba installimise käigus. Viimaste hulka kuuluvad näiteks teenuste juurdepääsuõigustega kasutajate paroolid, mida rühmatarkvarasüsteemi komponendid kasutavad süsteemisiseste sideühenduste autentimisel. Tuleb tagada, et kasutajad valivad endale turvalised paroolid (vt M 2.11 Paroolide kasutamise reeglid). Paroolide valimisel peaks lähtuma organisatsioonis kehtivatest eeskirjadest. Uus parool tuleb kindlasti sisestada ka neil juhtudel, kui installimisprotsessi käigus antakse parool automaatselt ette. Rühmatarkvarasüsteemi riskianalüüsi tehes tuleb arvestada, et administraatoril, kes installib süsteemi ja määrab paroolid, on võimalik rühmatarkvarasüsteemi turvamehhanismidest mööda hiilida.

Tehnilistel kasutajatel, kellele antakse paroolid, on üldjuhul ulatuslikud õigused.

Seetõttu peavad usaldusväärsed administraatorid pärast installimistööde lõppu asjaomased paroolid ära muutma. See protsess tuleks juurutada tehnilise lahendusena.

Administraatorite puhul, kelle tööülesandeid ei ole võimalik lahutada, tuleks kaaluda parooli jagamist nõnda, et parooli sisestamisel järgitakse nelja silma põhimõtet, s.t kumbki administraator sisestab ainult ühe kindla parooliosa. Rühmatarkvarasüsteeme ei installita enamasti otse selleks otstarbeks loodud andmekandjatelt. Pigem tehakse IT-süsteemidele installimiseks vajalikud andmed kättesaadavaks lokaalselt või kasutatakse võrgus asuvat kataloogistruktuuri. Andmeid ei ole soovitatav hoida lokaalse koopiana selles arvutis, kuhu hakatakse

installima rühmatarkvarasüsteemi komponente, vaid eraldi installimisarvutis, millel on ühendus LAN-iga.

Suurtes ametiasutustes ja ettevõtetes saab sama kataloogi kasutada ka järgnevate rühmatarkvarasüsteemide installimiseks. Kui süsteemi ei installita muust võrgust eraldatud ja kaitstud võrguossa, tuleks installimisarvuti võrguühendus selleks ajaks, mil seda ei kasutata, katkestada. Kindlasti tuleks vähemalt serveri ühiskasutus välja lülitada. Juurdepääsu installimiseks kasutatavatele andmeallikatele tuleb kaitsta operatsioonisüsteemi vahenditega selliselt, et neile pääseksid ligi ainult volitatud administraatorid. Välistamaks installimisandmete muutmist, on ülimalt tähtis, et volitamata administraatoritel ei oleks installimise andmeallikatele kirjutamisõigusega juurdepääsu. Kui installimise andmeallikaid hoitakse lokaalsete koopiatena arvutites, kuhu on paigaldatud rühmatarkvarasüsteem, on soovitatav need andmed pärast installimist sealt ära kustutada.

Süsteemikompleksi turvaline installimine ja konfigureerimine

Lähtuvalt sellest, kuidas süsteemikompleksi planeeriti, tuleb installida ja konfigureerida ka rühmatarkvarasüsteemi käitamiseks vajalikud komponendid (nt turvalüüsid).

Kontrollküsimused:

- Kas kõik rühmatarkvarasüsteemi käitamiseks vajalikud komponendid on installitud ja konfigureeritud turvaliselt?
- Kas kõik rühmatarkvarasüsteemi installimisel valitud paroolid on turvalised?

M 4.357 Rühmatarkvarasüsteemide turvaline kasutamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator, kasutaja

Pärast rühmatarkvarakomponentide installeerimist ja konfigureerimist tuleb kasutusele võtta meetmed, millega tagada rühmatarkvara turvaline kasutamine. Seejuures tuleb kontrollida, kas vastavas asutuses rakendatakse infoturbenõudeid. Jälgida tuleb järgmisi turvalisust puudutavaid aspekte:

Tarkvara ja süsteemi hooldus

IT-süsteemide turvalise kasutamise juures on üheks oluliseks eelduseks see, et installeeritud oleksid kõik tarkvara jaoks tähtsad remondipaketid (*Service Pack*), uuendused ja paigad. Seetõttu on vaja, et administraatorid hoiaksid ennast kasutatava rühmatarkvara ja operatsioonisüsteemi uute teadaolevate turvaaukudega pidevalt kursis ning võtaksid nende kõrvaldamiseks kohe vastavaid meetmeid. Enne remondipaketi, uuenduse või paiga süsteemi installeerimist tuleks seda testkeskkonnas katsetada. Sedasi saab kindlaks teha soovimatuid kõrvalmõjusid. Lisaks tuleks kogu süsteemi konfiguratsiooni regulaarselt kontrollida ja veenduda, et see vastab etteantud nõudmistele ja infoturbedirektiividele.

Teenusetõkestamisrünnete (*Denial-of-Service-Attack* – DoS) tõrje

DoS-rünnakute tõrjeks on soovitatav kindlaks määrata maksimaalselt lubatud teate- või salvestusmahu suuruse piirang. See kehtib eelkõige sissetulevatele ühendustele. Kasutajaid tuleb piirangutest teavitada . Samuti tuleb kindlaks määrata, kuidas toimida liiga suurte sisenevate teadetega, näiteks kas saajat või saatjat tuleks teavitada, et teateid ei edastata. Vastavast otsusest tuleks kasutajatele teada anda. Üheks mehhanismiks on veel teadete filtreerimine. Sellega ei suudeta küll tõrjuda suursüsteemide rämpspostirünnakuid, kuid kasu on sellest üksikute saatjate aadresside filtreerimisel.

Meililistide kontroll

Meilide adresseerimise lihtsustamiseks kasutatakse tihtipeale alias-faile või meililisti. Kui nii meiliserveril kui ka meilikliendil hoitakse alias-faile, tuleb välja selgitada, millised sissekanded on esmatähtsad, st kas sama aliase valimisel aktsepteeritakse seda meiliserveri või meilikliendi poolt. Meilide saamisel peaks määravaks teguriks olema meiliserveri aliase teostus, saatmisel aga meilikliendi oma. Et kasutajad saaksid meilide saatmisel sellega arvestada, tuleb neile teada anda, milliseid aliaseid meiliserveril kasutatakse. Selleks, et kasutajad saaksid alias-faile meiliserveril kasutada, peab neil olema lugemisligipääs. Kirjutamisõigus aga peaks olema ainult meiliadministraatoril. Selleks, et meilid ei satuks vigaste, mitteaktuaalsete või manipuleeritud meililistide kaudu valede saajateni, tuleb meililistide korrektsust ja aktuaalsust regulaarselt kontrollida.

Andmevarundus

Andmete kiire taastamise huvides, näiteks pärast süsteemi rivist väljalangemist, tuleb regulaarselt luua rühmatarkvarasüsteemi uusi andmevarundusi (vt M 6.90 Andmete varundamine ja arhiveerimine rühmatarkvara ja e-posti puhul). Seda, kas koostatud andmevarundused lasevad ennast uuesti igas osakonnas installeerida, tuleks kontrollida juhuslike ajavahemike tagant.

Kaitse rivist väljalangemise vastu

Aluseks tuleks alati võtta hädaolukorra praktiline plaan (vt M 6.140 Hädaolukorra plaani koostamine rühmatarkvarasüsteemide avarii puhuks).

Regulaarne turvakontroll

Rühmatarkvarasüsteemi turvalisust tuleb regulaarselt kontrollida. Nii saab avastada ja kõrvaldada süsteemi nõrku kohti. Turvatestid peaksid toimuma regulaarselt ning neid peaksid tegema erinevad isikud. Suhteliselt lühikeste ajavahemike (näiteks kord kuus) tagant peaksid administraatorid läbi viima lühiteste. Seejuures on soovitatav koostada kontrollnimekiri, mis tagaks efektiivse kontrollprotsessi. Väiksemad avastatud probleemid saavad administraatorid tavaliselt kohe kõrvaldada, suurematest probleemidest tuleb vastavalt reeglitele teada anda. Keskmiste ajavahemike tagant (mitu kuud) tuleks turvateste läbi viia asutuse teistes osakondades (näiteks infoturve, IT-revisjon). Pikemate ajaperioodide järel võib olla mõttekas lasta süsteemi kontrollida ka välistel kontrollijatel.

Täiendavad kontrollküsimused:

- Kas rühmatarkvarasüsteemide turvalise kasutamise tagamiseks on võetud sobivaid meetmeid?
- Kas rühmatarkvarasüsteemi turvaliseks kasutamise täideviimiseks rakendatakse kõiki infoturbedirektiivis sisalduvaid aspekte?
- Kas rühmatarkvarasüsteemis tehakse regulaarseid turbeteste?
- Kas turbekriitilisi rühmatarkvaralogisid analüüsitakse regulaarselt?

M 4.358 Rühmatarkvarasüsteemide logid

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator

Selleks, et rakendada rühmatarkvarasüsteemi funktsioonide ja turbe seiret, tuleb protokollida kõiki turvalisust puudutavaid sündmusi. Üldjuhul tuleb logimisel pöörata tähelepanu järgmistele aspektidele.

Logimiskontseptsioon

Koostada tuleb logimiskontseptsioon. Vastavas kontseptisioonis tuleb kindlaks määrata, milliseid logiandmeid rühmatarkvarasüsteemis kogutakse ja analüüsitakse. Kuna logiandmed võivad sisaldada ka isikuandmeid, tuleb sellesse protsessi kaasata ka andmeturbespetsialist ja personali- või töönõukogu.

Logiandmete turvalisus

Logiandmed võivad sisaldada tähtsat süsteemiteavet või isikuandmeid. Seega tuleb ligipääsu logiandmetele piirata. Seetõttu võib juhtuda, et seadistusi on vaja teha nii rühmatarkvarasüsteemi sees kui ka sellest väljaspool (näiteks failitasandil).

Tähtsate süsteemijuhtumite analüüs

Tähtsad süsteemimuutused nagu riistvara, operatsioonisüsteemi, draiverite, teenuste ja muu tarkvara muudatused, vead ja rikked tuleb logida ja logisid tuleb regulaarselt analüüsida. Mitme rühmatarkvarasüsteemi kasutamisel on soovitatav kasutada keskset logimist, mis võimaldab kõiki logiandmeid ühel süsteemil analüüsida.

Ligipääsupiirang monitooringutööriistadele

Rühmatarkvarasüsteemi seiretööriistu tohivad kasutada ainult volitatud administraatorid.

Täiendavad kontrollküsimused:

- Kas rühmatarkvara jaoks koostati sobiv logimiskontseptsioon?
- Kas rühmatarkvaralogi analüüsitakse regulaarselt?

M 4.359w Veebiserveri koostisosade ülevaade

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

Veebilehe loomiseks on vaja erinevat riist- ja tarkvara. Olenevalt veebirakenduse funktsioonist läheb selleks tarvis eri tüüpi servereid. Baaskomponentideks on veebiserver ja veebirakenduste server. Üldjuhul on veebiserver ja veebirakenduste server installitud erinevatesse IT-süsteemidesse. Info püsivaks talletamiseks kasutatakse enamasti andmebaasiservereid. Seejuures kasutatakse lihtsamate operatsioonide jaoks kataloogiservereid, mille andmetele on klientidel enamasti ainult lugemisõigusega ligipääs. Sellised kataloogid on kasutusel näiteks kasutajaandmete salvestamisel.

Veebiserver

Veebiserver on riistvarakomponent, millega saab HTTP ja HTTPS-i kaudu hoida üleval veebisaite. Sellega luuakse raamistik, mille funktsioone saavad kasutada veebirakendused. Tihti nimetatakse veebiserveriks ka riistvara, millel paikneb veebiserveri tarkvara. Veebiserver on iga veebilehe tuumkomponent. Veebiserver võtab vastu kasutajate päringud ning saadab võimaluse korral ka vastuse. Nii on see näiteks staatiliste veebirakenduste korral. Veebiserver tarnib päringus küsitud info kohe, ilma dünaamilisi funktsioone käivitamata. Dünaamiliste veebirakenduste korral juhib veebiserver päringu enamasti edasi veebirakenduste serverile. Seal käivitatakse dünaamilised funktsioonid, nt veebilehe kuvamine lähtuvalt andmebaasi sisust, ja seejärel saadetakse tulemus tagasi veebiserverile. Mõned veebiserverid on veebirakenduste serveriga integreerinud ka programmeerimiskeele (nt Apache-veebiserver toetab PHP skriptikeelt (akronüüm PHP: Hypertext Preprocessor). Sellisel juhul ei pea rakendust veebirakenduste serverile edasi saatma, vaid see käivitatakse otse serveris. Kuna veebiserver on kasutajate päringutele otseselt avatud, muutub see ühtlasi ka kõige nähtavamaks ründeobjektiks.

Veebiserveri puhul tuleb tagada, et taustsüsteemidele edastatakse ainult legitiimsed päringud, et kasutajad pääseksid ligi ainult nende jaoks ette nähtud infole ning et veebiserverit ei oleks võimalik turvaaukude kaudu kompromiteerida. Veebileht võimaldab inimestel hankida infot ja kasutada funktsioone. Kasutaja pääseb neile ligi brauseri kaudu.

Dünaamiliste funktsioonidega veebilehtede käitamiseks on võimalik kasutada järgmist ülesehitust:

- Dünaamiliste funktsioonide teostamine väliste programmidega, mis käivitatakse liideste kaudu. Asjakohasteks näideteks on CGI (Common Gateway Interface) ja SSI (Server Side Includes). Veebilehe käivitamisel käivitatakse programmid otse veebiserveril. Programmipöörduse tulemused lisatakse vastusele, mis saadetakse kasutaja brauserile.
- Dünaamiliste funktsioonide realiseerimine funktsioonide või moodulitena, mis on integreeritud veebiserveriga, nt PHP kasutamine moodulina Apac-

hes. Suurim erinevus esimese punktiga võrreldes seisneb selles, et ei käivitata mitte ühtegi välist programmi. Dünaamiline funktsioon sisestatakse otse kuvatavasse veebilehte, nt skriptikoodina. Enne veebilehe edastamist brauserile interpreteeritakse skriptikood ning tulemus lisatakse serveri vastusesse.

- Dünaamilise funktsiooni realiseerimine iseseisval veebirakenduste serveril nagu JBoss, Weblogic või WebSphere. Sellise arhitektuuri korral võtab veebiserver päringud vastu ja asub neid töötlema. Need päringu osad, mis nõuavad dünaamiliste funktsioonide käivitamist, suunatakse edasi veebirakenduste serverile. Veebirakenduste server rakendab vajalikud funktsioonid ja loob vajaduse korral ka kommunikatsiooni taustsüsteemidega ning saadab tulemuse seejärel veebiserverile tagasi. Veebiserver lisab veebirakenduste serveri tulemuse seejärel oma vastusesse, mis saadetakse kliendi brauserile.

Veebirakenduste server

Paljud veebilehed vajavad peale veebiserveri ka teisi süsteeme. Näiteks läheb tarvis oma veebirakenduste servereid, kui veebilehe tööshoidmiseks kasutatakse Javat või.NET-i. Sellised programmeerimiskeeled nagu PHP, ASP või Perl toimivad sageli ka ilma veebirakenduste serverita, sest veebiserveris on vajalikud funktsioonid enamasti juba olemas. Veebirakenduste serverit kasutatakse dünaamiliste veebilehtede käitamiseks. Seejuures edastab veebiserver talle laekunud päringud koos vastavate parameetritega veebirakenduste serverile. Veebirakenduste server käivitab edasise toiminguna pöörduse töötlemise jaoks vajalikud skriptid, meetodid või funktsioonid. Olenevalt pöördusest teostab rakendusserver päringuid taustsüsteemides, nt andmebaasi- või kataloogiserverites. Seejärel saadetakse veebirakenduste serveri vastus uuesti tagasi veebiserverile. Veebirakenduste serverid sisaldavad mõningaid olulisi funktsioone ja raamistikke, mis on sageli vajalikud veebilehtede tööshoidmiseks. Liideseid ja teisi süsteeme (nt taustsüsteeme) üksteisest eraldades ja abstraheerides saab rakendusi ja andmetalletust täielikult lahus hoida.

Raamistikud, mida veebirakenduste serveritel saab pakkuda, hõlmavad erinevaid funktsioone, mis võimaldavad kommunikatsiooni taustsüsteemidega. Näiteks pakutakse abstraktseid funktsioone andmebaasides paikneva info lugemiseks ja manipuleerimiseks, mis nõuavad tegelikult ainult väheseid teadmisi reaalselt rakendatavast andmebaasist. Lisaks on raamistikesse juba kaasatud erinevad turvafunktsioonid (nt näiteks SQL-päringute jaoks on olemas Prepared Statesments, mis tõkestavad SQL-süst-turvaaukude ärakasutamise). Lisades klastrisse uusi veebirakenduste servereid, pole skaleerimiseks vaja rakendust modifitseerida.

Andmebaasiserver

Andmete püsivaks salvestamiseks kasutatakse veebilehtede puhul enamasti andmebaase. Neid käitatakse koos sinna juurde kuuluva andmebaasihaldussüsteemiga (Database Management System, DBMS).

Põhiliselt eristatakse järgmiseid andmebaaside liike:

- Hierarhilised andmebaasid kuvavad andmeobjekte suhtes vanemad-laps.
- Võrgupõhised andmebaasid võimaldavad andmeobjekte võrgu kaudu omavahel ühendada.
- Relatsioonilised andmebaasid kajastavad andmeobjekte tabelites. Tabelid võivad olla omavahel seostatud.
- suursooObjektandmebaasid paigutavad andmed andmebaasidesse objektidena, lähtudes seejuures objektipõhisest programmeerimisest. See tähendab, et objektandmebaasis paiknevatel objektidel on samad omadused mis programmeerimisobjektidel.

Andmebaasiservereid tuleb spetsiaalselt turvata (vt B 5.7 Andmebaasid). Andmebaasis paiknevale DBMS-ile tohib ligi pääseda ainult volitatud ressursside kaudu. Lisaks tuleb miinimumpõhimõtte alusel selgelt defineerida andmeobjekti tasandi ligipääs ja seda hooldada. Nagu igasugune tarkvara, võib ka DBMS sisaldada turvaaukusid, mille abil saavad ründajad luua ligipääsu konfidentsiaalsetele andmetele. Seepärast peab peale ligipääsu piiravate meetmete võtma ka meetmeid, mis kõrvaldaksid teadaolevad turvaaugud. Kuna ründajad võivad teatud juhtudel pääseda volitamata ligi andmebaasis paiknevale infole ja seda muuta, tuleb veebilehtede andmebaasisüsteemide jaoks võtta meetmeid, mis kaitseksid neid SQL-süsti tüüpi rünnete eest. Andmebaasi eriti konfidentsiaalne sisu (nt paroolid) tuleks volitamata ligipääsu eest kaitseks krüpteerida. See eeldab sobivat võtmehaldust ja ei lase avatekstina salvestatud andmeid lugeda.

Kataloogiteenus

Kataloogiteenusel põhineb kasutajaandmete ja arvutite keskne haldus. Need andmed paiknevad enamasti hierarhilises andmebaasis. Kataloogiteenusele pääseb üldjuhul ligi lihtsustatud kataloogisirvimise protokolli (Lightweight Directory Access Protocol, LDAP) kaudu. LDAP põhineb TCP/IP-l ning lubab kataloogiteenuse serveril paikneva info kohta teha päringuid ja infot muuta. Kuna kataloogiteenustesse salvestatakse tihti konfidentsiaalset infot, tuleb arvestada ka turvalisuse jaoks oluliste faktoritega (vt B 5.15 Üldine kataloogiteenus). Ühest küljest tuleks konfidentsiaalseid andmeid (näiteks paroole) kaitsta volitamata ligipääsu eest krüptograafiliste meetoditega. Teisest küljest on LDAP puhul, samamoodi nagu SQL-i kasutamisel, võimalik pöördusi manipuleerida. Seepärast tuleb võtta meetmeid, millega saaks ära hoida nn LDAP-injektsiooni tüüpi ründeid.

Reverse Proxy

Klientsüsteem kasutab proksisid tavaliselt veebilehtede avamiseks. Teise võimalusena saab proksisid kasutada serverites ligipääsu optimeerimiseks (puhverdamine) ehk filtreerimiseks. Kui proksi paikneb serveri poolel, räägitakse Reverse Proxyst (vt M 4.223 Proksiserverite integreerimine turvalüüsi koostisesse). Kõik veebiserverile suunatud pöördused võtab esmalt vastu proksi. Proksi otsustab konfigureeritava reeglistiku alusel, kas ta vastab päringule ise (puhverdamine), saadab päringu edasi mõnele klastris paiknevale veebiserverile või keeldub päringu täitmisest turvalisuse huvides.

Järgnevalt kirjeldatakse lühidalt Reverse Proxy tähtsamaid funktsioone:

- Puhverdamine - Reverse Proxyt on võimalik kasutada staatilise sisu, nt piltide või staatiliste HTML-tekstide vahesalvestamiseks. Kui selle info kohta esitatakse päring, on Reverse Proxyl võimalik sellele kohe vastata. Puhverdamisega saab lühendada vastamise aega ja vähendada veebiserveri koormust. Samas võib puhverdamine tekitada turbeprobleeme. Kui Reverse Proxy vahemällu salvestatakse info, mille salvestamiseks oleks tavaolukorras vaja veebiserveri heakskiitu, tuleb tagada, et asjakohane info edastataks ainult volitatud kasutajatele.
- Koormuse jaotamine - Kui Reverse Proxy suudab päringule vahemälus olevate andmete abil iseseisvalt vastata, puudub vajadus päringu edastamiseks veebiserverile. Sedasi on võimalik koormus veebiserverite vahel ära jagada. Kuna kõik päringud saadetakse esmalt Reverse Proxyle, saab proksi ka päringud mitme serveri vahel ära jagada. Nõnda on võimalik realiseerida Load-Balanceri funktsioon.
- Autentimine - Reverse Proxy võimaldab autentimise veebiserverist välja viia. Kui Reverse Proxy võtab enda kanda kasutaja autentimise korraga mitme veebiserveri suhtes, võimaldatakse sellega ühekordne autentimine (erialakirjanduses kasutatakse ka nimetust Single Sign On). Kui kasutaja on ennast üks kord Reverse Proxyl sisse loginud, saab ta kasutada mitut serverit, ilma et peaks ennast uuesti sisse logima. Lisaks võib päringu edastamine sõltuda kasutaja autentimisest Reverse Proxyl.
- Krüpteerimine - Otspunktšifreerimise kohaks (nt HTTPS-i kasutamisel TLS-i või SSL-i kaudu) võib olla Reverse Proxy. Vaid siis, kui andmeid dekrüpteeritakse juba Reverse Proxys, on seda võimalik kasutada päringute filtreerimiseks. Lisaks vähendab dekrüpteerimine Reverse Proxyl selle taga asuva veebiserveri töömahtu, sest veebiserver ei pea enam andmete dekrüpteerimiseks kasutama lisaressursse. Sellise variandi lisaeelis on kasutatava krüpteerimiskanali sõltumatus tegelikult kasutatavast veebiserverist. Sel moel on võimalik töödelda eri serveritest saadetud järjestikuseid päringuid, ilma et oleks tarvis muuta krüpteerimiskanalit. Kui andmeid dekrüpteeritakse ja filtreeritakse proksis, tuleb arvestada ka asjakohaste andmekaitseaspektidega. Näiteks on võimalik logida iga kliendi IP-aadress, sisselogimise aeg ja avatud veebilehed.
- Sideühenduste piiramist valikuga „Kõik ebausaldusväärsest võrgust saadetud päringud” on võimalik juhtida läbi Reverse Proxy. Proksis saab ebasoovitud päringute täitmisest loobuda – see lihtsustab turvalüüsi haldust ja vähendab väärkonfiguratsioonide tõenäosust. Veebiserveri IP-pinu eraldatakse ebausaldusväärsest võrgust.
- Salastamine - Kuna veebiserverid suhtlevad ainult Reverse Proxyga, mitte klientsüsteemiga, ei ole tarvis veebiserverite IP-aadresse avalikustada. Vajaliku info puudumise tõttu raskendatakse otsese ja tihtipeale soovimatu ühenduse loomist veebiserveriga. Reverse Proxyd hoolitsevad selle eest, et sisese võrgustruktuuri kaudu ei oleks võimalik infot üle kanda kliendile. Keskselt on võimalik koguda ka veateateid, mis võivad anda infot kasutatava veebiserveri rakenduse või kompromiteerimise kohta. Soovitatav on, et tegelikud veebiserverid seda informatsiooni ei edastaks, Reverse Proxyt on võimalik kasutada nn teise kaitseliinina.

M 4.360 Veebiserveri turvaline konfiguratsioon

Algatamise eest vastutavad: infoturbespetsialist, IT-juht
Rakendamise eest vastutab: administraator

Pärast seda, kui veebiserveriteenus on veebiserverile installitud, tuleb luua turvaline aluskonfiguratsioon. See puudutab näiteks lisamoodulite ühendamise võimalusi ja viisi, kuidas kataloogidele failisüsteemi piires või väljastpoolt failisüsteemi ligi pääseda, lisaks ka seadistusi, mis mõjutavad serveri jõudlust.

Seostamine privileegideta kasutajaga

Veebiserveri rakenduse käivitamisel saab privileegideta kasutaja tavaliselt samad pääsuõigused nagu rakenduse avanud kasutaja. Näiteks kui rakenduse käivitab administraator, kellel on IT-süsteemi failisüsteemi kogu info täielik lugemis- ja kirjutamisõigus, on ka veebiserveri protsessil selle info jaoks lugemis- ja kirjutamisõigus. Seetõttu tuleks veebiserveri protsess seostada privileegideta kasutajakontoga. IT-süsteemi failisüsteemisisesed pääsuõigused tuleb väljastada selliste piirangutega, et see kasutajakonto ja koos sellega ka veebiserveri protsess pääseksid ligi ainult vajalikule infole. Sellele vaatamata on veebiserveriteenust sageli tarvis käivitada privileegidega kasutajana (root). Neil juhtudel tuleks protsess võimaluse korral tagantjärele seostada privileegideta kasutajaga. Apacheveebiserveris saab näiteks kasutaja-direktiivi abil konfiguratsioonifailis kindlaks määrata kasutajatunnuse, mille alt käivitatakse serveri protsess privileegideta kasutajana.

Serveri kataloogid

Olenevalt sellest, millist veebiserveri rakendust kasutatakse, tuleb määrata failisüsteemi asukohad, millele veebiserveril on juurdepääsuõigus. Selle alla kuuluvad näiteks failisüsteemi kataloog infoga, mida veebiserver peab klientidele pakkuma (WWW-juurkataloog), ja logifailide asukoht. Kui WWW-juurkataloog on määratud, tuleb jälgida, et kataloogis hoitav info oleks ainult sellist laadi, mis on mõeldud kõigile potentsiaalsetele kasutajatele. Veebiserveri kasutajale määratud juurdepääsuala ei tohi olla liiga suur. Kasutajatel ei tohi näiteks olla ligipääsu Unixsüsteemi root -kataloogile ("/) ja Windows-süsteemi süsteemipartitsioonidele. Kataloog, milles asuvad kasutatavad failid, peab asetsema eraldi partitsioonil või kõvaketta lõigul, et võimaldada kergemat taastamist pärast kõvaketta riket. Veebiserveriteenusel peab üldjuhul olema juurdepääs ainult sellisele infole, mis asub WWW-juurkataloogis. Lugev, eriti aga kirjutav juurdepääs infole väljaspool WWWjuurkataloogi peab olema takistatud. Seega ei tohiks kasutada failisüsteemi viiteid (links) aladele, mis asuvad väljaspool WWW-juurkataloogi. Võimaluse korral tuleb veebiserveriteenus konfigureerida selliseks, et juurdepääs infole väljaspool WWW-juurkataloogi oleks tõkestatud. Apache-veebiserveri puhul saab seda teha näiteks lõiguga Limit.

Kirjutamisõigused

Käivitatud veebiserveriteenuse protsessil peavad olema ainult tööks vajalikud õigused. Veebiserveri tööprotsessi pääsuõigused lähtuvad tavaliselt veebiserveri protsessi käivitanud kasutaja pääsuõigustest. Veebiserveri tööprotsess ei vaja üldjuhul operatsioonisüsteemi suhtes kirjutamisõigust ja ei tohiks seega ka seda omada. Kui logifailid suunatakse eraldiseisvasse logiserverisse, ei ole IT-süsteemi failisüsteemis, kus veebiserver käivitati, lokaalseid kirjutamisõiguseid tarvis (erand: kui logiserveriga ei saada ühendust, tuleb info ajutiselt salvestada

vahemällu). Kõikidele failidele, mida pole enam tarvis muuta, nt staatilistele HTML-lehekülgedele, tuleb määrata kirjutamiskeeld. Kui veebiserveriteenus on suuteline looma automaatseid kataloogiloendeid, tuleks see funktsioon välja lülitada.

Protsesside piiramine

Veebiserveriteenust tuleb käitada piiratud protsessikeskkonnas, nt Unixsüsteemides käsuga chroot. chroot -keskkond on arvutisüsteemisisene eraldatud ala, nn sandbox , mis raskendab ründaja jaoks pärast veebiserveriteenuse kompromiteerimist kogu süsteemile ligipääsu (vt M 4.198z Rakenduse installeerimine chroot -puuri).

Serveriinfo

Standardsed veateated võivad sageli sisaldada liiga palju infot. Päringute kohta laekunud vastuste HTTP-päiseridadest või veateadetest võib ründaja sageli saada infot kasutatava serveritarkvara või muude üksikasjade kohta. Seda infot on võimalik kasutada ründemeetodite valimiseks ja see viib serveri kiirema kompromiteerimiseni. Seega peaksid need nn lisainfokanalid pakkuma võimalikult vähe infot. Selleks saab luua kohandatud veateated, mis küll teavitavad kasutajat esinenud veast, kuid ei reeda mingit olulist infot.

Autentimine

Veebiserveritele või veebilehtede üksikutele aladele juurdepääsupiirangute seadmiseks võib kasutada mitmeid võimalusi, millest osa on juurutatud juba veebiserveriteenusesse, teisi saab aga lisada täiendmoodulitega. Juurdepääsude määramisel piiratakse need sageli teatud IP-aadressivahemike või domeenidega (nt intranetis) või lastakse kasutajatel end enne teatud ressursside kasutamist autentida, nt kasutajanime ja parooliga (vt M 4.176 Autentimismeetodite valimine veebilehtede jaoks). Olenevalt veebiserverile juurdepääsu õigust omavast kasutajast (nt ainult oma töötajad, kliendid või kasutajad, kes peavad end küll registreerima, kuid on siiski tundmatud) ja kättesaadava info konfidentsiaalsusastmest peaksid juurdepääsuõigused olema piiratud miinimumini. Üldjuhul tohivad kasutajad ligi pääseda ainult vajalikule infole. Erandiks on avalikud veebiserverid, nt internetis asuvad avalikud veebiserverid, mille WWW-infole tohivad ligi pääseda kõik huvilised.

Andmeedastuse krüpteerimine

Tavaliselt edastatakse infot veebiserveri teenuse ja klientsüsteemi vahel HTTP kaudu. HTTP näol on tegemist avatekstiprotokolliga, mille puhul on ründajal võimalik näha ja lugeda kõiki edastatud andmeid, nt paroole ja veebi sisu. Seega tuleks kindlasti kaitsta veebiserveriteenuse ja klientsüsteemi vahel edastatava konfidentsiaalse info terviklust ja konfidentsiaalsust, nt kasutades selliseid krüpteerimisprotokolle nagu TLS (Transport Layer Security) või SSL (Secure Sockets Layer) (vt M 5.66z SSL-i/TLS-i kasutamine kliendis).

Haldamine

Veebiserveriteenuseid hallatakse sageli konfiguratsioonifailide või graafiliste kasutajaliidestega nii lokaalselt kui ka võrgu kaudu. Kui veebiserveriteenust osutavat IT-süsteemi hallatakse läbi võrguühenduse, peab võrguühendus ja veebiserveri haldamiseks kasutatava IT-süsteemi ning veebiserveri vaheline andmevahetus olema kaitstud. Selle juurde kuulub haldamiseks mõeldud juurdepääsude piirami-

ne, nt sellega, et rakendatakse paketifiltreid, mis keelavad kõik kaugadministreerimisteenuse pordinumbritele suunatud ühenduse loomise päringud, mis ei laeku administraatorite jaoks eeldefineeritud IT-süsteemidest (vt M 4.238 Lokaalse paketifiltri rakendamine). Selleks, et andmevahetust ei saaks pealt kuulata ega muuta, tuleb see krüpteerida, nt SSH-ga (vt M 5.64z Secure Shell (SSH)). Konfigureerimist kergendavate rakenduste või veebiliideste kasutamisel tuleb ka neid volitusteta isikute eest kaitsta.

Ebavajalike teenuste desaktiveerimine

Veebiserveriteenuse tüüpinstallimisel võidakse installida mitmeid võrguteenuseid, mida ei lähe tarvis ning mis just seetõttu võivadki muutuda turvaaukudeks. Liigseks võib osutuda näiteks veebiserveri konfigureerimiseks mõeldud veebiliides, kui veebiserveriteenust seadistatakse hoopis teiste mehhanismidega. Seega tuleb kontrollida, millised võrguteenused on koos veebiserveriteenusega IT-süsteemi installitud ja sisse lülitatud. Ebavajalikud võrguteenused tuleb desaktiveerida või isegi maha installida.

Ühenduse piiramine

Kuigi veebiserverid on tavaliselt IT-süsteemid, millele tohivad juurde pääseda paljud kasutajad, tuleks andmesidet siiski võimalikult piirata. Kui serveril käitatakse võrguteenuseid, mida tohivad kasutada ainult väljavalitud IT-süsteemid kindlates IP-aadressivahemikes, tuleks juurdepääsu teatud IP-aadressidele piirata paketifiltritega. Juurdepääs administreerimiseks mõeldud juurdepääsudele tuleb üldjuhul paketifiltritega piirata nõnda, et seda võimaldataks ainult administraatorite IT-süsteemidele. Sideühendust tuleb piirata ka andmebaaside või rakendusserverite kasutamisel. Lisainfot paketifiltrite kohta leiate meetmetest M 4.98 Side piiramine miinimumini paketifiltritega ja M 4.238 Lokaalse paketifiltri rakendamine . Kui veebiserverit peavad kasutama ainult organisatsioonisisesed töötajad, tuleks veebiserverit käitada sellises võrgusegmendis, millele pääseb ligi ainult kohtvõrgust. Kui veebiserveris asuvale infole peavad ligi pääsema ka välised/võõrad kasutajad, tuleks veebiserverit käitada demilitariseeritud tsoonis.

Logimine

Logiandmed peavad piisavas mahus kajastama pöördusi veebiserveriteenusele ja IT-süsteemile, millele veebiserveriteenus on installitud, et ründeid, ründekatseid ja turvarikkumisi õigel ajal tuvastada ja vajaduse korral jälitada. Seega tuleb otsustada, milline info vajab logimist, kuidas ja millal logiandmeid analüüsida ja millal neid kustutada. Veebiserveriteenus ja IT-süsteem tuleb vastavalt seadistada. Isikuandmeid tohib logida ainult seaduses lubatud määral. Lubatud määra väljaselgitamiseks tuleb pöörduda andmekaitsespetsialisti poole.

Näidisdokumentide kustutamine

Sageli installitakse veebiserveri installimisel ka näidisdokumendid. Nii saab näiteks administraator kohe pärast installimist brauseriga veebiserverisse pääseda, ilma et oleks ise veebisisu loonud. Kui kuvatakse olemasolevat näidis-indeksifaili, näeb administraator kohe, kas veebiserver on installitud õigesti. Sageli sisaldab näidis-indeksifail aga ka infot kasutatava veebiserveri kohta, nt versiooni numbrit. Tihti installitakse ka muid serveriprogramme (CGI-, Perl- või PHP-skripte). Kui administraator aktiveerib moodulid, mis võimaldavad käivitada skripte, saab ta va-

hetult kontrollida, kas moodul töötab probleemideta. Kõik näidisdokumendid ja -skriptid tuleb pärast installimist eemaldada.

Moodulitega täiendamine

Mõnede veebiserveriteenuste funktsioone saab täiendada nn moodulitega. Nende abil saab lisada funktsioone, mida veebiserveriteenuse arendajad ei ole oma tootele ette näinud. Täiendmoodulitega saab näiteks käivitada rakendusi otse veebiserveril ja sel viisil dünaamiliselt genereerida lehekülje sisu. Näideteks on PHP ja Perl, mille puhul ei saa rakendusi erinevalt aktiivsisust käivitada kasutaja klientsüsteemis (vt M 5.69 Aktiivsisu tõrje). Kui veebiserveriteenuse funktsioone täiendatakse moodulitega, peavad need vastama samadele nõuetele mis veebiserveriteenus. Lisaks tuleb moodulid valida miinimumpõhimõtte alusel. Moodulid, mille installib veebiserver näidetena ja mis on ebavajalikud, tuleb kustutada. Nii veebiserveriteenuseid kui ka mooduleid arendatakse üldjuhul pidevalt ja avaldatakse eraldi versioonidena. Mooduli versioon, mis mõne veebiserveriteenuse konkreetse versiooniga veatult töötas, võib veebiserveriteenuse uuema versiooni puhul tekitada probleeme. Ka mooduli uuem versioon võib veebiserveriteenusega töötada teisiti kui vanem. Seega peab peale kasutatava serveriteenuse versiooni katsetama ka konkreetse mooduli versiooni. Osade veebiserveriteenuste jaoks on olemas spetsiaalsed turvaraamistikud (nt Apache jaoks mod_security), mille abil saab juurutada erinevaid turvafunktsioone, nt selleks, et filtreerida andmesisestusi. Teatud turvafunktsioone saab osalt teoks teha ka teiste veebiserveriteenuste täiendustega. Näiteks saab mooduliga mod_rewrite kehtestada päringute edasisuunamisele reeglid, st päringuid saab filtreerida. Tuleb otsustada, kas ja milliseid turvaraamistikke kasutada.

Aktiivsisu

Veebilehtede interaktiivseid funktsioone saab realiseerida ka klientsüsteemis käivitatava aktiivsisuga. Samas saab neid funktsioone peaaegu alati pakkuda ka dünaamilise või lausa staatilise sisuna. Üldmõiste „aktiivsisu" alla on koondatud mitmesugused tehnoloogiad, mis erinevad üksteisest muu hulgas HTML-lehega integreerimise viisi poolest. Skriptikeelte nagu JavaScripti, JScripti või VBScripti kood lisatakse teksti kujul otse HTML-koodile või salvestatakse faili, mis käivitatakse HTML-koodis sisalduva käsuga. Lisaks on võimalik integreerida käivitatav kood HTML-leheküljega: selleks viidatakse HTML-koodis käivitatavale koodile ja kood käivitatakse selliste eelkompileeritud programmimoodulitega nagu Java-Applet või ActiveX-i komponendid (controls). Aktiivsisu jaoks on olemas JavaScriptil ja XML-il põhinev uus tehnoloogia nimega AJAX (Asynchronous JavaScript and XML). Sageli loetakse aktiivsisu hulka ka Flash, sest uuemates versioonides suudab see animatsioonide kuvamisest juba enamat ja seda ei saa seega vaadelda enam ainult pluginana. Aktiivsisuga kaasnevad mitmed turvaprobleemid, sest klientsüsteemil käivitatakse „võõras" kood. Brauserite tootjad ja pluginate pakkujad püüavad neid probleeme küll vähendada, nt piirates Java aplettide, ActiveX-i komponentide või muude pluginate õiguseid, kuid sellegipoolest on praegusel ajal aktiivsisuga seotud ohud kõige sagedasemad. Seetõttu soovitatakse veebilehtede loomisel aktiivsisust üldjuhul loobuda.

Operatsioonisüsteem

Veebiserveril pakutava info turvalisuse eeldusena peab operatsioonisüsteem, millele veebiserveriteenus installiti, olema turvaliselt konfigureeritud. Tavaliselt to-

hiks IT-süsteemi installida ainult sellised teenused ja rakendused, mis on tööks vajalikud. See tähendab, et mitmed ebavajalikud rakendused (nt kompilaatorid või redaktorid) tuleb eemaldada. Väljapoole nähtavad tohivad olla ainult sellised teenused, mis on tööks ilmtingimata hädavajalikud (vt M 5.95 E-kaubanduse turve Internet-PC kasutamisel). Operatsioonisüsteemi ja selle teenuste info varjamiseks saab kasutada banner-spoofing'ut. See tähendab, et serveril töötavad teenused ei edasta oma õiget programminime ega versiooninumbrit, vaid asendavad selle valeinfoga. Seeläbi on ründajal raskem näha, mis programme süsteem tegelikult kasutab. Ka standardsed kasutajakontod tuleb eemaldada või ümber nimetada. Selle näiteks on Windowsi operatsioonisüsteemides ohtralt leiduv külaliskonto. Privileegidega kasutajakontod, nt „Administraator" või „Root", tuleb desaktiveerida ja nende asemel luua vajalike administratiivõigustega kasutaja.

Kontrollküsimused:

- Kas veebiserveril on loodud turvaline aluskonfiguratsioon?
- Kas veebiserver pääseb ligi ainult WWW-juurkataloogis asuvale infole?
- Kas veebiserveril on salvestatud infole ainult lugemisõigus?
- Kas veebiserveri haldamise juurdepääsud on kaitstud selliselt, et neile pääsevad ligi ainult volitatud administraatorid?
- Kas on kontrollitud, millised võrguteenused, rakendused ja veebiserverite moodulid on veebiserverile installitud ja seal aktiveeritud ning kas kõik ebavajalikud teenused, rakendused ja moodulid on desaktiveeritud või maha installitud?
- Kas juurdepääsud on kasutajate volitusi ja info turbevajadust arvesse võttes piiratud miinimumini?
- Kas veebiserveri ja klientsüsteemi vahel edastatavate andmete terviklus ja konfidentsiaalsus on kaitstud?

M 4.362 Bluetoothi turvaline konfigureerimine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator, kasutaja

Tootjafirmade algsed seadmekonfiguratsioonid on alati soovitatav üle kontrollida, kuna need on sageli ebaturvalised ning võimalusel tuleks neid järgnevalt muuta:

- tehasest väljudes on Bluetooth-seadmetes sageli suur osa teenuseid juba sisse lülitatud, et tagada võimalikult suured kommunikatsioonivõimalused kõikvõimalike teiste seadmetega. Kõik ebavajalikud teenused tuleb alati desaktiveerida. Harva vajaminevaid teenuseid tuleks sisse lülitada ainult reaalsel vajadusel ning pärast kasutamist tuleb need taas välja lülitada.
- Seadmete Bluetooth-liidesed tuleb ajaks, mil neid ei kasutata, välja lülitada.
- Bluetooth-seadmete konfigureerimisel tuleb arvestada, et need ei oleks liiga „avatud“. Võimalusel tuleks tööle lülitada režiimid non-discoverable , nonconnectable ja non-pairable või non-bondable.
- Bluetooth'i leviala ei tohiks väljuda selle jaoks ette nähtud kasutusvaldkonna piiridest. Selle tagamiseks tuleb Bluetooth-seadmete saatmisvõimsus reguleerida nii madalaks kui võimalik ja nii kõrgeks kui funktsiooni toimimiseks on vajalik. Näiteks kui on tegemist sülearvutiga, mille külge on ühendatud vaid mõned meetrid eemal asuv mobiiltelefon, tuleks sülearvutiga ühendada ainult selliseid seadmeid, mis kuuluvad Bluetoothi klassi nr 3.
- Kui võimalik, tuleks eelseadistatud PIN-koodid viivitamata ära muuta.
- Valitud PIN-koodid peaksid olema võimalikult pikad ja mitteaimatavad.
- Rakendatavad autentimis- ja krüpteerimismeetodid tuleb valida vastavalt turbevajadustele.
- Tavapäraste turvanõuete täitmiseks, eriti krüpteerimisnõuete täitmiseks, piisab Bluetooth'i poolt pakutavatest turbemeetmetest. Eelnev väide kehtib hetkel teadaolevate turvaaukude kohta. Kõrgemate turbenõuete täitmiseks tuleb rakendada täiendavaid meetmeid, mis väljuvad Bluetooth'i pakutavate võimaluste raamidest.
- Tugeva krüpteeringu tagamiseks peab võtmepikkus olema vähemalt 64 bit ning krüpteerimisprotseduurina tuleks aktsepteerida vaid punktist-punktikrüpteerimist. Võti peab olema maksimaalse võimaliku pikkusega. Kuna krüpteerimiseks kasutatava võtme pikkust ei saa kasutaja ise määrata, tuleks võimalusel kasutada ainult selliseid seadmeid, mis suudaksid nimetatud nõudeid ka reaalselt täita.

Lisaks on soovitav Bluetooth-seadmed asjakohaste abivahenditega regulaarselt kontrollida, et avastada võimalikke peidetud teenuseid või avatud porte.

Seadmetootjate turvapaiku ja püsivara uusimaid versioone tuleb eelnevalt kindlasti testida ning neid tuleks paigaldada juhul, kui tekib vajadus vastava turbeastme järele. Bluetooth-lisaseadmete turvalise käitamise tagamiseks peavad ka kõik sellega ühendatud seadmed olema turvaliselt konfigureeritud. Klientsüsteemidele sobivad IT-turvasuunised leiate moodulite kihist nr 3.

Kontrollküsimused:

- Kas kõik Bluetooth-lisaseadmed on piisavalt turvalise konfiguratsiooniga?

- Kas neid eelseadistatud PIN-koode, mida saab muuta, on muudetud?

M 4.363 Bluetooth-seadmete turvaline käitamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator, kasutaja

Bluetooth-seadmeid tuleb sobival moel turvata. Järgnevalt kirjeldatakse, kuidas vastavaid meetmeid rakendada.

Statsionaarsed seadmed

Statsionaarsete seadmete korral, kus Bluetooth-funktsiooni rakendatakse kaabliühenduste asendamiseks, nt selleks, et ühendada ühtesid ja samu lisaseadmeid, tuleks kasutada autentimist. Selleks võiks eelistada lahendusi, mis kasutavad poolpüsivaid ühendusevõtmeid. Kõikidel juhtudel tuleks sisse lülitada krüpteerimine.

Mobiilsed seadmed

Mobiilseid Bluetooth-seadmeid, mis suhtlevad võõraste seadmetega (st seadmetega, mille turbeaste ei ole teada), tuleb kaitsta tavapärasest hoolikamalt:

- kahe seadme paaristamisfunktsiooni tuleks kasutada alati ainult pealtkuulamiskindlates keskkondades. Pealtkuulamiskindlaks võib keskkonda lugeda siis, kui puudub võimlaus Bluetooth-funktsiooniga märkamatult väljast poolt sisse tungida. Enda kasutatavate Bluetooth-seadmete leviala ei ole siinkohal ainumäärav.
- Eelistada võiks lahendusi, mis kasutavad poolpüsivaid ühendusevõtmeid.
- Paaristamisfunktsiooni tuleks rakendada vaid usaldusväärsete seadmete suhtes.

Olukorras, kus mobiilne (või ka statsionaarne) seade läheb kaduma või varastatakse, tuleb kõik nendega seotud ühendusevõtmed alles jäänud seadmetest kustutada. Selleks tuleb alles jäänud seadmetes üldjuhul ära kustutada vastav sissekanne Bluetooth-seadmete loetelus.

Secure Simple Pairing funktsiooni kasutamine

Kui mõlemad paarsitatavad seadmed vastavad vähemalt Bluetooth'i spetsifikatsioonile 2.1 + EDR, tuleks kasutada funktsiooni Secure Simple Pairing ning turvarežiimi nr 4 koos atribuudiga authenticated (vt M 3.79w Sissejuhatus Bluetooth'i põhimõistetesse ja tööpõhimõtetesse). Teenuseid, mis seda funktsiooni ei toeta, ei tohiks kasutada.

Juhiseid PIN-koodide kohta ilma SSP-ta Bluetooth'i korral

PIN-koodid ei tohiks olla suvalised numbri- ja tähekombinatsioonide jadad, st kindlasti tuleks vältida triviaalseid PIN-koode nagu „0000“ või „1234“. Selleks, et kahe Bluetooth-seadme paaristamisfunktsioon saaks toimuda piisavalt turvaliselt, peab PIN-kood tingimata olema piisava pikkusega. PIN-koodid peaksid olema vähemalt kuuekohalised. PIN-kood tuleb tavatingimustes sisestada vaid üks kord ehk siis kui kaks seadet omavahel esmakordselt ühendust loovad (poolpüsiv ühendusevõti). Juhul kui kahe juba paaristatud seadme korral peaks kasutajalt nõutama, et ta uuesti PIN-koodi sisestaks, tuleks võimalusel seda edasi lükata, kuni jõutakse pealtkuulamiskindlasse keskkonda. Soovitatav on läbi viia asjakohane kasutajakoolitus või juhendamine.

Täiendavad turbemeetmed

Ajaks, mil Bluetooth'i ei kasutata, tuleks seadmete Bluetooth-liidesed desaktiveerida. Selle nõude täitmist tuleks pisteliselt kontrollida. Lisaks tuleks Bluetooth-seadmetesse installeerida täiendavaid lokaalseid turvameetmeid või need tööle lülitada, kui tehnilised olud seda võimaldavad. Siia alla kuuluvad:

- juurdepääsukaitse (nt vargusevastane kaitse),
- kasutaja autentimine,
- kahjurvara vastane kaitse (nt viirusetõrje),
- Personal Firewall ,
- piiratud juurdepääs operatsioonisüsteemi tasandi failidele ja ressurssidele ja lõppseadme krüpteerimine.

Regulaarselt tuleb kontrollida, kas kõik defineeritud turvaseadistused on jätkuvalt ajakohased ning kas nendest on kasu.

Täiendavat asjakohast infot leiate lõppseadmete turvet käsitlevatest moodulitest. Kahtluste korral peaksid kasutajad rakendama meetme B 3.208 Interneti-PC ja sellega seonduvate meetmete asjakohaseid põhimõtteid.

Kontrollküsimused:

- Kas selleks ajaks, mil Bluetooth-andmesidet ei toimu, lülitatakse kõikide seadmete Bluetooth-liidesed välja?
- Kas ühenduse loomiseks teiste seadmetega kasutatakse Secure Simple Pairing funktsiooni?

M 4.364 Bluetooth-seadmete kasutusest kõrvaldamise reeglid

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator

Olukorras, kus Bluetooth-seadmed soovitakse kasutusest kõrvaldada, tuleb kogu nende sisse salvestud tundlik info kustutada. Selle saavutamiseks tuleb esmajoones eemaldada või kehtetuks kuulutada autentimisalane info, mis on salvestatud kas turbealasesse infrastruktuuri või teistesse seadmetesse ning mis võimaldab juurdepääsu Bluetooth-võrkudele ja teistele ressurssidele. See tähendab nt krüptograafiliste võtmete turvalist kustutamist ning digitaalallkirjade sertifikaatide kasutamise sulgemist.

Bluetooth-seadmete hulka kuuluvad väga paljud erinevad seadmed. Siia alla kuuluvad muuhulgas:

- sülearvutid,
- PDA-d, nutitelefonid jms Bluetoothi toega seadmed,
- Bluetooth-liidesega telefonid, printerid ja kaamerad,
- Bluetoothi toega lisaseadmed nagu peakomplektid, hiired, klaviatuurid jne.

Bluetoothi funktsioon on sellistes lõppseadmetes reeglina vaid üks erinevatest funktsioonidest. Seetõttu tuleb niisuguste lõppseadmete kasutusest kõrvaldamisel arvestada, et ka neis seadmetes võib olla nt järgmisi, turbe seisukohast kriitilise tähtsusega Bluetooth-andmeid, mis tuleb kas kustutada, ümber paigutada või arhiveerida:

- andmed lõppseadme kasutaja kohta,
- sertifikaadid ja nende privaatvõtmed (kasutajate või seadmete omad),
- andmed ühendatud lõppseadmete kohta (paaristamise andmed),
- autentimisprotseduuride võtmematerjal, nt Bluetooth-lõppseadmete Pairing-funktsiooni võti.

Sõltuvalt seadmest ja selle mälu liigist tuleb kasutada erinevaid meetodeid, kuidas turbe seisukohast olulisi andmeid hävitada, kustutada või edasi kasutada. Sertifikaatide korral tuleb nende kasutamise lõpetamiseks nt teha vastav sissekanne sertifikaaditühistusnimistusse (*Certificate Revocation List*, CRL). Olukorras, kus Bluetooth-seade varastatakse, tuleb arvestada vähemalt kogu eelnevalt loetletud infoga ning tuleb hoolitseda selle eest, et varastatud seadmetel ei oleks enam juurdepääsu ei olemasolevatele Bluetooth-seadmetele ega ka võrgustruktuuridele. Kõige parem viis, kuidas seda saavutada, on varastatud lõppseadmete Pairing-andmete kustutamine olemasolevatest lõppseadmetest.

Täiendavad kontrollküsimused:

- Kas Bluetoothi toega lõppseadmete kasutusest kõrvaldamisel jälgitakse, et turbe seisukohast kriitilise tähtsusega Bluetooth-andmed saaks neist kustutatud?
- Kas Bluetooth-seadmetes leiduvate, turbe seisukohast oluliste andmete hävitamiseks, kustutamiseks ja edasikasutamiseks on välja töötatud asjakohased protseduurid?

M 4.365z Terminaliserveri kasutamine graafilise tulemüürina

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator

Põhimõtteliselt põhjustavad ligipääsuvõimalused ebaturvalisse võrku ja ITinfrastruktuuri põhiväärtuste kaitse eesmärkidevahelise konflikti. Esiteks tuleb näiteks kasutada aktiivsisudega veebiteenuseid. Teiseks toimub ligipääs rakenduste kaudu, mis peavad saama ligipääsu ebaturvalisele võrgule. Klassikalistes klient-server võrkudes teostatakse need rakendused pordi-, pakett- või rakendusfiltri taga kliendil ja kasutaja kontekstis. Klienttarkvara kompromiteerimine ohustab nii kliendi kui kogu sisevõrgu turvalisust. Terminaliserverid pakkuvad rakenduste eraldamise kaudu eraldiseisval IT-süsteemil veel lisaturvalisust, sest ligipääs ebaturvalisele võrgule toimub terminaliserveri kaudu. Terminaliserverit, mis kliendi asemel ebaturvalisse võrku siseneb, nimetatakse graafiliseks tulemüüriks.

Viirused, ussid või muu kahjurvara ei ole graafilise tulemüüri järjepideval planeerimisel ja realiseerimisel mitte ühelgi ajahetkel võimalik kasutaja kliendil realiseerida ega sisend ja väljundandmetega terminaliserveri ja terminali vahel üle kanda.

Graafilise tulemüüri kontseptsiooni juures mängivad põhilist rolli kaks teatud juhtudel üksteist täiendavat eesmärgipüstitust:

- Siseste IT-süsteemide kaitse ebaturvalise välise võrgu eest.
- Takistamine, et tehniliste puuduste, kahjurvara või sabotaaži kaudu ei satuks konfidentsiaalseid andmeid välisvõrku. Selleks vajalik sise- ja välisvõrgu vaheline informatsioonivahetuse keeld, näiteks andmeedastuse või lõikelaua kaudu, vähendab aga praktilist kasu märgatavalt.

Joonis: Graafiline tulemüür eraldatud tsoonis (Unsicheres netz – ebausaldusväärne võrk, DMZ - demilitariseeritud tsoon, Grafische Firewall – graafiline tulemüür, dateiserver – failiserver, druckserver - prindiserver)

Mõlemal juhul on meetmete toimimiseks oluline, et side välisvõrguga toimuks ainult graafilise tulemüüri kaudu. Et kompromiteerimise korral sisevõrku mitte ohustada, tuleks terminaliserver paigutada kaitset vajavatest aladest eraldatud tsooni (DMZ-i, turvalüüsi demilitariseeritud tsoon). Turvalisele võrgule tehtavate rünnakute vähendamiseks on kahe võrguosa vahelisel marsruudil mõttekas lubada ainult transpordiprotokolli ja terminaliserveri teenuste pordid. Järgnev tabel sisaldab mõningate terminaliserveri teenuste standardseadistusi:

Teenus	Protokoll	serveri port	serveri tsoon
Windows Update	Kaugarvuti protokoll (RDP)	3389	demillitartiseeritud tsoon (DMZ)
Citrix Presentation Server	ICA	1494	demillitartiseeritud tsoon (DMZ)
X Windows	X11	6000	Kohtvõrk (LAN)

Teenus	Protokoll	serveri port	serveri tsoon
X Windows SSH-ga	X11+SSH	22	demillitartiseeritud tsoon (DMZ)
VNC	VNC	5900	demillitartiseeritud tsoon (DMZ)

Tabel: Erinevate terminaliserverlahenduste logi ja pordinumbrid

Teatud juhtudel on vajalik avada lisaporte, et tagada näiteks ligipääs failiserverile või printimisteenusele LAN-is. Selle vältimiseks võib mõningate lahenduste korral paljude teenuste andmeside edastada otse terminaliserveri logi andmeside sees. Protokollid, mis võimaldavad seda suvandit virtuaalsete kanalite kaudu, on teiste hulgas Windows terminaliserveri RDP protokoll või ICA Citrix Metaframe, Presentation Server või XenApp all. Peale selle on näiteks X Windowsi jaoks kasutada tunneldamist SSH abil, mis algselt ei ole selleks ise võimeline. Hiljem tuleb X Windowsi kasutamisel arvestada X11 protokolli eripäradega. Kui levinud meetodite korral saadab terminal oma väljundi terminaliserverilt, saadab X-Window rakendus ehk siinkohal graafiline tulemüür oma ekraaniväljundi X-serverile, mis siis teostatakse kasutaja kliendil. Selle tulemusena tuleb marsruuteri port 6000 DMZ-ist LAN-i juhtida. Igale järgnevale kliendile, kes terminaliserveri kaudu LANis suhtleb, tuleb avada uus port, mille pordinumber on 6000-st suurem. Selles stsenaariumis viib see suure hulga sisevõrgu ligipääsudeni ja võimalusel tuleks seda vältida. Selle asemel on soovitatav luua ühendus SSH tunneli või virtuaalse privaatvõrgu (VPN) kaudu.

Graafilise tulemüüri erilise ohustatuse tõttu on ilmtingimata vajalik viirusetõrjeprogrammi kasutamine M 4.3 Viirusetõrjeprogrammide kasutamine . Meetmed M 4.368 Terminaliserveri keskkonna regulaarne audit ja M 5.163 Piirav õiguste jaotus terminaliserveritel hoolitsevad selle eest, et kasutatud oleks minimaalselt vajalike õiguste põhimõtet.

Kontrollküsimused:

- Kas kommunikatsioon ebaturvalise võrguga toimub ainult graafilise tulemüüri kaudu?
- Kas graafilise tulemüürina toimiv terminaliserver on paigutatud eraldi DMZ-i

M 4.366 Liikuvate kasutajaprofiilide turvaline konfiguratsioon terminaliserveri keskkonnas

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator

Et anda rakendus suurema hulga kasutajate käsutusse, kasutatakse ühes süsteemis mitut terminaliserverit. Seda nimetatakse ka terminaliserveri farmiks. Siin kirjeldatud stsenaariumi korral tekivad kasutajaprofiilidele mõningad spetsiifilised infoturbenõuded. Kasutajaprofiilis salvestatakse isiklikud kasutajaseaded, lõppseadmekonfiguratsioon (näiteks printeri jaoks) ja vajadusel ka rakendustele ise loodud failid. Terminaliserveri süsteemides ei ole kasutajate kaudu märgata, millise terminaliserveriga nad seanssi üles ehitavad. Vastava terminaliserverlahenduse haldusteenus reguleerib seda automaatselt, arvestades enamasti farmis paiknevate üksikute serverite koormust.

Kui kasutaja ennast sisse logib, laetakse sellelt serverilt tema isiklik profiil. Kui ei kasutatud vastavaid ettevaatusabinõusid on selleks lokaalselt serveril salvestatud profiil. Kui kasutaja ennast välja ja siis uuesti sisse logib, luuakse suure tõenäosusega ühendus mõne teise terminaliserveriga ning seeläbi ka uus lokaalne kasutajaprofiil. Esimesel terminaliserveril salvestatud seadistused ja failid on kasutajale jälle kättesaadavad alles siis, kui ta juhuslikult ennast jälle selle serveriga ühendab. Kui soovitakse, et kasutajate profiilisisesed muudatused säiliksid, tuleb terminaliserverite farmi kasutamisel kasutada failide keskseks salvestamiseks failiserverit. Seda profiiliandmete salvestamise meetodit nimetatakse ka „liikuvaks profiiliks“.

Tuleb tähele panna, et rakendusstsenaariumites, mille korral pääsetakse üksikutele rakendustele otse ligi ega kasutata täisväärtuslikku kasutajaliidest (*Desktop*), võib see olla mittevajalik või isegi soovimatu. Windows'i serverite kasutamisel on liikuva kasutajaprofiili (*Windowsi all ka roaming profile*) valimisel mõningad puudused. Kasutajal on küll arvukalt võimalusi oma kasutajaseanssi välimust ja käitumise muutmiseks, aga ta võib enda vea tõttu kogu seansiprofiili ka väga kergesti kasutuskõlbmatuks muuta. Peale selle kasvab niimoodi konfigureeritud profiili suurus. Iga sisselogimisega läheb kaua aega, enne kui failiserver üles laetakse ning samuti suurendab see võrgu- ja serverikoormust. Soovitatav on kasutada nn *mandatory profiles* i, mis kiirendab terminaliserveri tööd ja takistab, et kasutaja ennast ise kasutamisest välja lukustab. Selle profiilitüübi võib samuti paigutada eemal asuvale serverile, loodud failid ja seadete muudatused salvestatakse aga ainult seniks, kuni seanss kestab. Vastavate skriptide loomisega on võimalik enne seanssi lõpliku sulgemist profiili kindlad osad failiserveril salvestada (näiteks loodud dokumendid).

Takistamaks profiili suuruse kasvu üle vastuvõetava määra, peaksid administraatorid kindlaks määrama profiili suuruse piiri.

Täiendavad kontrollküsimused:

- Kas määrati ja realiseeriti meetod, terminaliserveri seanssi ajal kasutajate poolt loodud failide sünkroonne kättesaadavaks tegemine kõigil terminaliserveri farmi terminaliserveritel?
- Kas terminaliserveril määrati kindlaks kasutajaprofiili poolt kasutatava mälu ülempiir?

- Kui jah, kas see ülemmäär on dokumenteeritud ja kas kasutajaid on teavitatud?

M 4.367 Klientrakenduste turvaline kasutamine terminaliserveril

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator

Terminaliserveri teenuseid kasutatakse tihti klientsüsteemi kaudu, millel on oma operatsioonisüsteem (Fat Client). Sellises keskkonnas on kasutajal tihtipeale potentsiaalseid võimalusi klienttarkvara või selle konfiguratsiooni muutmiseks. Ta võib vähendada näiteks oma enda ühenduse turbeastet või avaldada volitamata kolmandatele isikutele detaile informatsioonisüsteemi sisesest ülesehitusest. Selle takistamiseks tuleks kõik ühendusparameetrid, nagu krüpteerimissügavus ja meetod, administraatorite poolt serveri poolel ette anda. Sedasi tuleks juhtida ka informatsioonikanaleid nagu lokaalsed ajamid, printerid, liidesed või lõikelaud (*Clipboard*). Mitte alati ei ole see kasutatava terminaliserveri lahenduse korral keskne, kasutajast lähtuv ning kõigi rakenduste juures saavutatav ning lisaks võivad ka kasutajate vajadused varieeruda. Tavalise kaitsevajadusega terminaliserveri keskkondades tuleb kasutajadirektiivides määrata, et kasutaja ei tohi mitte mingil juhul konfiguratsioonifaile, näiteks .ICA või .RDP faile, saata volitamata isikutele. Peale selle ei tohi muuta ühtegi eelnevat seadistust ega luua ligipääse kõrvalekalduvatele serveriaadressidele (vt M 2.464 Infoturbesuuniste loomine terminaliserveri kasutamiseks).

Kõrge või väga kõrge turbevajadusega informatsioonisüsteemi korral sellistest organisatoorsetest määratlustest ei piisa. Võimaliku alternatiivina saaks vaadelda mitte konfigureeritavate klientprogrammide kasutamist, nagu näiteks *Citrix Program Neighborhood* i nn *Gray Version.* Seejuures on eelduseks, et klient, millele terminaltarkvara paigaldatakse, on täielikult administraatorite kontrolli all. Lisaks tuleb efektiivselt keelustada kirjutusligipääs klienttarkvara failidele. Selle meetodi jaoks ei ole sobivad arendussüsteemid, mille juures on näiteks tarkvaraanalüüsitööriistadega (*Debugger*) või võrgumonitoridega (*Sniffer*) võimalik sideülesehituse monitooring või manipuleerimine. Seeläbi on võimalik kergesti murda automaatset autentimist (*Pass Through Authentication*). Ülalnimetatud turbeprobleeme on võimalik vältida, kui terminaltarkvara lokaalne installatsioon ja selle konfiguratsioon kasutajate arvutitele saadetakse. Teostatavaks muutub see portaal lahenduste kasutamisel, näiteks:

- Microsoft Terminaliserver Web-Access
- Citrix Access Gateway
- NX-Builder X-Window süsteemidele

Kasutaja autentimiseks portaalilahenduse suhtes ebaturvalise võrgu kaudu on soovitatav kasutada kahe-faktorilist autentimist. Ka terminaliserveri klienttarkvara tarnimisel veebiserveri kaudu ei ole piiravad määratlused kliendi konfigureerimise suhtes tavaliselt veel standard. Need tuleb enne terminaliserveri keskkonna kasutusele võttu administratiivselt kindlaks määrata. Lisaks tuleb portaali korral arvestada meetmetega moodulis B 5.4 Veebiserver .

Täiendavad kontrollküsimused:

- Kas terminaliserveril määrati administratiivsel tasandil ühendusparameetrid ning krüpteerimissügavus ja meetod?
- Kas terminaliserveri kasutajaid on teavitatud nende kohustusest kaitsta konfidentsiaalseid konfiguratsiooniandmeid?
- Kas kõrge või väga kõrge turbevajadusega süsteemide korral kasutatakse terminaliserveri kasutamiseks spetsiaalset klienttarkvara või portaallahendusi?

M 4.368 Terminaliserveri keskkonna regulaarne audit

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: Administraator, kasutaja

Kõigi terminaliserveri infrastruktuuri komponentide juures tuleb regulaarselt kontrollida, kas kõik kindlaks määratud turbemeetmed on realiseeritud ja korrektselt konfigureeritud. Terminaliserveri enda kõrval kuuluvad siia hulka haldusteenused nagu istungiandmebaasid ja litsentsiserverid, aga ka turbe infrastruktuuri elemendid. Regulaarselt tuleks kontrollida kahe võrgu vahelistes ühenduspunktides paiknevaid autentimisservereid ja turvalüüse, millega terminaliserveri keskkond pidevalt ühendatud on. See kehtib ka marsruuteritele, tulemööridele ja VLAN-i loovatele kommutaatoritele (*switch*). Seejuures tuleb arvestada ka veebiportaalidega (vt B 5.4 Veebiserver), mis vahelülidena võivad võimaldada rakendustele ligipääsu.

Üksikute komponentide logiandmed võivad seejuures anda olulist informatsiooni kriitiliste juhtumite kohta. Protokollimisel tekib tavaliselt palju sissekandeid, nii et neid on mõttekas analüüsida ainult tööriista abiga. Võimalike turbejuhtumite otsingul tuleks analüüsida nii kasutajate sisse- ja väljalogimisaegu kui ka kasutusaega. Lisaks tuleb jälgida, et ei oleks autoriseerimata seansside replikeerimist. Tähtis aspekt terminaliserveri keskkonna kättesaadavuse osas on ressursside nagu mälu, protsessor ja kõvakettaruumi koormus aga ka võrgus kasutatav ribalaius või aktiivsete seansside arv. Et siinjuures arenguid õigesti hinnata, tuleb eelnevalt läbi viia vastavad analüüsid (vt M 2.465 Terminaliserveri vajalike ressursside analüüs ja M 5.162 Ribalaiuse planeerimine terminaliserverite kasutamisel). Ainult nii on võimalik teha järeldusi probleemsete kohtade kohta individuaalses terminaliserveri keskkonnas. Peale informatsiooni, mis saadakse logiandmetest, tuleb kindlasti kontrollida terminaliserveri aluskonfiguratsiooni. Siin tuleks vähemalt pisteliselt kontrollida terminaliserveri süsteeme, nende failisüsteeme ja allavooluteenuseid tugevdavaid meetmeid.

Erilist tähelepanu tuleks pöörata unustatud ajutistele failidele, mis automaatsel installeerimisel tekkida võivad, sest nendes paikneb tihti kriitiline informatsioon, nagu näiteks krüpteerimata sisselogimisandmed. Lisaks tuleb kontrollida ka klientsüsteeme, mille kaudu terminaliserveritele ligi pääsetakse. Suure hulga korral peaks seda tegema vähemalt pisteliselt. Esmalt tuleb kontrollida, kas lokaalselt installeeritud klienttarkvara konfiguratsioon sisaldab autoriseerimata muudatusi. Kui terminaliserveri käitamisel kasutatakse spetsiaalseid printeri draivereid, tuleks ka need uurimisse lisada. Lisaks tuleb klientide juures, millel on iseseisev operatsioonisüsteem (*Fat Clients*) jälgida ka operatsioonisüsteemi versiooni ja klienttarkvara ning viirusetõrjeprogrammi aktuaalsust ja terviklust. Lisaks eelnevalt nimetatud tehnilistele turvalisuse analüüsivahenditele võib turbeprobleeme välja selgitada ka kasutajaid küsitledes. Kui avastatakse ebakõla või nõrgad kohad, tuleb need dokumenteerida ja kirja panna, kuidas nendega tegelda.

Terminaliserveri komponentide auditi kõrval tuleks tsüklilisel läbi viia ka terminaliserveri infoturbesuuniste revisjon. Siinkohal tuleks anda hinnang, kas terminaliserveri keskkonna turbeks kasutusele võetud meetmed vastava veel tehnilistele standarditele ja kas määratud turbeaste on ikka veel kehtiv. Lisaks tuleks ikka ja jälle järele pärida, kas kõik kasutajad terminaliserveri keskkonna jaoks vajalike turbemeetmeid teavad ja neid ka realiseerivad. Lisaks tuleb kindlaks määrata, kes protokolle ja auditi andmeid analüüsib. Siinjuures tuleb eristada põhjustajat ja analüüsijat (näiteks administraator ja audiitor). Kõigi kogutud andmete suhtes kehtib

andmekaitseseadus.

Täiendavad kontrollküsimused:

- Kas terminaliserveritel viiakse läbi regulaarsed turbeauditid?
- Kas avastatud ebakorrapärasused dokumenteeritakse ja jälitatakse?

M 4.369 Telefoni automaatvastaja turvaline kasutamine

Algatamise eest vastutavad: kodukeskjaama eest vastutav töötaja, infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator

Automaatvastajaid võib lisaks telefonile ühendada majasisesesse telefonivõrku. Nende tööeesmärgiks on sissetulevate kõnede või teadete salvestamine hetkel, kui soovitud isik ei ole telefoni teel kättesaadav. Üheks võimaluseks on salvestada automaatvastajale ainult äraolekuteade ning mitte salvestada helistaja teadet helistatavale. Automaatvastajad võivad olla kas välised seadmed (*stand-alone*) või olla lisaks telefonile ühendatud majasisesesse telefonivõrku, kuid nad võivad telefonis (integreeritud automaatvastaja) või kodukeskjaamas juba ka olemas olla. Kui kasutatakse VoIP-i võib paljude VoIP-seadmetega saata kõneteate vastuvõtjale kõnepostiga (*voice mail*). Olenevalt tehnilisest teostusest võib automaatvastajad jagada kahte klassi: analoogse ja digitaalse salvestamisvõimalusega. Analoogseadmete puhul salvestatakse teated audiokassettidele (sageli mini- või mikrokassettidele). Praegu selliseid seadmeid enam ei toodeta. Digitaalsete automaatvastajate puhul, mis on nüüd enamasti juba otse telefoni või telefoniseadmesse integreeritud, salvestatakse teated seadme salvestusmoodulile või mass-salvestile, nagu nt kõvaketas. Vanemat tüüpi salvestusmooduliga digitaalsetelt automaatvastajatelt võib sinna salvestatud info pärast voolukatkestust kaduma minna. Seepärast tuleks selliste seadmete (puhver)patareisid regulaarselt vahetada. Põhimõtteliselt ei tohiks kaitsmist vajavat infot automaatvastajasse jätta. Oluline on jälgida, et automaatvastajasse ei jäetaks teksti, mida helistaja saaks ära kasutada inimestega manipuleerimiseks (vt G 5.42 Inimestega manipuleerimine (Social Engineering)). Eriti ei tohi jätta infot selle kohta, kus viibib parajasti inimene, kellele helistati, või kui kaua ta ära on . Automaatvastajasse salvestatav tekst ei tohiks sisaldada salajast teavet.

Integreeritud automaatvastajaga telefonidel on lisaks sissetulnud teadete salvestamise ja nende kuulamisele võimalusele veel teisigi rakendusi nagu kaugjuurdepääs, kõnede ümbersuunamine, ruumi valve või võrku ühendatud elektriliste seadmete kaugjuhtimine. Mõnel telefonil saab neid funktsioone kaugjuhtida automaatvastaja vastuvõetud kõnede ajal. Kuna kaugjuurdepääsu- ja kaugjuhtimisvõimalus kujutavad endast tuntavat ohtu, võiks need võimalusel jätta aktiveerimata ning kasutamise korral kaitsta neid turvakoodiga (salanumber, PIN), mis peaks olema vähemalt kolme kuni viiekohaline ja vabalt valitav. Kõik tehases seadistatud paroolid tuleb enne kasutuselevõttu ära muuta. Nii nagu paroolid, tuleb ka turvakoodid deponeerida (vt M 2.22 Paroolide deponeerimine) ning neid tuleks regulaarselt vahetada. Tuleks jälgida, et koodi sisestamisel ei oleks läheduses võõraid, kes võiksid seda näha või kuulda. Üheks lisameetmeks selle jaoks, et kõrvalistel isikutel ei oleks võimalik teateid pealt kuulata või teisi rakendusi väärkasutada, on blokeerimislülitus, mis laseb automaatvastaja ühendusel pärast kolme kutsungit katkeda. Veel paremad on aga seadmed, millel pärast kolme kutsungit blokeeritakse kaugjuhtimisfunktsioon täielikult ja mida saab vaid seadmel uuesti aktiveerida. Otstarbekad on ka blokeerimisajad, mida pärast iga ebaõnnestunud katset pikendatakse. Lisaks kasutaja algatatud kaugjuhtimisele on olemas ka seadmeid, mis informeerivad varem sisestatud numbrile või SMS-i kaudu mobiiltelefonile helistavat kasutajat uutest saabunud teadetest.

Olenemata sellest, kuidas saabunud teateid kuulatakse, tuleb salvestatud kõned regulaarselt ära kuulata. Mittevajalikud salvestused tuleb regulaarselt kustuta-

da, et automaatvastaja salvestusmeediumile (digitaalsele salvestile või audiokassetile) ei tekiks ülekoormust, sest see muudaks uute kõnede salvestamise võimatuks või siis salvestataks uued teated vanadele teadetele. Lisaks tuleks määrata ühe kõne maksimaalne kestus, sest võimalik ründaja saaks muidu automaatvastaja piiratud salvestusvõimalused täita mõttetu teabega, mis takistaks uute kõnede salvestamist. Kui analoogseadmetel ei ole kustutamine võimalik, tuleks magnetlinti regulaarselt algusesse tagasi kerida, et salvestada uued kõned vanadele. Iga töötaja, kes hakkab kasutama automaatvastajat, peaks olema tutvunud selle kasutamisega, et teada seadme võimalusi ja piire. Selleks peab töötajatele jagama kasutusjuhendeid.

Täiendavad kontrollküsimused.

- Kas automaatvastaja kaugjuhtimine on võimalik ja kui on, siis kas see on PIN-iga kaitstud?
- Kas automaatvastajale salvestatud teksti puhul on kinni peetud nõudest, et seade ei jagaks välja salajast infot?
- Kas automaatvastajale tulnud teateid kuulatakse regulaarselt ning kas mittevajalikud teated kustutatakse?
- Kas automaatvastaja teateedastamisaeg on ajaliselt piiratud?

M 4.370z Anoubise kasutamine Windowsis

Algatamise eest vastutavad: administraator, infoturbespetsialist

Rakendamise eest vastutavad: kasutaja, administraator

IT-süsteemide vastu suunatud ründed põhinevad väga sageli pääsuõiguste väärkasutusel. Mida laialdasemaid pääsuõigusi kasutajatele välja jagatakse, seda lihtsamaks muutub ka süsteemide ründamine. Halvimal juhul võib näiteks veebilehitsejaga seotud viga või veebilehitseja liiga lubav, st piiranguid mittekehtestav seadistus anda ründajale täieliku juurdepääsu kõikidele ühe kasutaja andmetele. Kuna veebilehitseja kasutab üldjuhul kasutajale väljastatud õigusi, tekib veebilehitsejal piiranguteta juurdepääs kõikidele andmetele ja kataloogidele, mille jaoks kasutajal on olemas kirjutamisõigused. Siin peitubki peamine probleem: pääsuõigusi väljastatakse Unixi keskkonnas kasutajapõhiselt, st iga kasutaja jaoks määratakse kindlaks tema individuaalsed pääsuõigused. Protsess, mis käivitatakse kasutajale väljastatud õigustega, saab rakendada kõiki vastava kasutaja jaoks kindlaks määratud õigusi. Selle tagajärjel kasutab käivitatud rakendus oma töös palju suuremaid õigusi, kui selle otstarve tegelikult ette näeb. Kasutajal puudub üldjoontes võimalus piirata enda käivitatud rakenduste pääsuõigusi. Rakendustes esinevad vead seavad aga vahetult ohtu kasutajale kuuluvate andmete konfidentsiaalsuse, tervikluse ja käideldavuse. Anoubis on vabavara, millega saab juhtida rakenduste tööd ja kehtestada Unixi süsteemides failide terviklust reguleerivaid nõudeid. Selleks arvutatakse rakenduste ja failide jaoks välja kontrollsummad ning signeeritakse need digitaalselt. Salvestatud kontrollsummade haldamiseks ja kontrollimiseks tuleks kasutada Anoubise graafilist kasutajaliidest.

Anoubise kasutamine

Kuna Anoubis on individuaalselt konfigureeritav toode, mis koosneb paljudest komponentidest, nt *application level firewall*, *sandbox*, *playground,* ning on varustatud turvalise failisüsteemiga, peaksid vastutavad administraatorid end selle kasutusvõimalustega kurssi viima. Anoubis kaitseb kõiki Unixi arvuteid, millesse see on installitud, esmalt oma standardkonfiguratsiooniga. Standardkonfiguratsiooni tuleks kohandada suunistega, mille kohta Anoubises kasutatakse terminit *policies* . Nendega tagatakse, et konfiguratsioon arvestab piisavalt erinevate kasutajarühmade või kasutusvaldkondade erivajadustega. Anoubise suunised kehtestab tsentraalselt süsteemiadministraator ja kasutajatel pole neid võimalik tühistada ega eirata, kuid neid saab täiendavalt piirata. Lisateavet Anoubise suuniste kohta leiate toote installimise ja konfigureerimise käsiraamatust. Erinevate tüüpiliste kasutusvaldkondade vajadustele vastamiseks saab suunistega ette valmistada ka sobivad profiilid. Ettevalmistatud profiilide korral tuleb töötajatel üksnes välja valida enda töövaldkonna jaoks sobiv profiil, st nad ei pea suuniseid enam ise muutma. Selleks peavad administraatorid koostama kasutajatele sobivad profiilid ning kasutajaid ka juhendama, kuidas neid profiile õigesti rakendada. Profiile saab rakendada näiteks sülearvutite puhul, mida kasutatakse erinevates asukohtades ja võrkudes. Olenevalt kasutuskeskkonna ja otstarbe eripäradest on mõeldavad näiteks järgmised kohandatud profiilid:

- Büroo - Kui kohtvõrku kaitstakse turvalüüsidega ja kasutajatele on antud suhteliselt vaba juurdepääs sisevõrgus pakutavatele teenustele, ei tarvitse

bürootööks rakendatav sülearvutiprofiil kehtestada rangeid piiranguid. Sellistel juhtudel on sageli lubatud juurdepääs kõikvõimalikele sisestele ja teatud väljavalitud välistele teenustele. Kui aga kliendile on tarvis võimaldada juurdepääs ka väljavalitud võrguteenustele, nt sülearvuti konfigureerimiseks, võib profiili koostada nii, et teised IT-süsteemid pääsevad sülearvutisse vaid selles turvalises keskkonnas.

- Kodu - Sellistes kasutuskeskkondades puudub väga sageli sülearvutit kaitsev turvalüüs. Seetõttu võiks profiil keelata kõik väljast tulevad pöördused ja lubada internetiühendust vaid teatud väljavalitud rakendustele. Näiteks võiks profiil ette näha, et HTTP-ühendusi tohib avada ainult veebilehitseja, sisevõrkudega ühendusi luua ainult VPN Client ning värskendusi alla laadida üksnes viirustõrjetarkvara.
- Võõrvõrk - Kui kasutajal on tarvis oma töös kasutada ka avalikke võrgukeskkondi, nt lennujaamade WLAN-võrke, peab rakendatav profiil kehtestama võimalikult suured piirangud. Internetiühenduste loomine HTTP-ga tohiks olla lubatud ainult veebilehitsejale, meiliklient peaks teenusepakkujaga ühenduse loomiseks kasutama üksnes turvalisi kanaleid (POP3 ja IMAP) ning VPN-tunnelite kasutamine peaks ettevõttes olema lubatud vaid andmete vastuvõtmiseks. Kõik muud ühendusvõimalused tuleb blokeerida.

Kasutajal tuleb programmi kasutajaliideses üksnes välja valida sobiv turvaprofiil, mis tagab vastava kasutusvaldkonna jaoks kehtestatud nõuete täitmise. Kasutajaid on soovitatav juhendada, et nad teaksid, kuidas profiile õigesti valida.

Rakenduste kontrollimine

Kui osa rakenduste juurdepääsu võrgule või failisüsteemile on tarvis piirata, saab Anoubisega nendele rakendustele kehtestada asjakohased reeglid. Näiteks kui soovitakse, et PDF Readeril poleks lubatud värskendusi iseseisvalt alla laadida, või kui kõik failid tuleks salvestada ühte kindlaksmääratud failikausta, saab selleks koostada Application Level Firewalli reeglid ja sisse seada Sandboxi, mis tagavad nende piirangute rakendamise. Et vältida võltsitud ja pahavaraga sisse toodud rakenduse käivitamist, tuleks vastavad failid varustada digitaalselt signeeritud kontrollsummadega. Lisaks tuleb Anoubises sisse seada nn SFS-reeglid (*secure file system*), mis blokeerivad lugemisõigusega juurdepääsud ning muudetud ja signeerimata failide käivitamise. Need reeglid hoiavad ära rakenduse käivitumise ja seega välistavad võltsitud konfiguratsioonide sisselugemise. Anoubise konfiguratsioonist olenevalt saab reeglite rikkumise korral kuvada kasutajatele ka hoiatusteateid.

Reeglite määratlemine ja mõistetavus

Anoubise konfigureerimiseks kasutatakse graafilist kasutajaliidest. Reegleid saab koostada ja muuta reeglite redaktorprogrammiga (*editor*). Lisaks on võimalik rakenduste jaoks vajalikke reegleid koostada viisardiga. Sellega saavad ka kasutajad ise reegleid koostada. Kõiki koostatud reegleid, st vaadeldava rakenduse standardkonfiguratsiooni, kuvatakse protsessilehitsejas (*browser*).

Kaitstud keskkonnad failisüsteemi turbe suurendamiseks

Selleks, et protsessidel poleks võimalik failisüsteemi midagi kirjutada, tuleks tagada, et protsessid käivitatakse mõnes spetsiaalselt turvatud keskkonnas (*playground*). Näiteks kui veebilehitsejat kasutatakse *playground* 'is, ei jää pärast kasutust, st pärast seda, kui *playground* ära kustutatakse, failisüsteemi sellest mitte mingeid jälgi.

Kui kaitstud keskkonnas hoitavaid faile on tarvis kasutada ka failisüsteemis, tuleb need selleks spetsiaalselt kasutajaliidese kaudu failisüsteemi üle kanda. Sellist andmeedastust tuleks vajaduse korral kaitsta viirustõrjetarkvaraga. Selleks tuleb installida ja konfigureerida sobiv viirustõrjetarkvara. Lisaks saab kasutaja seansi lõppedes otsustada, kas kaitstud keskkonnas hoitud failid säilitatakse või kustutatakse.

Täiendavad kontrollküsimused:

- Kas administraator on end Anoubise laialdaste võimalustega kurssi viinud?
- Kas erinevatele kasutajarühmadele või kasutusvaldkondadele on koostatud sobivad Anoubise policy 'd?
- Kas kasutajaid on juhendatud, kuidas Anoubise profiile õigesti kasutada?
- Kas olulised rakendused ja failid, mida soovitakse Anoubisega kaitsta, on varustatud signeeritud kontrollsummaga?
- Kas Anoubises on konfigureeritud SFS-reeglid, mis tõkestavad juurdepääsu tundlikele failidele ja rakendustele juhul, kui nende kontrollsumma on kehtetu?
- Kas Anoubises kasutatavate playground 'ide jaoks on installitud ja konfigureeritud viirustõrjetarkvara?

M 4.371 Mac OS X-ga töötavate klientsüsteemide konfigureerimine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

Pärast Mac OS X installimist klientsüsteemidesse tuleb need konfigureerida. Vajalik seadistustöö oleneb suurel määral süsteemide kasutusotstarbest. Selles meetmes käsitletakse klientide turvalist konfigureerimist. Mac OS X-ga töötava süsteemi turvalise aluskonfiguratsiooni loomiseks tuleb arvestada järgnevate alltoodud aspektidega.

Operatsioonisüsteemi värskendamine

Operatsioonisüsteemi tuleks värskendada alati kohe pärast installimist, et likvideerida kõik tarkvarakomponentides ilmnenud vead. Lisaks tuleks regulaarselt kontrollida, kas tootja on avaldanud programmivärskendusi. Mac OS X-s saab seda konfigureerida süsteemiseadistustes tarkvaravärskenduse all.

Värskendusserveri swupdate.apple.com kasutamiseks võib rakendada käsuviiba järgmist käsku:

#sudo defaults write /Library/Preferences/com.apple.SoftwareUpdate CatalogURL

#http://swupdate.apple.com:8088/index-leopard- snowleopard.merged-1.sucatalog

Operatsioonisüsteemi värskendamiseks käsuviibaga saab terminalis kasutada käsku „ softwareupdate –download –all –install”. Värskenduste (updates) installimiseks on ilmtingimata tarvis administraatorivolitusi. Kui kohtvõrgus on olemas update server , tuleks kasutada seda.

Apple’i update server ’i määratlemine sisevõrgus

Mac OS X operatsioonisüsteemi saab värskena hoida ka integreeritud värskendusfunktsiooni abil. Selleks on soovitatav kasutada sisevõrgu update server it. Nii saab kasutada sisevõrguühendusi ja suuremaid andmeedastuskiiruseid. Ühtlasi väheneb seeläbi ka internetiühenduse kasutamise sagedus ning värskendusi on tarvis viiruste ja muudatuste suhtes kontrollida vaid üks kord. Lisapõhjus, miks võiks eelistada just sisevõrgu update server ’it, seisneb asjaolus, et see võimaldab vajalikus ulatuses kontrollida ka värskenduste ühilduvust olemasolevate tarkvarakomponentidega ja seda juba enne, kui värskendus kogu võrgus laiali jagatakse.

Sudo-käsu kehtivusaja lühendamine

Kui mõne programmi käivitamiseks root -volitustega on kasutatud sudo-käsku ning selleks sisestati vastav parool, salvestatakse see parool viieks minutiks süsteemi. Isegi kui konsooli protsess suletakse ja avatakse uus konsooliaken, ei järgne sellele parooli korduva sisestuse nõuet ja kõiki programme saab jätkuvalt käivitada root -volitustega.

Seetõttu tuleks faili /etc/sudours muuta järgmiselt:

#Defaults timestamp_timeout=0

#Defaults tty_tickets

Nii luuakse olukord, kus root -volitustega saab ühe autentimise kohta käivitada ainult ühe käsu ja autentimisandmed seotakse selle terminaliprotsessiga, mille sees autentimine aset leidis.

Viimati kasutatud objektide loetelu lühendamine

Mac OS X salvestab viimati kasutatud rakenduste, dokumentide ja serveriühenduste loetelu. Selline info hõlbustab küll esmajoones töötegemist, kuid aitab teha ka järeldusi konfidentsiaalsete andmete kohta, nt võimaldab teada saada, mis dokumentidega viimati tööd tehti ja millised on viimati kasutatud serverite aadressid. Et sellist infot oleks võimalikult vähe, tuleks süsteemiseadistuste valiku „Number of recent items" väärtuseks määrata „None".

Alternatiivina võib seda teha ka käsuviiba järgmise käsuga:

#defaults write com.apple.recentitems Applications -dict MaxAmount 0

Turvaliste failide automaatse avamise desaktiveerimine Safaris

Apple'i veebilehitseja Safari abil saab faile avada kohe pärast allalaadimist selleks kindlaks määratud programmiga. Seesama seadistus võimaldab automaatselt, st ilma kasutajalt küsimata, käivitada kahjurvara sisaldavaid faile. Kui mõnest ebaturvalisest allikast, nt manipuleeritud veebilehelt, laaditakse alla ja avatakse automaatselt mõni kahjulikku koodi sisaldav PDF-fail, võivad selle tagajärjel tekkida kas andmekaod või muud probleemid. Automaatse avamisfunktsiooni desaktiveerimiseks tuleb Safari General-seadistustes desaktiveerida valik „Open 'safe' files after downloading".

Viirustõrjetarkvara installimine

Igasse Mac OS X klienti peab olema installitud viirustõrjetarkvara. Siinjuures tuleb arvestada, et selle tarkvara signatuure tuleb pidevalt värskendada. Viirustõrjetarkvara peaks töötama taustaprogrammina ja rakenduma aktiivselt tööle vähemalt siis, kui mõnda faili hakatakse kasutama. Lisateavet selle teema kohta saate meetmest M 4.3 Viirusetõrjeprogrammide kasutamine . Arvesse tuleks võtta, et viirustõrjeprogramm peab suutma tuvastada ka Windowsi süsteeme ohustavaid viirusi, et koostöö Windowsi süsteemidega oleks võimalikult probleemivaba.

Andmevarundus

Tõrgetega kaasnevate andmekadude minimeerimiseks ja tavapäraste tööprotsesside kiireks taaskäivitamiseks on tarvis teha andmetest regulaarselt varukoopiaid. Täpsema kirjelduse leiate meetmest M 6.146 Andmete varundamine ja taastamine Mac OS X klientsüsteemides .

Ajatsooni ja aja sünkroniseerimise kohandamine

Igas IT-süsteemis tuleb kasutada korrektselt seadistatud kellaaega ja kuupäeva. Kui kellaaja erinevus kahe IT-süsteemi vahel on liiga suur, võivad sellega kaasneda autentimisvead. Korrektset kellaaega ja kuupäeva eeldab näiteks Kerberose protokoll. Kellaaega ja kuupäeva saab vaadata ning muuta süsteemiseadistustes kuupäeva ja kellaaja menüüs. Selleks on soovitatav kasutada enda sisevõrgu ajaserverit. Kui selline võimalus puudub, võib kasutada mõnda välist teenust (vt M 4.227 Lokaalse NTP -serveri kasutamine aja sünkroniseerimiseks).

Prügikasti turvalise tühjendamise aktiveerimine

Et vältida Mac OS X-s prügikasti visatud failide taastamist, tuleb prügikasti regulaarselt tühjendada. Mac OS X-s on turvaliseks kustutuseks olemas funktsioon „ Empty Trash securely ”, mille puhul kirjutab operatsioonisüsteem prügikasti kustutamise järel selle sisu teatud bitimustriga üle. Selle seadistuse aktiveerimiseks tuleb rippmenüü „Finder” valiku „Preferences” alamvalikus „Advanced” ära märgistada kastike funktsiooni „Empty Trash securely” ees.

Autostart funktsiooni desaktiveerimine

Autostarti funktsioon võimaldab käivitada programme otse välistelt andmekandjatelt kohe, kui need (nt CD-d, DVD-d või välised kõvakettad) ühendatakse arvutiga. Kuna automaatselt käivitatavad programmid võivad sisaldada ka kahjurvara, tuleks see funktsioon kõikide kasutajate puhul desaktiveerida. Selleks tuleb menüü „System Preferences” valikus „CDs & DVDs” kõikide loetletud parameetrite väärtuseks määrata „Ignore”. Märkus. Autostarti funktsioon töötab vaid juhul, kui Mac OS X tuvastab, et sisestatud andmekandja on kas tühi CD/DVD, muusika-CD, foto-CD või video-CD.

Neid seadistusi saab teha ka konsoolis:

```
# Disable blank CD automatic action:
defaults write /Library/Preferences/com.apple.digihub
com.apple.digihub.blank.cd.appeared -dict action 1
# Disable music CD automatic action:
defaults write /Library/Preferences/com.apple.digihub
com.apple.digihub.cd.music.appeared -dict action 1
# Disable picture CD automatic action:
defaults write /Library/Preferences/com.apple.digihub
com.apple.digihub.cd.picture.appeared -dict action 1
# Disable blank DVD automatic action:
defaults write /Library/Preferences/com.apple.digihub
com.apple.digihub.blank.dvd.appeared -dict action 1
# Disable video DVD automatic action:
defaults write /Library/Preferences/com.apple.digihub
com.apple.digihub.dvd.video.appeared -dict action 1
```

Ebavajalike programmide eemaldamine

Mac OS X installatsioon sisaldab ka mõningaid selliseid standardseid programme, mis tuleks eemaldada, et ründeobjekte oleks võimalikult vähe. Selliste programmide hulka kuuluvad näiteks mängud ja multimeediarakendused. Otsus, mis programmid eemaldada ja mis alles jätta, tuleb muidugi langetada konkreetset otstarvet silmas pidades. Tootmissüsteemidesse tohib installida üksnes tööks hädavajalikke programme. Standardprogrammide eemaldamine kuulub süsteemi muudatuste alla ja kõik muudatused tuleb dokumenteerida.

Eemaldada tuleks vähemalt järgmised programmid:

- AppleScripti kaust koos selle sisuga,
- Automator,

- Chess,
- Front Row,
- iTunes,
- iChat,
- Photo Booth,
- QuickTime,
- Dashboard.

Nende programmide leidmiseks tuleb siseneda menüüsse „Finder”, valida käivitatav ajam ja avada programmide kataloog. Osale programmidest pääseb juurde ka OS X Docki kaudu. Need viited tuleb samuti eemaldada.

Alternatiivina saab Dashboardi välja lülitada ka käsuviiba järgmise käsuga:

defaults write com.apple.dashboard mcx-disabled -boolean yes

Alati tuleks ära kustutada kõik minirakendused (widgets) kataloogist „Finder | Hard Disc | Library | Widgets”. Juurde installitud minirakendused võivad paikneda ka kodukataloogides „ Library | Widgets”. Alternatiivina võib kõikide süsteemis asuvate minirakenduste ülesleidmiseks kasutada ka otsingut „*.wdgt”.

Turvalise virtuaalmälu aktiveerimine

Olukorras, kus töömälu ei ole enam piisavalt, näeb Mac OS X ette töömälu teatud osade salvestamise lokaalsele kõvakettale. Andmed salvestatakse krüpteerimata kujul Swap-faili ning need failid võivad sisaldada ka tundlikke andmeid. IT-süsteemi väljalülitamisel kõik töömälus olnud andmed kustutatakse.

Seevastu Swap-failidena salvestatud andmed jäävad alles ka pärast taaskäivitust ja säilivad seni, kuni need üle kirjutatakse. Kui süsteem lülitatakse säästurežiimile (hibernation mode), salvestatakse peale juba olemasoleva Swap-faili ka kogu töömälu sisu (samuti krüpteerimata kujul) nn Sleepimage-failina. Juhul kui on aktiveeritud turvalise virtuaalmälu funktsioon, salvestatakse nii Swap- kui ka Sleepimage-fail lokaalsele kõvakettale üksnes krüpteeritult. Turvalise virtuaalmälu funktsiooni saab aktiveerida asukohas „System Preferences | Security | General | Use secure virtual memory”.

Alternatiivina saab sama seadistuse teha ka rakenduses „Terminal”, kasutades järgmist käsku:

defaults write /Library/Preferences/com.apple.virtualMemory UseEncryptedSwap -bool YES

Positsioonimisteenuste desaktiveerimine

WLAN-võrkude andmete põhjal on võimalik välja selgitada Mac OS X kliendi ligilähedane asukoht. Neid asukohaandmeid saab kasutada erinevate süsteemiteenuste, nt kuupäeva ja kellaaja seadistuses rakendatava ajatsooni automaatseks seadistamiseks. Samas võivad neid andmeid ära kasutada ka veebilehed, et määrata kindlaks veebilehe külastaja asukoht. Selline funktsioon võib olla küll kasulik, kuid andmekaitse ja turbe tagamise seisukohast on see siiski problemaatiline.

Positsioonimisteenustega (location services) saab välja selgitada näiteks lähima pangaautomaadi või postkontori asukoha ja seda kuvada. Kui veebileht soovib asukohta välja selgitada, ilmub tavaliselt dialoogiaken, mis küsib kasutajalt selleks luba. Sellest hoolimata tuleks positsioonimisteenused asukohas „System Preferences | Security | General” desaktiveerida.

Automaatse sisselogimise desaktiveerimine

Automaatne sisselogimine süsteemi tuleb alati desaktiveerida. Kui Mac OS Xga töötavasse süsteemi on võimalik sisse logida parooli sisestamata, tähendab see seda, et väga paljud turvafunktsioonid ei rakendu. Suvandi „Disable automatic login” leiate menüü „System Preferences” alammenüü „Security & Privacy” valikust „General” ja see tuleb aktiveerida.

Ekraaniluku aktiveerimine

Pärast ekraaniluku väljalülitamist ja säästurežiimilt naasmist tuleb ilmtingimata tagada, et sisselogitud kasutaja sisestaks uuesti enda parooli.

Suvandi „Require password:

- immediately,
- 5 seconds,

M 4.372 FileVaulti kasutamine Mac OS X-s

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: kasutaja, administraator

Alates Mac OS X versioonist Panther (10.3) saab kasutajate kaustu krüpteerida FileVaultiga, mis rakendab algoritmi AES-128. FileVaulti põhiparool krüpteeritakse siiski RSA-1024-ga, mis tagab efektiivse 112-bitise krüpteerimispikkuse. FileVault on integreeritud otse operatsioonisüsteemiga, st kasutajate kaustade krüpteerimiseks ei ole tarvis mitte mingisugust lisatarkvara. Kuna FileVaulti on väga lihtne kasutada, on soovitatav krüpteerida ka kõik kodukataloogid. See kehtib ennekõike kaasaskantavates arvutites hoitava tundliku info kohta, sest nende seadmete puhul on varguse oht tavapärasest suurem. FileVault aitab ka varguste korral. Arvestada tuleb aga sellega, et FileVaulti eeldatav kaitsetoime avaldub vaid siis, kui klientsüsteem on nõuetekohaselt välja lülitatud või kui kasutaja ei ole end veel sisse loginud. Pärast seda, kui kasutaja on end edukalt sisse loginud, liidetakse FileVaulti abil krüpteeritud kettakujutis (disk image) süsteemiga kui kodukataloog (home) ning seda on võimalik kasutada. Samas ei dekrüpteerita kettakujutist mitte kunagi tervenisti, vaid töömällu laaditakse ainult parajasti vajaminevad osad. Fail krüpteeritakse uuesti kohe pärast seda, kui see on töömälust lahkunud. Kui kasutaja logib end välja, ühendatakse FileVaultiga krüpteeritud kettakujutis failisüsteemist lahti ja failid on kaitstud. Juhul kui kasutajatel on võimalik end klientsüsteemi sisse logida nii, et nad ei pea end autentima (automaatne sisselogimine), dekrüpteeritakse FileVaultiga kaitstud andmed ilma parooli küsimata. Selleks, et FileVault saaks andmeid tõhusalt kaitsta, peab automaatne sisselogimine olema välja lülitatud ning paroolkaitsega sisselogimise jaoks valitud piisavalt turvaline parool (vt M 2.11 Paroolide kasutamise reeglid).

FileVaulti kasutuselevõtu ettevalmistamine

FileVaultiga saab kaitsta üksnes selliseid kodukatalooge, mis on salvestatud Mac OS Extendedi failisüsteemide alla ning mille puhul ei ole suur- ja väiketähe eristust (case sensitive) sisse lülitatud. Kui FileVaulti soovitakse kasutusele võtta, tuleks kodukataloogide partitsioonide loomiseks kasutada failisüsteemi Mac OS Extended (Journaled). Üldjuhul võib soovitada, et kodukataloogid installitaks eraldi partitsioonile. Partitsioonide suuruse ja nende jaoks vajamineva kõvaketta mälumahu planeerimisel tuleb arvestada, et krüpteerimisprotsessi tarbeks peab kõvakettal olema vähemalt nii palju täiendavat mäluruumi, kui suur on krüpteeritav kodukataloog. Selline vajadus tuleneb FileVaulti tööpõhimõttest. Kui kasutaja jaoks aktiveeritakse FileVault, koostab Mac OS X krüpteeritud kettakujutise, kopeerib kõik kasutaja kausta andmed kettakujutise alla ning kustutab seejärel kasutaja originaalkausta ära. Siinkohal tuleb tagada, et kasutajate kustutatud krüpteerimata kaustade sisu ei oleks võimalik taastada. Selleks tuleks kasutada turvalist kustutamisfunktsiooni „Use secure erase”.

FileVaulti aktiveerimine

Enne FileVaulti kasutamist tuleb see aktiveerida. FileVaulti saab aktiveerida juba kasutajakonto loomise käigus, märgistades kasutajaatribuutide (user properties) all ära suvandi „Turn on FileVault protection”. Kui FileVaulti on tarvis aktiveerida tagantjärele mõne juba sisselogitud kasutaja jaoks, tuleb asukohas „ System Preferences | Security & Privacy | FileVault” aktiveerida suvand „Turn on FileVault ”.

Mõlemal juhul tuleks FileVaulti eripära silmas pidades kasutada kindlasti ka turvalist kustutamisfunktsiooni „Use secure erase”. Lisaks tuleks aktiveerida turvalise virtuaalmälu funktsioon „Use secure virtual memory”, sest muidu salvestatakse andmed või ka parool ilma krüpteerimata asukohta „ /var/vm”.

Andmete taastamine

Selleks, et FileVaulti kasutajaparooli kaotsimineku korral oleks võimalik kõiki kasutaja FileVaultiga krüpteeritud kaustu taastada, peab a dministraator arvuti jaoks kindlaks määrama põhiparooli. Taastamisparool peaks olema piisavalt keeruline.

Võimalikult keerulist parooli tuleb ilmtingimata kasutada ka siis, kui efektiivsuse kaalutlustel valitakse erinevate klientsüsteemide jaoks identne parool. Kui kahtlustatakse, et põhiparool võib olla saanud avalikuks, nt kui seda hoiti mõnes ebaturvalises kohas, tuleb põhiparool viivitamata ära muuta, sest muidu tekib vaba juurdepääs kõikidele arvutis hoitavatele krüpteeritud andmetele. Põhiparooli tuleks hoida kohas, mis võimaldaks administraatoril tõrgete korral andmeid kiiresti taastada, ilma et ta sõltuks muust personalist (vt M 2.22z Paroolide deponeerimine).

FileVault ja energiasäästurežiimid

Mac OS X-ga töötav arvuti, mida parasjagu ei kasutata ja mis pole välja lülitatud, võib töötada energiasäästurežiimis. Selle alla kuulub ka puhkeseisund (sleep). Mac OS X puhul väljendatakse selle terminiga nii sellist seisundit, milles arvuti kirjutab RAM-i sisu kõvakettale, kui ka seisundit, mille korral külmutatakse üksnes töömälu aktiivne sisu. Puhkeseisundis oleva Mac OS X puhul hoitakse FileVaulti parooliandmeid kas klientsüsteemi töömälus (RAM) või kõvakettal. Selline olukord ohustab FileVaultiga krüpteeritud andmete konfidentsiaalsust. Kui turbevajadus on tavapärasest suurem, ei tohiks Mac OS X-ga töötavat klientsüsteemi mitte kunagi ilma järelevalveta puhkeseisundisse jätta. Järelevalve alternatiiv on kasutaja väljalogimine ja süsteemi väljalülitamine. Ekraaniluku funktsioon, nagu ka puhkeseisund, ohustab konfidentsiaalsust, sest ka ekraaniluku kasutamisel jäävad parooliandmed töömällu, kust neid on võimalik välja lugeda.

Töötajate turbeteadlikkuse suurendamine

Töötajaid tuleb teavitada sellest, et FileVault krüpteerib üksnes kasutaja enda kausta ja seda ka ainult siis, kui Mac OS X-ga töötav klientsüsteem lülitatakse nõuetekohaselt välja. Samuti tuleb töötajaid teavitada sellest, kuidas toimib File-Vaulti krüpteerimisfunktsioon energiasäästurežiimide korral, ning sellest, et administraatoril on võimalik parooli kaotsimineku korral andmeid põhiparooliga taastada.

Lisateavet andmete turvalise talletamise ja transportimise kohta leiate meetmest M 4.379 Andmete turvaline talletamine ja transportimine Mac OS X-s .

FileVaulti sobivuse piirid

FileVault ei paku võimalust valida, milliseid andmeid soovitakse krüpteerida. Krüpteerimisfunktsioon toimib üksnes kasutaja kausta suhtes. Tundlikku infot võivad aga sisaldada ka paljud teised kataloogid. Näiteks sisaldavad kataloogid /Library/Logs ja /var/log erinevaid detailset süsteemiinfot kajastavaid logifaile ning kataloogid /Library/Caches ja /tmp ajutisi faile ja osa andmevarundusprogrammide cache -faile ning kataloog /Library/Preferences süsteemiüleseid seadistusfaile. Seetõttu tuleks tavapärasest suurema turbevajaduse korral kasutada FileVaulti asemel mõnda muud krüpteerimisprogrammi, mis krüpteerib kogu kõvaketta.

Kontrollküsimused

- Kas FileVaultiga krüpteeritavate partitsioonide jaoks kasutatakse failisüsteemi Mac OS Extended (Journaled) ning kas sellisel juhul on suur- ja väiketähe eristus (case sensitive) välja lülitatud?
- Kas FileVaulti kasutamisel on Mac OS X jaoks valitud piisavalt tugev kasutajaparool ja kas automaatne sisselogimine on välja lülitatud?
- Kas Mac OS X jaoks on valitud piisavalt tugev FileVaulti põhiparool ja kas seda hoitakse turvalises kohas?
- Kas Mac OS X kasutajatele on teada, et FileVault krüpteerib üksnes kasutaja kausta?
- Kas Mac OS X kasutajad teavad, et FileVaulti kasutajaparooli kaotsimineku korral on neil FileVaulti põhiparooliga võimalik ise enda andmeid taastada?

M 4.373 Mittevajaliku riistvara desaktiveerimine Mac OS X-s

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

Kõik need seadmed ja liidesed, mida Mac OS X puhul ei vajata, tuleb desaktiveerida. Näiteks kui ettevõttes või ametiasutuses on veebikaamerate või mikrofonide kasutamine ära keelatud, saab vastava kernelilaienduse (kext) ära kustutada, et raskendada juurdepääsu pealtkuulamist võimaldavale riistvarale.

kext-d asuvad järgmises kataloogis:

/System/Library/Extensions

Välja tuleb välja valida õiged kext-d ja need turvaliselt kustutada.

Kernelilaienduse WLAN-failinimi	Kernelilaienduse funktsioon
WLANIOBluetoothFamily.kextBluetoothAppleAN	WL
AirPort2.kextAppleAirPort.kext	
IOBluetoothHIDDRiver.kextAppleAirPortFBluetooth	
AppleIRController.kext	Infrapunavastuvõtjad
AppleOnboardAudio.kext	Audio
AppleUSDAudio.kext	Audio
AudioDeviceTreeUpdater.kext	Audio
IOAudioFamily.kext	Audio
VirtualAudioDriver.kext	Audio
Apple_iSight.kext	Video
AppleUSBVideoSupport.kext (see fail asub IOUSBFamily.kext sees kataloogis / Contents/Plugins).	Video
IOUSBMassStorageClass.kext	USB massmälu
IOFireWireSerialBusProtocolTransport.kext	Firewire

Seejärel tuleb kausta muutmise kuupäeva värskendamiseks käivitada allesesitatud käsk. Selle tulemusel kustutatakse *extension cache* esmalt ära ja seejärel laaditakse see uuesti:

sudo touch /System/Library/Extensions

Enne, kui kernelilaiendused turvaliselt prügikastist ära kustutatakse, et vältida nende liiga lihtsat taastamist, tuleks andmetest teha varukoopiad ja salvestada need näiteks võrgukettale. Andmete varukoopiat tuleks hoida mõnes turvalises kohas ning sellele tohivad juurde pääseda ainult administraatorid. Ka siis, kui mõni kext on eemaldatud, ei pruugi juurdepääs vastavale riistvarale olla piisavalt tõkestatud, sest vana tarkvara võib näiteks Apple'i tarkvaravärskenduse tulemusel olla asendatud uuema versiooniga. Seetõttu tuleks pärast igat süsteemivärskendust kontrollida, kas kext-d on endiselt kustutatud. Mac OS X muudatused, mis puudutavad kext-sid, tuleb sobival viisil dokumenteerida. Kui kernelilaienduste

eemaldamist ei peeta piisavalt turvaliseks lahenduseks, võib selle asemel ka vastavad riistvarakomponendid füüsiliselt süsteemist eemaldada.

Täiendavad kontrollküsimused:

- Kas kõik seadmed ja liidesed, mida Mac OS X-s ei vajata, on desaktiveeritud?
- Kas pärast Mac OS X süsteemiuuendusi kontrollitakse, et kernelilaiendused on jätkuvalt kustutatud?
- Kas Mac OS X originaal-kext-failidest on tehtud varukoopia ja kas seda varukoopiat hoitakse turvalises kohas?
- Kas Mac OS X muudatused on dokumenteeritud?

M 4.374 Kasutajakontode juurdepääsukaitse Mac OS X-s

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

Mac OS X-ga töötavate klientide kasutajakontode seadistusi tuleb kohandada, et suurendada süsteemi turvet. Näiteks võivad volitamata isikud enda huvides ära kasutada paroolide meelespidamise funktsiooni, mis võib anda vihjeid kasutatava parooli kohta. Seadistuste kohandamiseks tuleb siseneda süsteemiseadistuse alammenüüsse „Users". See, kas kasutajakonto on volitamata juurdepääsu eest turvaliselt kaitstud, oleneb väga suurel määral kasutatavast paroolist, mis tähendab, et parool tuleks valida võimalikult tugev. Võtta tuleks vähemalt meede M 4.376 Paroolisuuniste kindlaksmääramine Mac OS X-s . Teine oluline tingimus kasutajakonto turbe tagamisel on parooli meelespidamise funktsiooni desaktiveerimine, et ründajal ei oleks võimalik hankida vihjeid kasutatava parooli kohta. Kuna parooli meelespidamise funktsioonis talletatav info võib halvimal juhul sisaldada ka parooli ennast, tuleks see funktsioon kindlasti desaktiveerida. Kui parooli meelespidamise funktsiooni siiski kasutatakse, tuleb kõiki kasutajaid sellega kaasnevatest ohtudest ilmtingimata teavitada. Samuti on oluline, et sisselogimisaknas ei kajastuks kõikide kasutajate loetelu, sest nii saaks ründaja enda valdusse ammendava ülevaate süsteemi kasutajatest. Seejärel on ründajal tarvis hankida üksnes vastavad paroolid ja ta ongi saanud volitamata juurdepääsu süsteemile. Süsteemi sisselogimine ei tohiks mitte mingil juhul olla automaatne, vaid see peab toimuma alati kasutajatunnuse ja parooliga. Alternatiivina saab parajasti sisselogitud kasutajatele rakendada piiranguid ka käsuviibaga:

```
# Paroolivihjete väljalülitamine
defaults write /Library/Preferences/com.apple.loginwindow RetriesUntilHint - int
0
# Nime ja parooli küsimine sisselogimisaknas, nimede loetelu kuvamata jätmine
defaults write /Library/Preferences/com.apple.loginwindow SHOWFULLNAME
-bool yes
# Funktsioonide „Restart", „Sleep" ja „Shut Down" desaktiveerimine
defaults write /Library/Preferences/com.apple.loginwindow PowerOffDisable -
bool yes
```

Ülalkirjeldatud seadistusi tuleks kontrollida iga kord pärast süsteemivärskendusi.

Täiendavad kontrollküsimused:

- Kas Mac OS X automaatne sisselogimine on desaktiveeritud?
- Kas Mac OS X kasutajakonto parool on piisavalt tugev?
- Kas Mac OS X kasutajakontoga seotud paroolide meelespidamise funktsioon on desaktiveeritud või kas töötajaid on selle ohtudest teavitatud?

M 4.375z Sandbox ’i funktsioonide kasutamine Mac OS X-s

Algatamise eest vastutavad: infoturbespetsialist, IT-juht
Rakendamise eest vastutab: administraator

Operatsioonisüsteemil Mac OS X on olemas sandbox ’i funktsioonid. Sandbox’i funktsioonid võimaldavad protsesse käivitada piirangutega keskkonnas, mille suhtes on ülejäänud IT-süsteem täielikult kaitstud. Näiteks saab sandbox ’i sisse lukustatud rakenduselt ära võtta võrgule või failidele juurdepääsu õiguse, et minimeerida võimalikke kahjusid, mis võivad kaasneda rakenduse töös esinevate vigadega. Sandbox ’i funktsioonid kujutavad endast laialdasi piiranguvõimalusi ja nende kasutamine ei tühista muid suuri piiranguid, nt pääsuloendeid. Seetõttu ei saa sandbox lubada mitte midagi sellist, mida mõni muu tehnoloogiline lahendus keelab. Pigem pakub see üksikasjalikku võimalust katsetada ja piirata programmide mõju.

Uusi programme ja teenuseid, mis hakkavad osalema võrgusides, on soovitatav enne kasutuselevõttu sandbox ’is katsetada. Kui uus laps-protsess käivitatakse sandbox ’is, siis pärib see muu hulgas ka sandbox ’is kehtestatud piirangud. Näiteks kui Safari töötab sandbox ’is ning selle kaudu laaditakse alla ja avatakse automaatselt mõni kahjurvaraga nakatatud PDF-fail, siis kehtivad selle PDF-faili avamisele sandbox ’is kehtestatud piirangud ja võimalik kahjulik mõju on tavapärasest tunduvalt väiksem. Kui kasutajatele võimaldatakse veebilehitsejat kasutada üksnes sandbox ’i keskkonnas, saab sellega tõkestada ka kasutusse mittelubatud pluginate installimist, sest pärast igat taaskäivitust on veebilehitseja taas selle algses seisundis. Valiku, mis rakendusi tohib käivitada üksnes sandbox ’is, peab tegema administraator ning seejärel tuleb tal luua ka vastav konfiguratsioon.

Safari käivitamiseks sandbox ’is ilma failijuurdepääsuta saab kasutada järgmist käsku:

#sandbox-exec -p “(version 1) (allow default) (deny file-write*)” /Applications/ Safari.

#app/Contents/MacOS/Safari

Kui seda käsku täiendada asjakohase parameetriga („debug all”), saab kõiki tegevusi jälgida rakenduses Console.app.

Lisaks saab sisse seada sandbox ’i profiili, et kõik konfiguratsiooniparameetrid ühte kohta kokku koondada. Kataloogis /usr/share/sandbox asuvad mitu erinevate süsteemiteenuste jaoks defineeritud sandbox ’i profiilimalli.

Kui vajaminev profiil on olemas ja kohandatud lokaalsete suunistega, võib rakendust käivitav käsk välja näha järgmine:

#sandbox-exec -f /usr/share/sandbox/safari.sb /Applications/Safari.app/ Contents/

#MacOS/Safari &

Kontrollküsimus:

- Kas administraator on ära otsustanud, mis rakendused peaksid töötama üksnes sandbox 'is?

M 4.376 Paroolisuuniste kindlaksmääramine Mac OS X-s

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

Mac OS X-ga töötavate klientsüsteemide jaoks tuleb määrata kindlaks paroolisuunised, mis tagavad, et valitavad paroolid on piisavalt tugevad. Selleks tuleks Mac OS X puhul võtta meede M 1.1 Vastavus normidele ja eeskirjadele . Siinkohal saab kasutada ka käsuviibaga käivitatavat programmi pwpolicy. See programm võimaldab kindlaks määrata näiteks paroolide miinimumnõuded paroolis sisalduvate tähtede ja numbrite arvu kohta, parooli minimaalse pikkuse ning ebaõnnestunud sisselogimiskatsete maksimaalse lubatud arvu. Kui paroolis kasutatakse tähti ja numbreid, näevad nõuded ette, et parool peab olema vähemalt kaheksakohaline. Samuti kehtib nõue, et parooli tuleb regulaarselt vahetada. Allesitatud käsuga määratakse kindlaks paroolisuunis, mille kohaselt peab parool olema vähemalt kaheksakohaline, seejuures on lubatud ebaõnnestunud sisselogimiskatsete arv samuti kaheksa ja selle ületamisel konto blokeeritakse.

pwpolicy -n /Local/Default -setglobalpolicy “minChars=8 maxFailedLoginAttempts=8”

Võimalik on kasutada ka järgmisi paroolisuuniseid.

Muutuja

Funktsioon

usingHistory

0 = kasutaja tohib praegust parooli edasi kasutada; 1 = kasutaja ei tohi praegust parooli edasi kasutada; 2–15 = kasutaja ei tohi viimast n hulka paroole uuesti kasutada

usingExpirationDate

Kui seadistusväärtus on 1, palutakse kasutajal expirationDateGMT-s kindlaksmääratud aja möödudes oma parool ära vahetada

usingHardExpirationDate

Kui seadistusväärtus on 1, desaktiveeritakse konto pärast hardExpireDateGMT-s kindlaksmääratud aja saabumist

requiresAlpha

Kui seadistusväärtus on 1, nõuab süsteem, et paroolis peab olema vähemalt üks täht

requiresNumeric

Kui seadistusväärtus on 1, nõuab süsteem, et paroolis peab olema vähemalt üks number

expirationDateGMT

Kohustusliku paroolimuutmise kuupäev. Andmevorming: kk/pp/aa

hardExpireDateGMT

Konto desaktiveerimise kuupäev. Andmevorming: kk/pp/aa

maxMinutesUntilChangePassword

Kasutaja parooli kohustusliku muutmise intervall

maxMinutesUntilDisabled

Näitab, mitu minutit on jäänud konto automaatse desaktiveerimiseni

maxMinutesOfNonUse

Näitab, mitu minutit on jäänud konto desaktiveerimiseni, kui kontot ei kasutata

maxFailedLoginAttempts

Maksimaalne ebaõnnestunud sisselogimiskatsete arv, mille ületamisel konto blokeeritakse

minChars
Parooli miinimumpikkus, st parool ei tohi olla sellest seadistusväärtusest lühem
maxChars
Parooli maksimumpikkus, st parool ei tohi olla sellest seadistusväärtusest pikem
Lisateavet paroolisuuniste täiendavate parameetrite kohta leiate Mac OS X juhendilehtedest (Manual Pages).
Täiendavad kontrollküsimused:

- Kas Mac OS X jaoks on kindlaks määratud sobivad globaalsed paroolisuunised?
- Kas Mac OS X puhul kasutatakse vähemalt kaheksakohalisi paroole?

M 4.377z Mac OS X digisignatuuride kontrollimine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

Alates versioonist Mac OS X 10.5 on kõik Apple'i käitatavad operatsioonisüsteemi komponendid digitaalselt signeeritud. Ka teistel tootjatel palutakse oma programmid varustada digisignatuuridega. Signeeritud programmide muutmisel (nt kahjurvara tõttu) kaotab signatuur kehtivuse. Seepärast tuleb olukorras, kus soovitakse hakata kasutama uut programmi, esmalt kontrollida selle signatuuri. Kui signatuuriandmed puuduvad, tuleks programm üle kontrollida vähemalt viirustõrjetarkvaraga. Signatuuri kehtivuse kontrollimiseks kasutab Apple avaliku võtme infrastruktuuri, mis sarnaneb HTTPS-veebilehtedel kasutatavaga. Administraatorid peaksid õppima, kuidas kasutada õigesti codesign- käsku, et tagada iga uue programmi signatuuri kontrollimine.

Seda, kas programmil on kehtiv signatuur või mitte, saab selgitada välja käsuviiba järgmise käsuga:

#codesign –verify –verbose / -v /path/to/MyApp.app

Kehtiv signatuur osutab, et fail vastab tootja originaalile ja faili ei ole muudetud. Signatuuri kehtivuse kontrollimisega saab välistada edastamisel aset leidvad manipulatsioonid. Lisaks kasutatakse signatuure programmide eksimatuks tuvastamiseks. Näiteks võimaldab see tagada, et programmid töötavad kindlasti vastavalt nende jaoks tehtud seadistustele (parental control, firewall, keychain).

Kontrollküsimus:

Kas enne Mac OS X rakenduste installimist kontrollitakse nende digisignatuuri?

M 4.378 Programmide pääsuõiguste piiramine MAC OS X-s

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

Arvuti teatud funktsioonidele juurdepääsu piiramiseks saab Mac OS X-s kasutada nn lapsevanemate järelevalvefunktsiooni Parental Controls. Kuigi seda funktsiooni nimetatakse lapsevanema järelevalveks või lapselukuks, on seda siiski mõistlik kasutada ka ametiasutustes ja ettevõtetes. Süsteemiseadete („System Preferences") all leiduva funktsiooniga Parental Controls saab kasutajakontodele kehtestada lisapiiranguid. Sellesama, nn lapseluku funktsiooniga saab piirata ka programmide pääsuõigusi, eeldusel et ebavajalikud programmid on turvaliselt eemaldatud (vt M 4.371 Mac OS X-ga töötavate klientsüsteemide konfigureerimine). Vajaduse korral saab selle funktsiooni tööd seadistada ka tavapärasest palju detailsemalt. Näiteks saab selle seadistusega blokeerida kasutajate juurdepääsu teatud rakendusprogrammidele, veebilehtedele ja arvutikomponentidele. Seda seadistust sobib kasutada ka kausta „Utilities" blokeerimiseks, et tõkestada juurdepääs arvuti haldamiseks vajalikele programmidele, millega tutvumine annaks liiga palju detailset infot süsteemi kohta. Kui kasutajatele soovitakse võimaldada juurdepääs ainult kindlatele domeenidele ja veebilehtedele, saab menüüpunktis „Content" lubada juurdepääsu näiteks domeenile „*.ria.ee". Lisaks saab piirata meilivahetust, st lubada meilivahetust üksnes eelmääratud osaliste vahel.

Menüüpunktis „Mail & iChat" saab koostada kõikide lubatud meili- ja iChat-teenust kasutavate sidepartnerite loetelu. See seadistus võimaldab vältida info lekkimist programmidest Mail ja iChat. Siinkohal tuleb siiski arvestada, et meilide saatmiseks volitamata isikutele saab jätkuvalt kasutada HTTP-Webmaili. Samas ei ole praegu võimalik kohandada lubatud sidepartnerite loetelu regulaarsete väljatrükkidega. Kasutajakontode lubatud sisselogimisaega saab seadistada menüüpunktis „Time Limits". Näiteks kui töötajate puhul võib eeldada, et nende põhitööaeg jääb vahemikku 7–17, peaks lubatud sisselogimisaja seadistus vastama enam-vähem sellele ajavahemikule. Lisaks tuleks võimalikult laialdaselt kasutada teisi piiranguvõimalusi, nt blokeerida CD-/DVD-ajamite kasutamine. Arvesse tuleks võtta ka seda, et liiga ranged piirangud võivad raskendada töötamist ja õõnestada töömotivatsiooni. Seetõttu peaksid IT-juht ja infoturbespetsialist eeltööna välja selgitama, millistes klientsüsteemides mis piiranguid rakendada. See tuleks ka dokumenteerida.

Klientarvuteid on võimalik ka tsentraalselt juhtida. Kui süsteemiseadetes „System Preferences" aktiveerida Parental Controlsi funktsiooni suvand „Manage parental controls from another computer", saab kasutajakontode kasutusvõimalusi lapseluku funktsiooniga piirata ka eemal asuvast arvutist. Selleks läheb tarvis juhitava IT-süsteemi administraatori kasutajatunnust ja parooli. Nende pääsuandmete abil saab haldusarvutiga töötades piirata juhitava IT-süsteemi kasutaja õigusi, nagu kirjeldatud eespool.

Täiendav kontrollküsimus:

- Kas programmide pääsuõigusi on vastavate meetmetega piiratud võimalikult suures ulatuses, nii et pääsuõigused vastavad turvapoliitika nõuetele?

M 4.379 Andmete turvaline talletamine ja transportimine Mac OS X-s

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: kasutaja

Mac OS X-s saab koostada kettakujutisi (disc images). Kettakujutised näevad välja nagu failid, kuid need sisaldavad ka operatsioonisüsteemi, mida on võimalik virtuaalse ajamina arvuti operatsioonisüsteemiga ühendada. Selleks läheb tarvis üksnes ühte topeltklõpsu. Kettakujutisi saab tihendada ja krüpteerida. Iga Mac OS X-ga töötav süsteem suudab selliselt koostatud kettakujutisi ilma probleemideta lugeda. Teiste platvormide puhul läheb selleks tarvis lisatarkvara. Seetõttu tuleb alati pöörata tähelepanu sellele, et konfidentsiaalseid andmeid transporditaks ja hoitaks Mac OS X-s kas krüpteeritud kettakujutise vormingus või mõnel muul sobival krüpteeritud kujul. Kasutajaid tuleb teavitada, kuidas kettakujutistega õigesti ümber käia. Kui kettakujutis koostatakse mõnest juba olemasolevast kataloogist, saab valida kahe seadistusvõimaluse vahel. Üks seadistusvalik puudutab kettakujutise andmevormingut, nt compressed , read only või read/write . Täpsete CD-/DVD-kujutiste loomiseks saab kasutada vormingut DVD/CD-Master. Teine seadistusvalik puudutab krüpteerimist. Kui kettakujutis sisaldab konfidentsiaalseid andmeid, tuleks kujutis krüpteerida. Selleks tuleks valida 256-bitine AES-krüpteering ja piisavalt keeruline parool, st triviaalseid paroole tuleks tingimata vältida (vt M 1.1 Vastavus normidele ja eeskirjadele).

Uue, täiesti tühja kettakujutise koostamiseks saab lisaks kasutada seadistusvõimalusi, mis erinevad olemasoleva kataloogi põhjal koostatava kujutise omadest. Olulisemate valikute hulka kuuluvad kettakujutise maksimumsuuruse ja andmevormingu kindlaksmääramine. Kui valida „Sparse disk image”, kasutatakse kõvaketta mäluruumi vaid siis, kui seda vajatakse. Kettakujutis muutub lisatud andmete võrra suuremaks. Ent andmete eemaldamisel sparse -tüüpi kettakujutiselt selle maht ei vähene. Kujutise jaoks hoitavat mälumahtu saab vabastada käsuga „hdiutil compact image ’i nimi”. See funktsioon toimib ainult sellistes arvutites, mis ei tööta parajasti akurežiimil. Uue, tühjalt koostatava kettakujutise seadistusvõimaluste hulka kuulub ka võimalus määrata kujutise kasutamise jaoks kindlaks mõni enam levinud Apple’i või Microsofti failisüsteem. Kettakujutise parooli saab salvestada samamoodi nagu muud konfidentsiaalset infot, st võtmekimbu all olevate nn turvaliste märkmete alla. Kui ühe kettakujutisega peab saama tööd teha korraga mitu inimest, tuleb parooli jaoks välja valida mõni tsentraalne ja turvaline hoiukoht, et kehtiv parool oleks kõikidele volitatud töötajatele alati kättesaadav.

Täiendavad kontrollküsimused:

- Kas Mac OS X-s hoitakse ja transporditakse andmeid turvaliselt?
- Kas kõiki Mac OS X kasutajaid on õpetatud, kuidas kettakujutistega turvaliselt ümber käia?
- Kas Mac OS X kettakujutiste kaitsmiseks rakendatakse tugevaid paroole?
- Kas Mac OS X kettakujutiste parooli hoitakse turvalises kohas?

M 4.380w Apple Software Restore'i kasutamine Mac OS X-s

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

Apple Software Restore'i (ASR) rakendusega saab Mac OS X-s failisüsteeme duplitseerida ja kloonida. ASR ei paku mitte üksnes partitsioonide kloonimise võimalust, vaid lubab kettakujutist (disc image) ka võrgukeskkonnas kasutada ning võrgu kaudu klientidesse laiali jaotada. Kui Mac OS X kliendi installimisel on järgitud kõiki institutsiooni või ettevõtte nõudeid ja kui klient vastab turvapoliitikale, võib seda süsteemi kloonida ja kasutada ka teiste klientide installimiseks võrgukeskkonna kaudu. Nii tagatakse, et kõikides Mac OS X-ga töötavates klientides kasutatakse ühesugust aluskonfiguratsiooni, mis järgib institutsiooni turbeettekirjutusi. Esimese sammuna tuleb selleks luua kettakujutis standardsüsteemist. Selleks tuleb läbida järgmised sammud:

- Asetage seadmesse installi-CD.
- Valige sobiv menüükeel ja käivitage kõvaketta teenusprogramm.
- Valige välja kloonitav partitsioon ja desaktiveerige see parempoolse hiireklõpsuga.
- Seejärel koostage menüüpunktis „File | New | Image from Disc XYZ" vastavast partitsioonist kettakujutis, mida soovite teistesse klientarvutitesse kloonida. Selle protsessi lõpetamiseks võib kuluda mitu minutit (oleneb kopeeritava ajami suurusest).
- Protsessi lõppedes tuleb kontrollida, kas koostatud kettakujutises leidub vigu. Selleks tuleb arvuti taaskäivitada ning käsuviibale sisestada järgmine käsk: sudo asr –source /Path/to/Image.dmg –imagescan

Kui kettakujutise kontroll osutub edukaks, tuleb koostada Plist (property list). Plist-loetelu sisu määrab kindlaks muutuja Data Rate ja selle tüüp on Number. Võrgu eripärast ja voogedastuse soovitud ribalaiusest olenevalt tuleb selle muutuja alamjaotisse „Bytes per second" sisestada väärtus, seejuures ei tohi sisestamisel kasutada ei komasid ega punkte. Näiteks kui sisestatakse 1000000, siis tähendab see seda, et läbilaske soovitud väärtus on üks megabitt sekundis (Mbit/s). Apple'i kindlaks määratud nimega muutujasse Multicast Address kantakse sisse selle serveri aadress, mis teeb kettakujutise teistele kättesaadavaks. See on String-tüüpi muutuja ning sisestuse kirjapilt võib olla näiteks järgmine: 239.255.0.1. Plisti koostamiseks on olemas programm Property List Editor asukohas „/Developer/Applications/Utilities". See programm on saadaval installi-DVD-l programmipaketis Developer Tools. Kettakujutise kasutusseandmiseks võrgukeskkonnas tuleb ASR käivitada nagu server, kasutades selleks järgmist käsku:

sudo asr server –source /kataloog/Image.dmg
–config /kataloog/server.plist

Viimane tööetapp on kopeerimise käivitamine võrgu kaudu. Selleks tuleb klientsüsteemi asetada installi-DVD ning avada teenusprogrammide all terminal. Kopeerimisprotsessi käivitab järgmine käsk:

asr restore –source asr://Server IP aadress –target /Volumes/ Volumes –erase

Kõik see saab toimida vaid siis, kui klientsüsteemil õnnestub luua töötav võrguühendus.

Täiendavad kontrollküsimused:

- Kas koostatud Mac OS X kettakujutis vastab institutsiooni turbenõuetele?
- Kas Mac OS X kettakujutisi kontrollitakse pärast koostamist, et neis ei leiduks vigu?

M 4.381z Exchange'i System-andmebaaside krüpteerimine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: kasutaja, administraator

Microsoft Exchange'i andmesalvestid on andmebaasid, mis haldavad tsentraalselt näiteks kasutajate postkaste ja teisi olulisi serverivaldkonna andmeid. Microsoft Outlookis kasutatakse nn Personal Store'i (PST) Containeri tüüpi faile, mille struktuur sarnaneb andmebaaside omaga ning mis salvestavad andmemälust lokaalsesse klientsüsteemi kasutajapõhise koopia. PST-failide krüpteerimisvõimalusi mõjutab väga olulisel määral nii serveris kui ka lokaalses kliendis salvestamiseks valitud koht. Failide tasandil toimivatest krüpteerimisfunktsioonidest, nt Encrypted File Systemist (EFS), tuleks Exchange'i serveri andmemälufailide krüpteerimisel loobuda, sest seda liiki online -krüpteeringud Microsoft Exchange'i serveri jaoks ei sobi. Microsoft Outlooki lokaalsete PST-failide puhul tuleb arvestada järgmiste aspektidega:

- PST-faili salvestatakse erinevad kasutajaandmed: kaustad, meilid ja meilide lisad, kontaktandmed, kalender. PST-failide jaoks on olemas eraldi krüpteerimisfunktsioonid.
- Krüpteerimisprotsessi saab reguleerida kolmes järgnevas tugevusastmes:
- krüpteerimine puudub;
- tihendatud krüpteerimine: kasutatakse Outlooki enda protseduuri;
- tugev krüpteerimine: rakendatakse Outlooki enda protseduuri.
- Mitte ükski neist võimalustest ei kaitse konfidentsiaalseid andmeid piisavalt.
- PST-failides hoitavate andmete kaitsmiseks on soovitatav kasutada EFS-i, Windows BitLockeri ajamikrüpteeringut vms.
- Faile, mida on krüpteeritud funktsiooniga „Tugev krüpteerimine", tohib tihendatud olekus hoida ainult teatud tingimustel.
- Faili krüpteerimise käigus serveri ja kliendi vahel edastatavad andmed on krüpteerimata. See tähendab, et pealtkuulamise vältimiseks tuleb neid muul viisil kaitsta (vt M 5.125 SAP-süsteemi siseneva ja väljuva kommunikatsiooni kaitse).

Andmebaasi salvestatud infost ning sellele kehtivatest konfidentsiaalsus- ja terviklusnõuetest olenevalt tuleb andmeid vajaduse korral ka krüpteerida. Selleks tuleb kindlaks määrata krüpteerimise raamtingimused, nt Microsoft Exchange'i süsteemide turvapoliitikaga. Kasutajaid tuleb teavitada, milline on PST-failide tööpõhimõte ja kuidas toimivad nende krüpteerimisfunktsioonid. Selle meetme soovitusi saab versiooni 2010 puhul rakendada järgmiselt:

- Exchange'i andmebaaside krüpteerimiseks tuleb kasutada Windows BitLockeri ajamikrüpteeringut. Selle tootelahendusega saab protsessi kaasata nii andmebaasid kui ka tehingute logid, ilma et sellega kaasneks süsteemi jõudluse märkimisväärne langus. Microsoft Exchange Server 2010-t saab BitLockeriga krüpteerida alates operatsioonisüsteemist Windows Server 2008. Lisateavet leiate dokumendist „Microsoft Support Policy for Exchange 2007 Database Encryption: Exchange 2007 Help" Microsoft Technetis.
- PST- ja OST-failides hoitavate lokaalsete andmete kaitsmiseks on soovitatav kasutada kas EFS-i või Windows BitLockeri ajamikrüpteeringut.

Täiendavad kontrollküsimused:

- Kas PST-failide andmesalvestifailide krüpteerimiseks on olemas krüpteerimiskontseptsioon?
- Kas kasutajaid on teavitatud, milline on PST-failide tööpõhimõte ja kuidas toimivad nende krüpteerimisfunktsioonid?

M 4.382 OpenLDAP installatsioonipakettide valik ja kontrollimine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

OpenLDAP installatsioonipakettide valimisel tuleb olemasoleva taristu põhjal langetada otsus kas lähteteksti või binaarpaketi kasuks. Juhul kui kasutatakse mõnda operatsioonisüsteemi distrot, sisaldab see väga sageli ka OpenLDAP binaarpaketti. Sellega kaotatakse automaatselt sõltuvus muudest tarkvarapakettidest ja vajaminevad lisapaketid saab tagantjärele juurde installida. Ükskõik mis lahendust ka ei kasutata, esmalt tuleb alati välja valida ja hankida kõige uuem sobiv versioon ning kontrollida selle autentsust (vt M 1.1 Vastavus normidele ja eeskirjadele). Installitava tarkvara valimise ja päritolu kindlakstegemise protsess tuleks dokumenteerida sama moodi, nagu seda tehakse tarkvara tervikluse kontrollimise protsessi puhul.

Versiooni valimise põhitõed

OpenLDAP arendajad teevad lähteteksti kõige uuema versiooni ja sellele eelnenud versioonid kättesaadavaks enda tarkvara versioonihaldussüsteemi kaudu. Sellest versioonihaldussüsteemist on võimalik mis tahes ajal endale hankida kõikide failide kõige uuem versioon (*head branch*). Teatud ebareeglipäraste ajavahemike möödudes n-ö külmutatakse arendustöös juba saavutatud tulemus ja see lahutatakse muust arendustööst, st lahutatud seisundis tootele jäetakse teadlikult uued funktsioonid juurde lisamata (*feature freeze*). Selline tarkvara puhastatakse, seda katsetatakse ja see avaldatakse eraldi redaktsioonina (*release)*. Igale redaktsioonile lisatakse selle versiooni number kirjapildiga [tarkvarageneratsioon].[põhiversioon].[redaktsiooni nr], nt 2.4.23. OpenLDAP on avatud lähtekoodiga tarkvara, mida saab kasutada väga paljudes operatsioonisüsteemides ja erineval otstarbel. Seetõttu ei ole võimalik, et OpenLDAP arendajad suudaks välja töötada ühe konkreetse redaktsiooni, mis sobiks kõikidele mõeldavatele tarkvaradele ja kasutusjuhtudele. Samas töötavad OpenLDAP arendajad hoolikalt läbi kasutajatelt ja professionaalsetelt levitajatelt redaktsiooni kohta laekuva tagasiside. Kui redaktsioonis ilmnevad probleemid, koostatakse selle asemele enamasti uus redaktsioon. Redaktsioonid, mida on piisavalt kaua kasutanud nii professionaalsed levitajad kui ka kogenud kasutajad ning mille puhul pole probleeme tuvastatud, kuulutavad OpenLDAP arendajad stabiilseteks redaktsioonideks (*stable release*). Redaktsioonide kohta edastavad OpenLDAP arendajad teavet enda meililistis „openldap-announce” (`http://www.openldap.org/lists/openldap-announce`). OpenLDAP arendustöödest parema ülevaate saamiseks tuleks selle meililistiga liituda ja selle teated arhiveerida.

Installimine lähtetekstipaketist

OpenLDAP veebilehel on mitmeid linke maailma eri paigus asuvatele serveritele, kust saab alla laadida kõige uuemaid ja stabiilseid redaktsioone. FTP-serveriga on kättesaadavaks tehtud ka tarkvara vanemad versioonid. Lisaks saab versioonihaldussüsteemist endale hankida arendusmeeskonna kõige värskema tööversiooni ja tarkvara vahepealseid versioone, mida ei ole redaktsioonidena vormistatud. Tootmiskeskkondades tohib kasutada üksnes redaktsioone või stabiilseid redaktsioone. Soovitatav on kasutada kõige uuemat stabiilset redaktsiooni. Mitte mingil juhul ei tohi kasutada ei tarkvara kõige uuemat tööversiooni ega ka teisi, käitamiseks veel heaks kiitmata versioone. Siinkohal on oluline meeles pidada, et OpenLDAP arendajad ei kasuta lähtetekstipakettide kaitsmiseks digisignatuure. Seevastu iga redaktsiooni lähteteksti tihendatud versiooni (tgz-laiendiga failide)

jaoks arvutatakse siiski MD5- ja SHA1-protseduuriga välja ka räsiväärtused ning need avaldatakse meililistis „openldap-announce”. Enne paketi installimist tuleks võimaluse korral alati välja arvutada mõlemad räsiväärtused ja kontrollida, kas need langevad kokku avaldatud andmetega. Kui mõlema räsiväärtuse asemel otsustatakse kontrollida ainult üht, tuleks eelistada SHA1-protseduuri, sest see on turvalisem. Tarkvara ja andmeid räsiväärtuse kohta ei tohi alla laadida samal ajal samast serverist. Kontrollimiseks kasutatavad räsiväärtuste andmed tuleb hankida meililistist „openldap-announce”.

Installimine distro binaarpakettidest

OpenLDAP installimisel rakendatava distro ametlike installimisallikate puhul selgub vajamineva versiooni number enamasti distro levitaja tootevalikust. Paketihalduri kasutamisel (nt yum või rpm) hoolitseb paketihaldur ka pakettide autentsuse ja tervikluse kontrollimise eest.

Installimine võõraste allikate binaarpakettidest

Kui binaarpaketid hangitakse installimisallikatest, mis ei kuulu kasutatava distro versiooni hulka, tuleb kindlasti veenduda, et pakkuja on usaldusväärne. OpenLDAP puhul puudutab see eriti just Windowsi installipakette, mida saab küll alla laadida erinevatest tarkvaraportaalidest, kuid mis ei ole OpenLDAP arendajate tooted. Sel juhul peab versiooni valimine ning binaarpakettide tervikluse ja autentsuse kontrollimine toimuma järk-järgult, nagu on kirjeldatud alalõigus „Installimine lähtetekstipaketist” või „Installimine distro binaarpakettidest”.

Täiendavad kontrollküsimused:

- Kas OpenLDAP installipakettide päritolu dokumenteeritakse ja kas nende pakettide terviklust kontrollitakse?
- Kas on tagatud, et tootmiskeskkondades kasutatakse üksnes redaktsioone või stabiilseid redaktsioone?

M 4.383 OpenLDAP turvaline installimine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

OpenLDAP installimisel tuleb arvestada mitmete turvalisust otseselt mõjutavate asjaoludega. Käesolevas meetmes juhitakse tähelepanu üksnes olulistele punktidele.

Siin käsitletakse OpenLDAP installimist lähtetekstist. Operatsioonisüsteemide tootjate ja tarkvaralevitajate binaarpaketid võivad sellest erineda, kuid sõltuvussuhteid teiste rakendustega kirjeldatakse neil juhtudel enamasti vastavates binaarpakettides.

Lisateavet leiate OpenLDAP-ga kaasas olevast dokumentatsioonist, eeskätt juhendilehtedest (Manual Pages) ja configure -skripti väljaandest „help”.

Serveri kaitse

IT etalonturbe nõuete kohaselt tuleks kaitsta ka seda serverit, milles OpenLDAP-d käitatakse. OpenLDAP-ga töödeldavate kataloogide sisu tuleb salvestada mõnele lokaalsele andmekandjale, mida kontrollib serveri operatsioonisüsteem, sest sellistes jagatud failisüsteemides nagu NFS (Network File System) ei saa mõningaid OpenLDAP jaoks hädavajalikke funktsioone kasutada. Serveris peab olema ligipääs pordile 389. „ldaps://” kasutamisel (vt M 5.170 OpenLDAP-d kasutavate sideühenduste turve) tuleb avada ka port 636. Teiste teenuste käitamisest selles serveris tuleks hoiduda (vt M 4.97z Ainult üks teenus serveri kohta).

Täiendavad tarkvaratooted

OpenLDAP installimisel tuleb kontrollida, kas planeerimise raames (vt M 2.484 OpenLDAP planeerimine) kindlaks määratud lisarakenduste puhul on installitud ühilduvad versioonid. See kehtib eriti Berkeley DB kohta. Kui see on juba installitud, saab selle versiooni välja lugeda „db.h” faili sissekandest „DB_VERSION_STRING”. Selle faili salvestuskoht oleneb Berkeley DB installatsioonidest, nt Unixi ja Linuxi süsteemi puhul on levinud asukohad „/usr/include/db.h”, „/usr/local/include/db.h” ja „/usr/local/BerkeleyDB/include/db.h”. Operatsioonisüsteemi distro kasutamisel saab versiooni teada ka paketihaldussüsteemist (package manager). Kui installida tuleb teisi rakendusi, võib oluliseks osutuda ka installimistööde järjekord, et iga rakenduse jaoks vajalik päiseinfo (header) üles leitaks.

Mõistlik installimisjärjekord on näiteks järgmine:

1. OpenSSL või GnuTLS,
2. Berkeley DB,
3. Heimdali Kerberos või MIT Kerberos,
4. Cyrus SASL,
5. OpenLDAP,
6. Heimdali Kerberos (kui seda ei installitud kolmandana),

7. Cyrus-SASL.

Heimdali Kerberose (mitte MIT Kerberose) kahekordne installimine ja Cyrus SASL-i installimine nii enne kui ka pärast OpenLDAP-d võib olla vajalik selleks, et need programmid saaksid oma kasutajaandmed omakorda OpenLDAP-sse salvestada.

OpenLDAP tõlkimine ja installimine

Lähtetekstipaketi lahtipakkimiseks tuleks kasutada mõnd sellist kasutajakontot, millel ei ole suuri volitusi, ning pakett tuleks konfigureerida configure -skriptiga.

Tagaprogrammid (backends) ja katted (overlays), mida ei soovita kasutada, tuleb konfigureerimisparameetritega installimisest välja jätta, sest muidu võib nendega (nagu mis tahes installitud tarkvaraga) kaasneda turvaaukude ja väärkonfiguratsioonide oht. Lisaks tuleks arvesse võtta, et installimisel, st configure -skriptis kasutatud parameetrid mõjutavad ka seda, millist konfiguratsiooni tuleb kasutada. Näiteks võivad tagaprogrammid ja katted olla püsivalt sisse kompileeritud, kuid neid saab ka dünaamiliselt moodulitena laadida. Kui aktiveeritakse dünaamiline laadimine, ei saa OpenLDAP-d niisama lihtsalt kasutada konfiguratsiooniga, mis eeldab püsivalt sisse kompileeritud tagaprogramme ja katteid. Pärast paketi konfigureerimist tuleb esmalt käivitada „make depend", et määrata eelloetletud rakenduste jaoks kindlaks sõltuvussuhted, ja alles seejärel tuleb OpenLDAP tõlkida, kasutades selleks käsku „make". Tõlgitud tarkvara tuleks kirjeldatud sõltuvussuhete tõttu kontrollida käsuga „make test". Tavapärasest suuremaid volitusi võib vaja minna alles viimases sammus, kus tõlgitud programm installitakse tegelikult käsuga „make install". Kui aga väikeste volitustega kasutajakontol on kõikide installimise sihtkataloogide jaoks olemas kirjutamisõigused, saab isegi selle viimase sammu teha ilma root -volitusteta. Nii suurendatakse installimisprotsessi turvet, sest vigane või manipuleeritud programm saab sel juhul enda käsutusse ainult piiratud volitused. Kui OpenLDAP tõlgitakse lähtetekstist, tuleb selleks valitud parameetrid täpselt dokumenteerida. Lisaks on soovitatav konfigureerimise ja tõlkimise protseduuri tulemuste kohta koostada logi (nt suunates väljundiandmed edasi mõnda faili) ja see säilitada. Kõik installimisetapid tuleks dokumenteerida, et neid oleks võimalik hädaolukordades kiiresti korrata. See ei puuduta mitte üksnes tõlkimiseks kasutatud seadistusi, vaid ka installimise sihtkohti, volitusi, konfiguratsioonimuudatusi jms teavet. slapd-server tuleks üldjuhul käivitada operatsioonisüsteemi startup -skriptidega. Nii on slapd-server pärast serveri taaskäivitust kohe kasutusvalmis, mis tagab, et näiteks serveri käivitamisel ei unustata ühtki parameetrit.

Kontrollküsimused:

- Kas lokaalsete paketifiltrite kasutamisel on slapd-serveri jaoks vajalikud pordid kasutusele võetud?
- Kas OpenLDAP installatsiooni puhul on tagatud arusaadav dokumenteerimine?
- Kas OpenLDAP jaoks tõlgitakse ainult sellised tagaprogrammid (backends) ja katted (overlays), mida ka reaalselt kasutatakse?
- Kas rakenduste puhul, millest sõltub OpenLDAP töö, kontrollitakse, et installitaks ühilduvad versioonid?

M 4.384 OpenLDAP turvaline konfiguratsioon

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

Meetmes kirjeldatakse, kuidas slapd-serverit korrektselt konfigureerida, et see täidaks oma ülesandeid võimalikult turvaliselt. Kataloogiteenuse andmete turvalisuse tagamiseks on tarvis, et ka kataloogiteenust kasutavate klientrakenduste konfiguratsioon oleks turvaline. Selleks võib, kuid ei pea kasutama OpenLDAP ldap*-tarkvaratööriistu. IT etalonturbe kataloogide piiratud maht ei võimalda siinkohal esitada täpset ülevaadet kõikidest võimalikest tarkvaralahendustest. Palju tähtsam on tagada slapd-serveri turvaline konfiguratsioon, et ei tekiks liigset sõltuvust rakendatavate klientide turvaseadistustest.

Erinevad konfigureerimisvõimalused

Alates OpenLDAP versioonist 2.3 on slapd-serveri konfigureerimiseks kaks võimalust. Klassikaline konfigureerimisviis on sisestada kõik seadistused faili nimega slapd.conf. OpenLDAP salvestab selle faili Unixi ja Linuxi süsteemides asukohta „usr/local/etc/openldap/slapd.conf", kuid salvestuskoht võib asuda ka mujal, eriti kui kasutatakse distro spetsiifikat järgivaid installipakette. Alates versioonist OpenLDAP 2.3 on täiendusena kasutusele võetud andmevorming slapd-config.

See on hierarhiline andmebaas, mis salvestatakse LDIF-failidena kas asukohta „/usr/local/etc/openldap/slapd.d" või mõnda teise, distro eripära järgivasse asukohta.

Iga kord, kui muudetakse slapd.conf-faili, tuleb slapd-server taaskäivitada.

Siin avaldubki slapd-config-faili peamine eelis slapd.conf-faili ees: slapd-config-faili saab muuta ka tööd katkestamata. Seetõttu kasutatakse slapd-config-andmebaasi käsitlustes sageli ka termineid „ online -konfiguratsioon" ja mõnikord ka RunTimeConfiguration (RTC). Online -konfiguratsioon moodustab enda kindlalt ette antud sufiksiga „CN=config" slapd-serveri kataloogipuu osa. Planeerimisel tuleb valida, millist konfiguratsioonimeetodit hakatakse kasutama, ning seejärel tuleb seda ka läbivalt ühtmoodi rakendada. Samuti tuleb arvestada, et slapd.conf-faili nähtavad muudatused ei kehti juhul, kui kasutatakse slapd-config-andmebaasi.

Kasutaja õigused operatsioonisüsteemi tasandil

Kui slapd.conf-failiga tehtavad muudatused rakenduvad juba faili muutmise ajal, siis online -konfiguratsiooni muudatuste jõustumiseks tuleb need muutmiskäskude ja LDAP-protokolliga eraldi käivitada. Sellest järeldub, et administraatoril, kes töötab slapd.conf-failiga, on kindlasti tarvis ka juurdepääsu slapd-serverit käitava IT-süsteemi failisüsteemile. Seevastu kasutajad, kelle kontekstis slapd-server töötab, peaksid saama sellele failile üksnes lugemisõigusega juurdepääsu. Kui konfigureerimistöid tehakse slapd-config-andmebaasiga, piisab ka kataloogiteenuse tavalisest kasutajakontost, kuid süsteemi kasutajal, kelle kontekstis slapd-server tööle pannakse, peab andmebaasikataloogile olema kirjutamisõigusega juurdepääs.

Olukordades, kus OpenLDAP installimiseks ja seadistamiseks on kasutatud root -volitusi, juhtub sageli, et kataloogi jaoks on kehtestatud valet tüüpi volitused.

See võib viia vale järelduseni, et slapd-serveri käitamiseks on kindlasti tarvis root-volitusi.

Konfiguratsiooni struktuur

OpenLDAP konfiguratsiooniseadistusi nimetatakse direktiividеks. Direktiivid liigituvad globaalseteks, tagaprogrammide (backend) ja andmebaaside direktiividеks.

Globaalseid direktiive nimetatakse mõnikord ka font-end -direktiividеks, et eristada neid backend 'idest ja andmebaasidest. Direktiivid toetuvad hierarhiliselt üksteise peale: globaalsete ehk front-end -direktiivide mõju võivad tühistada backend -direktiivid ning backend -direktiivide mõju võivad omakorda tühistada andmebaasidirektiivid.

Direktiividel võib olla ka sub -direktiive, millega saab direktiivi jaoks kehtestada lisaseadistusi. Seda esineb eriti backend 'ide ja overlay 'de puhul, mida käivitatakse direktiividega ja konfigureeritakse sub -direktiiviga.

slapd.conf-faili muutmine slapd-config-failiks

Mõlema konfigureerimisvõimaluse direktiivide vahel on mõningad otsesed seosed ning slapd-config-andmebaasi vastavale atribuudile lisatakse üldjuhul ette tähekombinatsioon olc (tähistab online -konfiguratsiooni). Nii näiteks on slapd.conf-i backend 'i vaste slapd-config-andmebaasis olcBackend. Kõik OpenLDAP slap*-tööriistad suudavad klassikalise konfiguratsiooni muuta online -konfiguratsiooniks, kasutades selleks parameetrit „?f", millega tähistatakse slapd.conf-i paiknemist, ja parameetrit „-F", mis määrab kindlaks slapd-configandmebaasi sihtkataloogi. Näide: slaptest -f /usr/local/etc/openldap/slapd.conf -F /usr/local/etc/openldap/slapd.d. Ükskõik kumma konfigureerimismeetodi kasuks ka ei otsustata, on tähtis, et uute ja ka muudetud konfiguratsioonide süntaksit kontrollitaks alati slaptest-tööriistaga. Süntaksi õigsust tuleb kontrollida kindlasti enne slapd-serveri käivitamist uute parameetritega. Kui töötava süsteemi online -konfiguratsiooni muutmisel tehakse mõni loata seadistus, jätab slapd-server sobimatud muudatused üle võtmata. Kõik konfiguratsiooni seadistused tuleb dokumenteerida, et neid oleks võimalik hädaolukordades kiiresti korrata.

slapd.conf

slapd.conf-faili süntaks vastab RFC 2849-s defineeritud LDAP Data Interchange Formati (LDIF) andmevormingule, mis peaks olema administraatoritele tuttav. Konfiguratsioonifail slapd.conf algab globaalsete direktiividega. Globaalsed direktiivid sisaldavad skeemi spetsifikatsioone. Kuna skeemi sisestamine slapd.conf-faili võib osutuda väga töömahukaks, on soovitatav koostada skeemi jaoks eraldi lokaalne fail ning see fail ja slapd.conf-konfiguratsioonifail üheskoos include 'iga käivitada. Globaalsetele direktiividele peavad järgnema backend -direktiivid, juhul kui neid kasutatakse. Need algavad direktiiviga „backend ", mille puhul „" osutab

backend 'ile, st see on tüübinimi ilma sufiksita „back-", nt „backend hdb". Sellele järgnevad direktiivid ei ole enam global -tüüpi, vaid kehtivad üksnes kõikidele seda tüüpi andmebaasidele. Andmebaasidirektiivid algavad direktiiviga „database " ning „" on analoogne backend 'idega, st määrab kindlaks andmebaasi tüübi. Sellele järgnevad direktiivid kehtivad ainult selle andmebaasi kohta. Oluline on meeles pidada, et juba olemasoleva andmebaasi tüüpi ei tohi muuta lihtsalt andmebaasi teistsuguse käivitusviisi kasutuselevõtuga. See ei mõjuta mitte kuidagi juba olemasolevaid andmestruktuure, mis võivad erinevate andmebaasitüüpide puhul olla erinevad.

slapd-config

slapd-config-andmebaasi konfiguratsiooni osapuusse (subtree) sisestatakse globaalsed direktiivid kas väärtustena vahemikus „CN=config" või spetsiaalsesse Dummy-andmebaasi „olcDatabase=frontend, CN=config". Skeemid on „CN=schema, CN=config" osapuu lapselemendid. Backend 'id ja andmebaasid on omakorda „CN=config" lapselemendid. Algkonfiguratsiooni koostamiseks saab kasutada olemasoleva slapd.conf-konfiguratsioonifaili teisendamist, kuid koostada võib ka LDIF-andmevormingus sufiksi „CN=config" koos selle elementidega ning seejärel selle slapadd abil kataloogiteenusesse importida. Tuleks arvestada, et slap-config-konfiguratsiooni ei tohi muuta slapd.d-andmebaasikataloogis asuvate LDIF-failide kohandamisega. Vastasel korral jääksid operatsiooniatribuutidena kasutatavad ajatemplid värskendamata. Neid muudatusi slapd-server ei märkaks ega saaks neid rakendada.

Overlay 'd

Overlay 'd käivitatakse slapd.conf-konfiguratsioonifailis kas globaalsete direktiivide juures või mõnes andmebaasi lõigus. Overlay 'd tuleks käivitada alles pärast kõiki teisi andmebaasi spetsiifikat järgivaid direktiive, et vältida väärkonfiguratsioone, mille puhul andmebaasidirektiive käsitletaks kui overlay 'de alamdirektiive. slapd-config-andmebaasis on overlay 'de puhul tegu kas „CN=config" lapselementidega (globaalsed overlay 'd) või andmebaasielementidega (andmebaasi spetsiifikaga seotud overlay 'd). Kuna overlay 'de toimimist võib suuresti mõjutada nende käivitamisjärjekord, tuleb neid konfiguratsiooni lisades olla väga hoolikas.

slapd.conf-konfiguratsioonifailis käivitatakse overlay 'd järjekorras, mis on vastupidine nende asukohale failis. Järgnevalt tuuakse mõningaid näiteid olulisematest ja turbega seotud direktiividest, mille standardväärtusi tuleks konfigureerimisel kontrollida ja vajaduse korral ka kohandada.

Lisateavet direktiivide kohta leiate OpenLDAP Administrator's Guide'ist ja juhendilehtedelt (Man Pages):

- suffix ja olcSuffix (andmebaasidirektiiv) - See on andmebaasi käivitamise olulisim alamdirektiiv. Sellega määratakse kindlaks, milline kataloogi osa tuleb salvestada andmebaasi, nt „DC=ria, DC=riigiasutus, DC=ee". Kui andmebaas peaks sisaldama ka mõnda struktuuris allpool paiknevat, kuid kõrgema struktuuriastmega seotud alampuud, tuleb esmalt käivitada madala-

ma struktuuriastme andmebaas ja alles seejärel kõrgema astme oma. Näiteks tuleb „DC=etalonturve, DC=ria, DC=riigiasutus, DC=ee” defineerida enne „DC=ria, DC=riigiasutus, DC=ee”-d, sest muidu valib süsteem tööks üksnes kõrgema struktuuriastme andmebaasi.

- include (ainult slapd.conf) - Selle direktiiviga saab tekitada lingi väljaspool slapd.conf-konfiguratsioonifaili paiknevatele failidele ning sellisel juhul hakatakse slapd.conf-faili läbi töötades direktiivi sisu asemel analüüsima vastavate failide sisu. Seda direktiivi on soovitatav kasutada näiteks siis, kui on vaja lahutada skeemidefinitsioonide ja pääsuloendite haldamist. Direktiivi saab kasutada ka selle välistes failides. Samas tuleb arvestada, et slapd-server ei oska tuvastada ringviiteid, mis võib lõppeda sellega, et süsteem hakkab sisse lugema lõputuna näivat konfiguratsiooni (slapd.conf sisaldab ka include ACL1.conf-i, ACL1.conf sisaldab ka include ACL2.conf-i, ACL2.conf sisaldab ka include ACL1.conf-i). Sellises olukorras muutub slapd-server kasutuskõlbmatuks ning kogu IT-süsteemi töö võib seiskuda, sest slapd-serveri ressursivajadus muutub ülemäära suureks. Samuti tuleb pöörata tähelepanu sellele, et slapd-serveri käitamiseks vajalik kasutajatunnus saaks lugemisõigusega juurdepääsu välistele failidele. Kui slapd.conf-konfiguratsioon teisendatakse slapd-config-konfiguratsiooniks, kaasatakse sellesse ka include'iga juurde lisatud failid.
- idleTimeout ja olcIdleTimeout (globaalne direktiiv) - Selle direktiiviga määratakse kindlaks väärtus sekundites, mille järel kliendiga loodud, kuid mittekasutatav ühendus kohustuslikus korras katkestatakse (unbind). Algseadistuses on selle direktiivi väärtuseks määratud null, mis tähendab, et see on desaktiveeritud. Direktiivi väärtus tuleks kindlasti seadistada suuremaks kui null, et mittekasutatavaid ühendusi ebakorrektselt välja lülitatud klientsüsteemidega või tähelepanuta jäetud tööjaamadega ei saaks ära kasutada rünneteks. See, mis väärtus valida, tuleb hoolikalt läbi mõelda, et seadistus ei hakkaks pärssima institutsiooni harjumuspärast tööd. Mõistlik väärtus võiks olla väiksem kui 900 sekundit, mis tähendab, et mittekasutatavad ühendused suletakse hiljemalt 15 minuti möödudes.
- referral ja olcReferral (globaalne direktiiv) - Selle direktiiviga määratakse kindlaks LDAP-server, mis vastab slapd-serverile päringu esitanud kliendile slapd-serveri asemel ise, juhul kui slapd-server ei suuda kliendi soovitud operatsiooni täita. Käideldavuse suurendamiseks tuleks võimaluse korral selles direktiivis kasutada mõnda kõrgema struktuuritasandi LDAP-serverit.

Oluline on jälgida, et võrdsete volitustega serverite vahel ei seataks sisse ringviiteid, sest osale klientrakendustest võivad need jääda märkamatuks.

- readonly ja olcReadonly (andmebaasidirektiiv) - Selle direktiiviga lülitatakse andmebaas ainult lugemist võimaldavasse töörežiimi.
- rootDN ja olcRootDN ning rootPW ja olcRootPW (andmebaasidirektiivid) - Mõlemad direktiivid määravad kindlaks andmebaasi administraatori kasutajatunnuse ja selle juurde kuuluva parooli. Juurdepääsupiirangud ja limit 'id (vt M 4.387 OpenLDAP pääsuõiguste turvaline andmine) seda kasutajatunnust ei mõjuta. Parooli turvalist salvestamist, mida käsitletakse meetmes M 4.388 OpenLDAP turvaline autentimine , tuleb rakendada ka rootDN-parooli puhul.

- sizeLimit ja olcSizeLimit (globaalne direktiiv) - See direktiiv piirab otsinguprotsessi tulemuste arvu. Direktiivi algne seadistusväärtus on 500. Selle väärtuse sobivust tuleks analüüsida ja vajaduse korral muuta, kuid mitte mingil juhul ei tohiks seadistuseks valida „unlimited", sest see lihtsustaks liigselt Denial-of-Service-ründeid ning võimaldaks andmebaasi täielikult kopeerida ka volitamata kasutajatel.
- timeLimit ja olcTimeLimit (globaalne direktiiv) - Selle direktiiviga määratakse kindlaks aeg sekundites, mille täitumisel otsing katkestatakse. Direktiivi algne seadistusväärtus on 3600. Selle väärtuse sobivust tuleks analüüsida ja vajaduse korral muuta, kuid mitte mingil juhul ei tohiks seadistuseks valida „unlimited", sest see lihtsustaks liigselt kataloogiteenuse vastu suunatud Denial-of-Service-ründeid.
- limits ja olcLimits (andmebaasidirektiiv) - See direktiiv võimaldab andmebaasi tasandil kehtestada piiranguid sarnaselt direktiividega sizeLimit ja timeLimit.

Selle rakendamisel globaalsete piirangutega ei arvestata. Piiranguid on võimalik kehtestada ka kasutajapõhiselt. Kasutajaandmed sisestatakse sama moodi nagu pääsuloendite korral (vt M 4.387 OpenLDAP pääsuõiguste turvaline andmine). Kasutajapõhiseid piiranguid (limits) on soovitatav kasutada näiteks selleks, et autentimata kasutajad ei saaks kataloogistruktuuriga tutvuda ega leevendada piiranguid, mis võivad takistada replikeerimist.

Teisi direktiive käsitletakse ülejäänud OpenLDAP meetmetes, peamiselt aga meetmes M 4.385 OpenLDAP kasutatava andmebaasi konfiguratsioon .

Kontrollküsimused:

- Kas OpenLDAP konfigureerimiseks slapd.conf-failiga on operatsioonisüsteemi jaoks kindlaks määratud õiged volitused
- Kas kõikide OpenLDAP oluliste konfiguratsioonidirektiivide seadistusväärtusi kontrollitakse ja vajaduse korral muudetakse?
- Kas OpenLDAP konfiguratsiooni on kaasatud ka backend 'ide ja overlay 'de alamdirektiivid?
- Kas OpenLDAP-s tehtavate otsingute jaoks kehtestatakse sobivad suuruse- ja ajapiirangud?
- Kas slapd-serveri konfiguratsiooni kontrollitakse iga kord pärast muudatuste tegemist tarkvaratööriistaga slaptest ja kas need kontrollid dokumenteeritakse arusaadavalt?

M 4.385 OpenLDAP kasutatava andmebaasi konfiguratsioon

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

OpenLDAP-s saab konfiguratsioonidirektiividega seadistada tegelikult kasutatavat andmebaaside haldussüsteemi (DBMS). Seadistusi on võimalik teha ainult Berkeley DB jaoks, kasutades selleks tagaprogramme back-bdb või back-hdb. Need ei mõjuta küll vahetult OpenLDAP tööd ega selle kasutamist, kuid neil on oluline mõju kataloogiteenuse jõudlusele. Allpool on esitatud loetelu turvet puudutavatest seadistustest ja sagedastest veaallikatest. Täiendavate seadistuste tegemiseks tuleks vajaduse korral pöörduda andmebaaside spetsialisti poole. Näiteks on võimalik vahesalvestamise ja tehingulogide seadistamisega saavutada eeliseid kiiruses, kuid seda tehakse optimaalse tervikluse arvelt, mistõttu tuleb nende seadistusvõimaluste puhul lähtuda konkreetsest olukorrast:

- dbDirectory ja olcDbDirectory - Selle direktiiviga saab slapd-serverit käitavas IT-süsteemis kindlaks määrata andmebaasifailide salvestuskoha. Kasutajatunnusel, mille kontekstis OpenLDAP käivitatakse, peavad olema vastava kataloogi jaoks kirjutamisõigused.
- dbConfig ja olcDbConfig - Selles direktiivis tehtud seadistused olenevad andmebaasist ja need kirjutatakse DBMS-i faili DB_CONFIG. Kui sellist faili pole, luuakse see selle direktiivi kasutamisega. Kindlasti tuleb arvestada, et sihtfaili hilisemad (nt tekstiredaktoriga tehtud) muudatused kirjutavad siin valitud seadistused üle. Seepärast peab olema täpselt kindlaks määratud, kuidas seadistada, kes seda teeb ning kus seda tehakse. Direktiivi muudatustega kaasneb alati DBMS-i, kuid mitte slapd-serveri taaskäivitamine. Olenevalt andmebaasis tehtud seadistuste mahust võib selleks kuluda üpris palju aega ning selle aja vältel ei saa kataloogiteenust kasutada. Seega tuleb andmebaasi konfiguratsiooni muutmisi hoolikalt planeerida ja võimaluse korral teha neid hoolduseks ettenähtud aegadel, nt öösel või nädalavahetusel.
- dbIndex ja olcDbIndex - Selle direktiiviga saab kataloogiteenuse objektide jaoks kindlaks määrata atribuudid, mille kohta tuleb koostada indeks. Ilma indeksita tuleks iga otsingu käigus pöörduda kõikide objektide poole ja need üle kontrollida. Indeksit tuleks kindlasti kasutada sagedaste otsingute abistamiseks, sest see võimaldab ühtlasi suurendada käideldavust. Puuduvad, kuid vajalikud indeksid on nähtavad OpenLDAP logides (vt M 1.1 Vastavus normidele ja eeskirjadele). Kui sinna ilmub sageli teade, et juurdepääs teatud atribuudiindeksile ebaõnnestus, tuleks vastav indeks luua. Direktiivis toodud indeksid koostab slapd-server automaatselt. Kui slapd-serveri töö peatatakse indeksi koostamise ajal, siis hiljem see protsess enam automaatselt ei jätku. Sel juhul tuleb indeks koostada käsitsi tööriistaga slapindex.
- dbMode ja olcDbMode - Selle direktiiviga määratakse kindlaks uutele andmebaasifailidele kehtivad kasutajaõigused. Algseadistus 0600 või -rw——- annab juurdepääsu ainult sellele kasutajatunnusele, mille kontekstis slapd-serverit käitatakse. Selline algseadistus on mõistlik ja seda ei tohiks muuta.

Täiendav kontrollküsimus:

- Kas uute andmebaasifailide pääsuõigused on piiratud selle kasutajatunnusega, mille kontekstis slapd-serverit käitatakse?

M 4.386 Atribuutide piiramine OpenLDAP puhul

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraato r

slapd-serveri saab katete (overlays) abil sundida rakendama piiranguid, ilma et selleks oleks tarvis olemasolevaid skeeme mugandada või uusi skeeme koostada. Sellised piirangud on kataloogiteenuse sisu kvaliteedi ja tervikluse parandamise seisukohalt väga mõistlikud. Kasutada saab järgmisi katteid:

- Constraint - Constraint-kate (Constraints) võimaldab kehtestada kitsenduse, mis käsib, et väärtused vastaksid kindlatele regulaaravaldistele. Näiteks saab kehtestada sundreegli, mille kohaselt on atribuudiga „mail” võimalik siduda ainult enda organisatsiooni meiliaadressid.
- Unique - Unique-kate (Attribute Uniqueness) lubab väljavalitud väärtusel esineda kataloogipuus ainult ühe korra. Nii saab vältida olukorda, kus personaalne numbrikood määrataks korraga kahele kasutajale.
- Refint - Refint-kate (Referential Integrity) tagab viiteatribuutide viidete tervikluse. Näiteks kui Distinguished Names (DN) sisestatakse grupi liikmetena või kui ülemuse DN kantakse mõnda kaastöötaja atribuuti, siis muudab refint-kate neid viiteid juhul, kui muudetakse vastavat DN-i. Selleks algatab refint iga DN-i muutmisel otsingu, et kontrollida, kas DN on sellistesse atribuutidesse kantud. Refint-kate viib muudatused atribuuti ning kui atribuut kustutatakse, kustutab kate ka DN-i. Tähelepanu: kui kate eemaldab grupist viimase liikme, siis lisatakse selle asemele alamdirektiivis „refint_nothing” defineeritud DN, sest tühjad grupid võivad rikkuda grupi skeemi. Seejuures tuleb jälgida, et selleks määrataks sobiv DN, nt ametlik administraator. Nii ei saa väiksemate õigustega DN gruppi kuuludes endale liigseid õigusi.

Selliste piirangute puhul tuleb arvestada, et need kehtivad ainult uute või muudetud atribuutide ja objektide kohta. Nende katete piirangud ei avalda mõju olukordades, kus enne katete aktiveerimist on rikutud reegleid või kui ebasobivaid andmehulki lisatakse kasutatavasse andmebaasi otsejuurdepääsuga. Selliseid piiranguid tohib rakendada ainult kasutajaandmetele. Kui piiranguid kasutatakse näiteks operatsiooniatribuutide etteandmiseks või sunniviisiliselt slapd-config-konfiguratsiooni piires, võivad tagajärjed olla ettearvamatud ning slapd-server võib muutuda koguni kasutuskõlbmatuks.

Täiendav kontrollküsimus:

- Kas OpenLDAP atribuutide piiranguid rakendatakse eranditult ainult kasutajaandmetele, mitte operatsiooniatribuutidele?

M 4.387 OpenLDAP pääsuõiguste turvaline andmine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

Pääsuõiguste õige andmine ja rakendamine on infoturbe tagamise elementaarsed eeldused. Alati, kui kasutaja tahab teha kataloogiteenuse objektiga mõnd operatsiooni, tuleb otsustada, kas see operatsioon on lubatud. Rakendada tuleb volituste kontseptsiooni, nagu on kirjeldatud meetmes M 1.1 Vastavus normidele ja eeskirjadele . Selles kehtestatud reeglid tuleb OpenLDAP jaoks tehniliselt ellu viia (vt M 4.309 Kataloogiteenuste pääsuõiguste seadmine). LDAP standard kehtestab vaid juurdepääsukontrolli kohustuse ja defineerib standardi raames serveri vastused olukordadeks, kus operatsioonidest keeldutakse ebapiisavate volituste tõttu. Juurdepääsukontrolli täpset rakendust LDAP standardis lähemalt aga ei kirjeldata ning see sõltub suurel määral kasutatud kataloogiteenusest. Seepärast selgitatakse selle meetme raames põhjalikult pääsuõiguste andmist OpenLDAP-s.

OpenLDAP pääsuloendid

OpenLDAP-s hallatakse pääsuloendeid (Access Control Lists – ACLs) konfiguratsioonisiseste direktiividena. Iga operatsiooni puhul, mille kasutaja algatab, kontrollitakse, kas sellele vastab mõni direktiiv. Juurdepääsudirektiivi süntaks on järgmine:

access to [sihtobjekt]
by [kasutaja] [kasutajaõiguste komplekt]
by [kasutaja] [kasutajaõiguste komplekt]
. . .

Sihtobjektid võivad seejuures olla ka sufiksid, objektid ja atribuudid. Siin saab kindlaks määrata isegi LDAP otsingutulemused ja teatud atribuudimääratlused. Detailsus ja kombinatsioonide arv on siinkohal peaaegu piiramatud, mistõttu ei saa siin neid kõiki lähemalt kirjeldada. Eriti tuleb aga esile tõsta sihtobjekti *, mis hõlmab kõiki kataloogiteenuse võimalikke sihtobjekte.

Kasutajad

Kasutajatele on OpenLDAP-s muu hulgas ette nähtud järgmised sissekanded:

- * (kõik kataloogiteenuse kasutajad, k.a autentimata kasutajad);
- anonymus (autentimata kasutajad);
- users [autenditud kasutajad (autenditud ja autentimata kasutajate eristamise kohta vt M 4.388 OpenLDAP turvaline autentimine)];
- self [kasutajad, kes on sidumisfunktsiooni (bind) kasutanud sihtobjekti identiteediga];
- Distinguished Names (DNs) (täielikult kvalifitseeritud kasutajad või regulaaravaldised);
- atribuudi filter (võimaldab anda juurdepääsu objektile, mille kasutaja on sisse kantud atribuuti, nt ühe konkreetse töötaja ülemusena);

- grupi atribuudid (pääsuõiguste juhtimine staatiliste või dünaamiliste grupipoliitikatega);
- IP-sissekanded (kõikidele kasutajatele, kelle klient pärineb kindlaks määratud IP-aadressiruumist või on seotud eelmääratud domeeniga).

OpenLDAP võimaldab küll pääsuõigusi juhtida ka IP-aadresside alusel, kuid sellest tuleks kindlasti loobuda, sest IP-aadresse on lihtne võltsida.

Kasutajaõiguste komplektid

Kasutajaõiguste komplektid jagunevad OpenLDAP-s järgmiselt:

- none : juurdepääsuõigused puuduvad;
- disclose : olemasolu kontroll vigade tuvastamiseks;
- auth : võimalik rakendada bind -funktsiooni sihtobjektina;
- compare : võrdlemine;
- search : otsingufiltrite rakendamine sihtobjekti suhtes;
- read : lugemisõigusega juurdepääs sihtobjektile;
- write : kirjutamisõigusega juurdepääs sihtobjektile (muutmine, nime muutmine, kustutamine);
- manage : täielik juurdepääs koos vajalike õigustega, et pääseda juurde ka operatsiooniatribuutidele.

Lisaks on olemas veel eriõigused, nagu „selfwrite”. See võimaldab kirjutada ainult enda DN-i, nt selleks, et hallata enda kuulumist erinevatesse gruppidesse. Iga kasutajaõiguste komplekt sisaldab automaatselt kõiki sellele eelneva komplekti õigusi. Näiteks lugemisõigusega „read” kaasnevad ka õigused sellisteks tegevusteks nagu „disclose”, „auth”, „compare” ja „search”. See on üldjuhul mõistlik lahendus ja enamasti piisab üksnes juurdepääsutasemete (access level) kasutamisest. Vajaduse korral saab õigusi anda ka täpsemalt, kasutades selleks privileegide operaatorit.

Mitu „by”-klauslit

Üksteisele järgnevate „by”-klauslite arv ei ole juurdepääsudirektiivi puhul piiratud, st ühe direktiivi piires võib neid olla mis tahes arv. Direktiivisisene kontrollimine peatatakse kohe, kui leitakse sobiv „by”-klausel. Selline olukord tekib siis, kui mõni „by”-klauslis nimetatud kasutaja langeb kokku päringu esitanud kasutajaga või sisaldab seda. Klassikaline juurdepääsudirektiiv on näiteks järgmine:

- access to *
- by self write
- by anonymus auth
- by group.exact=“CN=admin, ou=groups, DC=ria, DC=riigiasutus, DC=ee” write
- by users read

See direktiiv võimaldab igal kasutajal enda sissekannet muuta, anonüümsel kasutajal rakendada mis tahes sissekannet enda autentimiseks, administraatorigrupi liikmetel sissekandeid muuta ja autenditud kasutajal kõiki sissekandeid lugeda. Viimase „by”-klausli kirjapilt võiks olla ka „by * read”, kuid selle mõju oleks ikkagi sama. Kuna autentimata kasutajate suhtes toimib juba teine „by”-klausel, kontrollitakse neljandat klauslit ainult autenditud kasutajate puhul, kes pole administraatorid. Kui esimene ja neljas „by”-klausel oleksid omavahel ära vahetatud, puuduksid sissekannete kirjutamisõigused, sest „users”-klauslile järgnevad „group”-klausel ja „self”-klausel jääksid sel juhul töötlemata. Kui direktiivis ei leidu ühtki kasutajakirjet, mis langeks kokku päringut esitava kasutaja andmetega, siis ei anta talle ka õigusi. Kontrollimisel käsitletakse igat direktiivi, nagu lõppeks see klausliga „by * none”, ja seda ka siis, kui sellist klauslit seal kirjas ei ole.

Mitu juurdepääsudirektiivi

Üksteisele järgnevate juurdepääsudirektiivide arv pole piiratud. Direktiive töödeldakse järgemööda. Pääsuloendi edasikontrollimine peatatakse sobiva direktiivi leidmisel. Direktiiv on sobiv, kui päringus esitatud sihtobjekt vastab direktiivi sihtobjektile või sisaldub selles. Näiteks on direktiivide:

- access to dn.subtree=“DC=etalonturve, DC=ria, DC=riigiasutus, DC=ee”
- by users write
- access to dn.subtree=“DC=ria, DC=riigiasutus, DC=ee”
- by users read

tulemused, et autenditud kasutajad saavad lugeda fiktiivse osakataloogi ria.riigiasutus.ee kogu olemasolevat sisu ja neil on kirjutamisõigusega juurdepääs etalonturve.ria.riigiasutus.ee sisule. Kui direktiivid oleksid antud vastupidises järjekorras, puuduks kirjutamisõigus, sest operatsioon sihtobjektiga „DC=etalonturve” on juba „DC=ria, DC=riigiasutus, DC=ee” osahulk. Kui mitte ükski direktiivi sihtobjekti kirje ei lange kokku päringus esitatud sihtobjektiga, siis ei anta ka sihtobjektile õigusi. Kontrollimisel käsitletakse igat pääsuloendi nimekirja nii, nagu oleks see direktiivi „access to * by * none” lõpp, ka siis, kui seda pole seal kirjas.

Järjekord ja juhtlülitid (control flags)

Eelnevate näidete põhjal on selge, et pääsuloendite sissekannete järjekord on ülitähtis. Üldjuhul kehtib nõue, et esmajärjekorras tuleb defineerida eriõigused ja alles seejärel üldised õigused. Kui pärast sobiva reegli leidmist on siiski tarvis õigusi suurendada, saab seda teha juhtlülititega „continue” (et jätkata edasiste „by”-klauslite kontrollimist direktiivi piires) ja „break” (et jätkata edasiste direktiivide kontrollimist). Juhtlüliteid tuleks kasutada võimalikult vähe, sest nende korral väheneb pääsuloendi ülevaatlikkus. Arvestada tuleb sellega, et järgmine leitud sobiv reegel asendab juba antud õigusi. Kui pääsuloend on õigesti planeeritud, pole tegelikult juhtlülitit „continue” üldse vaja kasutada. Seda läheb tarvis ainult siis, kui kasutatakse „privilege”-operaatoreid. Juhtlüliti „break” sobib teatud väljavalitud kasutajatele mõeldud laiaulatuslike õiguste asetamiseks pääsuloendi algusse. Näiteks annab järgmine direktiiv replikeerimiseks loodud kasutajale kogu kataloogi suhtes lugemisõiguse, kuid kõikide teiste kasutajate puhul jäetakse see direktiiv n-ö lugemata:

- access to *
- by dn.exact=“[replikeerimiskasutaja DN]” read
- by * break
- pääsuloend slapd-config-is

Seni kirjeldatud süntaks kehtib slapd.conf-konfiguratsioonifailiga konfigureerimise kohta. Slapd-config-andmebaasi kasutamisel kehtib:

- olcAccess: {n}to [sihtobjekt]
- by [kasutaja] [kasutajaõiguste komplekt]
- by [kasutaja] [kasutajaõiguste komplekt]

Valikuline indeks {n} määrab kindlaks sissekannete järjekorra, mis ei saa erinevalt slapd.conf-konfiguratsioonifailist tuleneda nende asukohtadest failis, sest kataloogiteenuse olcAccess-objektid asetsevad samal tasandil. Ilma indeksita on konfiguratsioonisisene järjekord ja seega sissekannete toimimistõhusus ettearvamatu.

Globaalsed ja andmebaasipõhised pääsuloendid

Pääsuloendid võivad olla globaalsed või piirduda andmebaasi tasandiga. OpenLDAP rakendamisel peab nende seostega õigesti arvestama. Andmebaasidirektiivid on globaalsetest direktiividest prioriteetsemad. Seejuures järgneb globaalne pääsuloend andmebaasipõhisele ja kontrolli üldnimekiri lõpetatakse direktiiviga „access to * by * none”, ja seda ka siis, kui vastav sissekanne puudub. Seetõttu jäävad globaalse pääsuloendi alguses paiknevad eridirektiivid vastupidi soovitule sageli rakendamata, juhul kui neid kombineeritakse andmebaasipõhise pääsuloendiga.

Pääsuõigused grupikuuluvuse alusel

Õiguste andmine grupikuuluvuse alusel võimaldab organisatoorsel tasandil eraldada pääsuõiguste haldamist ja slapd-serveri tehnilist hooldamist. Pääsuõiguste haldamiseks tuleb muuta ainult grupiobjekte, juurdepääs konfiguratsioonile endale pole enam vajalik. Kui pääsuõigusi hallatakse grupikuuluvuse alusel, tuleb arvestada järgmiste punktidega:

- OpenLDAP versioonis 2.4 ei teisendata pääsuõigusi, kui grupid asuvad gruppide sees. OpenLDAP pakub lahenduseks Set-kontsepti. Seni, kuni versiooni 2.4 Setid on veel eksperimenteerimisfaasis, ei tohiks neid tootmiskeskkonnas kasutada.
- Soovitatav on kasutada memberof-katet (Member of). Kui DN seotakse grupiobjektiga, tagab memberof-kate, et vastav omadus märgitakse ka DN-is operatsiooniatribuudina ära. Seeläbi välditakse pääsukontrolli keerukaid otsinguid.

Veel üks viis hallata OpenLDAP-s pääsuõigusi väljaspool konfiguratsiooni on anda pääsuõigusi kasutajatele Access Control Informationi (ACI) mehhanismiga. Kahjuks on ACI seadistamine taas väga töömahukas, sest iga kasutaja tuleb eraldi sisse seada. Lisaks pole süntaksi mehhanism standardiseeritud, st versioonis 2.4 on mehhanism alles eksperimentaalne, mitte valmis tootelahendus. Seni, kuni ACI on eksperimenteerimisfaasis, ei tohiks seda kasutada.

Pääsuõiguste katsetamine

Igat pääsuloendisse tehtud muudatust tuleks kontrollida tööriistaga slapacl. Sellega simuleeritakse kasutajat ja operatsiooni ning kontrollitakse, kas kasutaja saaks selle operatsiooni edukalt lõpuni viia, kuid operatsioon ise jääb tegemata. Sellist kontrolli tuleks rakendada eriti siis, kui tahetakse mõnda juurdepääsu takistada. Tööriist slapacl võrdleb andmeid slapd.conf-konfiguratsioonifaili andmetega. Muudetud pääsuloend hakkab kehtima alles pärast slapd-serveri käivitamist või taaskäivitamist. Seepärast tuleks slap*-tööriistade kasutamisel slapd-serveri töö alati peatada. Isegi kui slap*-tööriistade kasutamisel serveri jaoks tehniline mõju puudub, võivad järeldused, mida tehakse töötava slapd-serveri puhul, siiski valeks osutuda. Järgmisteks juhtudeks on soovitatav tuletada volituste kontseptsioonist katsetamisprotsessid ja need slapacl-tööriistaga läbi katsetada:

- pääsuloendites tehtavad märkimisväärsed muudatused;
- uute tagaprogrammide, andmebaaside või sufiksite defineerimine;
- OpenLDAP värskendamine.

rootDN-ile piirangud ei kehti

Pääsuloendite mõju andmebaasi rootDN-ile üldjuhul ei laiene. Kui see siiski pääsuloenditesse kaasatakse, toob see kaasa üksnes haldustööde mahu kasvu ja süsteemi jõudluse vähenemise. Teisalt tuleb jälgida, et pääsuloenditest loobumine ei viiks olukorrani, kus lõppkokkuvõttes on OpenLDAP-s kataloogiteenusele juurdepääs ainult rootDN-il. Ilma pääsuloenditeta hakkab kehtima eelseadistus, mille järgi saavad kõik, st ka anonüümsed kasutajad, lugemisõiguse kogu kataloogiteenuse sisule. Pääsuloendite kasutamisest ei tohi mitte mingil juhul loobuda.

Pääsuõiguste keerukus

Pääsuloenditel on palju spetsiifilisi seadistusvõimalusi ja seetõttu pole ka loendite keerukusel peaaegu mitte mingisuguseid piire. Administraatorid peaksid tutvuma põhjalike näidiskonfiguratsioonidega, mille võib leida tasuta saadaolevast OpenLDAP Administrator's Guide'ist. Siiski juhime tähelepanu sellele, et antud meetmesse kogutud juurdepääsutasemeid (access levels) on juba praktikas kontrollitud ja tavaolukorras nendest pääsuõiguste andmiseks piisab. Võimalikult ettevaatlik tuleb aga olla just regulaaravaldiste ja otsingufiltritega, sest neid on väga kerge liiga mahukaks defineerida ja seega võivad need ekslikult anda ebasobivaid pääsuõigusi. Lisaks piiravad need märkimisväärselt pöörduste läbitöötamise kiirust, sest nende kontrollimiseks kulub palju ressursse. Mida laialdasemad on pääsuõigused slapd-serveri konfiguratsioonis, seda olulisem on need põhjalikult slapacl-iga läbi katsetada. Korduvate vigade korral tuleb pääsuõiguste ülesehitust põhjalikult muuta.

Täiendavad kontrollküsimused:

- Kas OpenLDAP objektidele juurdepääsemiseks viiakse volituste kontseptsioon tehniliselt ellu?
- Kas OpenLDAP rakendamisel on õigesti arvestatud globaalsete ja andmebaasipõhiste pääsuloendite seostega?

M 4.388 OpenLDAP turvaline autentimine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

OpenLDAP kasutamiseks on üldjuhul hädavajalik, et kataloogiteenus suudaks seanssi seostada kasutaja identiteediga. Ainult siis saab kataloogiteenust rakendada mõistlikult (nt operatsioonisüsteemi ressursside haldamiseks) ja vaid siis toimivad ka kindlaksmääratud pääsuõigused (vt M 1.1 Vastavus normidele ja eeskirjadele). Seepärast määratakse slapd-serveri bind -funktsiooniga kindlaks kasutaja identiteet. Kui seda ei tehta, on tegu anonüümse juurdepääsuga (anonymus). Kui bind 'i raames on identiteet ette antud, peab kasutaja tõestama, et tal tõesti on väidetud identiteet. Kui selline tõendamine pole vajalik, võib iga kasutaja logida sisse suvalise identiteediga. Sel juhul on tegu autentimata kasutamisega (unauthenticated).

Anonüümsed kasutajad

Kui OpenLDAP planeerimisel (vt M 2.484 OpenLDAP planeerimine) ei otsustatud, et kataloogiteenust võib kasutada anonüümselt, tuleb anonüümset kasutust takistada konfiguratsioonidirektiiviga „disallow bind_anon". Kui kataloogiteenus peab eristama kasutajaid, tuleb rakendada ka autentimist. Seega tohib ilma identiteedi tõestamiseta sisselogimist kasutada üksnes katsetamisel, mitte kusagil mujal. Autentimist tuleb sundida konfiguratsioonidirektiiviga „require authc".

Parooliga autentimine

Põhiline meetod, mida OpenLDAP kasutaja autentimiseks nõuab, on kasutajanime ja parooli kombinatsioon. Selle kohta kasutatakse terminit *simple bind* . Selline autentimismeetod on turvaline üksnes siis, kui kasutatavat parooli teab ainult vastav kasutaja.

Parooli edastamine

Standardi LDAPv3 spetsifikatsioonide kohaselt edastatakse autentimiseks vajalik parool serverile loetava teksti kujul. Kliendi ja serveri vaheline sideühendus peab olema krüpteeritud (vt M 5.170 OpenLDAP-d kasutavate sideühenduste turve), sest nii ei saa ründaja parooli pealt kuulata. On soovitatav teha sideühenduse krüpteerimine slapd-serveri poolt *bind* -operatsiooniga kohustuslikuks, mitte pakkuda seda ühe võimalusena. Vastasel korral sõltub ühenduse turvalisus kasutaja otsusest ja teadmistest ning kasutatud klienttarkvara võimalustest. Direktiiviga „security" saab globaalselt või andmebaasipõhiselt kindlaks määrata ühenduse turvalisusele kehtivad nõuded, määratledes erinevate operatsioonide krüpteerimistugevuse, nt „security simple_bind=XYZ". Tähed XYZ tuleb asendada Security Strength Factoriga (SSF). SSF on arv, mis tähistab krüpteerimismeetodit ja võtmepikkust, mida kasutatakse tegeliku teate krüpteerimiseks sümmeetrilise šifriga, nt 56 on DES, 112 on Triple DES ja 128, 192 või 256 on AES. Valida tuleks vähemalt 112. Mõistlik oleks arvestada ka uusimate uuringute ja BSI soovitustega. Direktiivis loetletud operatsioonidest keeldutakse, kui ühenduse turve osutub liiga nõrgaks.

Parooli salvestamine

Isegi kui on tagatud parooli turvaline ülekandmine, võib parool olla siiski serveri poolel jätkuvalt ohus. Kui server kompromiteeritakse või kui ründajal õnnestub juurde pääseda kataloogiteenuse objektide andmevarundusele, võib ta enda valdusse saada ka kasutajate paroolid. Seepärast tohib salvestada ainult paroolide kontrollsummasid ehk räsiväärtusi (*hash*). Siin tekib aga probleem, et LDAP-standard ei toeta paroolide *hash* -vormingut. OpenLDAP tagab *hash* -vormingus

paroolide salvestamise serveris ja toetab erinevaid *hash* -algoritme. Kasutada tuleks Secure Hash Algorithmi (SHA) grupi algoritmi varianti SSHA, st „soolatud" varianti. „Soolatud" tähendab, et parooli täiendatakse enne *hash* -väärtuse genereerimist veel lisaväärtusega, et raskendada sõnaraamaturündeid. Mitte mingil juhul ei tohi *hash* -algoritmiks valida CRYPT-i. CRYPT juurutatakse operatsioonisüsteemipõhiselt ja seepärast ei pruugi OpenLDAP-s autentimine pärast üleminekut teisele operatsioonisüsteemile enam töötada. slapd-serverile antakse direktiiviga „password-hash {algoritm}" käsk salvestada kataloogi ainult kindlaks määratud algoritmiga genereeritud parooli *hash* -väärtus. Looksulud on osa süntaksist, seega määratakse SSHA kasutamine kindlaks süntaksiga „password-hash {SSHA}". Direktiiv kehtib alati siis, kui slapd-serveri vahendusel, s.t rakendusega ldappasswd või mõne teise klientrakendusega, võetakse paroolid kasutusele või muudetakse neid. Kui *hash* -väärtust tahetakse kasutada LDIF-failide genereerimisel ja importimisel, peavad failis kuvatava „userPassword" andmevälja sissekanded juba *hash* -väärtustena olemas olema. Sama kehtib rootDN-parooli andmete kohta konfiguratsioonis (vt M 4.384 OpenLDAP turvaline konfiguratsioon). Paroolide *hash* -väärtuste genereerimiseks tuleb kasutada slap*-tööriista slappasswd. Parameetriga „-h" määratakse kindlaks kasutatav *hash* -algoritm, SSHA soovitatav väärtus on eelseadistus. Parameetri „-s" järel tuuakse loetava tekstina ära parool. Tööriista väljund tuleb seejärel eelseadistatud {SSHA} abil LDIF-faili või konfiguratsioonifaili üle võtta. Kui tööriista kasutatakse käsuviibaga, tuleb tavaolukorras alati aktiveeritud sisestuste ajaloo funktsioon välja lülitada, sest muidu salvestatakse parool loetava tekstina.

Parooli kvaliteet

Isegi kui parool edastatakse krüpteeritult ja see salvestatakse *hash* -väärtusena, jääb ikkagi oht, et kasutajad valivad endale liiga nõrgad paroolid. Neid on näiteks sõnaraamaturünnetega kerge lahti murda. Seega tuleb töökorralduslike meetmetega nõuda, et kasutajad väldiks nõrku paroole (vt M 2.11 Paroolide kasutamise reeglid). OpenLDAP toetab selliseid nõudeid tehniliselt kattega ppolicy (Password Policy). Selle abil saab kehtestada näiteks reeglid parooli minimaalse pikkuse, minimaalse ja maksimaalse vanuse ning võimaliku või vajaliku muutmise kohta. Lisaks saab sellega kontrollida paroolide kvaliteeti ja pidada kasutajapõhist varasemate paroolide nimekirja, mis tagab, et neid ei saa enam uuesti kasutada. Paroolireeglite kehtestamise kõrval suudab ppolicy-kate parooli atribuuti pärast korduvaid ebaõnnestunud autentimisi teatud ajaks igasuguse juurdepääsu eest ka täiesti ära blokeerida, et takistada paroolide vastu suunatud Brute-Force-ründeid. Vastavad andmed, nt parooli kohustuslik pikkus või lubatud logimiskatsete arv enne blokeerimist, saab detailselt kindlaks määrata suunistes (*policies*). Suunised võivad olla kasutajapõhised, aga need võivad kehtida ka kogu kataloogile ja ka osapuudele. ppolicy-kate rootDN-i ei piira.

Täiendavad autentimismehhanismid

OpenLDAP suudab kasutajate autentimisel rakendada ka teiste rakenduste funktsioone. Nii saab kasutada autentimismehhanisme, mis on kasutajatunnuse ja parooli kombinatsioonist turvalisemad (*strong bind*). Selleks läheb tarvis abstraktsioonikihti Simple Authentication and Security Layer (SASL). SASL toetab nn Mechide kaudu erinevaid autentimis- ja krüpteerimismehhanisme ning suudab ise omakorda kasutada väliseid meetodeid. Nii saab kasutajaid muu hulgas autentida SSL/TLS-sertifikaatidega (vt M 5.66 TLS-i/SSL-i kasutamine) või Kerberose krüpteerimisprotseduuriga. OpenLDAP suunab autentimisülesande edasi SASL-ile. Kui IT-koosluse turbevajadus on suur või väga suur või kui on juba ole-

mas OpenLDAP-väline autentimistaristu, tuleks sidumisfunktsiooni jaoks kasutada SASL-i.

Täiendavad kontrollküsimused:

- Kas on tagatud, et OpenLDAP kataloogiteenuses toimub autentimine eranditult läbi krüpteeritud ühenduste?
- Kas OpenLDAP paroole salvestatakse ainult hash -väärtustena ja kas selleks kasutatakse sobivat hash -algoritmi?

M 4.389 OpenLDAP partitsioonid ja replikatsioonid

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

Kataloogiteenuse osapuude ümberpaigutamine erinevatesse serveritesse (partitsioonide loomine) on efektiivne koormuse jaotamise viis, mis tagab süsteemi suurema käideldavuse. Selleks, et kataloogiteenuse andmetest tehtavad koopiad oleksid värsked, peavad serverid omavahel vahetama infot andmete võimalike muutuste kohta, kasutades selleks replikeerimist. Sobiva replikeerimismeetodi valimisel tuleb lähtuda võrguühendustest ja käideldavusele esitatud nõuetest. Meetmes kirjeldatakse nende kahe kontseptsiooni võimalikke lahendusi OpenLDAP jaoks, seevastu üldisemat teavet partitsioonide ja replikatsioonide planeerimise kohta leiate meetmest M 1.1 Vastavus normidele ja eeskirjadele .

Partitsioonide loomine

Kataloogiteenuste partitsioonide loomist on OpenLDAP keskkonnas väga lihtne konfigureerida. Kui mõnda kataloogi osa soovitakse kuhugi mujale ümber paigutada või kui serveril on tarvis teada, millises serveris hoitakse teatud osapuid, tuleb selle serveri globaalses konfiguratsioonis võtta referral- objektiklassi objektina kasutusele vastav sufiks. Eraldatud osapuud sisaldava serveri referentsaadress märgitakse ära atribuudiga ref. Klientide operatsioonidele, mis puudutavad kataloogiteenusest ümber paigutatud osa, vastab server viitega sellele aadressile. See seos kannab nimetust subordinate knowledge information . Server teab, millised kataloogipuu osad asuvad eri serverites. Kui soovitakse, et päringute korral hakkaks server enda seest kuhugi mujale ümber paigutatud osapuid ise läbi otsima, tuleb vastava andmebaasi ja serveri andmebaasi ühendamiseks kasutada kas direktiivi subordinate või olcSubordinate . Sellist tegevust nimetatakse liimimiseks (gluing). Alama astme serverile ei edastata aga täpset infot selle kohta, milliste teiste serverite osapuid salvestatakse kõrgema või võrdse astmega asukohtadesse. Kui mis tahes operatsioon ei sobi kokku serveri sufiksiga, vastatakse sellele globaalse viitega (referral), st päringu esitanud klient saab viite serverile, mis suudab võib-olla sellele päringule vastata. Partitsioonide korral sisestatakse siinkohal kõrgema astme kataloogiteenuse andmed. Referral kannab selle seose puhul ka veel nimetust superior knowledge information, kuigi direktiivi saab tegelikult kasutada ka partitsioonidest sõltumatult. Neid referral 'i aadressidega identifitseeritavaid kataloogiteenuseid ei pea käitama OpenLDAP-ga. Overlay 'ga chain (chaining) suudab server referral 'eid ka ise eristada. Nii jäävad partitsioonid kliendile märkamata, st kliendile laekub lõplik vastus alati sellest serverist, millesse ta enda päringu esitas. Selline lahendus ei sõltu kliendi suutlikkusest ja toimib ka siis, kui klient ei tule ise viidete töötlemisega toime.

Replikeerimine

OpenLDAP-s kasutatakse replikeerimiseks LDAP Sync Replication Engine'i (syncrepl) mehhanismi. See mehhanism on kohandatud koostööks Berkeley DB-ga ning selle kasutamist toetavad üksnes tagaprogrammid back-bdb ja back-hdb. See tähendab, et OpenLDAP-d ei saa niisama lihtsalt kasutada kataloogiteenuste replikeerimise agendina selliste kataloogiteenuste puhul, mis käsitlevad slapd-serverit kui tavalist proksit. Enne syncrepl-mehhanismi väljatöötamist kasutati replikeerimiseks Stand-Alone LDAP Update Replication Daemonit (slurpd). Nii nagu slapd-server, käivitati ka see lihtsalt teenusena ning sellega hallati kataloogiteenuse sisust tehtavaid koopiaid. Kuna see teenus ei töötanud usaldusväärselt, eemaldati see ametlikult OpenLDAP seest alates versioonist 2.4. Vananenud ver-

sioonide dokumentatsioonis kajastuvaid viiteid slurpd-le tuleb käsitleda ajaloolise arenguetapina. slurpd-d ei tohi mitte mingil juhul kasutada.

Master ja slave, provider ja consumer

Replikeerimisse kaasatud servereid nimetatakse traditsiooniliselt master 'iks ja slave 'iks. Master sisaldab tegelikku kataloogiteenust ja võimaldab kirjutamisõigusega juurdepääsu kataloogiteenuse sisule. Seevastu slave võtab üle üksnes kogu kataloogiteenuse andmed ja võimaldab lugemisõigusega juurdepääsu nende andmete koopiale. Sellist ranget lahusust alates OpenLDAP versioonist 2.3 enam ei järgita. OpenLDAP replikeerimisel võtab tarbija (consumer) teenus üle teenusepakkuja (provider) teenuse andmed. Siinkohal on tähtis mõista, et teenusepakkuja jaoks on tarbija klient, olgugi et tarbija võimaldab iseseisvalt enda replikatsiooni ka teistel klientidel kasutada, st toimib teiste klientide jaoks serverina. Tarbija-serveri turvaseadistused ei kehti teenusepakkujaga loodavale ühendusele. Selle asemel kehtib kliendi konfiguratsioon, mis tuleb tarbija puhul teha väga hoolikalt, kuigi seda ei ole serveri jaoks tegelikult tarvis. Eriti tuleb arvestada, et tarbija peab sidumisfunktsiooni bind kasutama teenusepakkuja suunal ning rakendatava kasutaja võimalikud juurdepääsu- ja otsingupiirangud võivad replikeerimisfunktsiooni tööd tõkestada.

refreshOnly ja refreshAndPersist

Replikeerimisel saab valida kahe režiimi vahel: Pull Mode ja Push Mode. Pull Mode'i replikeerimisrežiimi puhul, mis OpenLDAP-s kannab nime refreshOnly, uurib tarbija kindlate ajavahemike möödudes järele, kas teenusepakkujal esineb muudatusi. Selle protsessi käigus saadab tarbija andmed talle seni laekunud andmete värskuse kohta vormingus Sync Cookies. Saadud andmete põhjal algatab teenusepakkuja otsingu, mis peab kokku koguma alates tarbija märgitud ajast aset leidnud muudatused. Sel juhul teenusepakkuja tarbijat ei tunne, vaid vastab üksnes päringutele. Selleks, et otsingud annaks korrektseid tulemusi, on väga tähtis, et nii teenusepakkuja kui ka tarbija süsteemi kell oleksid võimalikult sünkroonis (vt M 4.348 Aja sünkroniseerimine virtuaalsetes IT-süsteemides). Push Mode'i replikeerimisrežiimi puhul, mis OpenLDAP-s kannab nime refreshAndPersist, jääb teenusepakkuja ja tarbija vaheline ühendus püsima ning teenusepakkuja saadab ise kõik võimalikud muudatused tarbijale edasi. Sobiva replikeerimismeetodi valimisel kehtib reegel, et refreshOnly on mõistlik kasutusele võtta eelkõige siis, kui replikeeritavad andmehulgad on suured, ning refreshAndPersist sobib eelkõige siis, kui peaeesmärk on teenusepakkuja võimalikult kiire värskendamine.

Replikeerimise kasutuselevõtt

Kataloogiteenuse replikeerimine OpenLDAP-ga koosneb mitmest sammust:

- Tarbija installimine (vt M 4.383 OpenLDAP turvaline installimine) ja konfigureerimine (vt M 4.384 OpenLDAP turvaline konfiguratsioon). Selleks saab kanda (ja võimaluse korral tuleks seda alati teha) teenusepakkuja konfiguratsiooni koopiad üle tarbijasse. Tarbija konfiguratsiooni puhul on väga oluline, et tarbijas võetaks kasutusele täpselt samad skeemid nagu teenusepakkujas.
- Tarbijas tuleb replikeeritava andmebaasi jaoks tööle seada andmebaasidirektiiv syncrepl. Seda, mida replikeerida, on võimalik kindlaks määrata alamdirektiividega searchbase, filter, scope ja attrs. Nii saab terve kataloogitee-

nuse täieliku replikeerimise asemel replikeerimisprotsessi kaasata üksnes osapuud või ka näiteks objektide teatud atribuudid. Sisseseadmisel tuleb arvestada eriti sellega, et online -konfiguratsiooni kasutamisel on replikeerimisprotsessi võimalik kaasata ka konfiguratsioonisufiks CN=config. Alamdirektiividega määratakse kindlaks ka teenusepakkuja aadress, tarbija ja teenusepakkuja vahelise andmeside turvamisega seotud spetsiifilised replikeerimisseadistused, replikeerimismeetod ja ühenduse taastamine teenusepakkujaga, kui ühendus peaks katkema (refreshAndPersist) või kui teenusepakkujaga ei õnnestu enam ühendust saada (refreshOnly).

- Muu hulgas juhime teie tähelepanu alamdirektiivile schemachecking. Kui schemachecking on desaktiveeritud (vastab eelseadistusele), saab replikeerimisega sisestada ka selliseid andmeid, mis on skeemide põhjal keelatud. See võib osutuda mõnikord vajalikuks (eriti osareplikatsioonide korral), kuid võib kahjustada replikatsioonide terviklust.
- Kuigi replikeerimisseadistusi tuleb teha eeskätt tarbijas, on korrektse replikeerimise tagamiseks siiski vaja konfigureerida ka teenusepakkujat. Selleks, et teenusepakkuja saaks tarbija päringutele vastata täpselt ehk lähtuda enda vastuseid saates muudatuste toimumise hetkest, peab ka teenusepakkuja ise toimunud muudatused endale üles märkima, st haldama värskete ajatemplite loetelu context change sequence numbers (contextCSNs). Selleks tuleb käivitada overlay syncprov (Sync Provider).
- Tarbija-andmebaasi esmaseks täitmiseks on soovitatav sisse lugeda üksnes teenusepakkuja andmetest tehtud varukoopias sisalduvad vajalikud andmehulgad (vt M 6.150 OpenLDAP andmevarundus), sest kogu kataloogiteenuse sisu täielikuks edastamiseks läbi võrgu kuluks liigselt aega ja ressursse. Kuna syncrepl-il on olemas ka andmete võrdlemise mehhanism, ei pea kasutatav andmevarundus olema ilmtingimata kõige värskem. Kui andmebaas täidetakse slapadd-iga ja sisseloetav andmevarundus ei sisalda contextCSN-e, tuleb contextCSN-ide loomiseks sisestada parameeter „-w”. See osutub vajalikuks eelkõige esimese replikeerimise ajal, sest teenusepakkuja ei ole tavaliselt sellise funktsiooni kasutamiseks veel ette valmistatud ja overlay ’d syncprov ei ole veel käivitatud.

Delta-replikatsioon

Üldjuhul edastab teenusepakkuja kõikide muudetud sissekannete atribuudid kas otsingutulemusena või replikeerimisel. Seda tehakse ka siis, kui sissekande atribuutide hulgast on muudetud ainult ühte atribuuti. Kasutades overlay ’d accesslog (vt M 4.407 OpenLDAP kasutamise logimine), on võimalik atribuutide muudatusi fikseerida ka palju detailsemalt ning edastada syncrepl-mehhanismiga seejärel üksnes muudatused. See eeldab aga suuremahulisi konfigureerimistöid. Kui suhteliselt mahukate objektide korral esineb väikestes atribuutides sageli muudatusi, võiks sellist lahendust kaaluda, kuid kui objekte on vähe või muudatuste hulk väike, ei ole Delta-replikatsioon ilmtingimata vajalik.

Multi Masteri ja Mirror Mode’i töörežiim

Kasutada saab ka Multi Masteri töörežiimi. Multi Masteri režiimi puhul on süsteemis enam kui üks server, millele saab kirjutamisõigusega juurde pääseda, ning master -serverid toimivad omavahel nii teenusepakkujana (provider) kui ka tarbijana (consumer). Selle töörežiimi mõte seisneb selles, et kui üks server peaks rivist välja langema, jääb kirjutamisõigusega juurdepääs kataloogiteenusele siiski alles, ilma et konfiguratsiooni oleks tarvis muuta (erinevalt lahendusest, kus on

vaid üks slave / ainult consumer). Seda režiimi on aga ka kritiseeritud ning osa OpenLDAP arendusmeeskonna liikmetest ei pea seda mõistlikuks lahenduseks, sest see võib ebaühtlustada kataloogi sisu. Nii võib juhtuda, kui mõlemas masterserveris tehakse samal ajal üksteise suhtes vastuolulisi muudatusi. Tavalise turbevajadusega infokoosluses rakendatava OpenLDAP installatsiooni jaoks ei ole Multi Masteri režiimi tarvis. Seevastu suurte või väga suurte käideldavusele esitatavate nõuete korral võiks Multi Masteri režiimi otstarbekust siiski kaaluda. Siinkohal tuleks lähtuda põhimõttest, et mida olulisem on katkestustevaba käideldavus, seda mõistlikumaks muutub ka Multi Masteri töörežiimi kasutuselevõtt, ning mida olulisem on andmete terviklus mis tahes ajal, seda ebamõistlikum on Multi Masteri töörežiimi rakendamine. Single Masteri ja Multi Masteri režiimi alternatiiv on Mirror Mode'i töörežiim. Selles režiimis kasutatakse samuti korraga mitut serverit, mis võimaldavad kataloogiteenusele kirjutamisõigusega juurde pääseda. Erinevus seisneb muudatuste tegemises, st siin kasutatakse ka välist seirekomponenti, mis määrab alati kindlaks ainult ühe aktiivse serveri, millega saab teha muudatusi. Kui aktiivse serveri töö peaks katkema, nimetab väline seirekomponent automaatselt mõne teise serveri ümber aktiivseks serveriks. See töörežiim Delta-replikatsiooni veel ei toeta. Puuduseks võib pidada ka asjaolu, et seirekomponendi töö katkemisel kaob muidu liiasuse põhimõttega arvestava kataloogiteenuse käideldavus.

Täiendavad kontrollküsimused:

- Kas OpenLDAP teenusepakkuja ja tarbija serverites kasutatakse piisavalt täpseid ajateenuseid?
- Kas OpenLDAP jaoks sobiva replikeerimismeetodi valimisel lähtutakse võrguühendustest ja kehtivatest käideldavusnõuetest?
- Kas tarbija-serveri konfiguratsioonis on OpenLDAP-s kasutusele võetud täpselt samad skeemid nagu teenusepakkuja-serveris?

M 4.390 OpenLDAP turvaline ajakohastamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

OpenLDAP arendusmeeskond töötab pidevalt OpenCMR-i täiendamise kallal. Seega on sageli mõistlik ja tarkvara turvaaukude ilmnemisel koguni hädavajalik, et olemasolev OpenLDAP installatsioon asendataks uuema versiooniga.

Teabe hankimine uute versioonide kohta

Kõikide uute redaktsioonide ja stabiilseks tunnistatud redaktsioonides tehtud muudatuste kohta (release notes) edastavad OpenLDAP arendajad teavet enda meililistis „openldap-announce" (http://www.openldap.org/lists/openldap-announce). Administraatorid peaksid selle meililistiga liituma ja selles ilmuvaid teateid ka hoolikalt lugema. Äsja avaldatud uusi redaktsioone ei ole ilmtingimata tarvis kohe installida, välja arvatud juhul, kui uue redaktsiooniga kõrvaldatakse kas turvaaugud või kui redaktsioon sisaldab kasutaja jaoks väärtuslikke uusi funktsioone. Olukorras, kus stabiilseks redaktsiooniks on kuulutatud mõni uuem versioon kui see, mis on parasjagu kasutusel, on soovitatav järgmiste hooldustööde ajaks planeerida ka OpenLDAP ajakohastamine. Turbega seotud muudatuste korral, mille alla kuulub näiteks turvaaukude kõrvaldamine, tuleb OpenLDAP ajakohastamine ette võtta esimesel võimalusel. Olemasoleva OpenLDAP installatsiooni ajakohastamisel tuleb uurida kõiki asjakohaseid redaktsiooniteateid (release notes), et selgitada välja, mida on olemasoleva versiooniga võrreldes muudetud. Siinkohal on otseselt planeeritava versiooni kohta avaldatud teadete kõrval olulised ka need teated, mis käsitlevad kõiki teisi kasutatava ja planeeritava versiooni vahele jäävaid versioone. Eriti hoolikalt tuleks jälgida, kas muudatused puudutavad kasutatavaid backend 'e ja overlay 'sid ning tarkvara sõltuvussuhteid. Kui puudutavad, tuleb ajakohastada ka OpenLDAP planeerimisprotsessi (vt M 1.1 Vastavus normidele ja eeskirjadele).

Ajakohastamine

Eeltööna tuleb alla laadida OpenLDAP planeeritava versiooni installatsioonipaketid ja need üle kontrollida (vt M 4.382 OpenLDAP installatsioonipakettide valik ja kontrollimine). Kui kasutatakse mõne distro levitaja binaarpakette, saab levitaja käest hankida võib-olla ka spetsiaalseid ajakohastamispakette. Enne ajakohastamist tuleb slapd-serveri töö peatada ning olemasolevast kataloogist teha värske varukoopia (vt M 6.150 OpenLDAP andmevarundus). Seejärel tuleb installida OpenLDAP uus versioon (vt M 4.383 OpenLDAP turvaline installimine). Installatsiooni võib paigaldada uude sihtkataloogi, et seni kasutatud versiooni oleks võimalik vajaduse korral taas kasutusele võtta. Uus installitud tarkvara tuleb ka konfigureerida. Selleks võetakse üldjuhul andmevarundusest üle eelmine konfiguratsioon. Seejärel kontrollitakse konfiguratsiooni tööriistaga slaptest ja pääsuõigusi tööriistaga slapacl. Pärast seda võib slapd-serveri taaskäivitada. OpenLDAP ajakohastamisel tuleb eriti hoolikalt arvestada järgmiste punktidega:

- Administraatorid kasutavad väga sageli enda koostatud skripte, mis aitavad neil OpenLDAP-ga seotud töid automatiseerida. Kui OpenLDAP ajakohastatakse, tuleb sellised skriptid üle kontrollida, et veenduda, kas need töötavad ajakohastatud versiooniga veatult.

- Kui IT-süsteemi on paralleelselt installitud mitu OpenLDAP versiooni, on eriti oluline, et kontrollimiseks kasutataks kindlasti õige versiooni slap*-tarkvaratööriistu. Konfiguratsiooni ja pääsuõiguste katsetamiseks tuleb kasutada nn uue versiooni slaptest- ja slapacl-tööriista ning varukoopia sisselugemiseks nn uue versiooni slapadd-tööriista.

Täiendavad kontrollküsimused:

- Kas OpenLDAP turbevärskendused installitakse alati esimesel võimalusel?
- Kas OpenLDAP ajakohastamise raames kontrollitakse ja võetakse arvesse ka seni kasutatud backend 'e ja overlay 'sid ning tarkvara sõltuvussuhteid?
- Kas enda koostatud skriptide kasutamisel kontrollitakse nende koostalitlust OpenLDAP ajakohastatud versiooniga?
- Kas pärast OpenLDAP ajakohastamist kontrollitakse hoolikalt selle konfiguratsiooni ja pääsuõigusi õigete, nn uue versiooni tarkvaratööriistadega?

M 4.391 OpenLDAP turvaline käitamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

OpenLDAP turbe tagamiseks tuleb regulaarselt võtta erinevaid meetmeid, mis aitavad tuvastada võimalikke probleeme juba nende algfaasis. OpenLDAP käitamisel tuleb arvestada ennekõike järgmiste aspektidega:

- Enne slapd-serveri käivitamist tuleb veenduda, et käivitamiseks kasutatakse õiget konfiguratsiooni. Parameetriga „-f [path/filename]" määratakse kindlaks kasutatav slapd.conf ning parameetriga „-F [path]" kasutatav slapd-config-kataloog. Siinkohal on tähtis, et mõlema parameetri kooskasutamisel ei täiendaks konfiguratsioonid üksteist, vaid slapd.conf-konfiguratsioon peab slap-config-konfiguratsiooni üle kirjutama.
- Käivitamisel tuleks piirata slapd-serverit parameetriga „-h [protocols]", et see kasutaks ainult vajalikke protokolle, nt järgmiselt: „-h ldaps://".
- slapd-serveri tööd tuleb piirata parameetriga „-r [directory]", et see kasutaks käitusaja kataloogi (chroot-mehhanism). See kataloog peab sisaldama kõiki konfiguratsioonifaile ja andmebaase.
- Enne slapd-serveri plaanipärast seismajätmist tuleks kontrollida, kas serveril on veel operatsioone pooleli ja kas klientidega on ühendusi pooleli (vt M 4.407 OpenLDAP kasutamise logimine). See puudutab ennekõike neid operatsioone, mis taaskäivitamise järel automaatselt ei jätku (nt indekseerimine). Kuna slapd-serveril puudub stopp-käsk, tuleb selle töö peatamiseks vastav protsess lõpetada, nt järgmiselt: „kill -INT 'cat /usr/local/var/slapd.pid"'.
- Konfiguratsioonis tehtavad muudatused tuleb hoolikalt dokumenteerida, et igal ajal oleks võimalik kontrollida, kes ja mis põhjusel muudatusi tegi ning mida muudeti. Konfiguratsioonifailide muudatuste tegemiseks oleks mõistlik kasutada revisjoniprogramme (nt git, mercurial või RCS). Nii saab igal ajal taastada varasema konfiguratsiooni seisundi, samuti on alati näha, kes mida ja mis põhjusel muutis.
- Pärast igat konfiguratsioonifailis tehtud muudatust tuleb esmalt programmiga slaptest kontrollida, kas konfiguratsioonifaili süntaks on õige. Konfiguratsioonifaili süntaksivigade tagajärjel ei pruugi slapd-server enam käivituda ning tekkida võivad ka turvaaugud.
- Iga kord pärast pääsuõiguste muutmist tuleb programmiga slapacl kontrollida, kas äsja tehtud muudatus toimib.
- Administraatorid peavad kasutatud tarkvaras avastatud turvaaukudega end võimalikult kiiresti kurssi viima (vt M 1.1 Vastavus normidele ja eeskirjadele). OpenLDAP arendajad avaldavad teavet uute ilmsiks tulnud turvaaukude kohta väljaandes „Issue Tracking System" aadressil http://www.openldap.org/ its.
- Meetmes M 2.64 Logifailide kontroll kirjeldatud meetmeid tuleb võtta ka OpenLDAP kontekstis. Logide salvestuskohtade ja andmemahu kohta saab teavet meetmest M 4.407 OpenLDAP kasutamise logimine .

- Käitamisprotsessi turvalisuse tagamise juurde kuuluvad ka meetmed, mida tuleb regulaarselt võtta hädaolukordade ennetamiseks, ning andmetest varukoopiate tegemine (vt M 6.136 Hädaolukorraks valmisoleku plaani koostamine Samba serveri avarii puhuks ja M 6.150 OpenLDAP andmevarundus).

Täiendavad kontrollküsimused:

- Kas slapd-serveri tööd piiratakse käitusaja kataloogiga?
- Kas pärast OpenLDAP konfiguratsiooni ja pääsuõiguste muutmist kontrollitakse, kas süntaks on õige ja kas pääsuõigused töötavad õigesti?
- Kas on tagatud, et teave OpenLDAP võimalike uute turvaaukude kohta jõuab administraatoriteni ilma viivituseta?

M 4.392 Autentimine veebirakendustes

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: arendaja, administraator

Kui veebirakenduse või ka selle osa kasutajate ringi soovitakse piirata, peavad kasutajad end veebirakenduses autentima. Autentimiseks saab kasutada erinevaid meetodeid, mida kirjeldatakse meetmetes M 1.1 Vastavus normidele ja eeskirjadele ja M 5.160w Autentimine veebiserveril . Autentimismehhanismide tööleseadmisel veebirakendustes tuleb arvestada järgmiste punktidega.

Autentimiskomponentidele esitatavad nõuded

Autentimismehhanismi loogika peaks programmi koodis esinema vaid ühes kohas, mitte mitmes korraga. Kui autentimisprotsessis peaks tekkima viga, peab süsteem soovitud tegevuse katkestama ja päringu täitmisest keelduma. Autentimiskomponent peab toetama sunniviisilist turvaliste paroolide valimise funktsiooni, mis arvestab vastu võetud paroolisuuniste nõuetega. Paroolide turvalisusele esitatavad nõuded leiate meetmest M 2.11 Paroolide kasutamise reeglid . Lisaks on soovitatav kuvada kasutajale teavet sisestatud parooli hinnangulise tugevuse kohta (nt nõrk, keskmine, tugev). See abistab kasutajat turvaliste paroolide valimisel. Et vältida autentimiskomponendi arendustöös tehtavaid vigu, on soovitatav autentimiskomponent juurutada mõne tunnustatud standardtoote baasil (teegid või raamistikud, nt OWASP toode Enterprise Security API). Kui veebirakenduse turbenõuded on tavapärasest suuremad, tuleks kasutusele võtta kahefaktoriline autentimine. Et kasutajatel oleks võimalik tuvastada enda kasutajakonto võimalikku väärkasutust, saab veebirakenduses kasutajale pärast sisselogimist kuvada nii edukalt kui ka edutult lõppenud viimase sisselogimiskatse ning nende kuupäeva ja kellaaja.

Remember Me funktsioon

Kasutusmugavuse suurendamiseks salvestatakse veebirakenduste autentimisandmed, mõnikord lausa püsivalt, kasutaja klientsüsteemi (nt küpsistena veebilehitsejas). Sellist võimalust nimetatakse sageli Remember Me funktsiooniks. Kui autentimisandmed salvestatakse klientsüsteemi Remember Me funktsiooniga, kantakse need hiljem, kui veebirakendust hakatakse kasutama, automaatselt veebirakendusse üle. Nii ei pea kasutaja enda autentimisandmeid enam uuesti sisestama. Kui aga ründajal õnnestub juurde pääseda veebilehitsejale või kui klientsüsteemis käivitatakse kahjurvara kood, võivad need salvestatud autentimisandmed sattuda ründaja kätte. Seetõttu tuleks selle funktsiooni kasutamisest loobuda. Kui Remember Me funktsioonist siiski ei saa loobuda, tuleb kasutada lahendust, mille puhul peab kasutaja aktiveerimise (Opt In) eraldi heaks kiitma. Lisaks tuleks kasutajaid teavitada ka selle funktsiooni ohtudest.

Küpsistena salvestatavate autentimisandmete kõrval võivad veebilehitsejad sageli salvestada endale ka hilisemaks korduvaks kasutuseks mõeldud andmeplanke (nt kasutajanimi/parool või adressaatide loetelu). Kui veebikeskkonnas avatakse uuesti mõni andmeplank, mille jaoks on andmed juba varem salvestatud, täidab veebilehitseja vastava andmeplangi tühjad andmeread automaatselt. Seetõttu tuleks kõikide nende kasutusjuhtude tarbeks, milles puututakse kokku konfidentsiaalsete andmetega, kasutada seadistust „autocomplete=off”. Nii antakse veebil-

ehitsejatele mõista, et andmeplankide infot ei tohi salvestada.

Täiendav autentimine kriitiliste funktsioonide puhul

Pärast seda, kui kasutaja on end edukalt süsteemis autentinud, määrab veebilehitseja talle enamasti kindla seansi ehk seansi ID (SessionID). Seansi ID-ga saab veebilehitseja talle saabuvaid nõudeid (request) seostada sisse logitud kasutajatega. Seega võib seansi ID-d käsitleda ka kui ajutist sisselogimiskuupäeva, mille abil saab luua juurdepääsu sisse logitud kasutajate seanssidele (vt M 4.394 Seansihaldus veebirakendustes). Kuna praeguseks on teada, et paljudel juhtudel on ründe sihtmärk olnud just seansi ID (vt G 5.169 Veebirakenduste ja veebiteenuste puudulik seansihaldus), ei saa kehtivate seansside ülevõtmist täielikult välistada. Seetõttu tuleks turbe seisukohast kriitiliste tegevuste puhul (nt parooli muutmisel ja andmehulkade täielikul kustutamisel) rakendada kasutaja korduvat autentimist (nt vana parooli sisestamist uue parooli valimise protsessis).

Ebaõnnestunud sisselogimiskatsete arvu piiramine

Olukorda, kus kasutaja püüab lühikese ajavahemiku jooksul ennast mitu korda järjest veebirakendusse sisse logida, tuleks käsitleda kui võimalikku rünnet. Kui sisselogimiskatsete arv ületab kindlaks määratud normi (nt viis katset), tuleks kasutajakonto teatud ajaks blokeerida (nt kümneks sekundiks). Kasutajakonto blokeerimise kestus peaks vastavalt ebaõnnestunud sisselogimiskatsete arvu suurenemisele samuti pidevalt suurenema. See aitab vältida olukordi, kus kasutajad püüavad üksteise paroole katsetuse teel ära mõistatada. Lubatud katsete piirarvu ja blokeeringu kestuse valimisel tuleb arvestada, et sedasama turvafunktsiooni on võimalik ära kasutada Denial-Of-Service-rünneteks. Ründaja võib teadlikult esile kutsuda olukorra, kus võimalikult paljud kasutajakontod blokeeritakse, mis tagab, et need kasutajad ei saa teatud aja jooksul veebirakendust enam kasutada.

Autentimisandmete automaatne lähtestamine

Kuna veebirakenduste kasutajate hulk on sageli väga suur, võimaldavad paljud veebirakendused kasutada ka autentimisandmete automaatset lähtestamist (Password Reset). Sel viisil on võimalik vähendada haldamistööde mahtu näiteks olukordades, kus kasutaja on enda parooli ära unustanud. Võimalus autentimisandmeid volitamata lähtestada tähendab seda, et autentimisfunktsioonist saab loata mööda hiilida. Seetõttu tuleks arvestada, et kõik veebirakenduse autentimisandmete muutmist võimaldavad funktsioonid tuleb muuta vähemalt sama turvaliseks, nagu seda on veebirakenduse primaarne autentimisfunktsioon.

Näiteks kui parooli lähtestamise protsessi turvamiseks rakendatakse lahendust, mille puhul peab kasutaja talle esitatavale salajasele küsimusele vastuse sisestama, tuleb tagada, et kasutajal on võimalik seda küsimust ka ise sõnastada. Funktsioon peab kasutajale meelde tuletama, et küsimus ei tohi sisaldada avalikult kättesaadavaid andmeid ning vastus ei tohi olla lihtsasti äraarvatav. Turbeastme suurendamiseks võib kasutajakonto loomisel sisestada ka mitu küsimuse ja vastuse paari (nt kokku viis küsimust, millest peab edukaks autentimiseks õigesti vastama vähemalt kolmele). Samuti võib kasutada lisaturvamehhanismi, mille puhul saadetakse küsimustele õigesti vastates kasutaja kindlaksmääratud meiliaadressile vastav link või eelmääratud telefoninumbrile SMS-iga täiendav turvaluba (token), nt PIN-kood. Kasutaja saab end sisse logida alles pärast klõpsamist lingil või pä-

rast PIN-koodi sisestamist.

Kuna autentimisandmete lähtestamise funktsiooni turvet on üldjuhul väga raske primaarse autentimisfunktsiooni turbega ühtlustada, tuleks veebirakendustes autentimisandmete automaatse lähtestamise funktsioonist võimaluse korral alati loobuda. Seevastu kui veebirakenduse (nt ainult intranetis kasutatava veebirakenduse) kasutajate arv on piiratud, saab selle asemel kasutada parooli käsitsi lähtestamist, mille puhul rakendatakse turvalisi autentimistunnuseid ja heaks kiidetud protseduure, nt helistamist tugiteenuse numbril. Käsitsi lähtestamist tuleks kindlasti kasutada tavapärasest suurema turbeastme korral.

Kontrollküsimused:

- Kas veebirakenduses kasutatakse tsentraalselt toimivat autentimiskomponenti?
- Kas veebirakendus sunnib kasutajaid valima turvalisi paroole?
- Kui veebirakenduses kasutatakse Remember Me funktsiooni, kas kasutajatelt nõutakse eraldi kinnitust (Opt In)?
- Kas veebirakenduse kriitilise tähtsusega funktsioone turvatakse täiendava autentimisega?
- Kas veebirakenduses on kindlaks määratud ebaõnnestunud sisselogimiskatsete piirarv, mis peaks raskendama Brute-Force-ründeid?
- Kas kõik veebirakenduses kasutatavad autentimisprotseduurid (nt parooli automaatse lähtestamise funktsioon) on sama turbeastmega?
- Kas veebirakenduse kasutajat informeeritakse viivitamata olukorrast, kus veebirakenduse parooli lähtestamise funktsiooni on kasutatud?

M 4.393 Sisestuste- ja väljastuste põhjalik valideerimine veebirakendustes ja veebiteenustes

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: arendaja, administraator

Kõik veebirakendusele edastatavad andmed on olenemata koodist ja ülekande liigist potentsiaalselt ohtlikud ning neid tuleb filtreerida. Sisestatavate ja väljastatavate andmete põhjalik filtreerimine valideerimiskomponendiga võib pakkuda tõhusat kaitset levinud rünnete vastu. Siinkohal on oluline, et filtreerimist ja transformeerimist (output encoding) rakendataks nii kasutajate sisestatavate ja veebirakendusele edastatavate andmete kui ka veebirakendusest klientidele väljastatavate andmete puhul.

Nii tagatakse, et veebirakendus töötleb ja edastab üksnes oodatavaid andmeid, mitte kahjulikku sisu. Kui mõni funktsioon vajab vähem piiravat, st nõrgema toimega andmefiltrit, tuleb see selgelt andmepäringu protsessi jaoks defineerida ja dokumenteerida.

Lisaks on võimalik rakenduse protsessiloogikas või taustsüsteemides võtta kasutusele kontekstipõhised filtrid. Turvalise andmetöötluse tagamiseks tuleb valideerimiskomponendi konfiguratsiooni koostamisel arvestada järgmiste punktidega.

Andmete identifitseerimine

Veebirakenduse sisendi- ja väljundiandmete põhjalikuks valideerimiseks tuleb esmalt identifitseerida töödeldavate andmete struktuur (nt kas tegu on meiliga) ning seejärel nende jaoks lubatud väärtused. Iga andmestruktuuri kohta tuleb kasutusele võtta asjakohane valideerimisrutiin. Andmestruktuuri kõrval tuleb käsitleda ka seda, kuidas andmeid töödeldakse (andmete edastamist interpretaatorprogrammile, tagastamist kliendile, salvestamist andmebaasis).

Kõikide andmete ja andmevormingute käsitlemine

Valideerimiskomponent peab arvestama kõikide töödeldavate andmevormingute ja kasutatavate interpretaatoritega. Veebirakenduste puhul kuuluvad tüüpiliste andmevormingute hulka näiteks isikuandmed (nimi, telefoninumber, sihtnumber), fotod, PDF-failid ja küljendatud tekstid. Levinud interpretaatorid, mida kasutatakse veebirakendustes töödeldavate ja nendest väljastatavate andmete jaoks, on näiteks HTML-Renderer, SQL-, XML-, LDAP-Interpreter ja operatsioonisüsteem.

Andmete kehtivuse kontrollimiseks saab kasutada väga erinevat tehnoloogiat.

Nii näiteks võib valideerimiskomponent kontrollida sisestuste jaoks lubatud väärtusevahemikke, samuti võidakse reguleeritud väljundite abil valideerida lubatud tähemärke ja oodatavate andmete pikkust. XML-andmete kehtivust saab muu hulgas kontrollida asjakohase XML-skeemi põhjal.

Levinud andmevormingute jaoks pakuvad valideerimiskomponente ka raamistikud ja teegid. Allnimetatud märke interpreteerivad enamasti veebirakendustes käitatavad programmid ning seetõttu saab neid kasutada kahjurvarakoodi sissesmugeldamiseks. Nendega tuleb filtreerimisel kindlasti arvestada. Need märgid on nullväärtus, line feed, carriage return, ülakomad, komad, kaldkriipsud, tühikud, tabulaatorimärk, suurem kui ja väiksem kui, XML-i ja HTML-i tag 'id. See loetelu ei ole mitte mingil juhul täielik. Samuti tuleb arvestada, et erinevate toodete puhul võivad interpreteeritavad märgikombinatsioonid erineda (nt SQL-i süntaks).

Lisateavet kriitiliste märkide kohta leiate veebirakenduse mooduli abivahendite alajaotisest „Interpretaatoritele potentsiaalselt ohtlikud tähemärgid".

Tegelike kasutajaandmete kõrval (nt andmeplankide parameetrid GET- või POST-muutujates) tuleb valideerida ka muu päritoluga andmeid (sekundaarandmeid).

Nende hulka kuuluvad näiteks:

- Form-muutuja nimed (nendega on võimalik samamoodi piiramatult manipuleerida nagu Form-väärtuste muutujatega);
- HTTP päise väljad (header fields) (HTTP-Requestsi ja HTTP-Responsesi päiseväljad peaksid sisaldama eranditult ASCII tähemärke ja mitte ühtki line feed märki, nt märki \r\n);
- seansi ID-d (nt küpsiste seest).

Samuti vajavad kontrollimist klientide automaatsed käivitamised näiteks Ajaxi või Flashi skriptidega ning JSON-Requests. Taustsüsteemide puhul tuleb rakendada andmete (vajaduse korral korduvat) valideerimist. See nõue kehtib ka siis, kui näiteks pärast kirjutamisprotsessi loetakse andmeid andmebaasist, sest andmed võivad vahepeal, st ajal, mil neid hoiti andmebaasis, olla muutunud. Lisaks on teada erinevaid ründetehnoloogiaid, mille puhul edastatakse kahjurvara kood mõne sellise kanali kaudu, mida veebirakendus ei suuda ise kontrollida (nt FTP või NFS). Kui ründajal õnnestub nende teenuste vahendusel olemasolevaid faile muuta või koostada uusi faile, mille veebirakendus endaga integreerib, võib see viia kahjurvara sisseimbumiseni. Näiteks smugeldatakse Cross Channel Scriptingu puhul sel viisil sisse JavaScripti kood, mis käivitatakse veebilehitsejas umbes samamoodi nagu püsiva Cross Site Scriptingu puhul. Seetõttu tuleks veebirakenduse väljundiandmeid enne nende edastamist kasutajatele alati valideerida, olenemata andmeallikast.

Valideerimine serveri keskkonnas

Kasutajad loovad endale juurdepääsu veebirakendusele enamasti geneeriliste klientidega (nt veebilehitsejatega). Need kliendid ei tööta aga mitte veebirakenduse turbekontekstis, vaid alluvad kasutajate kontrollile. Seetõttu tuleb serveripõhine andmete valideerimise funktsioon tööle rakendada mõnes usaldusväärses IT-süsteemis. Kui neid andmeid töödeldakse veebirakenduse koodiga ka klientides (nt JavaScripti koodiga), tuleks neid valideerida ka kliendis.

Veebirakendusest väljastatavad skriptid peavad siinkohal sisaldama ka asjakohaseid valideerimisrutiine. Kui andmed saadetakse järeltöötlusprotsessi raames edasi serverisse, tuleb arvestada, et klientides tehtav kontroll ei asenda serveris tehtavat valideerimist.

Valideerimise lähtepunkt

Andmete valideerimise lähtepunktide valiku puhul räägitakse lubavatest ja keelavatest nimekirjadest (white- / blacklists).

Whitelist-lähtepunkti korral on lubatud üksnes sellised andmed, mis on lubavasse nimekirja sisse kantud. Selleks koostatakse võimalikult väikesest märkide hulgast lähtudes reeglid, mis lubavad ainult kindlaksmääratud märgiruumi piiresse mahtuvaid andmeid ja blokeerivad reeglitest kõrvalekalduvaid märke sisaldavad andmed. Selle lahenduse rakendamisel tuleks keerulise reeglistiku loomiseks kasutada lihtsaid reegleid sekventsidena.

Seevastu blacklist-lähtepunkti korral lähtutakse keelavasse nimekirja sisse kantud andmetest ja blokeeritakse üksnes need andmed, mis on nimekirja sisse kantud.

Kõik sellised andmed, mis ei ole konkreetselt ära keelatud, lubatakse selle lähtepunkti alusel läbi. Blacklist -lähtepunkti rakendamisel tekib siiski oht, et nimekiri ei pruugi alati sisaldada kõiki keelatud andmete variatsioone, mistõttu jääb osa keelatud andmetest lihtsalt tuvastamata. Sel põhjusel tuleks blacklist -lähtepunktile eelistada whitelist -lähtepunkti.

Valideerimisele eelnev kanoniseerimine

Andmed võivad olla väga erinevates kodeeringutes (nt UTF-8 või ISO 8859-1) ja noteeringutes (nt UTF-8 puhul kehtib “.” = “2E” = “C0 AE”). Olenevalt kasutatavast kodeerimisskeemist võidakse üht ja sama väärtust interpreteerida väga erinevalt. Kui valideerimisprotsessis kodeeringu ja noteeringuga ei arvestata, võivad potentsiaalselt ohtlikud andmed jääda tuvastamata ja seetõttu ka välja filtreerimata. Seega tuleb kõik andmed enne valideerimist viia ühtlasele normeeritud kujule. Sellist tegevust nimetatakse andmete kanoniseerimiseks. Sellisele kujule viidud andmeid töödeldakse edasi. AJAX-i kasutamisel tuleb järellaadimiseks rakendada omadust innerText, mitte innerHTML, sest innerText käivitab automaatselt kodeerimise. Lisaks peaks veebirakendus andmeid väljastades konkreetselt kindlaks määrama kodeerimisskeemi (nt Content Type Header: charset=ISO-8859-1).

Andmete kontekstipõhine maskeerimine

Olukorras, kus veebirakendus peab töötlema potentsiaalselt ohtlikke andmeid (nt tähemärke, millel on rakendatava interpretaatorprogrammi jaoks tähendus) ja filtreerimisfunktsiooni ei saa seega kasutada, tuleb need andmed ära maskeerida, st muuta nende kuvamisvormingut. Sellises maskeeritud vormingus ei interpreteerita neid andmeid enam kui käitatavat koodi. Kuna maskeering oleneb suuresti interpretaatorprogrammist, tuleb lähtuda kõikidest kasutatud interpretaatoritest (nt SQL või LDAP). Seega peab maskeerimisel arvestama nii oodatava sisendi- kui ka

väljundivormingu kontekstiga ning interpretaatori keelega. Kuna erinevate interpretaatorprogrammide keeled on keerulised ja spetsiifilised, on soovitatav kasutada maskeerimiseks spetsiaalseid teeke.

Markeerida tuleks kõik tähemärgid, mida peetakse kasutatava interpretaatorprogrammi jaoks ebaturvaliseks.

Siia kuuluvad näiteks:

- ootamatu JavaScript ja HTML, mis edastatakse kliendile (veebilehitsejale);
- volitamata sisestatud SQL Statementid andmebaasi jaoks (nt andmeplankidesse tehtud sisestused);
- operatsioonisüsteemile mõeldud käsud (nt manipuleeritud HTTP-muutujad).

Maskeerimiseks saab kasutada vastava interpretaatori keeles olevate andmete või metamärkide üleviimist nn märgireferentsidesse.

Järgmises näites on toodud mõned väljavalitud HTML-märgid koos märgireferentsidega:

- & => &
- < => <
- >=> >
- “=>”
- ‘=>’.

Siin tuleb tähelepanu pöörata sellele, et &-märgid saaksid asendatud esimese läbitöötamise käigus, sest neid märke kasutatakse teistes märgireferentsides uuesti metamärkidena. Kui veebirakenduse kasutamine eeldab kasutaja sisestustes ka HTML-vormindusmärgendite kasutamist (nt kasutaja sissekannete vormindamiseks), tuleks lubatud HTML-märgendeid eristada probleemsetest märgenditest ja need välja filtreerida (vt ka lõik „Andmete kontekstipõhine maskeerimine”).

Sellise lähtepunkti puhul tekib oht, et probleemsed märgendid (nt) jäävad tähelepanuta. Seetõttu tuleks eelistada lahendust, kus kasutaja märgistamiseks kasutatakse enda märgistuslipikuid (markup tags) (nt BBCode). Need märgistuslipikud tõlgitakse enne kasutamist ümber vastavateks HTML-märgenditeks. Tavalisi märgendeid ja probleemseid märke filtreeritakse nagu ennegi. Sobiv lahendus juhtudeks, kus mõnda lihtsat markup ’i peab lubama, on meetod, mille korral võetakse { and } kasutusele kui < and >. Paks kirjapilt oleks sel juhul kujul {F} see on paks {/F} ja pildi paigutus näeks välja järgmine: {img src=/ images/img.gif width=1 height=1 img}.

Siin ei tohi HTML-i ümbervormindamiseks asendada looksulge lihtsalt nurksulgudega, vaid igat märgendit (tag) tuleb vaadelda kui tervikut:

- {img pärast
- img} pärast >;
- src=file pärast src=“file” (kusjuures file tuleb filtreerida eraldi).

Kui HTML-märgendid on lubatud, tuleb põhimõtteliselt pöörata tähelepanu sellele, et vähemalt järgmised märgendid ei ole lubatud:

- applet
- base
- iframe
- link
- object
- script
- style

Ümberkäimine väärsisestuste puhastamisega (sanitizing)

Selle asemel, et andmete töötlemisest ebahariliku vormingu või mõne märgi tõttu keelduda, saab väärsisestusi ka korrigeerida ja automaatselt transformeerida (sanitizing). Nii on võimalik andmete sisestamist kasutajatele mugavamaks muuta ja arvestada kirjapildis esinevate kõrvalekalletega. Andmete edasitöötlemiseks saab need ebasobivatest märkidest puhastada, nt telefoninumbri kirjapildi (0049)-201-12345678 saab teisendada ainult numbritest koosnevaks vorminguks 004920112345678. Puhastamine võib seisneda näiteks märkide kustutamises, asendamises ja maskeerimises.

Puhastamisega kaasneb oht, et andmetes tehtud muudatused võivad tekitada uue ja keerulisema andmestruktuuri, mis pakub uusi võimalusi nii rünneteks kui ka väärtõlgendusteks. Seetõttu tuleks sanitizing -funktsioone siiski võimaluse korral alati vältida, st kasutada neid ainult juhtudel, kus on välistatud nende väärkasutus. Kui veebirakendus soovib andmete korrigeerimist, tuleks andmete teadlikud manipulatsioonid (nt seansi ID manipuleerimine ründaja poolt) jätta korrigeerimata ja nende töötlemisest keelduda. Lisaks tuleks alati keelduda selliste sisestusandmete vastuvõtmisest, mille tekkimine veebilehitseja sihipärase kasutuse käigus on välistatud.

Siia kuuluvad näiteks:

- andmeplankide täiendavad või puuduvad parameetrid;
- ebaharilike märkidega või ebahariliku pikkusega seansiküpsised (session cookies);
- ebaharilikud väärtused andmeplankide eeldefineeritud HIDDEN-, SELECT- või CHECKBOX-andmeväljast pärit parameetrite edastamisel;
- juhud, kus parameetrite (nt GET, POST, Cookie) edastusteekond ei lange kokku rakenduse nõuetega.

Astmelised ründevektorid

Andmete puhastamisel peaksid ründevektorid arvestama allutatud sisestusega. Problemaatiline on näiteks esmapilgul mõistlikuna paistev filter s/<script>//g; (siin kirjutatud Perl RegEx-Syntax'is, et kustutada sisestusvoos <script>-märgendid. Seda võib siiski vältida allutatud sisestusega (nt <sc<script>ript>). Seda tuleb seetõttu filtreerida rekursiivselt. Kahtluse korral tuleb sisestusandmed tagasi lükata. Andmete tagasilükkamisel tuleks vajalik tegevus samuti katkestada ja väljastada uus neutraalne veateade (vt ka M 4.400 Turbe seisukohalt oluliste andmete väljastamine veebirakendustes). Kõrge kaitsevajadusega veebirakenduste või veeniteenuste korral tuleks lisaks sessioon kehtetuks tunnistada (katkestada).

Kontrollküsimused:

- Kas valideerimisel võetakse arvesse kõiki veebirakenduse ja veebiteenuse (nt kasutaja, veebirakenduse, kliendisüsteemide ja taustasüsteemide vahel) andmeid (sisestus- ja väljastusandmeid)?
- Kas valideerimisel võetakse arvesse ka sekundaarseid andmeid (nagu nt Session-ID-d)?
- Kas veebirakendus või veebiteenus teostab serveripoolset andmete valideerimist usaldusväärsel IT-süsteemil?
- Kas veebirakendus või veebiteenus viib enne valideerimist läbi andmete kanoniseerimise?
- Kas veebirakenduses või veebiteenuses toimub andmete kontekstipõhine valideerimine, võttes arvesse oodatavat andmete tõlgendajat?
- Veebirakendustel/veebiteenustel automaatse valede sisestuse käsitlemisega (Sanitizing): kas valede sisestuste käsitlemine on rakendatud turvaliselt?

M 4.394 Seansihaldus veebirakendustes

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: arendaja, administraator

Veebirakendused kasutavad andmete edastamiseks väga sageli HTTP-protokolli, kuid sellel puuduvad seisundiandmed. See protokoll ei toeta kokkukuuluvate päringute liigitamist ja sidumist ühe konkreetse kasutajaga (nt veebilehtede avamist või virtuaalse ostukorvi täitmist). Ühe kasutaja kokkukuuluvate päringute tuvastamiseks ja nende sidumiseks seansiga väljastab veebirakendus kasutajale seansi ID-d (nt pärast edukat sisselogimist), mis edastatakse iga kord, kui avatakse mõni uus veebileht. Olukorras, kus kasutaja on end veebirakendusse sisse loginud, võib seansi ID-d käsitleda kui kasutaja pääsuandmeid. Veebirakendus tuvastab iga lehekülje avamisel seansi ID põhjal kasutaja ja annab tema käsutusse seansi (olenevalt olukorrast koos privileegidega).
Kui seansi ID saab enda valdusse volitamata isik, tuvastab veebirakendus ta ekslikult legaalse kasutajana ning ründajal tekib võimalus kasutada veebirakendust ohvri nime all. Veebirakenduse seansihalduse ülesanne on hallata seansse ja väljastada uusi seansi ID-sid. Selle raames tuleks arvestada alljärgnevate nõuete ja punktidega.

Seansi ID-le esitatavad nõuded

Arvesse tuleks võtta, et seansi ID kehtivusaeg peab olema tunduvalt lühem kui aeg, mis kulub ründajal seansi ID äramõistatamiseks. Seda aega saab iga kasutusvaldkonna jaoks valemiga eraldi hinnata. Seansi ID peaks vastama vähemalt järgmistele nõuetele:

- Seansi ID koostamiseks tuleb kasutada krüptograafilist juhuarvugeneraatorit ning selle entroopia peaks olema vähemalt 64 bitti, et potentsiaalsel ründajal poleks võimalik ID-d ära mõistatada. Seansi ID entroopia suurendamiseks saab suurendada näiteks ID pikkust (nt 128 bitini) ja märgiruumi (tähed, numbrid, erimärgid). Seansi ID jaoks pikkust valides tuleks lähtuda põhimõttest, et seansi ID pikkus bittides peaks olema vähemalt topelt nii suur, kui on seansi ID entroopia. Selle põhjal peaks seansi ID pikkus olema 128 bitti. Lähtudes sellest, et ühe märgi jaoks kasutatakse 8 bitti, peaks vastav seansi ID olema vähemalt 16-kohaline (128 bitti / 8 = 16 baiti).
- Seansi ID väljaarvutamise protsessi ei tohi kaasata väliseid teadaolevaid või äraarvatavaid andmeid (nt RFC-aadressi, kellaaega), välja arvatud juhul, kui kasutatav entroopia suudab nende mõju piisavalt vähendada.
- Kui veebirakenduse baasina kasutatav raamistik toetab seansi ID genereerimist, tuleks seansi ID koostamisel eelistada raamistiku funktsiooni. Juhtivate raamistike funktsioone on enamasti juba piisavalt katsetatud ning need toetavad seansi ID-de turvalist genereerimist. Veaalteid uusarendusi tuleks seega kindlasti vältida.
- Kui seansi ID-de haldamiseks ja koostamiseks kasutatakse raamistikku, tuleb hoolitseda raamistiku piisavalt turvalise konfiguratsiooni eest, mis tagaks vastavuse eespool seansi ID-de kohta loetletud nõuetele.

Seansi ID-de kaitsmine volitamata juurdepääsude eest

Seansi ID edastamiseks saab kasutada nii nõuete URL-i (GET-meetod), nõuete kehandit (POST-meetod) kui ka nõude päises olevat küpsist. Kui andmeid edastatakse GET-meetodiga, saavad andmesides osalevad IT-süsteemid neid endasse

salvestada ning see muudab need kolmandatele isikutele nähtavaks (nt veebilehitseja, ekraanitõmmised, lehtede koopiad ja väljatrükid). Seetõttu tuleb GET-meetodi kasutamisest (edastamisest URL-i sees) seansi ID-de edastamisel loobuda. Suurte turbenõuetega veebirakenduste korral on see lausa keelatud. Seansi ID-de edastamisel tuleks eelistada küpsiseid. Kui rakendus eeldab siiski GET-meetodi kasutamist (nt koostalitluse tagamiseks klientidega, mis ei suuda küpsiseid töödelda), tuleb arvestada järgmiste punktidega:

- Kasutajaid tuleb nimetatud ohtudest teavitada ning arvuti tagant lahkudes tuleb neil kindlasti kas seanss lõpetada või arvuti lukustada.
- Kasutajaid tuleb teavitada, et nad ei saadaks mitte kellelegi salvestatud lehekülgi ega ka veebirakendusest tehtud ekraanitõmmiseid, mille peal on URL-is näha seansi ID.
- Veebirakenduse kasutamisel mõnes avalikus arvutis tuleks kuvada teade, et pärast seansi lõpetamist kustutataks veebilehitseja kasutamise ajalugu ära.
- Et juhuslikel möödujatel oleks raskem seansi ID-sid välja lugeda või maha kirjutada, võib seansi ID-d venitada ülipikaks.
- Välistele lehekülgedele suunavate linkide kasutamisel ei tohi edastada seansi ID-d. See kehtib nii edastamisele URL-i sees kui ka referrer- andmeväljas. Selleks tuleb välistele lehekülgedele suunavate linkide puhul rakendada kohustuslikku edasisuunamisfunktsiooni, mis kustutab referrer -välja andmed ära.

Et tõkestada seansi ID volitamata lugemist, tuleks pärast edukat sisselogimist toimuva andmeside jaoks kasutada mõnda turvalist kanalit (nt SSL-i/TLS-i; vt M 5.66 TLS-i/SSL-i kasutamine). Seansi ID-d võib edastada ka turvamata kanali kaudu, kui poolelioleva seansi raames pole võimalik juurde pääseda veebirakenduses pääsukontrolliga kaitstud aladele. Sellisel juhul on kasutaja tavaliselt veel autentimata. Juurdepääs seansi ID-le kui autentimistunnusele peab olema rangelt reglementeeritud. Kui seansi ID edastatakse küpsisega, tuleks juurdepääsu kliendi küpsisele piirata järgmiste lippudega (täpsema kirjelduse cookie flag 'ide kohta leiate meetmest M 4.401 Konfidentsiaalsete andmete kaitse veebirakendustes):

- Path (nt /webapp/);
- Secure;
- HttpOnly.

Seansi kestuse piirang

Veebirakenduses peab kasutajatel olema võimalik töö lõpetamisel enda seanss ka eraldi sulgeda. Selleks peavad kõik veebilehed, mille kasutamine eeldab kindlasti autentimist, olema varustatud hästi nähtava väljalogimisfunktsiooniga. Pärast väljalogimist tuleb seanss täielikult lõpetada ja seansi ID peab kaotama oma kehtivuse. Eelnevale lisaks tuleb kasutajaid teavitada, et veebirakendustega ümber käies on ilmtingimata vaja järgida ja soodustada järgmisi käitumisreegleid:

- sisseloginud kasutaja peab ennast töö lõppedes veebirakendusest nõuetekohaselt välja logima;
- kui kasutaja ei loginud ennast viimasel kasutuskorral nõuetekohaselt välja, peab veebirakendus järgmise sisselogimise ajal kasutajat sellest teavitama ja viitama asjaolule, et kasutaja peab ennast töö lõppedes välja logima.

Katkestamata jäänud seansid, mida keegi ei kasuta, soodustavad seansi ID vastu suunatud Brute-Force-ründeid. Seepärast tuleb seansid, mida parasjagu ei kasutata, pärast teatud aja möödumist (idle time) kehtetuks tunnistada. Samuti tuleb seanssidele kehtestada maksimaalne kehtivus- ja kasutusaeg (timeout), et ka aktiivselt kasutatavate seansside seansi ID oleks siiski piiratud kehtivusajaga. Aeg tuleks valida piisavalt lühike, et see raskendaks Brute-Force-ründeid, kuid samas siiski piisavalt pikk, et see ei piiraks ebamõistlikult palju veebirakenduse kasutatavust. Sobiva kehtivusaja väljaselgitamiseks saab kasutada jaotises „Seansi ID-le esitatavad nõuded" kirjeldatud valemit.

Olukorras, kus veebirakenduse töös ilmnevad rasked vead, tuleks päringutes soovitud tegevused katkestada ja seanss lõpetada. Raskete vigade hulka kuuluvad näiteks erandivead (exceptions) ja tuvastatud ründekatsed. Suure turbeastme korral tuleks kaaluda seansi kehtetuks tunnistamise (invalidation) jaoks veelgi karmimate meetmete võtmist (nt kehtetud sisestused, katsed avada puuduvaid lehekülgi).

Seansi kehtetuks tunnistamisel tuleb seansi andmed nii serveris kui ka kliendis täielikult kustutada, et server seanssi enam ei aktsepteeriks ja kliendi sisse ei jääks alles teavet eelloodud seansi kohta. Näiteks võib selleks ära kustutada seansi ID-d sisaldava küpsise. Eelnevale lisaks on võimalik tõkestada mitmete paralleelsete seansside kasutamine ühes ja samas kasutajakontos. Olemasoleva seansi saab korduva sisselogimise korral kehtetuks tunnistada, nii et alles jääb ainult üks seanss. Vajaduse korral on võimalik esimesena loodud seanssi teatud piiratud aja jooksul (nt 15 min) siiski veel aktiivsena hoida ja alles siis see kehtetuks tunnistada. Paralleelse ehk teise seansi jaoks tehtava sisselogimise käigus tuleb kasutajale kuvada ka teade esimese lõppeva seansi kohta. Nii välistatakse võimalus, et kolmandad isikud saavad korduva sisselogimise järel kehtivaid, kuid enam mitte kasutatavaid seansse väärkasutada, või vähemalt raskendatakse nende tegevust. Session-Fixation-rünnete eest kaitsmiseks tuleks pärast edukat sisselogimist juba kehtiv seansi ID asendada uuega. Kehtiv seansi ID tuleks asendada uuega ka siis, kui ebaturvaliselt sidekanalilt (HTTP) minnakse üle turvalisele sidekanalile (HTTPS), sest ebaturvalist kanalit kasutades võidi muude andmete hulgas edastada ka seansi ID.

Seansiandmete kaitse

Konfidentsiaalsuse tagamiseks tuleks tekkivad seansiandmed (nt ostukorvi sisu) salvestada üksnes serverisse ja kindlasti usaldusväärsesse IT-süsteemi. Seansiandmeid tuleb kaitsta ka volitamata juurdepääsu eest, st kasutajatele tuleb rakendada juurdepääsukontrolli. Juhtudel, kus veebirakendus eeldab seansiandmete salvestamist klientsüsteemi, tuleks kindlasti ka klientsüsteemi kaitsmisel arvestada meetmega M 4.401 Konfidentsiaalsete andmete kaitse veebirakendustes .

Seansside seostamine lisaatribuutide põhjal

Seansi ID kõrval saab kasutajaid ja seansse omavahel seostada ka teiste tunnuste (nt IP-aadressi) põhjal. Nende abil saab raskendada olemasolevate seansside väärkasutust, sest seansi edukaks ülevõtmiseks läheb ründajal sel juhul peale kehtiva seansi ID tarvis ka lisatunnuseid. Lisatunnuste rakendamist kasutajate ja seansside seostamiseks tuleb kaaluda kindlasti vähemalt suurte turbenõuete-

ga veebirakenduste puhul. Kui seansside seostamiseks hakatakse lisatunnusena kasutama IP-aadressi, tuleb see salvestada serverisse ning IP-aadressi kontrollimine peab samuti toimuma serveris.

Kui IP-aadress peaks seansi ajal muutuma, tuleb see suure turbevajadusega rakenduste puhul lugeda ründekatseks ja sellele peab järgnema seansi kehtetuks tunnistamine. Siinkohal tuleb siiski arvestada, et IP-aadressi ei ole alati võimalik ilmeksimatult käsitleda ühe konkreetse kasutajana. Kui mitu kasutajat rakendavad veebirakendusega ühenduse loomiseks kas sama IP-aadressiga (reverse proxy) või muutuva IP-aadressiga proksit (nt vahelduvat, lõppevat proksit), tekib oht, et nende kasutajate IP-aadresse ei saa üksüheselt konkreetse seansiga siduda. Seega tuleb arvestada, et teatud liiki kasutajad saavad veebirakendust kasutada kas üksnes piiratud kujul või ei saa seda üldse teha. Kui identifitseeriva tunnusena kasutatakse referrer 'it, saab kontrollimisel aluseks võtta selle muutumatu andmetee (path), mis püsib kõikide pöörduste jaoks identsena (nt veebirakenduse domeeni). Sel juhul peavad kasutajad veebirakenduse ühe veebilehe referrer 'is ette näitama. Siin tuleb arvestada, et osas veebilehitsejaist saab referrer 'i edastamise välja lülitada ning sisufiltrid (content filters) võivad seda andmevälja filtreerida.
Et tõkestada seansside volitamata kasutamist, saab identifitseerimistunnused HTTP päise erinevate omaduste vahel ära jaotada. Mõeldavad on näiteks järgmised HTTP päise andmed:

- veebilehitseja tüübinimetus (User Agent Header);
- kliendi toetatavad vormingud ja keeled (Accept Header ja Accept Language Header);
- referrer (Referrer Header).

Kuna osa HTTP päise äsja nimetatud tunnustest varieerub üpris vähe, on selliste tunnustega saavutatav lisaturve samuti piiratud. Nende rakendamine suurendab aga kindlasti vajalike tööde hulka ning võib olenevalt olukorrast raskendada veaotsinguid. Seetõttu tuleks iga juhtumi korral eraldi kaaluda, kas nende rakendamiseks kuluv tööde maht on saavutatava turbega kooskõlas.

Kui veebirakenduse või veebiteenuse sessiooni haldamiseks kasutatakse järeleproovitud rakendust mingis raamistikus või levinud standardit (nagu WS-SecureConversation), on see igal juhul oma rakendusega võrreldes eelistatud, sest selle turvalisuse seiskohalt kriitilise ja keeruka funktsiooni oma rakendused osutuvad sageli haavatavaks.

Kontrollküsimused

- Kas veebirakenduse või veebiteenuse sessiooni ID-l on piisav entroopia, et pidada vastu sessiooni ID äraarvamisele (nt Brute-Force-tüüpi rünnaku kaudu)?
- Kas sessiooni ID konfidentsiaalsus on ülekandel ja kliendipoolse salvestuse korral piisavalt kaitstud?
- Kas sessioonil on piiratud kehtivusaeg (Timeout) ja kas see on vastavalt veebirakenduse või veebiteenuse kasutamise nõuetele valitud piisavalt lühike?

- Kas pärast edukat autentimist toimub sessiooni ID vahetus?
- Kas kõik sessiooni andmed (nii serveris kui ka kliendil) tühistatakse või kustutatakse pärast sessiooni kehtetuks muutmist?
- Kas sessiooni haldamisel kasutatakse järeleproovitud rakendust või levinud standardit?

M 4.395 Tõrkekäsitlus veebirakendustes ja veebiteenustes

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: arendaja, administraator

Kui veebirakenduse käitamisel peaks tekkima tõrge, tuleb sellega tegeleda nii, et säiliks veebirakenduse terviklik seisund, mis võimaldab näiteks andmeid kaitsvatel funktsioonidel edasi töötada. Veebirakendus muutub ebaterviklikuks siis, kui tõrke tõttu tekib ootamatu seisund, mille tagajärjel ei toimi andmetöötlusprotsessid enam nõuetekohaselt (nt kui andmete salvestamine ebaõnnestub, jäetakse veateade kuvamata).

Veebirakenduse terviklikku tööseisundit võivad muu hulgas ohustada järgmised sündmused:

- rakenduse kokkujooksmine;
- korrektselt lõpuni tegemata tehingud rakenduse tasandil;
- tegevuse lõpetamine tõrkest hoolimata (nt kui turvakomponendid töötavad puudulikult);
- teenuse tõkestamine (Denial-of-Service);
- õiguste volitamata suurendamine (privilege escalation);
- kahjurvarakoodi käivitamine (code execution).

Tõrgete käsitlemisel tuleb arvestada järgmiste punktidega.

Konfidentsiaalse info vältimine veateadetes

Tõrke korral peab veebirakendus suunama kasutaja neutraalse ja kohandatud sisuga lehtedele, kus ei kuvata konfidentsiaalset teavet. Ka veebiteenuste tagasiside ei tohiks vea korral sisaldada konfidentsiaalseid andmeid nagu sisemine andmetee või kasutatud tarkvarakomponentide versiooni numbrid. Vt ka M 4.400 Turbe seisukohalt oluliste andmete väljastamine veebirakendustes .

Tõrgete logimine

Esinenud tõrgete täpseks ja täielikuks mõistmiseks tuleb need logida kui sündmused, järgides meedet M 4.397 Veebirakenduste turvet puudutavate sündmuste logimine .

Protsessi katkestamine tõrke ilmnemisel

Kui veebirakenduste turvakomponendis peaks tekkima tõrge (nt kas volituste andmisel või autentimisel), tuleb soovitud tegevus katkestada ja juurdepääs soovitud ressursile või funktsioonile blokeerida. Tõrgete provotseerimine ei tohi võimaldada mitte ühestki turvamehhanismist mööda hiilida. Suure turbevajadusega veebirakenduste korral tuleks lisakaitsemeetmena kaaluda ka juba loodud ühenduse kehtetuks tunnistamist (vt M 4.394 Seansihaldus veebirakendustes).

Reserveeritud ressursside vabastamine

Veebirakendus kasutab töö käigus mitmeid ressursse, nt võrgu- ja failivooge, et tagada endale juurdepääs taustsüsteemidele, vahesalvestatud seisunditele ja muudele andmetele. Senikaua, kuni veebirakendus neid ressursse kasutab, on need veebirakenduse jaoks enamasti eksklusiivselt reserveeritud ja teised

protsessid ei saa neid kasutada.

Kui protsessis peaks ilmnema tõrge, tuleb reserveeritud ressursid, nt ajutisele failile viitav failipide (file handle), tõrkekäsitluse raames reserveeringust vabastada. Lisaks tuleb tõrkekäsitlusega ära kustutada ka vahesalvestatud failid.

Vahetu tõrkekäsitlus

Veebirakenduses esinevaid tõrkeid peaks käsitlema veebirakendus ise. Kui käsitlemata tõrge edastatakse mõnele teisele komponendile (nt rakendusserverile), võivad tõrke kõrvaldamiseks vajalikud andmed (nt andmed reserveeritud ressursside kohta) edastamisel kaotsi minna. Seetõttu ei tohiks käsitlemata jäänud tõrkeid edasi saata.

Liiga suure veatolerantsi vältimine

Kui tõrkeni viinud asjaolud ei ole täielikult välja selgitatud, ei tohi kasutusmugavuse tagamise eesmärgil tõrkega leppida, vaid kahtluse korral tuleks tegevus kindlasti katkestada. Suured tõrked peaksid alati viima tegevuse katkemiseni. Eesmärk on piisavalt kindel ja veatolerantne veebirakendus, mis suudab eristada sihipärast kasutamist väärkasutusest ja suurtest tõrgetest ning neile adekvaatselt reageerida.

Kontrollküsimused:

- Kas veebirakendustes ja veebiteenustes kuvatakse eranditult vaid selliseid tõrketeateid, mis ei avalda konfidentsiaalset infot?
- Kas tõrgetele kehtib logimiskohustus?
- Kas tõrke ilmnemisel soovitud tegevus katkestatakse ning kas selle tagajärjel blokeeritakse ka juurdepääs soovitud ressursile või funktsioonile?
- Kas tõrkekäsitluse protsessis on ette nähtud ka ressursside vabastamine reserveeringust?
- Kas tõrkeid käsitleb võimaluse korral alati seesama komponent, milles tõrge tekib?

M 4.396 Veebirakenduste kaitsmine keelatud automaatkasutuse eest

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: arendaja, administraator

Veebirakendusi kasutavad enamasti inimesed ja seetõttu pole automaatkasutust (nt skriptidega) nende jaoks ette nähtud. Seevastu Brute-Force-ründed (nt pääsuandmete mõistatamine) ja Enumeration-ründed (nt kehtivate *login* -nimede automaatne väljaselgitamine) põhinevad just nimelt veebirakenduse automaatkasutusel (*automation*). Sageli üritatakse seda tüüpi rünnete toimepanekul korduvate ja üksnes vähe varieeruvate (nt muutuva kasutajanimega) päringute abil kokku koguda konfidentsiaalseid andmeid. Et tõkestada automatiseerimist ja vältida sellega kaasnevaid ründeid, peab veebirakendus suutma eristada automatiseeritud ja käsitsi tehtud pöördusi. Automatiseeritud pöördusi iseloomustab see, et väga lühikese aja jooksul tehakse palju pöörduskatseid, mille arv erineb suuresti tavapärasest kasutusest.

Selliseid ründeid raskendab ressurssidele tehtavate korduvate pöörduste tolerantsiläve kehtestamine (nn tõrvaauk). Automatiseeritud päringute jaoks piirväärtusi kindlaks määrates tuleb arvestada, et need ei tohi liigselt takistada volitatud kasutajate töötamist veebirakendusega. Juhul kui veebirakenduse elementaarsete funktsioonide kasutamisele kehtestatakse liiga ranged piirväärtused, saavad ründajad seda ära kasutada Denial-of-Service-rünneteks. Näiteks kui kasutajakontodele on ette nähtud, et teatud arvu ebaõnnestunud sisselogimiskatsete korral blokeeritakse konto mingiks ettenähtud ajaks, võivad ründaja sihipäraselt tehtavad väärsisestused esile kutsuda korraga paljude kasutajakontode pikaajalise blokeerimise. Selle tagajärjel ei saa volitatud kasutajad blokeeringu kehtimisaja jooksul end veebirakendusse enam sisse logida. Automaatprotsessidel põhinevate rünnete efektiivsus oleneb väga sageli ka sellest, kui detailsed on andmed, mida veebirakendus päringutele vastuseks saadab (vt M 1.1 Vastavus normidele ja eeskirjadele). Järgmised näited kirjeldavad võimalikke kaitsemehhanisme:

- Brute-Force-ründeid raskendavad kunstlikult tekitatud viivitused kasutaja autentimisprotsessis, st viivitus pääsuandmete sisestamise ja ebaõnnestunud sisselogimisest informeeriva teate vahel, sest nii kulub ka automaatprotsessideks rohkem aega. Selle meetodi tõhusust saab suurendada viivitusaja progressiivse pikendamisega pärast igat ebaõnnestunud katset.
- Kui sisestusandmete vastuvõtmisest keeldutakse, tuleks selle kohta väljastatav teade sõnastada võimalikult üldistavalt. Ründajale ei tohi näiteks süsteemiteadetega anda otsest infot selle kohta, kas kasutajakonto on kehtiv, nt teate „Kehtetu parool” asemel tuleb kasutada teadet „Pääsuandmed kehtetud” (vt M 4.395 Tõrkekäsitlus veebirakendustes).
- Sageli iseloomustab ründeid suur ebaõnnestunud katsete arv. Seepärast tuleks suure arvu ebaõnnestunud katsete tuvastamisel töötav seanss kohe lõpetada ja tekitada olukord, kus kasutajal on kohustus end uuesti sisse logida.
- Automatiseeritud ründe kahtluse korral saab selle tõrjumiseks kasutada IP-aadressi ajutist blokeerimist. Siinkohal tuleb aga arvestada, et see kaitse-

meede võib mõjutada ka selliseid kasutajaid, kes pole ründega otseselt seotud (nt olukorras, kus mitu kasutajat rakendab korraga üht ja sama proksit).

- Automatiseeritud ja inimeste tehtavate pöörduste eristamiseks kasutatakse sageli nn robotilõkse ehk CAPTCHA-sid (Completely Automated Public Turing Test To Tell Computers and Humans Apart). Neil juhtudel palutakse kasutajatel täita mõni lisaülesanne (nt lugeda pildilt välja numbrid ja tähed ning need sisse tippida või vastata mõnele küsimusele), millega arvutiprogramm niisama lihtsalt hakkama ei saa. Olenevalt kasutatavast tehnoloogiast ja ülesande keerukusest võivad sellised kaitsemehhanismid väga tugevalt piirata veebirakenduse kasutusvõimalusi puuetega inimeste jaoks. Näiteks ei piisa sellest, kui ülesannet ainult ekraanil kuvada, vaid see tuleks kuuldavaks teha, et ka nägemispuudega inimesed saaksid veebirakendust kasutada. Siinkohal tuleb arvestada, et paljudes riikides loetakse CAPTCHA-sid diskrimineerivaks ning nende kasutus on kas väga rangelt reguleeritud või koguni keelatud.

Täiendavad kontrollküsimused

- Kas veebirakendus suudab tuvastada automatiseeritud pöördusi ning kas nende vastu võetakse sobivaid meetmeid, mis raskendavad automatiseeritud pöörduste tegemist või blokeerivad selle?
- Kas veebirakenduste jaoks vajalike piirväärtuste kehtestamisel arvestatakse piisavalt nende võimalike tagajärgedega (nt vastuvõtlikkusega Denial-of-Service-rünnetele)?
- Kas veebirakenduse puhul rakendatakse piiratud teabe põhimõtet?
- Kas enne kaitsemehhanismide rakendamist kontrollitakse, kas need avaldavad kasutajaskonnale piiravat mõju, mis võiks põhjustada diskrimineerimist (nt CAPTCHA)?

M 4.397 Veebirakenduste turvet puudutavate sündmuste logimine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: arendaja, administraator

Turvet puudutavad sündmused (nt ressurssidele tehtavad pöördused, autentimiskatsed) tuleb arusaadavalt logida, et vigade ja tõrgete ning ründekatsete korral oleks võimalik logiandmeid kasutada põhjuste väljaselgitamiseks. Peale meetmetes M 2.110 Andmeprivaatsuse suunised logimisprotseduurides ja M 5.9 Serveri logi logimisprotseduuridele toodud soovituste tuleb veebirakenduse turvet puudutavate sündmuste logimisel arvestada ka järgmiste punktidega.

Logimiskohustusega sündmused veebirakendustes

Serveris ja taustsüsteemides (nt operatsioonisüsteemis, veebiserveris, andmebaasis) toimuva logimise kõrval tuleb turbega seotud sündmusi logida ka veebirakenduses.

Rakenduse tasandil tuleks kajastada vähemalt järgmisi sündmusi:

- edukad ja ebaõnnestunud veebirakendusse sisselogimise katsed;
- veebirakenduse ressurssidele ja funktsioonidele tehtud pöörduste ebaõnnestunud volitamiskatsed;
- veebirakenduste sisendi- ja väljundiandmete ebaõnnestunud valideerimine;
- tekkinud vead (nt exceptions);
- veebirakenduse kasutajatele ja kasutajarühmadele antud volituste (nt pääsuõiguste) muutmine;
- kasutajakontodega seotud muudatused (nt parooli muutmine);
- veebirakenduse kustutusprotsessid (nt sissekannete kustutamine);
- tuvastatud manipuleerimiskatsed ja ootusvastased muudatused (nt sisselogimiskatsed kehtetute või aegunud seansi ID-dega);
- haldamisega seotud funktsioonide käivitamine ja konfiguratsiooni muudatused (nt kasutajaandmete hankimine, logimisfunktsiooni aktiveerimine ja desaktiveerimine);
- teenuste käivitamine ja peatamine,
- uute või olemasolevate veebiteenuste tootmise ülevõtmine (Deplyment).

Sündmuste logimiskohustusega tunnused

Turvet mõjutavate sündmuste mõistmiseks peavad logiandmed sisaldama sündmusi kajastavaid olulisi tunnuseid.

Seetõttu peavad logid sisaldama vähemalt järgmisi tunnuseid:

- kuupäev;
- kellaaeg ja ajatsoon;
- protsessiga seotud kasutajanimi;
- asjassepuutuv objekt (nt kasutajakonto, fail, andmeallikas);
- tegevuse seisund (nt ebaõnnestunud, edukas);
- esinemise koht (nt komponent);
- tegevus (nt autentimine, volitamine);

- raskusaste (nt teavitamine, hoiatus, viga).

Nende loetletud tunnuste kõrval võib olla kasulik logida veel ka järgmisi tunnuseid:

- allika (source) IP-aadress;
- seansi ID referentsid (mitte seansi ID-d);
- IT-süsteem, kus viga tekkis;
- veebirakenduse tarkvara seis (versioon).

Turbega seotud konfidentsiaalsete andmete (nt seansi ID) logimisest tuleks kindlasti hoiduda.

Sobivad andmevormingud ja mehhanismid

Kõikide logiandmete salvestamiseks tuleb kasutada ühesugust andmevormingut, et tagada nende kiire ja efektiivne analüüs. Seetõttu peaks veebirakenduse logimiskomponent kasutama mõnda sellist andmevormingut, mida saab olemasoleva lahendusega integreerida. Näiteks kui logiandmete analüüsimiseks kasutatakse mõnda tsentraalselt toimivat komponenti, tuleks valida mõni selline andmevorming, mida see komponent toetab.

Serveripõhine logimine tsentraalse logimiskomponendiga

Veebirakenduse logimiseks tuleb kasutada eranditult serveripõhist logimist, sest ainult sel juhul saab logiandmeid ka tsentraalselt analüüsida. Veebirakenduse logiandmeid peab tootma ainult üks tsentraalselt toimiv logimiskomponent, mitte mitu erinevat logimiskomponenti. Veaalteid uusarendusi tuleks logimiskomponentide valimisel kindlasti vältida. Nende asemel tuleks kasutada end juba tõestanud raamistikke (frameworks), mis toetavad enamasti nii ühte tsentraalselt töötavat logimiskomponenti kui ka enam levinud andmevorminguid.

Logiandmete kaitsmine volitamata juurdepääsude ja manipuleerimise eest

Kuna logiandmed võivad sisaldada ka konfidentsiaalseid andmeid (nt andmeid kasutaja harjumuste ning veebirakenduse ülesehituse ja konfiguratsiooni kohta), peab juurdepääs logiandmetele olema täpselt reglementeeritud ning juurdepääsu tohib võimaldada üksnes volitatud kasutajatele. Logiandmetele ei tohi juurde pääseda veebirakenduse avalike liideste kaudu. Seega tuleb logiandmed salvestada kuhugi väljapoole veebiserveriWeb-Root-kataloogi. Kui logiandmed salvestatakse mõnda andmebaasi, tuleks need tegelikest kasutajaandmetest lahutada. Lahutamiseks saab kasutada näiteks andmebaasi eraldi tabelit. Lisaks saab andmebaasi kasutaja logiandmete turvet suurendada. Selleks ei tohi andmebaasi kasutajal olla juurdepääsu andmebaasis hoitavatele logiandmetele. Suure turbevajadusega veebirakenduste puhul võib alternatiivse lahendusena logiandmed salvestada ka mõnda eraldiseisvasse andmebaasikomponenti.

Logiandmete turvaline analüüs

Ründaja võib teadlikult provotseerida kahjurvarakoodi sisaldavate logiandmete koostamist (nt andmesisestusväljade logimisfunktsiooni ära kasutades). Seetõttu tuleb logiandmete analüüsimisel tagada, et analüüsiprogramm ei hakkaks mitte mingil juhul logides sisalduvat võimalikku kahjurvarakoodi interpreteerima (nt

ei kuvaks seda veebilehitsejas ega interpreteeriks JavaScripti koodi). Kuna logiandmete analüüsimisel kehtib nõue, et logiandmete muutmine on keelatud, tuleb analüüsimiseks kasutada üksnes kirjutuskaitsega töörežiimi.

Aja sünkroniseerimine

Veebirakenduse erinevate komponentide (nt rakendus-, veebi-, andmebaasiserveri) logiandmed tuleb korreleerida, et komponentideülesed protsessid oleksid täielikult arusaadavad. Selleks tuleb erinevate süsteemide ajad sünkroniseerida. Nii kajastuvad logidesse märgitud sündmused õiges ajalises järjekorras. Selleks tuleb võtta meede M 4.227 Lokaalse NTP -serveri kasutamine aja sünkroniseerimiseks .

Kontrollküsimused:

- Kas veebirakendus või veebiteenus logivad turbega seotud sündmusi nõutavate tunnustega?
- Ega ei logita konfidentsiaalseid andmeid (nt pääsuandmeid)?
- Kas logimine viiakse läbi veebirakenduse või veebiteenuse tsentraalse komponendi poolt üksnes serveril?
- Kas logiandmetele on võimaldatud juurdepääs üksnes volitatud kasutajatele?
- Kas juurdepääs logiandmetele on lahutatud avaliku liidese kaudu?
- Kas veebirakendus või veebiteenus kasutab logimiseks andmevorminguid ja mehhanisme, mis võimaldavad integreerimist olemasolevatesse lahendustesse?
- Kas veebirakenduse või veebiteenuse komponentidele rakendatakse aja sünkroniseerimist?
- Kas kahjukoodi sisestamine logi hindamisse on takistatud?

M 4.398 Veebirakenduste turvaline konfiguratsioon

Algatamise eest vastutab: IT-juht
Rakendamise eest vastutavad: arendaja, administraator

Kui veebirakendus ei ole piisavalt hästi konfigureeritud, on ründajal võimalik turvamehhanismidest liiga kergelt jagu saada. Seetõttu tuleb veebirakenduse jaoks luua konfiguratsioon, mis lubab juurdepääsu üksnes selleks ette nähtud turvaliste andmesidekanalite kaudu. Juurdepääsu ebavajalikele ressurssidele ja funktsioonidele tuleb kindlasti piirata. Veebirakenduse konfigureerimisel tuleb arvestada järgmiste punktidega.

Tarbetute HTTP-meetodite desaktiveerimine
HTTP standardi kohaselt saab veebirakenduse juurdepääsuks kasutada erinevaid HTTP-meetodeid (nt GET, POST, PUT, DELETE, TRACE). Enamasti ei lähe veebirakenduses tarvis mitte kõiki HTTP-meetodeid, vaid ainult mõnda üksikut (nt GET ja POST). Kasutatavast HTTP-meetodist olenevalt võib veebirakendus talle laekuvatele nõuetele (requests) reageerida väga erinevalt. Näiteks kui sisestusandmete filtreerimist rakendatakse üksnes GET- või POST-nõuetele, võib ründajal õnnestuda filtreerimisest kui turbefunktsioonist mööda hiilida, nt käivitades selleks mitte ette nähtud HTTP-meetodi. Osa HTTP-meetodeid (nt PUT) võimaldab juurdepääsu ka turbe seisukohalt kriitilistele funktsioonidele (nt vabalt valitud failide üleslaadimisele), mis võimaldab omakorda mööda hiilida veebirakendusele kehtestatud piirangutest (failitüübi kontrollimisest faili üleslaadimisel). Eelnimetatud põhjustel tuleks kõik ebavajalikud HTTP-meetodid desaktiveerida ja tagada, et veebirakendus ei töötleks nende meetodite pöördusi. Sama kehtib fiktiivsete HTTP-meetodite kohta, mida RFC 2616 standardis ei defineerita. Isegi siis, kui ebavajalikud HTTP-meetodid on juba veebiserveri konfiguratsioonis desaktiveeritud, tuleb siiski tagada, et ka veebirakendus neid tarbetuid HTTP-nõudeid ei töötleks.

HTTP-POST-meetodi sundkasutus
Veebirakenduse käsitsemisel edastatakse sellele enamasti mitmesuguseid andmeid (nt andmeplankide andmed ja seansi ID). Neid andmeid võidakse edastada parameetritena URL-i sees (GET-meetod) ja HTTP-nõude kehandis (POSTmeetod).

GET-meetodi kasutamisel on konfidentsiaalsed andmed, nt andmeplangi andmed, URL-i sees (veebilehitsejas) nähtavad ning mis tahes vahelelülitatud süsteemid saavad neid logida ja salvestada. Seetõttu tuleks konfidentsiaalsete andmete edastamiseks kasutada POST-meetodit. Siinkohal tuleb arvestada, et raamistikud (frameworks) kipuvad HTTP-Request-meetodit sageli abstraheerima.

Raamistiku väär konfiguratsioon võib viia selleni, et POST-meetodi sundkasutus on ühelt poolt küll kehtestatud, kuid teisalt võib veebirakendus siiski lubada mõlemat meetodit (nt seeläbi, et raamistik kasutab HTTP-GET-Requesti edasisaatmiseks HTTP-POST-Requesti).

SSL-i/TLS-i turvaline kasutamine
Andmete edastamiseks veebirakenduse ja kasutaja klientprogrammi vahel saab andmete transpordikanalit kaitsta krüpteerimisega (nt SSL-i/TLS-iga). Konfidentsiaalseid andmeid tuleks alati edastada krüpteeritud transpordikanalis (vt M 5.66z SSL-i/TLS-i kasutamine kliendis). Samuti tuleb tagada, et olukordades, kus SSL-/TLSühenduse loomisel või andmete edastamisel krüpteeritud kanalis peaks esinema vigu, ei võetaks krüpteeritud kanali asemel kasutusele krüpteerimata kanalit. Sel juhul tuleks hoopis luua kas uus ühendus või keelduda krüpteerimata ühenduse loomisest. Konfidentsiaalsete andmete edastamist ebaturvaliste ühendustega tuleb kindlasti vältida, nt secure flag 'ide kehtestamisega küpsistele (vt M 4.401 Konfidentsiaalsete andmete kaitse veebirakendustes).

Märkide kodeerimise konfiguratsioon
Kasutaja kliendi ja veebirakenduse vahel toimuvas andmevahetuses saab andmete jaoks kasutada erinevaid kodeeringuid. Olenevalt sellest, millise kodeeringuga andmeid klient, veebirakendus või taustsüsteem ootab, võidakse neid ka erinevalt interpreteerida. Selleks, et kliendid oskaksid andmeid veebirakendusele saata õiges kodeeringus, peaks veebirakendus lehekülgede väljastamisel enda HTTPvastuste päiseväljades ära märkima ka märkide kodeerimise skeemi (nt UTF-8).

Rahvusvaheliselt kasutatavate veebirakenduste korral tuleks tähelepanu pöörata sellele, et kõik veebirakenduse loogilised tasandid ja kõik veebirakendusega ühendatud taustsüsteemid toetaks kõiki rahvusvahelisi märgikomplekte.

Konfiguratsioonifailide salvestamine väljapoole Web-Root-kataloogi Veebirakenduste konfiguratsioonifailid sisaldavad sageli konfidentsiaalset teavet, nt pääsuandmeid. Seetõttu tuleb tagada, et kasutajatel puuduks juurdepääs konfiguratsioonifailidele. Selleks tuleb konfiguratsioonifailid salvestada alati üksnes väljapoole veebiserveri Web-Root-kataloogi. Väljaspool seda kataloogi paiknevaid andmeid veebirakendus üldjuhul ei avalikusta. Konfiguratsiooniandmed tuleb alati salvestada lähtetekstist väljaspool asuvatesse eraldi konfiguratsioonifailidesse.

Konfidentsiaalseid andmeid sisaldavad konfiguratsiooniseadistused tuleb ka krüpteerida.

Piirväärtuste kindlaksmääramine
Osa kaitsemehhanisme näeb ette ka piirväärtuste rakendamist (vt M 4.396 Veebirakenduste kaitsmine keelatud automaatkasutuse eest). Piirväärtuse ületamisel tõkestatakse määratud ajaks juurdepääs vastavale funktsioonile või ressursile. Korduvad ebaõnnestunud sisselogimiskatsed võivad viia näiteks kasutajakonto blokeerimiseni (nt Brute-Force-rünnete ärahoidmiseks). Sedalaadi turbemeetmed võivad aga raskendada selliste kasutajate töötamist veebirakendusega, kes pole rünnetega üldse seotud. Näiteks kui kasutajakonto on blokeeritud, ei saa kasutajad enam veebirakendusse sisse logida. Seetõttu tuleb piirväärtuste kindlaksmääramisel arvestada ka nende võimalike negatiivsete tagajärgedega.

Failisüsteemivolituste piirangud
Veebirakendused pakuvad sageli kas otsest või ka kaudset juurdepääsu failisüsteemile, milles nad töötavad (nt käitusfailide ja upload -funktsiooniga). Et ründaja ei saaks kaitset vajavaid andmeid volitamata lugeda ega neid manipuleerida, ei piisa sellest, kui faile kaitstakse üksnes veebirakenduse pääsuõigustega, vaid rakendada tuleb ka piiratud failisüsteemivolitusi. Server, milles veebirakendus töötab, ei tule käivitada mitte administraatoriõigustega (root), vaid kindlasti piiratud õigustega.

Veebirakenduse haldamine
Veebirakenduse haldamisel tuleb eelistada sellist süsteemi, mis on veebirakenduse tööst lahutatud. Näiteks saab netikaubandusega seotud rakenduse puhul kaubaartikleid muuta eraldiseisva IT-süsteemiga, millele on antud juurdepääs veebirakenduse andmebaasile. Ideaaljuhul võiks sel süsteemil olla ainult üks kasutusotstarve ja mitte ühtki otsest ühendust veebirakendusega. Seega tohib veebirakendus kaubaartiklite andmeid hankida üksnes andmebaasist. Väga paljudes veebirakendustes on haldamiseks olemas ka samas serveris kasutatav veebiliides.

Sellist haldamisfunktsiooni tuleks vältida ning kasutada hoopis eraldiseisvat IT-süsteemi. Juhul kui haldamine samas serveris on möödapääsmatu, tuleb tagada, et haldusliidesele pääsetaks juurde üksnes haldusvõrgu kaudu ja veebirakenduse tavakasutajatele oleks juurdepääs haldusliidesele blokeeritud. Kõik sellised haldamisvõimalused, mida reaalselt ei kasutata (nt konsool), tuleb sulgeda.

Kontrollküsimused:

- Kas veebirakenduse puhul on lubatud kasutada üksnes vajalikke HTTPmeetodeid?
- Kas konfidentsiaalsete andmete (nt andmeplankide sisu) edastamisel eelistatakse HTTP-POST-meetodit?
- Kas konfidentsiaalsete andmete edastamiseks kasutatakse eranditult krüpteeritud transpordikanaleid?
- Kas on tagatud, et krüpteeritud ühenduse loomise ja krüpteeritud kanali kasutamise käigus tekkivate vigade korral ei lülituta ümber krüpteerimata kanalile?
- Kas veebirakenduse konfiguratsioonifailid salvestatakse väljapoole WebRoot-kataloogi?
- Kas veebirakenduse haldamiseks kasutatakse eraldiseisvat IT-süsteemi või kas veebirakenduse haldusliidesele pääseb juurde üksnes haldusvõrgu kaudu?

M 4.399 Andmete ja sisu kontrollitud lisamine veebirakendustesse

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: arendaja, administraator

Veebirakendus koostab enda töös veebilehti, mille sisu võib pärineda väga erinevatest allikatest. Veebilehe sisu võidakse veebilehega siduda dünaamiliselt, veebilehe koostamise käigus, kuid veebirakendus võib sisu ka ise genereerida. Kuna kasutajale tehakse veebileht kättesaadavaks valmis kujul, ei ole tal ka sageli aimu, mis allikatest kuvatavad andmed tegelikult pärinevad. Seetõttu peab veebirakendus tagama, et veebilehe koostamisel ja selle väljastamisel kasutajatele rakendataks üksnes selleks ette nähtud andmeid ja sisu. Sisu saab veebirakendusse lisada erinevate tehnoloogiatega. Alljärgnevalt on esitatud juhised enam levinud tehnoloogiate turvalise kasutamise kohta.

Failide kaasamine (File Inclusion)

Veebirakendus võib väljastatava veebilehekülje eri osade genereerimisel rakendada erinevate failide dünaamilist kaasamist (nt navigatsiooniriba). Selline lahendus vähendab veebilehe hooldustööde mahtu olukorras, kus veebilehte on tarvis muuta (nt teha uus navigeerimist puudutav sissekanne). Siinkohal on tähtis, et kaasatavate failide andmetee (path) muutmise õigus oleks kas ainult administraatoritel või suurte privileegidega kasutajatel. Seevastu tavakasutajatele peab veebilehte kaasatavate failide valimine ja muutmine (nt parameetrite muutmine) olema keelatud. Sel põhjusel ei tohi veebirakendus mitte kunagi töödelda tavakasutajate tehtud sisestusi, mille eesmärk on failide kaasamine. Olukordades, kus veebirakendusel on failide kaasamiseks kasutajasisestusi siiski tarvis, tuleb tagada, et andmeallikatena kasutatavate failide andmeteid ei saaks vabalt valida.

Kasutajatel ei tohi olla võimalik kogu andmeteed ise kindlaks määrata, vaid kasutajasisestused tuleb kapseldada juba eelmääratud andmeteede sisse. Erinevaid ründeviise, nt Path-Traversal-rünnet, kasutades võidakse üritada kaitset vajavate andmete teed vormistada relatiivsete suhete tekitamisega (nt /../../../etc/passwd), et andmetee jaoks kindlaks määratud nõuetest pääseda. Sedalaadi rünnete tõkestamiseks tuleks kasutajasisestusi kindlasti filtreerida, et tuvastada soovimatuid märke, mis võiksid andmeteed manipuleerida (nt „/” ja „\”) (vt M 1.1 Vastavus normidele ja eeskirjadele). Andmeallikatena kasutatavate failide valimisel saab failinimede asemel kasutada indekseid, millel on kindel seos serverisse salvestatud failinimedega. Nii ei saa ründaja failinimesid otseselt mõjutada ning indeksi manipuleerimine ei vii mis tahes sisu otsese kaasamiseni. Veebirakendustel on võimalik peale serverisüsteemis olevate failide kaasata veebilehte ka mujale salvestatud ressursse, kasutades selleks võrguühendust ja URL-i (Remote File Inclusion). Võimaluse korral tuleks eemal asuva sisu kaasamine täielikult blokeerida.

Kui eemal asuva sisu kaasamine on siiski vajalik, tuleb kindlasti veenduda, kas failid on piisavalt usaldusväärsed (nt rakendada whitelist -põhimõtet ja piirata allikad ühele serverile või loetleda absoluutsed URL-id).

Faili üleslaadimise funktsiooni kasutamine

Paljudes veebirakendustes võimaldatakse kasutajatel sisu kaasamiseks rakendada faili üleslaadimise funktsiooni (upload). Tüüpiline näide on kasutajaprofiilile lisatav foto. Failide üleslaadimise funktsiooni tarbeks tohib lubada ainult vajalikke andmevorminguid (nt kasutajaprofiilile fotot lisades tohib kasutada üksnes pildifaile). Siinkohal ei tule kontrollida mitte ainult failinime laiendit, vaid ka faili sisu, nt analüüsida faili päist.Üleslaaditavad failid tuleks võimaluse korral alati salvestada mõnda sellisesse kataloogi, millel puudub veebiliidesega juurdepääs (nt väljapoole veebiserveri juurkataloogi). Nii tagatakse, et kasutajal puudub enda üleslaaditud failidele otsene juurdepääs ja ta ei saa näiteks kahjulikke skripte käivitada. Kui üleslaaditavad failid salvestatakse esmalt mõnda ajutisse kataloogi, tuleb hoolitseda selle eest, et teised kasutajad nendele failidele volitamata juurde ei pääseks.

Kui veebirakendus võimaldab kasutajal rakendada ka failide üleslaadimise funktsiooni, tuleb arvestada järgmiste punktidega:

- Funktsiooni tohivad kasutada eelkõige üksnes sisselogitud kasutajad.
- Üleslaaditavaid faile ei tohi salvestada veebiserveriteenuse juurkataloogi.

Salvestamiseks tuleb kas ette anda kindlad kataloogistruktuurid, mille sisse on võimalik kaustu ja faile salvestada, või kasutada mõnda muud salvestuskonteksti (nt andmebaasi või rangelt kindlaks määratud andmeteed).

Välistada tuleb võimalus, et ründaja võiks ette antud kontekstist välja murda.

- Tuleb tagada, et kasutajad ei saaks üleslaaditavate failide salvestamiseks ette antud kindlat andmeteed muuta.
- Denial-of-Service-rünnete vastaseks kaitseks tuleks piirata lubatud failisuurust.
- Üleslaaditud failidega seotud volitusi tuleb piirata, et tõkestada volitamata juurdepääse. Nii on välistatud ka ründaja üleslaaditud failide käivitamine.
- Üleslaaditud faile tuleks kontrollida viirusetõrjetarkvaraga.
- Failinimede valimist tuleks piirata alljärgmiselt:
- failinimi ja selle laiend peavad mahtuma lubatud piiridesse (nt 200 märki);
- kõik nähtamatud märgid (nt juhtmärgid) ja kõik nende märkide kodeeritud variandid tuleks failinime seest eemaldada (nt Unicode);
- eemaldada tuleks kõik interpretaatorprogrammide jaoks eritähendusega märgid (nt ; : > < / \. * % $);
- kui võimalik, tuleb failinime laiendi jaoks lubada üksnes tähti, numbreid ja punkti.

Vastuvõetud parameetritest pärineva sisu kaasamine

Veebirakendused võtavad sisestatud andmeid sageli vastu parameetritena (nt andmeplankide andmed), töötlevad neid ja saadavad seejärel andmed vastusena tagasi (nt otsingusõnale antav vastus veebiotsingus). Ründajal võib õnnestuda seda protsessi enda huvides ära kasutada, rakendades sihipäraselt valitud andmesisestusi eesmärgiga muuta veebilehe kuva. Seetõttu tuleb kõik veebirakenduses

veebilehtede kuvamiseks kasutatavad parameetrid meetmes M 4.393 Sisestuste- ja väljastuste põhjalik valideerimine veebirakendustes ja veebiteenustes esitatud soovituste kohaselt valideerida.

Nõuete turvaline edasisuunamine (Redirect)

Veebirakenduses kasutatav edasisuunamise funktsioon ei tohi adressaatidena lubada mis tahes vabalt valitavaid veebilehti, vaid peab tagama, et kasutajad suunataks edasi üksnes usaldusväärsetele ja ettenähtud veebilehtedele. Näiteks tuleb tagada, et manipuleeritud link ei suunaks kasutajaid kasutama veebirakenduse edasisuunamisfunktsiooni, mis viib nad andmepetturlusega (phishing) tegelevatele veebilehtedele.

Edasisuunamisfunktsiooni piiramise võimalustest annavad ülevaate järgmised punktid:

- Piirdumine lokaalsete veebilehtedega - Kui edasisuunamist välistele veebilehtedele ei ole tarvis, võib edasisuunamiseks kasutatavaid aadresse kontrollida. Need ei tohi sisaldada üksnes lokaalseid aadresse. Siinkohal tuleks veebirakenduses aadresside sisestamisel lubada vaid relatiivseid andmeteid ning vajaminev host hiljem staatiliselt juurde lisada.
- Eeldefineeritud edasisuunamisaadressid - Kui edasisuunamisfunktsiooniga tohib kasutada üksnes teadaolevaid staatilisi aadresse, tuleks need salvestada serverisse eeldefineeritud loetellu koos indeksitega. Nii seotakse aadressid staatiliste indeksiväärtustega. Sihtaadressi asemel edastab klient sel juhul üksnes indeksiväärtuse (nt valib selle välja andmeplangi loetelust) ning server lisab indeksiväärtusele enda loetelust sihtaadressi.
- Käsitsi kinnitamine - Sihtaadressi kontrollimise ning seega selle usaldusväärsuse kontrollimise ja kinnitamise kohustus lasub kasutajal (nt võib ta kasutada spetsiaalset edasisuunamislehekülge). Nii kuvatakse kasutajale teave selle kohta, kui ta väljub veebirakenduse piiridest ja ühtlasi selle turvakontekstist.
- Referrer Test - Edasisuunamisfunktsioon saab lisatunnusena kontrollida ka HTTP-Requesti referrer -andmevälja, et veenduda funktsiooni sihipärases kasutamises. Edasisuunamist võidakse rakendada üksnes juhul, kui referrer -andmeväli sisaldab mõnda veebirakenduses edasisuunamiseks lubatud veebilehe sihtaadressi.

Kolmandate osapoolte sisu kaasamine

Kõikvõimalikke koostööpartnerite kaasatavaid andmeid ja mis tahes sisu (nt veebilehtedel kuvatavaid reklaame) tuleb käsitleda vähem usaldusväärse materjalina. Selliseid materjale on soovitatav põhjalikult kontrollida, sest kahjurvarakoodi ja ebausaldusväärse sisu kaasamise oht on nende puhul tavapärasest suurem.

Kontrollküsimused:

- Kas veebirakenduses on ressursside kaasamisel (nt File Inclusioni ja Remote File Inclusioni korral) nende ressursside manipuleerimine tõkestatud?

- Kas failide üleslaadimise funktsiooni kasutus on veebirakenduses piiratud (nt kas piirdutakse üksnes vajalike failitüüpidega) ning kas failide pääsu- ja käivitamisõiguste väljastamisel rakendatakse piiranguid?
- Kas failide salvestamisel on tagatud, et salvestusprotsessis kasutatakse üksnes kindlalt ette antud andmeteid (nt Path Traversali funktsiooniga)?
- Kas veebirakenduse edasisuunamisfunktsioonis kasutatavate sihtaadresside valik on piiratud (nt kas piirdutakse lokaalsete veebilehtedega) ning kas kasutajaid teavitatakse usaldusväärse domeeni piiridest väljumisest?

M 4.400 Turbe seisukohalt oluliste andmete väljastamine veebirakendustes

Algatamise eest vastutavad: erialaspetsialist, üksikute IT-rakenduste eest vastutavad töötajad

Rakendamise eest vastutavad: arendaja, administraator

Veebilehed ja veebirakendusest saadetavad vastused võivad sisaldada turbeandmeid, mida ründaja saab enda huvides (nt turbemehhanismidest möödahiilimiseks) ära kasutada. Seetõttu tuleb veebirakenduse käitamiseks ja kasutamiseks ebavajaliku turbeteabe kuvamisest kindlasti hoiduda. Järgmiste näidetega püütakse selgitada, mis liiki teavet võivad turbega seotud süsteemiteated sisaldada ning kuidas vältida liiga detailse teabe avaldamist.

Turbeteabe vältimine veateadetes

Kui veebirakenduse kasutamisel peaks tekkima mõni tõrge (nt pöörduse viga), tuleks kasutajale selle peale väljastada neutraalse sisuga veateade. Veateadete sisu ei tohi võimaldada teha järeldusi kasutatavate tehnoloogiate, turbemehhanismide ega ka veebirakenduse tööseisundi kohta. Veateated ei tohi sisaldada järgmist teavet:

- Stacktraces ja Debugging-andmed;
- teade „Kehtetu kasutajatunnus” või „Kehtetu parool” (nende asemel tuleb kasutada üldisemat sõnastust, nt „Kehtetu kasutajanimi või parool”);
- taustsüsteemidest edasi suunatud veateated, nt andmebaasi SQL-veateated (nende asemel tuleb kasutada teateid stiilis „Viga pääsuandmete kontrollimisel”);
- veakoodid „Tekkis viga” teadete asemel.

Näiteks tuleb ebaõnnestunud autentimiskatse korral väljastada üldistav teade „Valed või kehtetud pääsuandmed” ka siis, kui kasutajatunnus kehtib, et ründaja ei saaks teha järeldusi kasutajakontode eksisteerimise kohta. Erinevad HTML-koodid võivad veebilehitsejas viia ühe ja sama tulemuseni. Näiteks võidakse kahte HTML-lehekülge, milles on erinev arv tühikuid, kuvada veebilehitsejas täpselt ühtmoodi, olgugi et nende HTML-kood on tegelikult erinev. Seetõttu tuleb arvestada, et veateadetel ei pea olema mitte üksnes identne veebilehitseja kuva, vaid ka identne HTML-kood. Nii luuakse olukord, kus ründaja ei saa HTML-koodi muutmise põhjal teha järeldusi andmete osalise kehtivuse kohta (nt kehtiv kasutajatunnus, kuid vale parool). Vigade käsitlemise kohta leidub täiendavat teavet meetmes M 4.395 Tõrkekäsitlus veebirakendustes ja veebiteenustes .

Turvaline andmete kogumine väliste otsingumootoritega

Turbekommentaaride vältimine kuvatavates veebilehtedes

Veebirakenduste arendustööde käigus lisatakse kommentaare sageli otse HTML-koodi sisse. Sellised kommentaarid võivad sisaldada ka turbe seisukohalt olulist teavet, nt planeeritud tööde loendeid, versiooni numbreid, pääsuandmeid või interpreteerimata lähtekoodi, ning neid kommentaare saavad kasutajad veebilehitsejates kerge vaevaga lugeda. Seetõttu ei tohi kasutada kommentaare, mis viitavad otse turbeteabele. Ideaaljuhul peaksid töötava veebirakenduse puhul nii lähtetekstid kui ka HTML-kood olema ilma kommentaarideta.

Piiratud juurdepääs dokumentatsioonile

Veebirakenduse juurde kuuluv dokumentatsioon (nt veebirakenduse haldamise dokumentatsioon) võib ründajale pakkuda teavet potentsiaalsete turvaaukude

kohta (nt standardkasutaja seadistus vahetult pärast installimist) ja võimaldada nende põhjal ründeid ette valmistada. Seepärast tuleks veebirakenduse dokumentatsiooni ebavajalikud osad ja kõik selle juurde kuuluvad komponendid (nt andmebaas) ära kustutada. Kui veebirakenduse dokumentatsioon on kättesaadav ka online -versioonis, tuleb tagada, et sellele pääsevad juurde üksnes volitatud kasutajad. Näiteks ei tohiks veebirakenduse haldamist käsitlev dokumentatsioon olla internetis kättesaadav.

Ebavajalike failide kustutamine

Veebirakenduse tööprotsessis tekib pidevalt juurde uusi faile, mida rakenduse käitamiseks otseselt ei vajata (nt ajutised failid, failidest tehtud varukoopiad). Sellised failid võivad sisaldada turbe seisukohalt kriitilist teavet (nt katsetuste tulemusi) või funktsioone (nt katsetamiseks mõeldud tarkvaratööriistu, millega saab kindlaks teha kasutatud teekide versiooninumbri). Seda teavet saavad ründajad ära kasutada veebirakenduse ründamiseks. Samuti tuleb arvestada sellega, et eriti just ajutiste failide ja backup -failide puhul kasutatakse sageli teistsuguseid faililaiendeid (nt *.bak-failid redaktorprogrammide varukoopiatena). Kui veebiserver need failid avab, võib juhtuda, et failid jäävad tundmatu faililaiendi tõttu interpreteerimata ja selle asemel edastatakse veebirakendusele hoopis lähtetekst. Seetõttu tuleb kõik failid, mida veebirakenduse käitamiseks ei vajata, ära kustutada. Samuti tuleb regulaarselt kontrollida, kas vahepeal on tekkinud uusi sarnaseid faile ja kas need tuleks samuti ära kustutada. Kui faile pole võimalik ära kustutada, tuleb veebirakenduse juurdepääs nendele failidele blokeerida.

Andmete turvaline kogumine väliste otsingumootoritega

Võrgukeskkonda üles riputatud uue sisu ja ka muudatuste tuvastamiseks kasutavad otsingumootorid nn agente (kannavad ka nimetusi robots ja crawlers). Nendele agentidele on võimalik veebirakenduse juurkataloogis robots.txt failiga anda kohustus veebirakenduse teatud ressursse (nt andmeteid) ignoreerida . Sel viisil saab kaitset vajavad andmed otsingumootoris tehtavast indekseerimisest välja jätta. Konfidentsiaalsed ressursid (nt kataloogide andmeteed) tuleks robots.txt failis märgistada direktiiviga Disallow. Nii antakse agentidele mõista, et loetletud ressursse ei tohi indekseerida. Selleks, et robots.txt faili sisu ei annaks ründajale liigseid vihjeid veebirakenduse turbe seisukohalt kriitiliste ressursside kohta, tuleks kaitstavad kataloogid võimaluse korral koondada veebirakenduse eraldi kataloogi. robots.txt faili tuleks sisse kanda üksnes see eraldi kataloog, et fail ei sisaldaks kataloogide sisemisi struktuure ega muud turbeteavet.

Toodet ja selle versiooni kajastava teabe vältimine

Veebirakenduse erinevate komponentide vastused ja väljundid sisaldavad väga sageli ka toote nime ja versiooni numbrit. Seda liiki andmed võivad kajastuda näiteks veebilehtede HTTP-päistes või HTML-lähteteksti sisse lisatud kommentaarides. Nende andmete põhjal saab ründaja sihipäraselt otsida konkreetse toote kitsaskohti, mida veebirakenduse ründamisel sihtmärgiks võtta. Seetõttu tuleks viiteid kasutatavatele toodetele ja tooteversioonidele (nt rakenduse frameworkile, veebiserverile) kindlasti vältida.

Loobumine absoluutsetest andmeteedest

Absoluutsed andmeteed võimaldavad teha järeldusi veebirakenduse sisemiste struktuuride ja ülesehituse kohta. Näiteks saab nende põhjal välja selgitada kaitset vajavate andmete salvestuskoha. Seega tuleks absoluutsete andmeteede avalikustamisest veebirakenduses võimaluse korral alati loobuda.

Kontrollküsimused:

- Kas avaldatakse ainult andmeid, mis on vajalikud veebirakenduse või veebiteenuse käitamiseks või kasutamiseks?
- Kas veebirakendus ja veebiteenus väljastavad ainult neutraalseid veateateid ja kas need on lähtetekstis identsed?
- Kas turbega seotud andmed kustutatakse veebilehtedel (nt kommentaarides) või veebiteenuse vastustes enne kasutajale väljastamist?
- Kas veebirakenduse või veebiteenuse turbega seotud dokumentatsioonile pääseb ligi üksnes vastav adressaatide ring?
- Kas enne produktiivset kasutuselevõtmist kustutatakse kõik failid, mis ei ole vajalikud veebirakenduse või veebiteenuse käitamiseks ning kas viiakse läbi vastav regulaarne kontrollimine mittevajalike failide osas?
- Kas fail robots.txt sisaldab ainult URL-e, mis ei sisalda turbe seisukohalt olulisi andmeid?

M 4.401 Konfidentsiaalsete andmete kaitse veebirakendustes

Algatamise eest vastutavad: infoturbespetsialist, üksikute IT-rakenduste eest vastutavad töötajad

Rakendamise eest vastutavad: arendaja, administraator

Veebirakenduste puhul salvestatakse andmeid nii serverisse (nt veebirakenduses) kui ka klientidesse (nt veebilehitsejas) ning salvestamise eesmärgil transporditakse neid andmeid läbi võrkude. Need võivad olla näiteks konfidentsiaalsed pangaandmed, nagu krediitkaardi number või ülekannete andmed. Selliste andmete kaitseks tuleb võtta meetmeid, mis välistavad nende volitamata lugemise või manipuleerimise.

Üldised aspektid

Kõiki veebirakenduse tööprotsesse, mis on seotud konfidentsiaalsete andmete töötlemise, edastamise ja salvestamisega (nii serveris kui ka kliendis), tuleb kaitsta krüpteerimisprotseduuridega. Ka siis, kui veebirakendus on langenud kompromiteerimise ohvriks, peaksid krüpteerimislahendused selliseid andmeid edasi kaitsma.

Veebirakenduse konfidentsiaalsete andmete hulka kuuluvad näiteks järgmised andmed:

- pääsuandmed (nt kasutajatunnus ja parool);
- autentimisandmed (nt seansi ID);
- veebirakenduses töödeldavad kriitilised andmed (nt pangamaksete andmed või inimeste terviseandmed).

Krüpteerimisprotseduure saab kasutada nende andmete töötlemiseks, edastamiseks ja salvestamiseks nii veebirakenduses kui ka klientides.

Neid võib kasutada ka:

- andmete krüpteerimiseks;
- pääsuandmete salvestamiseks;
- transpordikanali turvamiseks.

Siinkohal on oluline, et iga konkreetse kasutusjuhu jaoks valitaks välja sobiv krüpteerimisalgoritm, mis vastab tehnika tasemele ja milles puuduvad teadaolevad turvaaugud (vt M 1.1 Vastavus normidele ja eeskirjadele). Krüpteerimisalgoritmid tuleb tööle rakendada serveris. Krüptograafia juures on eriti olulised kasutatavad võtmed. Kasutusvaldkonnast olenevalt peavad need olema ettenähtud miinimumpikkusega ja täitma mitmeid matemaatilisi nõudeid (nt olema piisavalt keerulised). Lisaks tuleb tagada võtmete turvaline transport ja vahetamine. Sama kehtib ka nende salvestamise kohta. Veebirakenduse koostamisel peavad need punktid olema reguleeritud ja krüptokontseptsiooniks kokku koondatud (vt B 1.7 Krüptokontseptsioon). Suure turbevajadusega veebirakenduste puhul tuleb vajaduse korral tagada kasutajaandmete lisakaitse. Näiteks kui veebirakendusega töödeldakse sotsiaalvaldkonna andmeid, millele kehtivad väga ranged konfidentsiaalsusnõuded, saab need veebirakenduses

enne salvestamist krüpteerida. Nii tagatakse, et ka siis, kui andmebaasile tekib otsene juurdepääs (nt andmebaasi administraatoril), ei saa keegi sealt kasutatavaid andmeid välja lugeda. Konfidentsiaalsete andmete lugemist ja manipuleerimist nende edastamisel saab ära hoida turvalise transpordikanaliga. Seega tuleks enne konfidentsiaalsete andmete edastamist kindlasti ümber lülituda turvalisele ühendusele. Andmeedastuseks tuleks turvalist ühendust kasutada ka siis, kui kasutaja on end sisse loginud. Transpordikanali turvamiseks kasutatakse siinkohal enamasti SSL-i/TLS-i (vt M 5.66z SSL-i/TLS-i kasutamine kliendis).

Klientsüsteemi salvestatud andmete kaitse

Kliendi ja veebirakenduse vahel liikuvaid andmeid võib klient vahesalvestada veebilehitseja vahemällu. Kui veebilehitseja salvestab veebirakenduse kasutaja andmeid vahemällu pidevalt, st terve seansi kestel, saavad isikud, kellel on juurdepääs vastavale arvutile, skriptide ja veebilehitseja pluginate abil need andmed vahemälust kätte, ilma et nad peaksid läbima täiendavat juurdepääsukontrolli.

Konfidentsiaalsete andmete salvestamist vahemällu (caching) saab veebirakenduses tõkestada järgmiste HTTP-päistes rakendatavate direktiividega:

- Cache-Control: no-cache, no-store;
- Pragma: no-cache;
- Expires: -1.

Kuna veebirakenduse käitaja ei saa tavaliselt veebilehitseja tööd täies mahus kontrollida, pole andmete vahesalvestamine siiski ka sel juhul täielikult välistatud. Seetõttu tuleb suure turbevajadusega veebirakenduste puhul vajaduse korral võtta ka lisameetmeid, nt panna kasutajatele kohustus, et veebirakendusega töötamise ajaks tuleb veebilehitseja vahemälu desaktiveerida või pärast töö lõpetamist see ära kustutada. Kasutajale saab näiteks pärast edukat väljalogimist kuvada teate, et ta peab veebilehitseja vahemälu ära kustutama. See puudutab eelkõige neid veebirakendusi, mida kasutatakse avalikes IT-süsteemides. Alternatiivne lahendus on juhendada kasutajat, et veebilehitsejaga töötades tuleb valida töörežiim Private Mode, mille puhul seansiandmeid vahemällu ei salvestata. Veebirakenduse kasutamise käigus salvestatakse klienti väga sageli andmeid ka küpsistena. Iga kord, kui pöördutakse veebirakenduse poole, edastatakse need küpsised kasutaja jaoks nähtaval kujul veebirakendusele. Ka need andmed võivad vajada kaitset (nt seansi ID). Seetõttu tuleks juurdepääsu konfidentsiaalseid andmeid sisaldavatele küpsistele võimalikult ulatuslikult piirata.

Juhul, kui küpsiseid koostab veebirakendus, tuleks kasutada järgmisi cookie flag 'e või hoiduda nende kasutamisest:

- Domain - Seda cookie flag 'i ei tohiks kasutada, sest sellega rakendub vaikeseadistus, mille korral vastatakse ainult selle domeeni päringutele, mis küpsise seadis. Kui vastuseid on tarvis võimaldada ka teistele (alam)domeenidele, tuleks domeeni võimalikult palju piirata, kuid need

piirangud ei tohi veebirakenduse funktsioonide kasutamist liigselt pärssida (nt domain.tld asemel tuleks kasutusele võtta webapp.domain.tld).
- Path - Path-atribuut piirab küpsise kehtivusala, st määrab küpsise kehtivusalaks veebirakenduse ühe kindlaksmääratud andmetee. Ka Pathatribuudi mõju tuleks võimalikult palju piirata, et see ei pärsiks liigselt veebirakenduse funktsioonide kasutamist (nt / asemel tuleks kasutusele võtta /webapp/).
- Secure - Kui Secure-direktiiv on kasutusele võetud, edastatakse küpsiseid vaid krüpteeritud andmesidekanalite kaudu, nt SSL-i/TLS-iga.
- HttpOnly - See direktiiv hoiab ära kliendis kasutatavate skriptide (nt JavaScripti) juurdepääsu küpsistele. Siinkohal tuleb aga arvestada, et kõik veebilehitsejad seda atribuuti ei toeta.

Järgnevalt on toodud näide käsust, mille eesmärk on küpsise koostamine eelmainitud direktiividega:

- Set-Cookie: SESSIONID=sl342kdfjslaal39skdj; path=/webapp; secure;
- HttpOnly

Kasutaja autentimiseks veebirakenduses kasutatakse sageli HTMLandmeplanki, mille sisse on vaja sisestada kasutajatunnus ja parool. Paroolireale trükitav parool ei tohi sisestamise ajal olla loetav, vaid see tuleb asendada metamärkidega (wildcards), nt tärnide või punktidega. Selleks tuleb andmeplangi defineerimisel valida parooli sisestusvälja jaoks õige väljatüüp (type="password").

Lisaks saab veebilehitsejas kasutada seadistust, mis hoiab ära konfidentsiaalsete andmete (nt kasutajanime ja parooli) salvestamise vahemällu ja nende andmete pakkumise valitavate väärtustena järgmine kord, kui andmeplank avatakse. Selleks tuleb andmeplangi defineerimisel selle päises kasutada suvandit autocomplete="Off". Seansi vältel, mil kasutaja veebirakendust kasutab, tuleb sageli salvestada kasutajaspetsiifilisi andmeid (nt virtuaalsesse ostukorvi asetatud kaubaartikleid).

Seda liiki andmeid ei saa salvestada mitte üksnes serverisse, vaid ka klienti (küpsisena) või veebilehitseja veebimällu (web storage). Konfidentsiaalsete andmete edastamist kliendile ja nende salvestamist klientsüsteemi tuleks võimaluse korral alati vältida, sest veebirakendusel puudub võimalus klientsüsteemidesse salvestatud andmeid turvata. Näiteks on veebilehitsejatega võimalik klientsüsteemis tööle rakendatud turbemehhanismidest sageli mööda minna (nt lokaalsetel kasutajatel, kel on otsene juurdepääs failisüsteemile, või ründajatel, kes kasutavad murdskriptimist). Seega tuleks konfidentsiaalsed andmed üldjuhul alati salvestada serverisse, seevastu klientsüsteemi tuleks salvestada üksnes kasutaja identifitseerimistunnus (nt seansi ID). Kui seansiandmete salvestamist klientsüsteemi pole võimalik vältida, tuleb need andmed krüpteerida ning kontrollida enne nende töötlemist veebirakenduses nende terviklust. Nii ei saa andmeid edastamise

käigus volitamata lugeda ega manipuleerida. Lisaks tuleks tagada, et andmeid ei salvestata püsivalt, vaid ainult seni, kuni seanss kestab. Web storage'i mehhanismi kasutamisel tuleks seega localStorage'i objektile eelistada sessionStorage'i objekti.

Serverisse salvestatud andmete kaitse

Funktsioonide puhul, kus kasutajad peavad end veebirakendusse sisse logima, tuleb veebirakendusse kõigepealt salvestada pääsuandmed. Et pääsuandmed oleksid ka veebirakenduse võimaliku kompromiteerimise korral jätkuvalt kaitstud, tuleb tagada, et neid ei salvestataks loetava tekstina. Selle asemel tuleks andmed ajakohaste krüpteerimisalgoritmide abil salvestada nn soolatud räsidena (salted hashes), mille puhul on loetavale tekstile juurde lisatud juhuarvude kombinatsioonid.

Siinkohal tuleks iga parooli jaoks kasutada erinevat juhuslikku soola (salt).

Lisaks tuleb tagada, et pääsuandmete salvestamisel serverisse kasutataks ilmtingimata mõnda usaldusväärset IT-süsteemi (nt seda, milles töötab veebirakendus) ning andmed salvestataks kaitstud alasse (nt väljapoole Web-Root-kataloogi või eraldi tabelisse mõnes andmebaasis). Pääsuandmeid ei tohi salvestada veebirakenduse lähteteksti (Hardcoded Passwords). Niisamuti tuleb tagada, et veebirakendusele oleks pääsuandmete suhtes antud üksnes kirjutusõigusega juurdepääs.

Pääsuandmete muutmiseks peab saama kasutada üksnes selleks ette nähtud liideseid ja veebirakenduse funktsioone, et kasutajatel ei oleks võimalik pääsuandmeid volitamata, nt otsejuurdepääsuga failisüsteemile, lugeda, muuta ega ka kustutada. Kui kasutaja soovib veebirakendusega mõnda veebilehte avada, pole see leht üldjuhul mitte kohe valmis, vaid veebirakendus koostab selle enda tööprotsessidega. Tööprotsessis avatakse koodi sisaldav fail, mida veebirakendus hakkab interpreteerima, ja selle tulemuse põhjal koostatakse veebileht.

Koostatud veebileht edastatakse kasutajale.

Seda tüüpi failid liigitatakse nende faililaiendi põhjal vastavalt kas interpretaatorprogrammi või parseri failideks. Kui faililaiend peaks muutuma, on võimalik, et need failid edastatakse kasutajatele otse, st ilma interpreteerimata. Selliste failide avamisel tekib kasutajal võimalus tutvuda programmiloogikaga ja konfidentsiaalsete andmetega, mis võivad olla salvestatud koodi sisse. See võib puudutada väga erinevaid faile, mille faililaiend ei liigita neid ei interpretaatori ega parseri juurde kuuluvaks.

Ohustatud failid on näiteks:

- ajutised failid (nt temp.tmp);
- andmevarundusfailid (nt backup.bak);

- konfiguratsioonifailid (nt config.conf);
- kaasatavad failid (nt include.inc).

Sellised failid võivad sisaldada konfidentsiaalseid andmeid, nt pääsuandmeid. Kuna juurdepääsu kontrollimehhanismid siin ei toimi, pole raske neid andmeid failidest ka kätte saada. Seega ei tohi veebirakendus edastada kasutajatele faile, mis on tegelikult ette nähtud interpreteerimiseks. Lisaabinõuna tuleks nende failide suhtes rakendada ka piiravaid failisüsteemivolitusi. Ebavajalikud failid tuleb võimalikult kiiresti kustutada (vt meetme M 4.400 Turbe seisukohalt oluliste andmete väljastamine veebirakendustes jaotist „Ebavajalike failide kustutamine").

Kontrollküsimused:

- Kas veebirakendustes kasutatakse andmete kaitsmiseks turvalisi krüpteerimisalgoritme ja kas need rakendatakse tööle serverites ning kas serveritena valitakse välja usaldusväärsed IT-süsteemid?
- Kas konfidentsiaalsete andmete edastamiseks kasutatakse veebirakendustes turvalisi transpordikanaleid (nt SSL-i/TLS-i)?
- Kas veebirakenduse HTTP-päistes kasutatakse direktiive, mis tõkestavad konfidentsiaalsete andmete vahesalvestamise klientides?
- Kas veebirakendus kasutab cookie flag 'e, et küpsiseid ei oleks võimalik volitamata lugeda?
- Kas veebirakenduse andmeplangid on konfigureeritud selliselt, et konfidentsiaalseid andmeid (nt parooli) ei kuvata sisestamisel loetava teksti kujul ja veebilehitseja neid andmeid ei salvesta?
- Kas veebirakenduse pääsuandmete kaitseks rakendatakse serveripõhiseid turbefunktsioone koos sobivate krüpteerimisalgoritmidega (salted hash)?
- Kas on tagatud, et kasutajad ei saa veebirakenduse lähteteksti sisaldavaid faile avada?

M 4.402 Juurdepääsukontroll veebirakendustes

Algatamise eest vastutavad: erialaosakonna juht, üksikute IT-rakenduste eest vastutavad töötajad

Rakendamise eest vastutavad: arendaja, administraator

Veebirakenduse volituskomponent peab tagama, et kasutajad saaksid teha ainult seda, milleks neil on olemas volitused. Volituste ja kasutajate seostamisel võib aluseks võtta kasutajarollid. Volituskomponent peaks enda töös arvestama kõikide veebirakenduses hallatavate ressurssidega. Siia kuuluvad näiteks:

- URL-id,
- failid,
- objektide referentsid,
- tööfunktsioonid,
- rakendusandmed,
- konfiguratsiooniandmed,
- logiandmed.

Pääsuõiguste kontrollimist tuleb veebirakenduses rakendada kõikidel tasanditel (nii veebirakenduses endas, rakendusserveris, veebiserveris kui ka operatsioonisüsteemis).

Seetõttu tuleb veebirakenduse pääsuõiguste kontrollifunktsiooni puhul arvestada ka veebiserveris ja taustsüsteemides olevate andmete kaitsega, nagu on kirjeldatud meetmetes M 1.1 Vastavus normidele ja eeskirjadele ja M 5.168 Taustsüsteemide turvaline sidumine veebirakenduste ja veebiteenustega . Veebirakenduse turvalise pääsukontrolli tagamiseks tuleb arvestada järgmisega.

Üldised aspektid

Volituste väljastamisel tuleb rakendada piiranguid ja järgida miinimumpõhimõtet. See tähendab, et veebirakenduse kasutajatele tuleb anda üksnes enda tööülesannete täitmiseks vajalikud volitused. Iga pöördus, mille eesmärk on saada juurdepääs kaitstud sisule või funktsioonidele, tuleb enne täitmist üle kontrollida. See kehtib ka siis, kui näiteks sama kasutaja soovib mõnele kaitstud ressursile korduvalt juurde pääseda. Ka veebitehnoloogiate (nt Ajaxi) automaatseid kliendinõudeid (client requests) tuleb käsitleda kui sõltumatuid nõudeid ja vastavalt sellele neid ka kontrollida.

Volituskomponentidele esitatavad nõuded

Veebirakendust kasutatakse tavaliselt geneerilise kliendiga, mis ei allu veebirakenduse kontrollile. Nii saab ründaja enda päringuid põhimõtteliselt piiramatult manipuleerida ja klientsüsteemides tööle rakendatud turbemehhanismidest mööda hiilida. Seetõttu tuleks alati kasutada serveripõhist volitusfunktsiooni, mis rakendatakse tööle mõnes usaldusväärses IT-süsteemis. Volitamiseks vajalikud protsessirutiinid tuleks tööle panna tsentraalselt, mitte veebirakenduse programmikoodi sisse laiali jaotada. Sel viisil lahutatakse volituskomponendi kood veebirakenduse protsessiloogikast ning välditakse ebavajalikku liiasust ja veaohtlikku lahendust.

Volituskomponentide arendamisel tuleks võimaluse korral kasutada juba olemasolevate raamistike funktsioone. Kui pääsuandmete kontrollimisel peaks tekkima viga (nt volitusprotsessis on kasutatud vajaminevast vähem andmeid), tuleb vastavate pöörduste töötlemisest keelduda. Vea korral ei tohi pöörduses soovitud ressursse kasutajale edastada ning ka funktsioonide käivitamine peab olema välistatud.

Kõikide ühe tegevusega seotud ressursside kontrollimine

Kasutajal ei tohi olla võimalik algatada ressursside suhtes tegevusi, milleks tal puuduvad volitused. Näiteks kui volitatud kasutaja peaks muutma enda pangakonto URL-i mõnda parameetrit, et tohi tal seeläbi tekkida juurdepääsu võõrale, st kellegi teise kasutaja pangakontole. Seega kui kontrollitakse üheks konkreetseks tegevuseks vajalikke pääsuõigusi, tuleks kontrolli laiendada ja sinna kaasata ka kõik selle tegevusega seotud ressursid. See puudutab muu hulgas ka veebilehitseja otsingufunktsiooni tööpõhimõtet ja konfiguratsiooni. Tähelepanu tuleks pöörata sellele, et volitamata kasutajatele ei edastataks otsingu tulemustena juurdepääsukaitsega turvatud ressursse. Selleks tuleb näiteks enne otsingutulemuste edastamist kasutajale kontrollida, kas otsingu teinud kasutajal on piisavad volitused, mis lubavad otsingutulemusi talle kuvada.

Juurdepääsukontroll URL-ide käivitamisel ja objektide referentside korral

Veebilehtede ja muude veebirakenduse ressursside identifitseerimiseks ja avamiseks kasutatakse tavaliselt URL-e. Veebilehtede ja -rakenduse funktsioonide avamiseks klõpsab kasutaja enamasti linkidel, mis kuvatakse juba valmis kujul oleval veebilehel. Kui veebirakenduse ressursse soovitakse kaitsta, ei piisa üksnes sellest, kui veebilehelt vastavale ressursile (nt administraatorite lehele) suunav link eemaldada, vaid tuleb tagada, et ressurssi ei saaks ka URL-iga otse avada. Veebirakenduses kuvatavad veebilehed koostatakse sageli dünaamiliselt objektide referentside (nt andmebaasi sissekande ID) abil. Kui sellised referentsid edastab veebirakendusele kasutaja (nt URL-i parameetritena), saab ta neid parameetreid ja seega vastavaid referentse piiramatult muuta. Kuna siin ei ole tegemist otseste referentsidega (nt viited failidele), vaid kaudsete referentsidega (viited objektidele), tuleb juurdepääsukontrolli rakendamisel aluseks võtta referentsväärtused (nt ID-d). Täiendava turbemeetmena tuleks pöördustes nõutud objektide suhtes rakendada pääsukontrolli ka taustsüsteemides. Näiteks saab sel eesmärgil kasutajate autentimise tööle rakendada taustsüsteemides (vt M 5.168 Taustsüsteemide turvaline sidumine veebirakenduste ja veebiteenustega).

Üleslaadimisfunktsiooni failisüsteemivolituste piirang

Veebirakenduse kasutajate juurdepääsu failidele tuleb üldjuhul alati piirata failisüsteemivolituste piiranguga (vt M 4.398 Veebirakenduste turvaline konfiguratsioon). Kui veebirakenduses on olemas failide üleslaadimise funktsioon, tuleb tagada, et pärast failide üleslaadimist oleks juurdepääs üleslaaditud failidele üksnes failisüsteemivolituste omanikul. Seejärel saab järgmise sammuna juurdepääsu failidele ka teiste kasutajate jaoks eraldi vabaks anda. Siinkohal tuleb alati arvestada, et üleslaaditavatelt failidelt tuleb eemaldada failide käivitamisvolitused, et ründajad ei saaks nende abil kahjurvarakoodi käivitada (vt M 4.399 Andmete ja sisu kontrollitud lisamine veebirakendustesse).

Ajutiste failide turve

Dünaamiliselt koostatavate veebilehtede puhul tekib sageli ka ajutisi faile (nt analüüsigraafikud, aruanded). Kui ajutised failid võivad sisaldada konfidentsiaalseid andmeid, ei tohi neid vahesalvestada failisüsteemi. Selle asemel tuleks need andmed edastada otsekasutajale.

Kui kaitset vajavate andmete vahesalvestamine ajutiste failidena on siiski vajalik, tuleb arvestada järgmiste punktidega:

- Failisüsteemi kasutamisega seotud pääsuõigusi väljastades tuleb rakendada piiranguid, mis tagavad, et juurdepääs antakse üksnes volitatud kasutajatele ja teenustele.
- Failinimed peaksid koosnema juhuarvudest (nt Globally Unique Identifier – GUID), et need ei annaks liiga otseseid viiteid enda sisule.
- Kõik failid, mida enam ei vajata, tuleks võimalikult kiiresti kustutada.
- Failid tuleks võimaluse korral alati salvestada mõnda sellisesse kataloogi, millel puudub veebiliidesega juurdepääs (nt väljapoole veebiserveri juurkataloogi).
- Failidele juurdepääsuks peab olema võimalik kasutada vaid selliseid veebirakenduse liideseid, mis suudavad nii pääsuandmete kontrollimisel kui ka sündmuste logimisel rakendada piisavalt tugeva toimega turbemehhanisme.

Kontrollküsimused:

- Kas pääsuõiguste kontrollimisel veebirakenduses lähtutakse kasutajate rollidest ja õigustest?
- Kas volituskomponent arvestab enda töös kõikide veebirakenduses hallatavate ressurssidega?
- Kas veebirakenduse volitamisprotsess on tööle rakendatud serveris ja toimib tsentraalselt mõnes usaldusväärses IT-süsteemis?
- Kas pääsuõiguste kontrollimise protsessis esinevate vigade korral jätab veebirakendus juurdepääsu andmata?
- Kas veebirakenduse volituskomponent arvestab enda töös URL-ide otseavamisega seotud ja objektide referentsidele kehtivate pääsuõigustega?
- Kas veebirakenduses kehtivad failisüsteemiõigused (nt failide üleslaadimise õigus) väljastatakse piirangutega?
- Kas veebirakenduses on ette nähtud turvaline ümberkäimine ajutiste failidega (nt piirangute seadmine volituste andmisel ja failide võimalikult kiire kustutamine)?

M 4.403 Päringuvõltsingu (CSRF, XSRF, Session Riding) tõkestamine

Algatamise eest vastutavad: infoturbespetsialist, üksikute IT-rakenduste eest vastutavad töötajad

Rakendamise eest vastutavad: arendaja, administraator

CSRF-rünnete (Cross-Site Request Forgery) korral seab ründaja kasutajale lõkse, mis suunavad teda kasutama veebirakenduse jaoks mõeldud käske (nt külalisteraamatusse lisatud lingid). Kui kasutaja sellel lingil klõpsab, saadetakse käsk veebirakendusele edasi ja rakendus käivitatakse vastava kasutaja kontekstis. Juhul kui kasutaja on veebirakendusse sisse logitud, kasutab ründaja tema usaldusväärset suhet veebirakendusega enda huvides ära ning käsk käivitatakse kasutaja volitustega. Seda laadi rünnete raskendamiseks peaks veebirakendus toetama turbemehhanisme, mis suudavad kasutaja soovitud tegevusi lehekülgede avamisel kolmandate osaliste edasisuunatud käskudest eristada. CSRF-rünnetega kaasnevate kriitiliste tegevuste käivitamist peaksid aitama vältida järgmised turbemeetmed.

Salajase loa (token) kasutamine

CSRF-ründe toimepanemine eeldab kehtiva HTTP-nõude järeletegemist ja selle edastamist rünnatavale. Veebirakenduse jaoks mõeldud HTTP-nõuet saab vormistada näiteks URL-iga (nt http://webapp.tld/addUser?name=user). Selleks peab ründaja teadma käivitamiseks vajalikke nõudeparameetreid, nt GET- ja POSTmuutujat.

Neid parameetreid on üldjuhul üpris lihtne välja selgitada. CSRF-rünnete tõkestamiseks saab kasutusele võtta salajase loa (token), mida ründajal on raske ära arvata. Iga kord, kui veebirakendusel palutakse avada mõni veebileht, edastatakse sellele parameetrina URL-i sees ka luba, mis paigutatakse peidetud elemendina (hidden field) andmeplangi sisse (Double Submit Cookies). Veebirakendus kontrollib iga kliendinõude (client request) korral, kas selle sees edastatud luba vastab seansi kohta salvestatud andmetele. Vea korral soovitud lehte ei avata. Seda luba tundmata ei saa ründaja kehtivat HTTP-nõuet järele teha. Kuigi ka seansi ID näol on tegemist usaldusväärse kuupäevaga, mis võiks seetõttu CSRF-rünnete tõrjumisel kõne alla tulla, tuleks praktikas eelistada siiski eraldi luba. Sellele loale peaksid kehtima seansi ID-ga sarnased nõuded.

CSRF-rünnete tõkestamiseks mõeldud turbemehhanismide juurutamisel on soovitatav rakendada juba kasutuses oleva raamistiku funktsioone, kui need on raamistikul olemas. Suure turbevajadusega veebirakenduste puhul tuleks kaaluda iga nõude jaoks eraldi lubade genereerimist – lahendust, kus iga veebirakenduse kasutuse korral saadetakse kliendile uus luba, mille ta peab seejärel veebirakendusele enda nõude sees edastama. Enne kriitiliste tegevuste käivitamist, st enne seisundit muutvate päringute täitmist (nt enne parooli muutmist), peaks kasutaja end veebirakenduses uuesti autentima. Nii ei saa neid funktsioone käivitada

märkamatult, vaid ainult pärast seda, kui kasutaja on protsessi sekkunud. Suure turbevajadusega veebirakendustes tuleks kasutada mitmest autentimisfaktorist (nt TAN, kiipkaart) koosnevat autentimisprotseduuri.

Teise võimalusena saab kasutajad kriitiliste tegevuste käivitamisel suunata ümber mõnele teisele veebilehele, kus nõutakse kasutaja sekkumist (nt palutakse tal sisestada juhuarvude kombinatsioon), et tegevus alles hiljem käivitada. Sel juhul suunatakse kasutaja algsele lehele tagasi ja tema päringut hakatakse täitma alles pärast seda, kui tema panus on olnud edukas (nt ta on sisestanud õige arvujada).

Arvujadade asemel võib kasutada ka teistsuguseid kasutaja sekkumist eeldavaid mehhanisme, nt CAPTCHA-d või vastamist küsimustele (vt M 1.1 Vastavus normidele ja eeskirjadele). Lisaturbe eesmärgil rakendatava tunnusena saab kasutada ka HTTP-nõude referrer -väljasid (nende veebilehtede URL-e, millelt kasutaja liikus praegusele veebilehele). Veebirakenduse kasutaja nõue (request) loetakse kehtivaks sageli vaid siis, kui referrer -väli sisaldab üksnes enda veebirakenduse URL-i. Nii saab lähtuda sellest, et nõude koostamisel pole klõpsatud mitte võõral, vaid enda veebirakenduse lingil. Siinkohal tuleb siiski arvestada, et referrer-välja saab nii desaktiveerida kui ka filtreerida (nt andmekaitsenõuete täitmiseks), mistõttu ei sobi selline lahendus kõikidele veebirakendustele.

Turbemehhanismide ülekavaldamine

CSRF-rünnete tõkestamiseks mõeldud turbemehhanisme, mis põhinevad referrer -väljal või lisalubadel, on võimalik üle kavaldada murdskriptimisrünnetega (Cross-Site-Scripting). Seetõttu on CSRF-rünnete tõkestamiseks mõeldud meetmete puhul kasutajaandmete filtreerimine väga tähtis (vt M 4.393 Sisestuste- ja väljastuste põhjalik valideerimine veebirakendustes ja veebiteenustes). CSRF-rünnete tõkestamiseks tuleks järgmises kahes esimeses kontrollküsimuses esitatud nõudest täita vähemalt üks.

Kontrollküsimused:

- Kas veebirakenduse kaitstud ressursside ja funktsioonide juurdepääsu turvamiseks kasutatakse seansi ID kõrval ka salajast luba (token)?
- Kas kasutaja taotluslike tegevuste tuvastamiseks veebilehtede avamisel kasutatakse veebirakenduses lisatunnusena ka HTTP-nõude referrer -välja?
- Kas veebirakendus hakkab kriitilisi tegevusi täitma alles pärast kasutaja korduvat autentimist või pärast kasutaja käsitsi sekkumist?

M 4.404 Veebirakenduste turvalise loogika kavandamine

Algatamise eest vastutavad: erialaosakond, infoturbespetsialist, üksikute ITrakenduste eest vastutavad töötajad

Rakendamise eest vastutavad: arendaja, katsetaja

Veebirakenduse tööprotsessid on keerulised ja seotud palju enamaga kui pelgalt üksikute veebilehtede kuvamisega. Protsesside tehnilisel kavandamisel tuleb pöörata tähelepanu sellele, et rakenduses realiseeritav loogika ei võimaldaks väärkasutusi. Näiteks tuleb tagada, et veebirakenduses ette nähtud tööprotsessist ei oleks võimalik välja murda ja seejärel hakata protsessi väljast juhtima. Rakendatava protsessiloogika nõuded peavad olema täpselt kindlaks määratud ja korrektselt täidetud, ühtlasi peavad need tagama, et aset leiaksid üksnes ettekavatsetud ja lubatud tööprotsessid. Kõik sellest nõudest kõrvale kalduvad protsessid tuleb tõkestada. Näiteks kui veebirakenduse soovitamisfunktsioon on ette nähtud üksnes artiklisoovituste edastamiseks, tuleb arvestada, et seda funktsiooni on võimalik väärkasutada ka rämpsposti saatmiseks. Seevastu kui edastatavate soovituste tekst on kindlalt ette antud, siis rämpsmeile selle funktsiooniga saata ei saa. Samuti tuleb kontrollida, et protsessiloogikas ei oleks vigu, mis lubaks korraga kahte seanssi (concurrent sessions) ehk konkureerivaid tingimusi (race conditions). Seetõttu tuleb veebirakenduse kontseptsiooni väljatöötamisel kõik funktsioonid dokumenteerida koos nende kasutusotstarbega (use cases). Siinkohal on oluline, et kirja pandaks kogu info selle kohta, mis otstarbel funktsioone kasutatakse ning mis meetmed on ette nähtud nende väärkasutuse tõkestamiseks. Olukordades, kus veebirakenduse töö mis tahes põhjusel katkeb, peab protsessiloogika tagama, et veebirakendus taastaks enda ette nähtud seisundi (roll back). Veebilehtede interaktiivseid funktsioone saab realiseerida ka klientsüsteemis käivitatava aktiivsisuga (nt JavaScriptiga). Samas saab neid funktsioone tihti pakkuda ka dünaamilise või staatilise sisuna. Kuna klientsüsteemides on aktiivsisu kasutamine turbenõuete tõttu sageli desaktiveeritud, on soovitatav veebirakenduse kontseptsioonis aktiivsisust loobuda ja kasutada selle asemel serveripõhist rakenduseloogikat. Veebirakenduse interaktiivsete funktsioonide jaoks on olemas erinevad lahendused: serveri- ja kliendipõhised lahendused.

Kuna veebirakendus ei saa klienti kontrollida, pole ka kliendi väärkasutust võimalik välistada. Veebirakenduste ja neis hoitavate andmete ründamiseks on seni kasutatud ja kasutatakse kindlasti ka tulevikus eriti just aktiivsisu, nt JavaScripti ja ActiveXi. Seetõttu on turbe seisukohalt soovitatav aktiivsisu tööle rakendada kas serveris või, kui vähegi võimalik, aktiivsisust üldse loobuda.

Kui aktiivsisu kasutamine on siiski möödapääsmatu, tuleks arvestada järgmisega.

- Veebirakendust peab saama edasi kasutada ka siis, kui aktiivsisu käivitamine on veebilehitsejas desaktiveeritud.
- Aktiivsisu kasutamisel peab olema võimalikult hästi aru saada, mis allikast see pärineb, et kliendis oleks võimalik seda tõhusalt kontrollida. Kontrolliks saab kasutada näiteks ActiveXi komponentide signatuure.
- Kui Ajaxit kasutades pole XML-andmete serialiseerimist ja dünaamilist koostamist võimalik vältida, tuleks eelistada raamistikke (frameworks).
- JavaScripti kasutades tuleks loobuda eval()-funktsiooni käivitusest.

- Kui veebirakenduses rakendatakse andmevahetuseks JSON-i, tuleb objekte kasutada eranditult kui top level -elemente.

Näited:

- Veebirakendus autendib kasutajad mitmes järjestikuses etapis. Esimeses etapis peavad kasutajad sisestama oma kasutajatunnuse ja parooli ning teises etapis autentimisloa (token). Siinkohal tuleb tagada, et kasutajad ei saaks esimest etappi vahele jätta ning kõik ette nähtud autentimistunnused sisestataks kindlasti. Viimases etapis leiab aset lõplik autentimine, milleks tuleb uuesti rakendada autentimistunnuste kontrolli.
- Pangatehingute jaoks ette nähtud veebirakenduse puhul tuleb juba kontseptsiooni koostamisel arvestada sellega, et kasutaja võib ülekannete jaoks mõeldud andmeplanki sisestada ka miinusmärgiga arve. Sel juhul peab veebirakendus tagama, et protsessiloogikat ei pööratakse pea peale ja kasutaja ei saaks ülekande asemel endale hoopis raha volitamata juurde.

Kontrollküsimused:

- Kas veebirakenduse funktsioonid on dokumenteeritud koos kasutusotstarbega (use cases)?
- Kas dokumentatsiooni üles märgitud kasutusotstarbed hõlmavad ka veebirakenduse funktsioonide väärkasutuse tõkestamist?
- Kas veebirakenduste puhul on analüüsitud võimalusi, kuidas saaks loobuda aktiivsisu kasutamisest?
- Kas aktiivsisu kasutamisel piirdutakse vaid hädavajalikuga?

M 4.405 Ressursside blokeerimise (DoS-rünnete) tõkestamine veebirakendustesja veebiteenustes

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: arendaja, administraator

Veebirakendused ja veebiteenused pakuvad kasutajatele sageli funktsioone, mis tarbivad intensiivselt kõikvõimalikke ressursse (nt keerukaid andmebaasipäringuid). Olukorras, kus suur hulk selliseid palju arvutusressurssi vajavaid operatsioone käivitatakse teadlikult järjest või kus veebirakendus koormatakse üle päringutega, võib see veebirakenduse tööd tugevalt pärssida ja selle kasutuse isegi peatada. Selliseid tegevusi nimetatakse Denial-of-Service-rünneteks (DoS). Nii nagu Brute-Force- ja Enumeration-ründed, põhinevad ka DoS-ründed enamasti automaatprotsessidel (vt M 4.396 Veebirakenduste kaitsmine keelatud automaatkasutuse eest). Seetõttu tuleb ka DoS-rünnete vastu kasutada sarnaseid turbemehhanisme. Selle alla kuuluvad näiteks allkirjeldatud meetmed. Juhiseid, milliseid spetsiifilisi kaitsemeetmeid tuleks veebirakenduse vastu suunatud Denial-of-Service-rünnete tõkestamiseks võtta, pakuvad ka järgmised näited:

- piirväärtuste kindlaksmääramine (nt ressursi ajutine blokeerimine korduvate ebaõnnestunud pöörduste korral);
- päringute esitamise ja töötlemise vahele jääva ajavahemiku teadlik pikendamine (nt korduvate edutult lõppenud sisselogimiskatsete korral);
- avatava IP-aadressi ajutine blokeerimine ründekahtluse korral;
- CAPTCHA-de kasutamine;
- sisestuste kinnitamine sisestusväljadel, enne kui alustatakse arvutusmahukaid operatsioone;
- XML-filtreerimismehhanismide ja XML-valideerimiskontrollide kasutamine.

Niisamuti sisaldavad ka järgmised näited juhiseid selle kohta, milliseid spetsiifilisi kaitsemeetmeid tuleks veebirakenduse vastu suunatud Denial-of-Service-rünnete tõkestamiseks võtta:

- DoS-ründed ohustavad kõige enam intensiivse ressursikasutusega operatsioone. Seetõttu tuleks iga kasutaja jaoks kehtestada piirang, st maksimaalne lubatud ressursikasutuse maht. Samuti tuleks juurdepääsu teatud liiki operatsioonidele (nt keerulise ülesehitusega andmebaasipäringutele) võimaldada üksnes sisselogitud kasutajatele.
- Iga kasutaja kohta tuleks lubada ühel ja samal ajal vaid ühe päringu töötlemist. Sama kasutaja mitme päringu töötlemine tuleks jaotada sekventsideks.
- DoS-rünnete koormavat mõju on võimalik osaliselt leevendada veebilehti avavate pöörduste vahesalvestamisega (caching). Nii ei käivitata igat soovitud ja palju arvutusressurssi nõudvat operatsiooni mitte kohe, kui pöördus laekub, vaid see fikseeritakse üksnes vahesalvestatud tulemusena. Ressursse tugevalt koormavate päringute teket on võimalik väiksema koormusega aegadel ka juba ette välja arvutada (varem kokku koondada).
- Veebirakenduse arhitektuur ja voogude kontroll peavad olema välja töötatud selliselt, et ressursimahukaid operatsioone peab saama vältida (nt seansi ID koostamisel tuleks kasutada vähe ressursse tarbivaid operatsioone). Ressursimahukate operatsioonide tuvastamiseks saab kasutada koormuskatseid.

- Mälumahu ammendumine logimisfunktsiooni töös võib põhjustada olukorra, kus kirjutusõigusega juurdepääsud andmekandjale blokeeritakse. Kui salvestamisprotsesse juhib veebirakendus, võib see ohustada veebirakenduse käitamist. Seetõttu tuleks juurdepääsu andmesalvestile piirata ja regulaarselt kontrollida, kas mälu on veel piisavalt. Samuti tuleks piirata töömälu kasutamist (RAM per thread).
- SOAP-sõnumid tuleb valideerida vastavalt XML-skeemile. Kui valideerimine ei ole edukas, sest see sisaldab elementidel näiteks defineerimata arvu, ei tohi SOAP-sõnumit edasi töödelda, sest see võib sellisel juhul kaasa tuua probleemid töötlemisel XML-parseri kaudu.

Veebirakenduste ja veebiteenuste korral, mille puhul tuleb nende iseloomu tõttu arvestada näiteks poliitiliselt motiveeritud DoS-rünnetega internetist, võib olla kasulik ka koostöö teenuseosutajaga, kes on spetsialiseerunud DoS-rünnete tõrjumisele. Sellised teenuseosutajad juhivad ründe korral IP-liikluse oma süsteemide kaudu, mis filtreerivad juurdepääsud ja/või vabastavad sihtsüsteemid muude meetmetega nagu näiteks vahemäludega (Cashing). Seejuures tuleb eelnevalt kaaluda, kas andmevoogude ümberjuhtimine kolmandate isikute kaudu tekitab lisaohtusid või -nõudeid. Üks armastatuim ründemeetod vahemäludega veebilehtedele on näiteks see, et ründe toimepanija käivitab olematud alalehekülje. Kui teenuseosutaja seda kinni ei püüa ja päringu arvatavalt uue alalehekülje kaudu algsele leheküljele suunab, teostab teenuseosutaja ettekavatsematu DoS-ründe. Selliste uute ründevektoritega peab Anti-DoS-teenuseosutaja valikul arvestama.

Kontrollküsimused

- Kas veebirakendused ja veebiteenused väldivad ressursimahukate operatsioonide rakendamist ja kasutamist ja kas need on eriti kaitstud?
- Kas veebirakendused ja veebiteenused teostavad järelevalvet protokolliandmete võimaliku üleliigse täitumise üle ja takistavad seda?
- Kas SOAP-sõnumid valideeritakse vastava XML-skeemi abil?
- Kas kriitiliste teenuste ja rakenduste korral kontrolliti koostööd Anti-DoS-teenuseosutajaga?

M 4.406z Clickjacking-rünnete tõkestamine

Algatamise eest vastutavad: arendusosakonna juht, üksikute IT-rakenduste eest vastutavad töötajad

Rakendamise eest vastutavad: arendaja, administraator

Veebirakenduse langemisel Clickjacking-ründe ohvriks ühendatakse veebirakenduse sisu nähtamatu raamiga. Kui kasutaja külastab sel viisil rünnatud veebilehte, röövib nähtamatu raam nähtavas sisus tehtud klõpsud kasutaja teadmata endale. Kui kasutaja on enne seda end juba sisse loginud, saab ründaja volitamata käivitada veebirakenduse tegevusi, mille suhtes peaksid tavaolukorras rakenduma pääsuõiguste kontrollifunktsioonid. Selle ärahoidmiseks peab veebirakendus tagama, et sisu ei oleks võimalik kasutada raamidega.

Eelnimetatud põhjustel tuleb Clickjacking-rünnete tõrjumiseks võtta järgmisi kaitsemeetmeid:

- Veebilehtedega integreeritud kood (nt JavaScript) peab kliendis kontrollima ja tagama, et veebirakenduse sisu kuvatakse veebilehitseja aknas kõige ülemisel tasandil. See peab takistama teiste tasandite ladustamist veebilehe algse sisu peale. Kui see ei ole võimalik, tuleks blokeerida veebirakenduse kuva (vt veebirakenduse mooduli abivahendite alajaotist „Clickjackingründeid tõkestav skript”).
- Veebilehtede väljastamisel veebirakenduses tuleks lisameetmena HTTPvastuse päises kasutada direktiivi X-FRAME-OPTIONS. Direktiiv XFRAMEOPTIONS DENY tõkestab veebilehe sisu kuvamise raamide sees. Selle asemel saab rakendada piiranguid ka selliste lehtede suhtes, mis ei pärine samast domeenist (X-FRAME-OPTIONS SAMEORIGIN).

Kontrollküsimused:

- Kas kõikide veebirakenduses kuvatavate veebilehtede puhul on tagatud, et sisu kuvatakse üksnes veebilehitseja kõige ülemistel tasanditel?
- Kas veebirakenduse HTTP-vastuse päistes kasutatakse direktiivi XFRAME-OPTIONS?

M 4.407 OpenLDAP kasutamise logimine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: erialaspetsialist, administraator

Kuna OpenLDAP toimib enamasti võrgu tsentraalse komponendina, on OpenLDAP-ga seotud tegevuste puhul oluline rakendada nii logimist kui ka seiret, et tuvastada varakult näiteks võimalikke tehnilisi probleeme ja ründekatseid. Sündmusi kajastavate logide koostamiseks ja süsteemi hetkeseisundi seireks on OpenLDAP-s mitu võimalust. Logifaile tuleb organisatsiooni sisenõudeid järgides regulaarselt analüüsida, et tuvastada võimalikke väärkasutusi ja süsteemi vigu. Kasutajate haldamiseks rakendatava kataloogiteenuse logimise ja seire käigus tekib vältimatu kokkupuude isikuandmetega, mille alusel saab analüüsida nii jõudlusnäitajaid kui ka inimeste käitumisharjumusi. Seepärast tuleb logimis- ja seirefunktsioonide juurutamisel kaasata protsessi ka andmekaitsespetsialist (vt ka M 2.110 Andmeprivaatsuse suunised logimisprotseduurides) ja töötajate esindus. Logisid saab analüüsida kas käsitsi või analüüsitarkvaraga. Eeltööna tuleks defineerida, mis sündmused loetakse kriitiliseks, st mis olukordadest tuleb kindlasti teavitada mõnda administraatorit.

Debug ja Syslog

slapd-serveril on olemas ka nn silumisfunktsioon (Debug), millega saab tuvastada eelkõige tehnilisi vigu. Selle funktsiooni kasutamiseks tuleb slapd-server käivitada parameetriga „-d”:

slapd -d [Loglevel] -d [Loglevel] . . .

Kui slapd-server käivitatakse parameetriga „-d”, jäetakse slapd-server, erinevalt silumisfunktsioonita käivitusest, käivitavast lahutamata ja serverit käitatakse esiplaanil. Silumisfunktsiooni teadete jaoks kasutatakse standardset teavitusfunktsiooni, st enamasti käivitavat terminali. slapd-server suudab silumisfunktsiooni teateid edastada ka süsteemiteenusele Syslog, mida kasutavad ka muud tsentraalsed seiretööriistad. Selleks tuleb serveri käivitamisel parameetri „-d” asemel kasutada parameetrit „-s”, logitasandi (log level) arvud ja alias ’ed jäävad samaks. Sama tulemus saavutatakse ka logitasandi sisestamisega globaalsesse direktiivi logLevel (slapd.conf) või olcLogLevel (slapd-config). Syslog ja teised tsentraalselt toimivad tööriistad sobivad väga hästi suurte struktuuride jaoks, kus sündmuste käsitsi kontrollimine ei ole enam mõeldav. Seevastu kiireloomuliste probleemide lahendamisel on konsoolis kasutatav silumisfunktsioon siiski tõhusam, sest koormuse suurenedes kajastab Syslog hetkesündmusi sageli viivitusega ning suure teadete arvu korral on oht, et see jätab osa neist töötlemata.

Tehnilistest logidest ei ole palju abi mitte üksnes kiireloomuliste tehniliste vigade tuvastamisel, vaid ka konfiguratsioonis seni märkamata jäänud kitsaskohtade leidmisel. Näiteks kui logist saab välja lugeda, et päringutes otsitakse väga sageli üht kindlat atribuuti, mille jaoks indeks puudub (index_param failed), tuleks see olukord lahendada, st koostada indeks, et otsingutes ei tekiks enam pikki viivitusi. Samas tuleb arvestada, et silumisfunktsioon ei sobi kataloogiteenuse erialase kasutamise logimiseks. Seetõttu tuleb vastavaid väljundeid pärast analüüsimist regulaarselt kustutada.

Logimine overlay ’ga auditlog

Overlay auditlog (Audit Logging) võimaldab andmebaasis tehtud muudatusi salvestada LDIF-vormingus failidena. See overlay suudab muudatusi üksnes üles kirjutada, kuid on halvasti kohandatav. Samuti on selle funktsioonide hulk palju väiksem kui uuemal overlay 'l accesslog. Overlay 'd auditlog rakendatakse mõnikord juhtudel, kus puudub vajadus fikseerida asetleidnud pöördusi või kus on koguni tarvis seda vältida, nt kehtivate andmekaitsenõuete tõttu.

Logimine overlay 'ga accesslog

Overlay accesslog (Access Logging) võimaldab fikseerida kõiki andmebaasile tehtud pöördusi. Seda overlay 'd kasutatakse ka Delta-replikatsioonides. See võimaldab fikseerida üksnes muutunud atribuudid, et seejärel saaks replikeerimisprotsessis tarbijale (consumer) edastada vaid muutused (vt M 4.389 OpenLDAP partitsioonid ja replikatsioonid). Overlay 'l on järgmised omadused:

- logops-alamdirektiiviga on võimalik logimisfunktsiooni piirata kindlate operatsioonide jaoks, nt üksnes kirjutamisõigusega pöörduste logimiseks.
- Samuti on võimalik fikseerida ebaõnnestunud pöördusi (alamdirektiiviga logsuccess FALSE). Kui ebaõnnestunud pöördusi tekib suurel hulgal, tuleks neid lähemalt analüüsida. Võimalikud põhjused on järgmised:
- valesti antud pääsuõigused,
- kasutajate ebapiisav juhendamine,
- ründaja üritab kataloogiteenuses käivitada keelatud operatsioone.
- Logiandmed salvestatakse teise andmebaasi, mis määratakse kindlaks alamdirektiiviga logdb. Pääsuõiguste andmise ja andmebaasi replikeerimise hästi läbimõeldud lahenduse korral saab pöörduste fikseerimise administraatorite mõjualast välja jätta.
- Kuna tehtud pöördused salvestatakse LDAP-andmebaasi, saab sissekannetele ka LDAP-ga juurde pääseda. See omakorda võimaldab kasutada palju mugavamaid analüüsilahendusi kui tavapäraste tekstifailina koostatud logide puhul.
- Overlay 'le on võimalik alamdirektiiviga logpurge anda käsk andmebaas määratud intervalli järel kustutada, nt käsk kustutada iga päev kõik sissekanded, mis on vanemad kui kaks nädalat.

Selle funktsiooniga saab muu hulgas tehniliselt toetada andmekaitsenõuete täitmist. Overlay accesslog on parim vahend, mis võimaldab koostada kataloogiteenuse erialast kasutamist kajastavaid logisid.

back-monitori kasutamine seires

Logifailide analüüsimisel avastatakse turbe seisukohalt olulised sündmused, nt turvaintsidendid, enamasti alles tagantjärele. Seevastu institutsiooni kataloogiteenuse kui tsentraalselt toimiva tarkvara puhul tuleb seirefunktsioonidega (monitoring) jälgida ka töötavat süsteemi. OpenLDAP-s on selleks vajalikud funktsioonid koondatud tagaprogrammi back-monitor. Kuna seirefunktsiooniga töödeldakse ka kaitset vajavaid andmeid, tuleks selle tagaprogrammi jaoks kaaluda enda ACL-i kasutamist (vt M 4.387 OpenLDAP pääsuõiguste turvaline andmine). Erinevalt paljudest teistest andmebaasidest OpenLDAP-s, on sufiks siinkohal kindlalt ette antud. See on alati CN=monitor. back-monitor kuulub dünaamiliste tagaprogrammide klassi, st ldapsearch-i või mõne muu sellise tööriistaga

tehtud otsingute puhul ei pöörduta mitte juba valmis kirjutatud andmekogumi poole, vaid andmed genereeritakse päringu alusel. Kasutaja jaoks jääb kõik siiski ülevaatlikuks, sest tagaprogrammi back-monitor saab kasutada OpenLDAP ldapsearch-tööriistaga, graafiliste kasutajaliidestega ja ka spetsiaalselt seire otstarbeks loodud rakendustega. Tagaprogrammiga back-monitor kogutavad andmed on väga mahukad ja nende hulk suureneb proportsionaalselt OpenLDAP-s kasutusele võetud funktsioonidega. Seetõttu on soovitatav koostada dokumentatsioon kohustuslike väärtuste kohta, millele tuleks analüüsimisel tähelepanu pöörata. Seirefunktsiooniga on mõttekas jälgida näiteks allnimetatud objekte:

- CN=Backends, CN=Monitor - See sufiks kogub teavet kasutatavate tagaprogrammide kohta. Lapselemendid sisaldavad teavet tagaprogrammi, selle seisundi ja toetatud funktsioonide kohta.
- CN=Databases, CN=Monitor - Databases hangib teavet sisseseatud andmebaaside kohta. Lapselemendid sisaldavad teavet vastava andmebaasi kohta.
- CN=Overlays, CN=Monitor - See osapuu sisaldab teavet kasutatud overlay 'de kohta. Lapselemendid sisaldavad teavet vastava andmebaasi kohta.
- CN=Connections, CN=Monitor - Connections sisaldab teavet olemasolevate ühenduste kohta. Lapselemendid sisaldavad detailset teavet konkreetse ühenduse kohta. Nende kõrval on olemas ka kaks spetsiaalset lapselementi, mis kajastavad koguarvu (CN=Total, CN=Connections, CN=Monitor) ja olemasolevaid ühendusi (CN=Current, CN=Connections, CN=Monitor). Olemasolevaid ühendusi tuleks kontrollida eelkõige enne kataloogiteenuse töö peatamist.
- CN=Listener, CN=Monitor - See sufiks kajastab andmeid IP-aadresside ja portide kohta, mille puhul slapd-server on ühenduste loomise ootel. Regulaarselt tuleks kontrollida, et aktiivsed oleksid üksnes teadlikult sisse seatud ühenduse loomise võimalused.
- CN=Operations, CN=Monitor - Operations kajastab andmeid algatatud ja lõpetatud operatsioonide kohta. Võimalike väljundite valik on väga suur. Seda tuleks kasutada üksnes vajaduse korral ning seejärel vastavad operatsioonid, nagu bind , add ja delete , välja filtreerida. Enne kataloogiteenuse töö peatamist tuleks kontrollida, mis operatsioonid on veel pooleli.
- CN=Statistics, CN=Monitor - Osapuus kajastuvad statistilised andmed serverist edastatud andmete kohta. Väljundite jaoks tuleks jooksvalt koostada ka andmeajalugu, et selle põhjal saaks regulaarselt tuvastada võimalikke anomaaliaid.

OpenLDAP seire peaks olema integreeritud OpenLDAP-d käitava IT-süsteemi omaga. OpenLDAP töö sõltub suurel määral andmebaasi jaoks kasutada olevast protsessorivõimsusest ja mälumahust. Nende näitajate kohta OpenLDAP seirefunktsioonid andmeid ei kogu.

Täiendavad kontrollküsimused:

- Kas OpenLDAP-s aset leidvaid tegevusi logitakse?

- Kas silumisfunktsiooni (Debug) väljundeid kasutatakse üksnes OpenLDAP tehniliste probleemide lahendamiseks ja kas neid kustutatakse regulaarselt?
- Kas slapd-serveri tööd jälgitakse selliste sobivate seiretööriistadega nagu back-monitor?
- Kas OpenLDAP logisid analüüsitakse regulaarselt, et kontrollida organisatsioonisiseste nõuete täitmist?
- Kas OpenLDAP-d käitava IT-süsteemi suhtes rakendatakse samuti seirefunktsioone?

M 4.408w Windows Server 2008 uute turbefunktsioonide ülevaade

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

Windows Server 2008 kasutuselevõtuga viidi operatsioonisüsteemi standardinstallatsiooni tööd miinimumini ning parandati seeläbi märkimisväärselt üldist turvet, sest pärast alusinstallatsiooni tegemist on tarvis aktiveerida ja konfigureerida üksnes vajaminevaid teenuseid. Samuti on Windows Server 2008 jaoks välja arendatud või kasutusse lubatud mitmeid uusi turvet puudutavaid tööriistu ja funktsioone. Järgnev ülevaade kajastab Windows Server 2008 olulisimaid turbeuuendusi ja viitab asjakohaseid valdkondi detailsemalt käsitlevatele lisameetmetele.

Server Manager

Server Manager on Windows Server 2008 tsentraalselt toimiv haldustööriist. Selle tööriistaga saab hallata rolle, valikuid (features), tulemüüri ja teenuseid. Osa konfiguratsioonide jaoks saab kasutada ka turbekonfiguratsioonide viisardit (SCW), mis on alates Windows Server 2008-st süsteemi kindel osa.

Server Core Installation

Server Core on minimaalne, enamjaolt ilma graafilise kasutajaliideseta töötav süsteem.

Server Core'i eelised on järgmised:

- vältimatute tarkvarahooldustööde mahu vähenemine;
- vältimatute haldustööde mahu vähenemine;
- süsteemi ründevõimaluste vähenemine.

Lisateavet Windows Server Core'i kasutamise kohta leiate meetmest M 4.416z Windows Server Core'i kasutamine .

Authorization Manager

Authorization Manager on Windowsi süsteemidele ja rakendustele mõeldud rollipõhise turbearhitektuuriga lahendus, mida on Windows Server 2008 jaoks edasi arendatud. See on oluline eelkõige Hyper-V haldamisel, kus host - ja guest - süsteemide haldamiseks kasutatakse vajaduse korral rollipõhist lahutamist (vt M 2.490 Hyper-V-ga virtualiseerimise planeerimine).

BitLockeri ajamikrüpteering

BitLockeri ajamikrüpteeringut saab kasutada ka Windows Server 2008 keskkonnas (vt M 4.337z BitLockeri Drive Encryption kasutamine).

Krüpteeriv failisüsteem (EFS)

Alates Windows Server 2008-st kätkeb EFS endas järgmisi uuendusi:

- krüpteerimissertifikaadi salvestamine kiipkaardile;
- failide kasutajapõhine krüpteerimine klientsüsteemi vahemälus;
- grupipoliitikate täiendatud valik.

Lisateavet EFS-i kasutamise kohta leiate meetmest M 4.147z EFS-i turvaline kasutamine Windows 'i keskkonnas .

Kasutajakontode juhtimine

Kasutajakontode juhtimist saab alates Windows Server 2008-st rakendada ka serverisüsteemides (vt M 4.340 Windows kasutajakonto haldamise (UAC) kasutamine).

AppLocker

Alates Windows Server 2008 R2 kasutuselevõtust asendab AppLocker kõiki varem kasutatud tarkvara piiramise poliitikaid. Sellega on võimalik juhtida failidele tehtavaid pöördusi, tõkestada teatud tüüpi failide, nt. exe ja.bat avamist ja DLLide käivitamist (vt M 4.419z Rakenduste juhtimine AppLockeriga alates Windows 7-st).

Active Directory

Kataloogiteenuses Active Directory on tehtud rohkelt uuendusi. Tähtsamad nendest on järgmised:

- võimalus installida Active Directory teenuseid eraldiseisvate rollidena. Selline lahendus lubab minimeerida Active Directory installatsiooni ja jagada AD rolle ühekaupa eraldiseisvatesse süsteemidesse laiali;
- Read-Only Domain Controlleri (RODC) juurutamine süsteemina, millel on Active Directoryle üksnes lugemisõigusega juurdepääs;
- uued haldusotstarbelised teenusekontod teenuste ja paroolide tsentraalseks haldamiseks Active Directorys ja hallatavad lokaalsed kontod ;
- paroolide ja kontode blokeerimise suuniste varasemast detailsemad konfigureerimisvõimalused, mis lubavad paroolisuuniseid domeeni sees paremini kohandada.

Lisateavet leiate meetmetest M 4.284 Teenuste rakendamine alates Windows Server 2003-st ja M 4.414w Windows Server 2008 Active Directory uuenduste ülevaade .

Windowsi tulemüüri laiendatud turve

Windows Server 2008 nn Hostfirewall on pärast installatsiooni standardseadistuses aktiveeritud ning blokeerib sissetulevaid ja vajaduse korral ka väljaminevaid ühendusi. See töötab seisundipõhiselt ning filtreerib kõiki IPv4- ja IPv6-ühendusi.

Võrgusidet kasutavaid rakendusi saavad administraatorid ühekaupa lubada ja blokeerida. Serverirollide muudatuse ja valikute (features) aktiveerimisel lülitatakse vajalike portide või protokollide kasutamine reeglistike sees tööle automaatselt.

DirectAccess

Meetmes M 4.411z DirectAccessi turvaline kasutamine Windowsis detailselt kirjeldatud VPN-tehnoloogia sisaldab integreeritud lahendust, millega saab Windows Server 2008 R2 keskkonnas kasutusse lubatud ressurssidele tagada turvalise juurdepääsu. Siinkohal tuleb arvestada, et DirectAccessi serveriga Windows

Server 2008 R2 keskkonnas kasutusse lubatud ressurssidele saavad juurde pääseda üksnes Windows 7 versioonid Enterprise ja Ultimate.

Network Access Protection

Võrgu juurdepääsukaitse on uus tehnoloogia, mis juurutati alates versioonist Windows Server 2008. Selle tehnoloogiaga saab defineerida võrgujuurdepääsu kaitsvaid tsentraalselt töötavaid reeglistikke. Lisateavet NAP kasutamise kohta leiate meetmest M 4.410z Võrgu juurdepääsukaitse kasutamine Windowsis .

Windows Security Auditingu funktsiooni uuendused

Alates versioonist Windows Server 2008 on turvaseirefunktsioonis tehtud olulisi muudatusi. Tähtsamad muudatused, mida kirjeldatakse detailsemalt meetmes M 2.489 Windows Server 2008 süsteemiseire planeerimine e , **on järgmised:**

- logide varasema andmevormingu asendamine XML-vorminguga;
- sündmuste ID-de uus numeratsioon;
- võimalus koguda sündmused kokku mõnda tsentraalsesse Windowsi süsteemi.

Lisaks on alates versioonidest Windows Server 2008 R2 ja Windows 7 kasutusele võetud veel teisi uuendusi, mida saab kasutada üksnes kahes nimetatud versioonis:

- Global Object Access Auditing - Eriti suurt kaitset vajavate failide ja kaustade juurdepääsude jälgimiseks saab kasutada nn süsteemipääsuloendeid (System Access Control Lists – SACLs). Need aitavad kontrollida, kas kõiki süsteemi turbe seisukohalt kriitilisi andmeid kaitstakse adekvaatsete pääsuõigustega.
- Pääsuõiguste juhtimist kajastavate sissekannete kuva - Pääsuõiguste juhtimist kajastavate sissekannete loendites (Access Control Entries – ACEs) saab kuvada objekti suhtes kehtivaid lubavaid ja keelavaid õigusi (allowed/denied). Näiteks võimaldavad need loendid kuvada jälgitava objekti suhtes kehtivaid grupikuuluvusi ja pääsuõigusi.
- Seirepoliitikate täiendatud seadistusvõimalused, juurutatud versiooniga Windows Server 2008 - 53 uut kategooriat suurendavad märkimisväärselt lokaalsete, st seirepoliitikate senist 9 alusseadistust. Versioonides Windows Server 2008 R2 ja Windows 7 saab neid kategooriaid grupipoliitikates hallata seirefunktsioonidega. Enda koostatud skriptide või tarkvaratööriista Auditpol.exe kasutamine ei ole enam vajalik.

Grupeerimissuuniste uuendused

Kuna versioonid Windows Server 2008 (R2) ja Windows 7 ühilduvad omavahel hästi ja on sarnased, kehtivad meetmes M 2.326 Windows 7 grupeerimissuuniste planeerimine detailselt kirjeldatud uuendused ka Windowsi serverisüsteemidele alates versioonist 2008.

Järgnevalt on esitatud lühike ülevaade olulisematest uuendustest alates versioonist Windows Server 2008:

- uute kategooriate kasutuselevõtt suuniste haldamises;
- administratiivsete mallide uus andmevorming ja uued funktsioonid (ADMX, vt M 2.368 Administratiivsete mallide kasutamine alates Windows Server 2003-st);
- uued Starter GPO-d (vt M 2.491 Windows Server 2008 rollide ja turvamallide kasutamine);
- kommentaaride lisamise võimalus GPO-des ja suuniste seadistustes.

Lisaks sisaldab Windows Server 2008 R2 veel järgmisi uuendusi:

- võimalus kasutada Windows PowerShell Commandlette grupeerimissuunistes;
- senisest paremad Starter GPO-d;
- uus kasutajaliides ja grupeerimissuuniste täiendavad seadistusvõimalused administratiivsete mallide haldamisel.

M 4.409w Windows Server 2008 soetamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Windows Server 2008 soetamisele peab nii riist- kui ka tarkvara lähtepunktist

vaadatuna eelnema põhjalik planeerimistöö, milles lähtutakse kavandatud kasutusotstarbest. Alates versioonist Windows Server 2008 R2 on olemas ka 32-bitise protsessoriarhitektuuri tugi. Vajaliku riistvara planeerimise kõrval tuleb kontrollida, kas installitavad rakendused ühilduvad ka 64-bitise töörežiimiga Samuti tuleb arvestada, et Windows Server 2008 R2 puhul on võimalik valida seitsme redaktsiooni vahel. Standardi, Enterprise'i ja Datacenteri puhul , mis on kolm eeldatavasti kõige sagedamini kasutatavat süsteemi, eristati Hyper-V-ga ja Hyper-V-ta versioone ning sellist eristust jätkati ka veel Windows Server 2008 puhul.

Alates versioonist Windows Server 2008 R2 sellist eristamist Microsoft enam ei rakenda. Hyper-V installitakse vastava rolli valimisel ja näiteks redaktsioonides Itanium, Web ja Foundation pole Hyper-V saadaval. Eeltoodud põhjustel tuleb enne serveri tarkvaralitsentsi soetamist välja selgitada, mis on serveri täpne kasutusotstarve. Ainult nii saab vältida Windows Server 2008 vale redaktsiooni soetamisest tingitud lisakulusid.

Sama nõue kehtib ka vajalike CPU-de arvu ja töömälu (RAM) suuruse kohta.

Ka siin on erinevate redaktsioonide vahel suured erinevused, nt Standard Edition suudab kasutada üksnes 4 CPU-d, samas kui Datacenter Editioni võimalike CPU-de arv on 64.

Windows Server 2008 R2 redaktsioonid	Kokkuvõte
Windows Server 2008 R2 Foundation	Alustuseks väikestele ettevõtetele
Windows Server 2008 R2 Standard	Standardplatvorm enamiku sihtotstarvete jaoks
Windows Server 2008 R2 Enterprise	- Failover Cluster - Hot-Add Memory

Windows Server 2008 R2 Datacenter	Lisafunktsioonid võrreldes Enterprise Editioniga: -Hot-Add Processors -Hot-Replace Memory - Hot-Replace Processors
Windows Web Server 2008 R2	Redaktsioon, mis on üksnes IIS-i platvorm
Windows Server 2008 R2 Itanium-süsteemidele	Operatsioonisüsteem üksnes Itaniumil põhinevatele CPU-dele
Windows HPC Server 2008 R2	Operatsioonisüsteem üksnes High-Performance Computingu lahendustele

---

Peale kasutatava riistvara piirangute erinevad redaktsioonid märkimisväärselt ka rollide kasutuse poolest. Näiteks vajab Web Server Edition IIS-i installatsioonile lisaks DNS-serverit, kuid sellega rollid piirduvadki. Microsoftil on vajamineva-te redaktsioonide valimiseks koostatud ka detailsed ülevaated, nt redaktsioonide võrdlustabelid, kuhu on märgitud toetatavad serverirollid. Nende dokumentidega tuleks enne redaktsiooni soetamist kindlasti tutvuda.

Lisateavet installitavate serverirollide kohta leiate meetmest M 1.1 Vastavus normidele ja eeskirjadele . Hulgilitsentsilepingute soetamisel tuleb arvestada veel ka süsteemide aktiveerimiseks vajaliku taristuga (vt M 4.336 Hulgilitsentslepinguga Windowsi süsteemide aktiveerimine alates Windows Server 2008-st).

Kontrollküsimus:

- Kas enne uute Windowsi serverite soetamist analüüsitakse põhjalikult süsteemide kasutusotstarvet?

M 4.410z Võrgu juurdepääsukaitse kasutamine Windowsis

Algatamise eest vastutab: IT-juht

Rakendamise eest vastutab: administraator

Terminiga „võrgu juurdepääsukaitse” (Network Access Protection) tähistab Microsoft kokkuvõtlikult operatsioonisüsteemide erinevaid kaitsetehnoloogiai d. Need tehnoloogiad juhivad IT-süsteemide juurdepääse võrgule, lähtudes seejuures IT-süsteemi jaoks kindlaks määratud turbeastmest. Sel viisil tagatakse võrgukeskkonnas paiknevatele tundlikele IT-süsteemidele piisav kaitse mis tahes teiste puuduliku turbeseadistusega (nt vananenud viirusesignatuuridega) süsteemide vastu.

Microsoft on osa toodetega integreerinud võrkude juurdepääsukaitse mehhanismi Network Access Protection (NAP). NAP kasutamine on vabatahtlik ning eeldab, et operatsioonisüsteemina kasutatakse serveris vähemalt Windows Server 2008-t ja klientsüsteemides Windows 7-t. Sellise lahenduse korral kasutavad Windowsi serveri komponendid juurdepääsude juhtimiseks kliente. Sisselogimisprotsessi käigus edastavad kliendid serverile andmed oma turbeastme, nt kasutatavate värskenduste (updates) ja viirusesignatuuride kohta. Seejärel langetab server salvestatud turvareeglite (policies) põhjal otsuse, kas kliendid tohivad juurde pääseda tervele võrgule või tuleb vastata eitavalt või võimaldada klientidele juurdepääs üksnes väljavalitud serveritele. Sellised serverid sisaldavad sageli teenuseid, mida kliendid vajavad soovitud seisundi taastamiseks. Need võivad olla näiteks viirusesignatuuride jaoks mõeldud värskendusmehhanismid või Windows Updatesi mehhanism.

Kaitstava võrgu juurdepääse on võimalik kontrollida eri tasanditel:

- VPN-juurdepääs. Selle lahenduse puhul juhib Windowsi server sisevõrgu juurdepääse VPN-ühendusega arvuti kaudu.
- IPSec. Windowsi server kontrollib klientide turvaseisundit IPSeciga loodud krüpteeritud andmesidekanalite kaudu.
- IEEE 802.1X. See standard hõlmab autentimist, mida rakendatakse võrgus paiknevate IT-süsteemide juurdepääsude juhtimiseks. Autentimisprotsess toimub otse lõppseadme ja nn LAN Service Access Pointi vahel, milleks kasutatakse sageli asjakohaste funktsioonidega varustatud võrgukommutaatorit.

Windows Server 2008 puhul saab IEEE 802.1X-i toega kommutaatoreid autentimisprotsessi käigus kasutada ka teabe hankimiseks kliendi turbeastme kohta, ühtlasi võimaldavad need kontrollida, kas turbeaste vastab võrgu turbenõuetele.

- DHCP. Pärast kliendi turvaseisundi kontrollimist saadetakse kliendile DHCP-konfiguratsioon, mis kas lubab või keelab juurdepääsu võrgule. Selline lahendus on ründajatele siiski liiga lihtne, mistõttu tuleks selle kasutamisest hoiduda.

- Terminalserver Access. Kui kliendid kasutavad RDP kaudu Windowsi terminaliserverit, saab autentimisprotsessi kaasata terminaliserveri lüüsis NAP kaudu toimiva turbekontrolli.

Kasutusvaldkonnast olenevalt tuleb rakendada erinevaid tehnilisi protsesse ja komponente. Klientidel on siiski kõikidel juhtudel tarvis lokaalselt töötavat komponenti, mida nimetatakse süsteemitervikluse agendiks (System Health Agent – SHA) ning mis selgitab nn süsteemitervikluse kontrollide (System Health Validators – SHVs) käigus välja turbekonfiguratsiooni lokaalsed parameetrid ja edastab need vastaspoolele. Klientides, mis töötavad Windows 7-ga, on SHA juba operatsioonisüsteemiga integreeritud. Ka Mac OS X-t või Linuxit kasutavatele klientidele on sobivad lahendused saadaval.

Windowsi klient suudab kontrollida:

- kas klientarvutis on installitud ja aktiveeritud tulemüüritarkvara;
- kas klientarvutis on installitud ja kas selles kasutatakse viirusetõrjetarkvara;
- kas klientarvutis on installitud kõige uuemad viirusetõrjetarkvara värskendused;
- kas klientarvutis on installitud ja kas selles kasutatakse nuhkvara tõrjetarkvara;
- kas klientarvutis on installitud kõige uuemad nuhkvara tõrjetarkvara värskendused;
- kas klientarvutis on aktiveeritud Microsoft Update'i teenused.

Väljavalitud kaitsemehhanismidest olenevalt kuuluvad protsessis osalevate serverikomponentide hulka kontrollitud klientidele sertifikaate väljastav tervikluse registreerimisüksus (Health Registration Authority – HRA), võrgupoliitikaid edastav ja haldav server (Network Policy Server – NPS), mis võrdleb edastatud konfiguratsioone asjakohase reeglistikuga, ning nn täidesaatev server (Enforcement Server – ES), mis hoolitseb NAP-kontrolli tulemuse rakendamise eest. Cisco pakub võrgujuurdepääsude kontrollimiseks ka spetsiaalset toodet, mille nimi on Network Admission Control. Kahte tehnoloogiat on võimalik omavahel kombineerida. Selleks integreerivad Cisco võrgukomponendid Windows Network Policy Serverisse saadetavad päringud klientide kontrollimisega. NAP-d võib soovitada tundlike süsteemide lisakaitseks võrgukeskkonnas. Sellega saavutatava turbe tõhusust ei maksaks siiski üle hinnata.

Kuna turbeastme väljaselgitamisega tegelevad agendid töötavad tahes-tahtmata klientsüsteemides, saab ründaja, kellel on klientsüsteemile administraatoriõigustega juurdepääs, klienti põhimõtteliselt nii palju manipuleerida, et ta saab võltsitud andmete abil siiski juurdepääsu võrgule. NAP ei kaitse sihipäraste rünnete (targeted attacks) eest, vaid sobib ennekõike kahjude minimeerimiseks ja sihipäratute rünnete tõrjumiseks (nende hulka kuulub ka kahjurvaraga nakatamine).

NAP kasutuse planeerimisel tuleb arvestada järgmiste aspektidega:

- NAP kaitse-eesmärkide defineerimine. Mis andmeid soovitakse NAP-ga kaitsta ja milliste ohtude vastu NAP-d rakendada?
- NAP arhitektuuri planeerimine. Millist tehnilist lahendust hakatakse NAP jaoks kasutama? Milliseid serverikomponente on kavas kasutada ja millistes serverites need tööle rakendada?
- NAP reeglistike planeerimine. Milliseid süsteeme ja võrke planeeritakse NAP-ga kaitsta? Mis nõuded kehtestatakse süsteemidele, mis soovivad juurde pääseda kaitstud valdkondadele? Mis teenused peavad olema kättesaadavad süsteemidele, millele juurdepääsu ei võimaldata, et need saaksid taastada enda soovitud seisundi?
- NAP halduse planeerimine. Kellel tohib olla juurdepääs NAP süsteemidele ja reeglistikele? Kes vastutab reeglistike ajakohasuse ja hooldamise eest?

Kontrollküsimused:

- Kas NAP kasutuselevõtu planeerimisel arvestati piisavalt turbe-eesmärkide, NAP arhitektuuri ja NAP haldamisega?
- Kas NAP planeerimise tulemused, k.a reeglistikud, on dokumenteeritud?

M 4.411z DirectAccessi turvaline kasutamine Windowsis

Algatamise eest vastutab: IT-juht

Rakendamise eest vastutab: administraator

Alates versioonidest Windows 7 ja Server 2008 R2 on operatsioonisüsteemiga integreeritud VPN-tehnoloogia DirectAccess. Selle eesmärk on hõlbustada lokaalvõrkudes paiknevatele ressurssidele tehtavaid kaugpöördusi ning võimaldada kasutajatel enda kliente kõikidel juhtudel rakendada nii, nagu nad oleksid otseühenduses LAN-iga. Selleks loob DirectAccess LAN-is ilma kasutaja sekkumata ja juba enne sisselogimist operatsioonisüsteemi IPSec-tunneli mõne vastaspoolega, mis kasutab Windows Server 2008 R2-t. Siinkohal tuleb arvestada, et DirectAccessi serveriga Windows Server 2008 R2 keskkonnas kasutusse lubatud ressurssidele saavad juurde pääseda üksnes Windows 7 versioonid Enterprise ja Ultimate.

Nimetatud vastaspoole kaudu muutuvad kättesaadavaks sellised tsentraalsed taristukomponendid nagu Active Directory ja DNS (Infrastructure Tunnel). Esimese tunneli autentimiseks kasutatakse üksnes klientarvuti arvutikontot, mis tähendab, et see tunnel on põhimõtteliselt kaitsetu ründajate vastu, kes on tekitanud klientsüsteemile volitamata juurdepääsu. Pärast kasutaja edukat sisselogimist luuakse teine IPSec-tunnel, mille kaudu pääseb juurde teistele sisemistele ressurssidele (Intranet Tunnel).

DirectAccessi juurdepääsu kasutuselevõtuks on mitu konfiguratsioonivõimalust:

- täielik intranetijuurdepääs: selle lahenduse korral on DirectAccessi kaudu ühendatud süsteemidel piiramatu juurdepääs kõikidele intranetis paiknevatele ressurssidele;
- väljavalitud serverid: DirectAccessi kaudu ühendatud süsteemidel on intranetis juurdepääs üksnes väljavalitud serveritele;
- End-to-end: kui DirectAccessi kaudu ühendatud süsteem soovib juurde pääseda mõnele intranetis paiknevale serverile (nt mõne sisevõrgurakenduse kasutamiseks), saab kliendi ja sihtserveri vahel kasutada IPSeciga krüpteeritud kanalit. Sel viisil pole kaitstud mitte üksnes väline juurdepääs, vaid ka andmetransport läbi LAN-i.

Siinkohal tuleb arvestada, et sisevõrgus paiknevate arvutitega kontakti loomiseks saab DirectAccessi puhul rakendada üksnes internetiprotokolli IPv6. Kõik sellised süsteemid, mis on sisevõrgus kättesaadavad üksnes protokolliga IPv4, jäävad DirectAccessile kättesaamatuks. Sellest piirangust on võimalik mööda minna NAT64 või prokside kasutamisega, kuid see võib tekitada probleeme rakenduste töös. Seevastu välise DirectAccessi kliendi ja lüüsi vahelisele kommunikatsioonile see piirang ei kehti. Leidub hulgaliselt lahendusi, mis võimaldavad vajalikku IPv6-ühendust realiseerida olemasoleva IPv4-ühenduse kaudu, nii et klientide ühendamine ei muutu seeläbi liiga keeruliseks. DirectAccessi klient analüüsib olemasolevaid ühenduse loomise võimalusi ja valib iseseisvalt välja sobiva protokolli. DirectAccessi konfiguratsioonitöid saab taha kas selle jaoks loodud konsooliga

(DirectAccess Management Console) või käsuviiba tööriistaga Network Shell ja grupipoliitikaobjektidega.

DirectAccessi kasutamine sisevõrgule juurdepääsemiseks on kõige kriitilisem kindlasti täielikku intranetijuurdepääsu võimaldava lahenduse korral. Seda liiki juurdepääsu kasutamine eeldab spetsiaalsete kaitsemeetmete võtmist. DirectAccessi juurdepääsude turvet saab mingil määral tõhustada autentimisprotsessis rakendatavate piirangutega, nt kiipkaardi ja PIN-koodi kasutuselevõtuga (kahefaktoriline autentimine). Selliseid piiranguvõimalusi tuleks DirectAccessi puhul kindlasti kasutada. Samuti on oluline, et sisevõrguga loodaks ühendav tunnel vaid siis, kui ühendatud süsteem on selle õigusliku kasutaja valduses. Ühtlasi tuleks sellised süsteemid varustada kõvaketta krüpteerimisfunktsiooniga (vt M 4.337z BitLockeri Drive Encryption kasutamine) ja automaatse blokeerimisfunktsiooniga ajaks, mil kasutaja viibib süsteemi juurest eemal (vt M 4.2 Ekraanilukk). Kui sisevõrgule soovitakse juurde pääseda kaasaskantavatest IT-süsteemidest, tähendab see sisevõrgu jaoks alati ka tavapärasest suuremat kahjurvaraga nakatumise ohtu. Selleks, et enne DirectAccessi ühenduse lubamist kontrollitaks lõppseadmes kas või vähemalt turbega seotud baasnäitajaid, saab DirectAccessi juurdepääsule kohaldada võrgu juurdepääsukaitset (vt M 4.410z Võrgu juurdepääsukaitse kasutamine Windowsis). Kuna DirectAccessi server peab olema väljaspool võrku asuvatele klientidele juurdepääsetav, on ta potentsiaalne ründesihtmärk, mis võib ohustada kogu sisemist IT-võrku. Selle serveri ühendamisel võrku tuleb järgida meedet M 4.224z Virtuaalsete privaatvõrkude integreerimine turvalüüsidesse . Siinkohal tuleb arvestada, et DirectAccessi server peab tingimata olema Windowsi domeeni liige.

Standardseadistuse korral jagavad DirectAccessi kliendid enda andmeside kaheks: andmesideks intraneti ja internetiga. Kui intranetis asuvate ressursside kasutamisel juhitakse vajalikud ühendused automaatselt läbi DirectAccessi tunneli, siis internetiga loovad klientsüsteemid hoopis otseühenduse väljaspool tunnelit. Sellise lahenduse eesmärk on vähendada sisevõrgus ja tunnelis andmesidekoormust.

Samas jällegi võib DirectAccessi klient sellise lahenduse korral muutuda võrguüleminekupunktiks ründajale, kes soovib internetist kliendi kaudu volitamata sisevõrku pääseda. Samuti tuleb arvestada, et kliendi otseühendusi internetiga ei saa kaitsta võimalike olemasolevate tsentraalselt toimivate turbemehhanismidega, nt sisu filtreeriva proksiserveriga. Eelnimetatud põhjustel tuleks standardseadistus ära muuta ja kogu kliendi andmeside sunniviisiliselt DirectAccessi tunnelisse suunata (Force Tunneling). Nii tagatakse olemasolevatel turbemehhanismidel põhinev, kontrollitav ja turvaline juurdepääs internetile ning välistatakse sisevõrgus nn tagauste tekkimise võimalus.

Erinõuete korral kehtib järgmine põhimõte: olukorras, kus suurte käideldavusnõuetega tööprotsessidele soovitakse anda DirectAccessil põhinev väline juurdepääs, tuleb selles osalevates serverites ja komponentides rakendada liiasust.

Kontrollküsimused:

- Kas DirectAccessi ühenduste loomiseks on tarvis kasutada kahefaktorilist autentimist?
- Kas kõikides DirectAccessi klientides on aktiveeritud kõvaketta krüpteerimine?
- Kas DirectAccessi server on sobival moel turvalüüsiga integreeritud?
- Kas kliendi andmeside on nii intraneti kui ka interneti kasutamisel suunatud DirectAccessi tunnelisse (Force Tunneling)?

M 4.412z Windows Server 2003 turvaline migreerimine Server 2008-ks

Algatamise eest vastutab: infoturbespetsialist

Rakendamise eest vastutab: administraator

Windows Server 2003 migreerimine Server 2008-ks eeldab põhjalikku planeerimist. Esmalt tuleb kindlaks määrata migreerimisstrateegia:

- Uusinstallatsiooni korral tehakse vana süsteemi andmetest esmalt varukoopia, seejärel installitakse samasse riistvarasse uus (ajakohane) süsteem ja pannakse tööle teenused, kasutades selleks andmetest tehtud varukoopiaid. Selle variandi puhul kaasnevad migreerimisprotsessiga ka seisakuajad ning see eeldab laialdast planeerimist. On oht, et ettenägematute probleemide korral võivad seisakud venida arvatust pikemaks.
- In-Place-Update'i migreerimisstrateegia rakendamisel käivitatakse töötavas süsteemis süsteemitarkvara värskendus (*update*). Selle variandiga kaasnevad eri liiki ohud, muu hulgas konfiguratsioonidega seotud „vana taaga" ülevõtmise oht, värskendamisest tingitud tootmisprotsesside seisakud ja värskendusprotsessi ebaõnnestumine.
- Nn päris migreerimisel installitakse uus süsteem uude riistvarasse ja seejärel kolitakse igapäevatöös kasutatavad teenused vanast töötavast süsteemist uude süsteemi ümber.

Sellise lahenduse eelis seisneb tööseisakute ja andmekadude vältimises, kuid kuna uut süsteemi ei installita seni kasutatud riistvarasse, läheb tarvis täiendavat riistvara. See on eelistatud migreerimislahendus, sest see pakub kõige paremaid katsetusvõimalusi.

Migreerimise planeerimine

Planeerimisel tuleb muu hulgas:

- välja selgitada, kui kaua migreerimistööd kestavad ja milline on nende võimalik mõju igapäevaste tööprotsesside kasutamisele nii migreeritavas süsteemis kui ka teistes sellest süsteemist sõltuvates süsteemides:
- kindlaks määrata isik, kes migreerib;
- kindlaks määrata migreerimisstrateegia;

Hädaolukorraks valmisoleku plaan ja andmevarundus

- kindlaks määrata katsetusetapid ja katsete katkestamise kriteeriumid;
- läbi arutada ja kindlaks määrata hädaolukorraks valmisoleku plaanid ja tegevusjuhised;
- teavitada migreerimisprotsessist mõjutatud töötajaid ja protsessiga seotud IT-süsteemide käitamise eest vastutavaid töötajaid migreerimise etappidest.

Tulemused tuleks dokumenteerida migreerimiskontseptsioonis. Lisateavet migreerimiskontseptsiooni ja selle sisu kohta leiate meetmest M 2.319 Serveri üleviimine . Kui kasutatavas Windowsi domeenis pole ühtki Server 2008 süsteemi, tuleb planeerimisel tähelepanu pöörata ka domeenikontrolleri migreerimisele (vt M

4.317 Windowsi kataloogiteenuste turvaline migratsioon) või vähemalt Active Directory funktsioonitasandi suurendamisele. Siinkohal tuleb kõigepealt katsetada, kas Active Directory muutmine võib endaga kaasa tuua probleeme olemasolevate rakenduste kasutamisel (vt G 2.156 Ühilduvusprobleemid Active Directory funktsioonitasandi suurendamisel). Kui migreerimise lähtesüsteemi andmeid hoitakse mõnes eraldi välises andmekandjas, nt SAN-is või NAS-is, või mõnel välisel kõvakettal, on tarvis kindlaks määrata, kas need failid tuleb migreerimisprotsessis kopeerida või tuleb uuele serverile tagada juurdepääs nendele andmetele. Kahest mainitust on teine variant lihtsam, sest kopeerida pole tarvis, kuid arvestada tuleb ka mõningate piirangutega. Näiteks on oht, et lokaalsete kasutajakontode volitused võivad kaotsi minna, kui sama nimega kasutajakontodel on sihtsüsteemis hoopis teistsugune SSID ning kui BitLockeri EFS-iga krüpteeritud faile ei ole võimalik sellisel moel migreerida. Seevastu kui andmed kopeeritakse sihtsüsteemis olemasolevatesse kataloogidesse, tuleb arvestada, et pääsuõiguste pärimisprotsess ei lähtu enam sihtkataloogis, mis sisaldab ka hierarhia madalama astme faile, lähtekataloogi algsetest õigustest, vaid sihtkataloogis töötavatest õigustest (vt G 2.116 Andmekadu andmete kopeerimisel ja teisaldamisel alates Windowsi Server 2003-st). Seetõttu tuleb lähte- ja sihtkataloogi pääsuõigused esmalt ühtlustada.

Abivahendid

Süsteemide migreerimiseks Windows 2008 Serveriks on Microsoftil pakkuda suur hulk abivahendeid. Näiteks kuuluvad valikusse migreerimise käsiraamatud serverirollide tarbeks. Nendes kirjeldatakse detailselt nii lähte- kui ka sihtsüsteemi ettevalmistusega seotud tööetappe, migreerimisprotsessi ja migreerimisprotsessi lõpetamiseks vajalikke operatsioone. Olukordades, kus migreeritav süsteem täidab korraga mitut ülesannet, tuleks juba eeltööna migreerimise käsiraamatute põhjal kõikide rollide jaoks koostada eraldi sobivad migreerimisjuhised. Migreerimise käsiraamatute lisades on toodud ka töölehed, mis aitavad migreerimise jaoks vajalikud konfiguratsiooniseadistused lähtesüsteemist üles leida ja ülevaatlikult dokumenteerida. Samas peaksid nende tööde käigus kogutavad andmed sisalduma ka heas süsteemidokumentatsioonis (vt M 2.25 Süsteemi konfiguratsiooni dokumenteerimine). Erinevate serverirollide jaoks kasutatakse osaliselt ka erinevaid Windowsi serverite migreerimistööriistu, mis installitakse nii lähte- kui ka sihtsüsteemi ning mis tagavad andmete automaatse edastamise lähte- ja sihtsüsteemi vahel. Windows Server 2008 R2 puhul saab migreerimistööriistad valikuna (*feature*) juurde installida. Selleks tuleb lähtesüsteemis teha eraldi installatsioon. Migreerimiseks väljatöötatud tarkvaralahendused toetavad ka serverite migreerimist sihtplatvormiks, mida käitatakse Server Core'i installatsioonina (vt M 4.416 Windows Server Core'i kasutamine), ning füüsiliste masinate migreerimist virtuaalseteks masinateks. Migreerimistööriistade kasutamiseks peab olema installitud .NET-Framework 2.0 ning Windows PowerShell, samuti peab installatsiooni jaoks olema piisavalt palju vaba mälumahtu. Lähte- ja sihtsüsteem peavad olema installitud samas keeles. Kuna ka migreerimistarkvara installimine võib nõuda serveri taaskäivitamist, tuleks selle asjaoluga migreerimist planeerides arvestada.

Migreerimise ettevalmistus

Migreerimiseks läheb nii lähte- kui ka sihtsüsteemis tarvis administraatorivolitustega kasutajakontot. Sihtserveris peab olema piisavalt vaba mälumahtu, et ülevõetavad andmed sinna ära mahuksid. Selleks tuleb arvestada ka võimaliku töölelülitatud kvoodihaldusega (*quota management*). Enne migreerimisega alustamist tuleb lähtesüsteemist teha täielik varukoopia, et probleemide korral, mida ei õnnestu lahendada migreerimiseks ette nähtud aja jooksul, saaks kasutada kindlat

taastepunkti. Nii lähte- kui ka sihtsüsteemi tuleks enne migreerimist installida kõik paigad, et kõik teadaolevad vead saaksid süsteemitarkvaras likvideeritud. Lähte- ja sihtserveri süsteemiajad peavad olema sünkroniseeritud, nt mõne ühise välise ajaallika põhjal. Serverirollist olenevalt tuleb lähte- ja sihtsüsteemi installida vajalikud migreerimistööriistad. Kommunikatsiooni jaoks läheb Microsofti migreerimistööriistadel tarvis porte udp/7000 ja tcp/7000. Nende portide kasutus tuleb lähte- ja sihtsüsteemi lokaalsetes tulemüürides ning neid ühendavas võrgus sisse lülitada. Kõiki asjasse puutuvaid töötajaid ning süsteemide ja rakenduste administraatoreid tuleb õigel ajal teavitada eesseisvast migreerimisest ja sellega kaasnevatest tööpiirangutest.

Migreerimine

Sihtsüsteemi soovimatute muudatuste vältimiseks tuleb tagada, et kolmandate isikute jaoks oleksid pöördused migreerimisprotsessi vältel kindlasti välistatud. Samuti ei tohi pärast migreerimisprotsessiga alustamist teha lähtesüsteemis mitte ühtki sellist tööd, mis võiks tuua kaasa kas konfiguratsiooni või andmekoosluse muudatusi. Selliseid pöördusi saab ära hoida kas töökorralduslike meetmetega või, veel parem, tehniliste meetmetega võrgu tasandil. Pärast migreerimistööde lõpetamist tuleb kõik serveri olulised tööfunktsioonid põhjalikult läbi katsetada, et tuvastada võimalikud migreerimisvead ja välistada nende negatiivne mõju igapäevastele tööprotsessidele. Selleks, et sihtsüsteemis ei tekiks liigseid ründevõimalusi, tuleks migreerimistarkvara pärast migreerimistööde lõpetamist süsteemist eemaldada ning migreerimiseks tööle lülitatud UDP- ja TCP-pordid lokaalses tulemüüris ja ka teistes võrgukeskkonnas paiknevates turvalüüsides taas blokeerida.

Täiendavad kontrollküsimused:

- Kas Windows Server 2008-ga seotud migreerimistööd on piisavalt hästi, st vajadusi arvestades planeeritud?
- Kas kõik eelneva serveri migreerimisel Windows Server 2008-ks vajalikud tarkvaratööriistad on välja selgitatud ja läbi katsetatud?
- Kas migreerimismeeskonna liikmete laiendatud õigused tühistatakse, kui eelnev server on Windows Server 2008-ks migreeritud?
- Kas eelneva serveri migreerimiseks Windows Server 2008-ks on koostatud IT-turbekontseptsioon?
- Kas on tagatud, et kõik eelneva serveri migreerimiseks Windows Server 2008-ks erandkorras kehtestatud reeglid tühistatakse pärast migreerimisprotsessi lõppemist?
- Kas kõik isikud, keda migreerimine puudutab, on eelneva serveri migreerimiseks Windows Server 2008-ks piisavalt ette valmistatud?

M 4.413z Hyper-V-ga virtualiseerimise turvaline kasutamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator, IT-juht, erialaspetsialist

Hyper-V-ga virtualiseerimise turvalisuse tagamiseks tuleb läbi teha vajalikud planeerimisetapid (vt M 2.490 Hyper-V-ga virtualiseerimise planeerimine) ja järgida moodulit B 3.304 Virtualiseerimine , eriti selle meetmeid M 4.349 Virtuaalse taristu turvaline kasutamine ja M 5.154 Virtuaalse taristu võrgu turvaline konfiguratsioon . Selles meetmes kajastatakse eelnimetatud materjalile toetuvaid ja Hyper-V eripäraga seotud aspekte. Enim tähelepanu tuleb pöörata järgmistele punktidele:

- planeeritud volituskontseptsioonide tõhus rakendamine;
- haldusüksuse karastamine.

Külaliste puhul on Hyper-V eripärast tulenevate kohandamistööde maht väike. Haldusüksuse turbe tõhustamiseks ja konfiguratsiooni parendamiseks tuleks kindlasti kasutada Microsofti põhjalikku dokumentatsiooni: Hyper-V Security Guide'i, mille *online* -versioonid on varustatud ka mugavate ristviidetega.

Haldusüksus

Haldusüksuse karastamise baaslahenduse moodustab ründevõimaluste minimeerimine, milleks tuleb vähendada kasutatavate funktsioonide hulka (vt M 2.490 Hyper-V-ga virtualiseerimise planeerimine). Selleks sobivad eriti hästi töörežiim Server Core (vt M 4.416 Windows Server Core'i kasutamine) ja Hyper-V serveri kasutamine eraldiseisva süsteemina. Kui selliseid baaslahendusi ei kasutata, tuleks rakendada vähemalt SSLF Baseline'i (Specialized Security Limited Functionality). Seda võib kasutada ka täiendusena. SSLF Baseline'i tuleb kindlasti kasutada enne Hyper-V rolli installimist, sest muidu peab pärast SSLF Baseline'i kasutamist tegema lisakorrektuure, mida kirjeldatakse Microsofti Hyper-V Security Guide'is. Haldusüksuse puhul kehtib põhimõte, mille kohaselt on kõikide lisateenuste ja -rakenduste käitamine keelatud. Põhimõttelise erandi moodustavad siinkohal üksnes kõikvõimalikud viirusetõrjetarkvarad, nt viiruseskannerid, Host-IDS-id ning standardselt kasutatavad taristuteenused (aja sünkroniseerimine), samuti kaughaldust ja tarkvarahooldust võimaldavad tööriistad. Samas tuleks ka nimetatud eranditest võimaluse korral siiski loobuda. Kui kasutatakse reaalajas töötavat viiruseskannerit, tuleks selle skaneerimisfunktsioonist kindlasti välja jätta kõik Hyper-V ressursid, et vältida valehäireid (külaliste töö seiskumist) ja jõudluse kadu. Neid ressursse kontrolliv viirusetõrjetarkvara tuleb tööle rakendada külalissüsteemides. Külalissüsteemide kasutusest kõrvaldamise tarbeks tuleks nendes hoida ka tarkvaratööriistu, mis võimaldavad turvaliselt kustutada ka VHD-faile (vt M 2.433 Ülevaade meetoditest andmete kustutamiseks ja hävitamiseks).

Hyper-V konfiguratsioon

Standardseadistuse korral ei ole ühte ja sama tuuma jagavate külaliste jaoks CPU kasutamine piiratud. See on halb, sest CPU piiramatu kasutuse korral saab külaline põhjustada häireid teiste teenuste töös sellega, et haarab kogu saadaoleva arvutusvõimsuse endale. Kuna vajaminevat CPU koormust pole võimalik alati täielikult ette teada, tuleks külalistele eraldatav CPU koormuse maht välja selgitada seirefunktsiooniga. Hyper-V puhul saab külalistele kehtestada kas CPU ma-

hupiirangu (*limit*) ehk kindla piirväärtuse või reguleerida mahu kasutamist prioriteetidega (suhteline hinnang). Nimetatud kahest võimalusest ei suuda kumbki välistada süsteemi „näljutamist". Seda saab ära hoida üksnes absoluutse reservi kehtestamisega (Virtual Machine Reserve). Seda võimalust tuleks kasutada kriitiliste funktsioonide jaoks. Host-süsteemide puhul, kus on palju CPU-sid/tuumi, esineb sellist probleemi harvem, sest neis on virtuaalsete CPU-de arv VM-i kohta piiratud. Selleks, et külalisi piisavalt hästi üksteisest lahutada, tuleb konfigureerimisel arvestada, et füüsilistele ressurssidele võimaldatud juurdepääsudes ei tohi esineda kattumist. Vältida tuleb ühiseid juurdepääse virtuaalsetele mälusüsteemidele (Virtual Hard Disks –VHDs) ja hosti füüsilistele seadmetele (USB-mälupulk, DVD-ajam). Serveri varundamisel Hyper-V VSS Writeriga ei hõlma varundamine ei virtuaalvõrgu ega ka virtuaalsete võrgukomponentide konfiguratsiooni. Seetõttu tuleks võrgu konfiguratsioon dokumenteerida selliselt, et hädaolukorras saaks vastava dokumentatsiooni põhjal konfiguratsiooni taastada.

Volitused

Sageli on tarvis lahendust, kus külalissüsteemide administraatoritel peab olema võimalik enda IT-süsteemi ise käivitada ja sulgeda ning konsoolile juurde pääseda, ilma et see mõjutaks kuidagi teisi süsteeme või võrke (vt M 2.466 Migratsioon terminaliserveri arhitektuurile). Selle tagamiseks tuleb Hyper-V volitustehalduris (Authorization Manager) anda volitused üksnes järgmiste protsesside kasutamiseks:

- Hyper-V Service- ja Network-tüüpi protsesside jaoks ainult lugemisõigusega juurdepääs;

Kõik lisavolitused võivad ohtu seada süsteemide lahutamise põhimõtte ning nende rakendamine eeldab olukorra eripära arvestavat turbeplaneeringut.

Külalissüsteemide konfiguratsioon

Meetmes M 4.348 Aja sünkroniseerimine virtuaalsetes IT-süsteemides nõutakse, et külalissüsteemide süsteemiaeg peab olema sünkroniseeritud, et tasakaalustada virtualiseerimisega põhjustatud koormusest sõltuvat triivimist (*drift*). Ilma aja sünkroniseerimiseta sõltuvad kõik külalissüsteemid virtuaalse CPU taimerikatkestustest (*timer interrupts*). Nii hakkab teiste süsteemide koormuse suurenedes VM-i kellades esinema rohkem ebatäpsusi. Hyper-V puhul tuleb arvestada veel ka erinevate ajatsoonide toetamise probleemistikuga (Windows soovib, et RTC töötaks kohaliku ajaga) ning *suspend* - ja *resume* -tüüpi sündmustega. Kui hetketõmmiste (*snapshot*) funktsioon reaktiveerida, nt pärast VM-i liigutamist ühest serverist teise, hakkab külalissüsteem kasutama vale süsteemiaega ning külalissüsteemil kulub palju aega, et enda süsteemiaeg mõne välise ajaallika põhjal uuesti sünkroniseerida. Sünkroniseerimiseks on Microsoftil välja töötatud eraldi sünkroniseerimisteenus, mis on osa külalissüsteemi installitavast Hyper-V Integration Servicesi teenusepaketist. See teenus ühtlustab külalissüsteemi süsteemiaja peremeessüsteemi süsteemiajaga ning korrigeerib kellad ka virtualiseerimisest tingitud ajahüpete (*suspend* / *resume*) korral. Peremeessüsteem peaks enda süsteemiaja sünkroniseerima mõne usaldusväärse võrguajaga (vt M 4.227 Lokaalse NTP -serveri kasutamine aja sünkroniseerimiseks). Probleeme võib esineda juhtudel, kus peremees- või külalissüsteemid on domeeni liikmed või pärinevad koguni eri domeenidest. Sel juhul korrigeeritakse süsteemiaega korraga nii võrgu kaudu kui ka lokaalselt. Tagajärg on sagedased väiksed kõrvalekalded. Seetõttu võib esineda replikeerimisprobleeme, eriti siis, kui külalissüsteemid on Acti-

ve Directory serverid. Neil juhtudel tuleks külaliste süsteemiaja sünkroniseerimine peremeessüsteemiga desaktiveerida. Kahjuks tuleb sel juhul leppida sellega, et virtuaalmasina taaskäivitamise järel ei saa algset süsteemiaega enam kiiresti taastada.

Windowsi külalissüsteemide puhul, kui nendesse on installitud Integration Servicesi teenusepakett, saab külalissüsteemi sünkroniseerimise peremeessüsteemi põhjal desaktiveerida ka ainult osaliselt, ilma et see mõjutaks aja kindlaksmääramist pärast buutimist ja *suspend-* / *resume-* sündmuste korral. Selleks saab kasutada järgmist käsku:

reg add HKLM\SYSTEM\CurrentControlSet\Services\W32Time \TimeProviders\VMICTimeProvider /v Enabled /t reg_dword /d 0

Seejärel tuleb külalissüsteemis konfigureerida väline ajaallikas. Millal iganes välise ajaallika põhjal sünkroniseerimist ka ei kasutata, alati tuleb valida võimalikult lühike intervall (iga 10–20 minuti möödudes), et kompenseerida situatsioonipõhist suurt triivimist.

Täiendavad kontrollküsimused:

- Kas Hyper-V serveri haldusüksus on tööle rakendatud minimaalse süsteemina (nt Server Core'i kasutamisega) või kas seda on karastatud SSLF Baseline'iga?
- Kas Hyper-V haldusüksuse puhul on tagatud, et see ei osuta mitte ühtki lisateenust?
- Kas viirusetõrjetarkvara puhul on tõkestatud Hyper-V ressursside skaneerimine?
- Kas Hyper-V süsteemides on kriitiliste teenuste jaoks vajalike CPU nõuete täitmiseks rakendatud CPU piiranguid?
- Kas Hyper-V võrgukonfiguratsioonist on tehtud eraldi varukoopia ja kas konfiguratsioon on dokumenteeritud?
- Kas otsejuurdepääs füüsilistele salvestusandmekandjatele on Hyper-V puhul antud vaid ühele VM-ile?

M 4.414w Windows Server 2008 Active Directory uuenduste ülevaade

Algatamise eest vastutavad: infoturbespetsialist, IT-juht
Rakendamise eest vastutab: administraator

Üldteave

Active Directory on Windows

Server 2008 ja Windows 7 puhul kujunenud nii kasutajate kui ka objektide haldamise elementaarseks baaslahenduseks. Kuigi Windows Server 2008 domeenikontroller pakub märkimisväärseid uuendusi, kehtivad Active Directory planeerimise ja konfigureerimise senised põhinõuded siiski edasi (vt M 1.1 Vastavus normidele ja eeskirjadele ja M 2.231 Windowsi grupipoliitika planeerimine).

Kuna aga Active Directory rollide lahutamise võimalusi on nüüd varasemast rohkem ning kasutusele on võetud ka Read-Only Domain Controller (RDOC), tuleb Windows Server 2008 ja selle Active Directory planeerimisele rohkem tähelepanu pöörata.

Windows Server 2008-ga kaasnevad uuendused

Varasemaga võrreldes on Active Directory tsentraalselt toimivale teenusele ehk Active Directory domeeniteenustele (Active Directory Domain Services – AD DS) lisandunud uued Active Directory teenused, mis installitakse rollidena:

- Active Directory sertifikaaditeenused (Active Directory Certificate Services – AD CS). Selle kasutusvaldkonna puhul rakendatakse Active Directoryt avaliku võtme infrastruktuuris (PKI) sertifikaatide avaldamiseks. Need sertifikaaditeenused olid olemas ka varasemates Windows Serveri versioonides, kuid siis puudus nende nimes täiend Active Directory.
- Active Directory ühendusteenused (Active Directory Federation Services – AD FS). See teenus juurutati alates versioonist Windows Server 2008 R2. Teenus hoolitseb nende kasutajate autentimise eest, kes ei ole Active Directory liikmed. Teenust kasutatakse sageli kasutajate autentimiseks veebirakendustes.
- Active Directory Lightweight Directory Services (AD LDS), varasema nimega Active Directory rakendusre?iim (Active Directory Application Mode – ADAM). See teenus võimaldab kataloogiteenuse toega rakendustel kasutada konkreetset LDAP-serverit andmehoidlana (data repository). Teiste kasutusvaldkondadega võrreldes pole selle lahenduse puhul tarvis hallata ei domeene ega tervikstruktuure. Iga AD LDS-i instantsi puhul hallatakse eraldi skeemi.
- Active Directory pääsuõiguste haldusteenused (Active Directory Rights Management Services – AD RMS). AD RMS-i teenus kaitseb andmeid ja faile tsentraalselt juhitava krüpteerimisfunktsiooniga.

Nende teenuste hulgast saab rolle ka ühekaupa välja valida ja eraldiseisvasse süsteemi installida.

Põhimõttelised lisamuudatused

Versiooniga Windows Server 2008 kaasnev märkimisväärne uuendus on Read-Only Domain Controller (RODC). See serverisüsteem kujutab endast domeenikontrollerit, mis võimaldab kataloogiteenusele juurde pääseda üksnes lugemisõigusega.

RODC sobib süsteemide jaoks, kus laialdast füüsilist juurdepääsu ei ole võimalik suure kasutajate hulga tõttu ära hoida, nt süsteemi ei saa paigaldada arvutuskeskuse kaitstud keskkonda.

Erinevused tavalise domeenikontrolleriga on järgmised:

- ühesuunaline replikeerimine, st replikeerimisprotsessist jäetakse välja vaba juurdepääsuga RODC-des aset leidnud manipulatsioonid:
- Active Directory skeemi muudatused,
- DNS-andmebaasi muudatused;
- serveri haldamise saab domeeniadministraatorite volitustest lahutada.

RODC kasutamisel võib siiski esineda ka kitsaskohti, millele tuleks tähelepanu pöörata:

- Tekib suur sõltuvus täisväärtuslikust domeenikontrollerist, sest ainult sellega saab Active Directorys luua uusi objekte.
- Kui RDOC-d püütakse kasutada kolmandate tootjate tarkvaralahenduste ja Active Directory integreerimiseks, võivad tekkida ühilduvusprobleemid. Selle tagajärjel suureneb katsetustööde maht.
- Kasutajaparoolide lokaalseks vahesalvestamiseks tuleb välja töötada sobiv turbestrateegia, sest muidu saavad kolmandad isikud (nt süsteemi kaotamise või varguse korral) põhimõtteliselt kõiki vahesalvestatud paroole süsteemist välja lugeda. Eriti suurt tähelepanu tuleks pöörata domeeniadministraatorite kontodele ja analüüsida, kas vahesalvestamist oleks vaja blokeerida.

Blokeerimisel tuleb tagada, et administraatorite kasutajarühma liikmed saaksid RODC-sse sisselogimiseks kasutada täisväärtusliku domeenikontrolleriga loodud ühendust.

Uuenduste hulka kuuluvad ka hallatavad teenusekontod, mis on kasutusele võetud alates versioonist Windows Server 2008 R2. Neid teenusekontosid saab hallata tsentraalselt Active Directoryga (vt M 4.284 Teenuste rakendamine). Uute, nii paroolidele kui ka kontodele kehtivate üksikasjalike blokeerimissuunistega on võimalik domeeni piires rakendada ka eriastmelisi paroolisuuniseid.

Active Directory põhimõttelised lisauuendused, mis on kasutusele võetud alates versioonist Windows Server 2008 R2, on järgmised:

- Active Directory paberikorv: Active Directorys kogemata ära kustutatud objekte saab tänu paberikorvi funktsioonile nüüd taastada.
- Active Directory halduskeskus: tsentraalselt toimiv ja PowerShellil põhinev haldustööriist koos laiendatud funktsioonidega Active Directory haldamiseks.

Siinkohal tuleb arvestada, et Active Directory halduskeskus ei asenda täielikult haldustööriista Active Directory Users and Computers, sest nende funktsioonid on kohati erinevad.

- Active Directory Best Practice Analyzer: Active Directorys rakendatavaid seadistusi analüüsiv tarkvaratööriist. Best Practice Analyzeri tulemusi saab kasutada lähtepunktina tõrgete kõrvaldamisel.
- Active Directory veebiteenus: see uus teenus toimib Active Directory domeenide jaoks veebiteenuse liidesena. Seda kasutavad enamasti teenused, mis võimaldavad Active Directoryle juurde pääseda HTTP(S)-i vahendusel.
- Domeeniga liitumine offline -re?iimis: süsteeme on võimalik domeeniga liita juba varem, ilma domeeniga ühendust loomata. Arvutid lisatakse domeeni pärast selle esimest käivitust.
- Active Directory Management Pack: tsentraalselt töötavate AD-teenuste (Active Directory Domain Services – AD DS) seisundi jälgimiseks.

M 4.415z Biomeetriliste autentimisvõimaluste turvaline kasutamine Windowsis

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

Alates versioonidest Windows Server 2008 R2 ja Windows 7 toetab Windows standardina ka sõrmejälgedel põhinevat biomeetrilist autentimist. Selleks töötati välja ja integreeriti operatsioonisüsteemiga eraldi raamistik Windows Biometric Framework (WBF). WBF võimaldab biomeetriliste lahenduste tootjatel enda sensoreid ja algoritme operatsioonisüsteemiga integreerida ning biomeetrilise tuvastamise käigus kogutud andmeid turvaliselt salvestada. Kui Windows tuvastab süsteemi külge ühendatud sõrmejäljelugeri, täiendatakse süsteemi juhtfunktsioone WBF-i näol biomeetriliste seadmetega.

Windows toetab sõrmejäljelugerite kasutamist järgmistel eesmärkidel:

- biomeetriline autentimine enne operatsioonisüsteemile või domeenile juurde pääsemist (Windowsi sisselogimine);
- biomeetriline autentimine enne volituste suurendamist seoses kasutajakontode haldamisega (vt M 4.340 Windows kasutajakonto haldamise (UAC) kasutamine);
- ühtne liides juurdepääsuks rakendustes kasutatavatele biomeetrilistele funktsioonidele.

Seda, kas domeeni sisselogimisel tohib kasutada biomeetrilist autentimist, saab seadistada grupipoliitikaobjektis. Seda tuleks võimaluse korral alati kasutada, et tagada kõikide domeenis olevate seadmete jaoks ühtlane turvaline konfiguratsioon.

Biomeetrilist autentimist ei ole võimalik kasutada ei külaliskontode ega ka eeldefineeritud administraatorikonto jaoks. Sõrmejäljelugerite kasutuselevõtu eelis on kahtlemata see, et autentimisprotseduur muutub kasutajatele seeläbi väga lihtsaks. Samas on senised katsetused ikka ja jälle näidanud, et näiteks sülearvutitesse paigaldatud sõrmejäljelugerid ei tööta alati piisavalt usaldusväärselt.

Tootelahendusest olenevalt saab sõrmejälgi kas suurema või vähema tehnilise vaevaga siiski kopeerida. Seepärast tuleb tavapärasest suurema turbevajadusega süsteemide korral põhjalikult analüüsida, kas nende nõutud turbeaste säilib ka siis, kui asjakohastes seadmetes kasutataks ainult sõrmejälgede tuvastamisel põhinevat autentimist. Enne biomeetriliste autentimislahenduste kasutuselevõttu tuleb hinnata nende tuvastusfunktsiooni usaldusväärsust ja analüüsida, kas see sobib süsteemide ja rakenduste turbenõuete täitmiseks. Suurte ja väga suurte turbenõuetega süsteemide jaoks kasutatakse tänapäeval pigem siiski kiipkaardil ja loal (token) põhinevat autentimist, sest sellega saavutatav turve on praeguste

biomeetriliste lahendustega võrreldes suurem. Planeerimisel tuleb ette näha lahendused ka nendeks olukordadeks, kus biomeetrilist autentimist sõrmejälgede tuvastamise kujul pole võimalik kasutada, nt kui sõrm on vigastatud. Siinkohal pakub Windows ka mitme sõrme tuvastamise võimalust, st ühe sõrme asemel saab kasutada ka mõnda teist. Lisavõimalusena tuleks juurdepääsu tagamiseks kasutada ka tsentraalselt deponeeritavat parooli.

Kontrollküsimused:

- Kas biomeetriliste autentimisfunktsioonide sobilikkust on hinnatud asjakohaste süsteemide ja rakenduste turbevajaduse põhjal?
- Kas biomeetriliste autentimisfunktsioonide kasutamist reguleeritakse grupipoliitikatega?
- Kas olukordadeks, kus biomeetrilisi autentimisfunktsioone ei saa kasutada, on tagatud ka muud autentimislahendused?

M 4.416z Windows Server Core'i kasutamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator, IT-juht

Alates Windows Server 2008-st saab operatsioonisüsteemi installida ka Server Core'i versioonis. Server Core on minimaalne, enamjaolt ilma graafilise kasutajaliideseta töötav süsteem. Süsteemi ennast saab konfigureerida üksnes kas käsuviibaga või versiooni Windows Server 2008 R2 puhul ka PowerShelliga, kui see on installitud. Server Core'i installatsiooni eelised on järgmised:

- märkimisväärselt vähem võimalusi süsteemi vastu suunatud rünneteks (vähem tarkvara tähendab ka vähem ründesihtmärke ja kitsaskohti);
- väiksem vajadus paikade (*patches*) installimise järele. Seetõttu väheneb ka tarkvara hooldamisest tingitud tööseisakute arv.

Mõnel juhul, nt Hyper-V kasutamisel, võib tekkida ka lisaeelis vähema ressursikasutuse näol. Server Core'i installatsiooni tuleks serveriteenuste jaoks kaaluda siis, kui rakendatakse põhjalikult defineeritud ja tsentraalselt töötavaid taristuteenuseid või kui võib eeldada, et tulevikus seistakse silmitsi suurema turbevajadusega. Kuna täismahus installatsiooni ei ole võimalik Server Core'i versiooniks migreerida, tuleb juba planeerimisetapis jõuda järeldusele, kas Server Core on vajalik ning milliseid lisavalikuid (*features*) on tarvis. Eriti hoolikalt tuleks planeerida halduslahendust. Server Core'i administraatorid peavad olema piisavalt koolitatud, et nad suudaksid serverit olemasolevate tööriistadega käsuviiba abil hallata.

Puuduvaid lokaalselt toimivaid ja interaktiivseid halduslahendusi asendavad enamasti geneerilised *remote* -tüüpi halduslahendused (Server-Manager, MMC) või rakendusepõhised kaughaldusvõimalused. Kontrollida tuleks ka seni kasutatud haldustööriistade sobivust. Server Core'i installatsiooni puhul ei saa kõiki rolle valikutena (*features*) installida, st toetatakse üksnes kindlaid rolle. Praktilise kasutuse poolest seab kõige suurema piirangu asjaolu, et standardinstallatsioonis puudub .NET tugi (Managed Code'i ei saa kasutada). Seetõttu lähtutakse toetatavate serverirollide puhul nn lihtsatest teenustest, mille hulka kuuluvad näiteks järgmised teenused:

- Active Directory Certificate Services;
- Active Directory Domain Services;
- Active Directory Lightweight Directory Services (AD LDS);
- DHCP-server, DNS-server;
- faili- ja printimisteenused;
- Hyper-V;
- Streaming Media Services;
- Veebiserver.

Kuna mitte igat tarkvara ei saa Server Core'i installatsioonis kasutada, tuleb kindlasti alati põhjalikult katsetada, kas planeeritud tarkvara sellise konfiguratsiooniga ka töötab.

Täiendavad kontrollküsimused:

- Kas taristuteenuste või tavapärasest suurema turbevajadusega serveri puhul kontrolliti, kas serverit saab käitada Server Core'i versioonis?
- Kas administraatoreid on käsuviibal põhineva halduslahenduse kasutamiseks piisavalt koolitatud?
- Kas kõikide Windows Server Core'i installatsiooni jaoks planeeritud tarkvarakomponentide tööd on piisavalt selles keskkonnas katsetatud?

M 4.417 Paikade haldus WSUS-iga alates Windows Server 2008-st

Algatamise eest vastutab: IT-juht

Rakendamise eest vastutab: administraator

Windows Server Update Services (WSUS) on teenus, mis hangib internetist Microsofti paikasid, värskendusi ja remondipakette ning teeb need kättesaadavaks teistele domeenis paiknevatele süsteemidele. Selline kokkukoondatud allalaadimisprotsess vähendab ühelt poolt institutsiooni võrguühenduse töökoormust ja võimaldab teisalt Microsofti operatsioonisüsteemide paikade haldust (Patch Management) vajaduse järgi automatiseerida. Selle teenuse kasutamisel paraneb märkimisväärselt oluliste turvapaikade laialijagamise kiirus. Kuna tarkvaras leitakse pidevalt uusi turvaauke, on paikade haldamise funktsioon üks olulisim tehniline turvameede (vt M 1.1 Vastavus normidele ja eeskirjadele). Seetõttu peavad kõik infokoosluses töötavad Windowsi süsteemid olema ühendatud asjakohase värskendusteenusega (Update Service). Versioonis Windows 2008 oli WSUS saadaval üksnes lisamoodulina, kuid alates Windows Server 2008 R2-st on see kasutusele võetud serverirollina. WSUS-i kasutamine eeldab serveris Internet Informationi serverit (Web Server serverirollis). Samuti peab olema piisavalt vaba mälumahtu, et värskendusi vahesalvestada, ning andmebaas haldusandmete tarbeks. Juhul kui ühtki sobivat MS-SQL-serverit pole võtta, saab serverisüsteemis andmebaasina kasutada ka mõnda Windows Internal Database'i instantsi.

WSUS-iga seotud tegevuste analüüsi ja seire tagamiseks tuleb installida ka Report Viewer Redistributable'i pakett.

Keerulisema struktuuriga infokooslustes saab mitut WSUS-serverit käitada ka paralleelselt või ridamisi, mis võimaldab teenindada mitut asukohta. Sel eesmärgil laadib iga WSUS-server defineeritavate ajavahemike möödudes endale mõnest kindlaks määratud allikast (nt kas Microsoftist või mõnest teisest vahele lülitatud WSUS-serverist) alla vajalikud värskendused. Selleks läheb hierarhias kõige kõrgemal paikneval WSUS-serveril tarvis internetiühendust, milleks saab kasutada ka näiteks WWW-proksit koos autentimisega või ka ilma selleta. Iga allalaaditud värskendus peab enne installimist läbima kasutusse lubamise protsessi. See võib toimuda käsitsi (administraatori otsuse põhjal), kuid selleks saab defineerida ka reegli. Reeglid tuleb nn WSUS-arvutirühmade jaoks defineerida erinevalt. Näiteks võidakse turbe seisukohalt kriitilisi värskendusi installida klientsüsteemidesse automaatselt, kuid kriitilisi rakendusi käitavate serverisüsteemide värskenduste installimine tuleb administraatoril eraldi käsitsi heaks kiita. Iga defineeritud rühma jaoks tuleb kindlaks määrata, kas tähtsam on turvapaikade automaatne paigaldus, millega saavutatakse kiiresti soovitud turbetoime, või süsteemi stabiilsus, milleks tuleb enne installimist teha põhjalikke katsetusi.

Ülejäänud domeenis paiknevatele süsteemidele tuleb juurdepääs WSUSserverile konfigureerida grupipoliitikatega. Konfiguratsiooniga saab süsteemidele teatavaks teha n-ö vastutava WSUS-serveri, kuid kasutada saab ka muid seadistusvõimalusi, nt määrata kindlaks intervalli, kui tihti kontrollitakse uute värskenduste ilmumist. Sel viisil konfigureeritud süsteemid küsivad WSUS-serverist

regulaarselt järele, kas sinna on ilmunud uusi olulisi värskendusi, mida installida (pull -mehhanism). WSUS-server teeb talle laekuva päringu põhjal kindlaks IT-süsteemis kasutusel oleva operatsioonisüsteemi ning kontrollib, kas selle jaoks leidub uusi värskendusi ja kas need värskendused on kasutusse lubatud. WSUS-i konfigureeritakse halduskonsooliga, kuid konsool ei pea töötama WSUS-serveris, vaid seda saab kasutada ka näiteks mõnes haldamisarvutis. Juurdepääsu WSUS-serveri halduskonsoolile tuleks kõikidel juhtudel kindlasti piirata, st juurdepääs tuleks tagada üksnes piiratud arvule volitatud administraatoritele.

Kui installitud on ka funktsioonipakett Report Viewer Redistributable, saab halduskonsoolis aruannete all tutvuda ühendatud süsteemide turvapaikade seisundiga (patch status). Seal saab muu hulgas välja selgitada, millal süsteemid end viimast korda WSUS-serveris värskendasid ning millised värskendused (updates) ja turvapaigad (patches) on süsteemidesse juba installitud. Näiteks võimaldab see eriti kriitiliste turvaaukude puhul jälgida turvapaikade paigaldamist ja vajaduse korral paigaldusprotsessiga viivitada.

Kontrollküsimused:

- Kas kõikide infokooslusse kuuluvate Windowsi süsteemide jaoks on konfigureeritud WSUS-server?
- Kas WSUS-serveril on juurdepääs internetile või mõnele teisele WSUSserverile, mis toimib värskenduste allikana?
- Kas juurdepääs WSUS-serveri halduskonsoolile on tagatud üksnes piiratud arvule volitatud administraatoritele?
- Kas WSUS-serveril on kasutada piisavalt vaba mälumahtu, et hallatavaid värskendusi vahesalvestada?
- Kas turvapaikade, värskenduste ja remondipakettide kasutusse lubamise jaoks on defineeritud sobivad WSUS-arvutirühmad ja reeglid?
- Kas iga defineeritud rühma puhul on kindlaks määratud, kas eelistada turvapaikade automaatset paigaldust ja selle kiiret toimet või süsteemi stabiilsust, mis eeldab põhjalikke katsetusi?

M 4.418 Windows Server 2008 kasutamise planeerimine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator, IT-juht

Windows Server 2008 kasutuse planeerimine on varasemate Windowsi versioonidega võrreldes muutunud keerukamaks ja nõuab enam tähelepanu, sest installimisetapis eristatakse kasutatavaid rolle varasemast palju rangemalt. Näiteks saab serverirolli Server Core valida üksnes installimisprotsessis, st installatsiooni tagantjärele Server Core'iks ümber muuta ei ole võimalik. Seetõttu tuleb kasutatavate rollide ja nende valikute (features) kindlaksmääramisel väga täpselt lähtuda Windows Server 2008 kasutusotstarbest. See meede toetub meetmetele M 1.1 Vastavus normidele ja eeskirjadele ja M 4.409w Windows Server 2008 soetamine ning kirjeldab peamisi aspekte, millega tuleb Windows Server 2008 kasutuselevõtu planeerimisel arvestada.

Üldkontseptsiooni koostamine

Windows Server 2008 planeerimine koosneb mitmest sammust. Planeerimisel võib järgida top-down -visandamispõhimõtet: terviksüsteemi üldkontseptsiooni visandi põhjal määratakse kindlaks spetsiifiliste osakontseptsioonide konkreetne planeerimistöö.

Üldkontseptsioonis käsitletakse näiteks järgmisi tüüpilisi lähteküsimusi:

- Kas üles ehitatakse uus võrk või migreeritakse olemasolev?
- Kas olemasolev Windowsi võrk migreeritakse täielikult või ainult osaliselt Windows Server 2008-ks ümber?
- Kas tegemist on lisaks kasutusele võetava serveriga või olemasoleva serveri kohandamisega (upgrade)?
- Millised komponendid (nt failiserver, printimisserver, DNS-server) asendatakse ning millised jäävad alles?
- Kas olemasolevaid protseduure või komponente (nt olemasolevat Kerberose süsteemi või PKI-d) on tarvis integreerida Windows Server 2008 süsteemiga?

Siinkohal tuleb muu hulgas arvestada ka teiste IT-süsteemide koostalitlusvõimega ja pakutavate funktsioonidega.

- Kas serveri planeeritud konfiguratsioon tuleb piisavalt hästi toime eeldatava andmekoguse ja tippkoormusega?
- Kas litsentseerimismudel on piisav ja sobib nii ettevalmistamise kontseptsiooni kui ka hädaolukorraks valmisoleku kontseptsiooni jaoks?
- Kas Windows Server 2008-t on tarvis käitada segarežiimis teiste operatsioonisüsteemidega, nagu Novelli või Unixiga?

Kui segarežiim on vajalik, võib see mõjutada süsteemis kasutatavaid autentimismeetodeid, mis võivad teistest kasutatavatest operatsioonisüsteemidest olenevalt sisaldada ka kitsaskohti ja seega vähendada kogu Windows Server 2008 keskkonna turvet. Sellise segakeskkonna jaoks tuleb välja töötada spetsiaalne turvapoliitika.

Rollide ja valikute (features) valimine

Microsoft on kasutusele võtnud nn serverirollid. Need on rakendused, mida saab kas tagantjärele juurde installida või mis tuleb, nagu Server Core'i puhul, installimise käigus kindlaks määrata. Kuni versioonini Windows Server 2003, viimane kaasa arvatud, installiti rakendused (nt Internet Information Services (IIS)) või muud baasteenused (nt printimis- või failiteenused) standardina juba üldise installimisprotsessi käigus. Seevastu Windows Server 2008 uusinstallatsiooni järel ei ole serveril veel mitte ühtki kindlat rolli ega funktsiooni. Rollid ja funktsioonid peab administraator iga süsteemi jaoks eraldi kindlaks määrama ja konfigureerima. Rollide kõrval on ka veel nn valikud.

Valikud on enamasti rollilaiendused, kuid need võivad olla ka täiesti eraldi funktsioonid, nt WINS-teenus. Minimaalne alusinstallatsioon ning sihipäraselt valitavad rollid ja valikud on märkimisväärne samm suurema turbe suunas, sest nende abil saab kõikide süsteemide jaoks installida üksnes vajaminevad funktsioonid. Seetõttu pole standardina installitud, kuid ebavajalikke funktsioone ja teenuseid enam tarvis süsteemist eemaldada. Serverirollide installimiseks ja konfigureerimiseks kasutatakse tavaliselt Server Manageri. See on Windows Server 2008 tsentraalne haldustööriist.

Versioonis Windows Server 2008 R2 saab kokku valida 17 serverirolli vahel.

Järgmine tabel annab ülevaate serverirollidest ja nende saadavustest eri väljaannetes.

Serveriroll
Enter-prise
Data-center
Standard
Web
Itanium
Foun-dation
Active Directory Certificate Services
Jah
Jah
Piiratud
Ei
Ei
Piiratud
Active Directory Domain Services
Jah

Jah
Jah
Ei
Ei
Jah
Active Directory Federation Services
Jah
Jah
Jah
Ei
Ei
Ei
Active Directory Lightweight Directory Services
Jah
Jah
Jah
Ei
Ei
Jah
Active Directory Rights Management Services
Jah
Jah
Jah
Ei
Ei
Jah
Rakendus-server
Jah
Jah
Jah
Ei
Jah
Jah
DHCP-server
Jah
Jah
Jah
Ei
Ei
Jah
DNS-server
Jah
Jah
Jah
Jah
Ei
Jah
Faksiserver
Jah
Jah

Jah
Ei
Ei
Jah
Failiteenused
Jah
Jah
Piiratud
Ei
Ei
Piiratud
Hyper-V
Jah
Jah
Jah
Ei
Ei
Ei
Võrgusuunised ja juurdepääsu-teenused
Jah
Jah
Piiratud
Ei
Ei
Piiratud
Printimis- ja dokumendi-teenused
Jah
Jah
Jah
Ei
Ei
Jah
Remote desktopi teenused
Jah
Jah
Piiratud
Ei
Ei
Piiratud
Veebi-teenused (IIS)
Jah
Jah
Jah
Jah
Jah
Jah
Windows Deployment Services
Jah
Jah
Jah

Ei
Ei
Jah
Windows Server Update Services (WSUS)
Jah
Jah
Jah
Ei
Ei
Jah
Windows Server 2008 (R2) ja Windows 7 koostoimimine

Windowsi domeeni piires võib kasutada põhimõtteliselt kõiki Microsofti heaks kiidetud ning toimiva kasutajatoega serveri- ja klientsüsteeme. Siiski tuleb arvestada, et kõiki olemasolevaid funktsioone, eriti näiteks uusi grupipoliitikaobjekte, saab täies mahus kasutada üksnes koos selleks sobivate klientsüsteemidega.

Hästi toimivad server-klient-kombinatsioonid on näiteks Windows Server 2008 või Windows Server 2008 R2 ja Windows 7.

Funktsioonid, mis töötavad üksnes kombinatsioonis Windows Server 2008 R2 ja Windows 7, on muu hulgas järgmised:

- DirectAccess: VPN-ühenduste loomine DirectAccessiga toimib ainult Windows Server 2008 R2 ja Windows 7 kombinatsiooni korral. Sama kehtib ka VPN-Reconnecti funktsiooni kohta;
- BranchCache: see Windows 7 klientfunktsioon võimaldab minimeerida WAN-andmesidet välisharudes.
- Remote Desktop Services: uusi funktsioone, mida versioonis Windows Server 2008 R2 tunti terminaliteenuste serverirollina, saab täies mahus kasutada üksnes koos Windows 7 klientsüsteemidega.

Kindlasti võib eeldada, et iga järgmine redaktsioon ja remondipakett toob endaga kaasa ka uusi funktsioone. Eriti kehtib see uute serveri- ja klientsüsteemide juurutamise kohta.

M 4.419z Rakenduste juhtimine AppLockeriga alates Windows 7-st

Algatamise eest vastutavad: infoturbespetsialist, IT-juht
Rakendamise eest vastutab: administraator

Tarkvara konfigureerimine ja installimine

Kliendi tarkvara konfiguratsioon võib mõnel juhul ise kohe pärast standardkonfiguratsiooni loomist etteantud nõuetest kõrvale kalduda, v.a juhul, kui on võetud tehnilisi meetmeid, mis seda takistavad. Kõrvalekaldumiste hulk kasvab enamasti sedamööda, kui pikalt on klienti kasutatud. Kõrvalekaldumiste põhjus seisneb lõppkasutajate installimistes, mille puhul ei järgita muudatuste haldamise protsessi standardseid ettekirjutusi. Tegu võib olla ka näiteks igapäevatööks vajalike tarkvaratööriistadega. Samas võivad kasutajad sageli installida ka sellist tarkvara, mida igapäevatööks üldse tarvis ei ole. Mõlemal juhul tuleb installimisel läbi teha muudatuste haldamise protsessis ette nähtud protseduurid. Täiendava tarkvara installimisel kaotab administraator peagi ülevaate kliendi tarkvara konfiguratsioonist. Selle tagajärjel võib tekkida olukord, kus võimalike vigade korral jäävad nende põhjused administraatori jaoks hoomamatuks. Sellest veelgi olulisem on aga fakt, et juurde installitud tarkvara suhtes ei toimi ei turvapaikade ega ka muudatuste haldus (vt M 2.273 Turvalisust mõjutavate paikade ja värskenduste kiire paigaldamine). Nii saavad ründajad tarkvaras leiduvaid turvaauke enda huvides ära kasutada ning klientsüsteemidesse näiteks kahjurvara koodi sisse smugeldada ja selle käivitada. Ka serverisüsteemidesse ei tohi tarkvara kontrollimatult juurde installida. Näiteks kui andmevarunduse eest vastutav administraator tahab endale mõnda konkreetset tarkvaratööriista juurde installida, et tohi ta seda teha niisama, vaid ta peab selleks kasutama muudatuste haldamise protsessi. Nii tagatakse, et installatsioon dokumenteeritakse ja tarkvaratööriist kaasatakse ka turvapaikade haldamise protsessi.

AppLocker

Alates versioonidest Windows 7 Ultimate, Windows 7 Enterprise ja Windows Server 2008 R2 kasutusele võetud AppLocker aitab administraatoril süsteemide üle kontrolli säilitada sellega, et tõkestab tehniliselt kasutajate jaoks nii tarkvara installimise kui ka selle käivitamise. AppLockerit tuleks kasutada süsteemi tervikluse kaitsmiseks. AppLocker on varasemate tarkvarapiiramispoliitikate (Software Restriction Policies – SRP) edasiarendus. Nende poliitikate konfigureerimiseks peab administraator kahjuks iga tarkvara ja iga vajaliku värskenduse kohta koostama eraldi reegli. Selle tagajärjel võib haldustööde maht paisuda väga suureks. Erinevalt tarkvarapiiramispoliitikatest on AppLockeri puhul administraatoril palju rohkem võimalusi suuniste defineerimiseks ning see aitab ka palju täpsemalt reageerida institutsiooni vajadustele. Näidetena võib siinkohal tuua viisardid ja reeglite koostamise tööriistad, mille abil saab reegleid koostada ka automaatselt. Neid tuleks kasutada näiteks oluliste süsteemifailide käivitamist lubavate standardsete reeglite defineerimiseks.

Kasutajatele mõeldud reeglite defineerimisel on administraatori töö lihtsustamiseks olemas ka sammsammulised juhised ja integreeritud abifunktsioon.

Standardsete reeglite kõrval tuleks eraldi suunised koostada ka käitusfailidele, installimisprogrammidele, skriptidele ja DLL-idele. Suuniseid saab eraldi konfigu-

reerida ja need pakuvad süsteemidele paremat kaitset, sest nende mõju ei piirdu üksnes käitusfailidega.

Reeglid

Reegleid on kolme tüüpi: lubatud, keelatud ja erandid. Nende põhjal saab koostada reeglid, mis lubavad institutsiooni jaoks defineeritud standardtarkvara käivitada (positiivne loetelu) või mis keelavad teadaolevate kahjurprogrammide käivitamise (negatiivne loetelu). Soovitame rakendada põhimõtet, et kõik rakendused tuleb keelata. Lubada tohib üksnes positiivses loendis kajastatud tarkvara installimist ja käivitamist. Nii tõkestatakse negatiivsesse loetellu seni veel sisse kandmata tarkvara installimine ja käivitamine. Standardsed reeglid analüüsivad ja hindavad andme- või kataloogiteed või tarkvara käitusfaili räsiväärtust (file hash). Lisareegleid saab kehtestada rakenduste signatuuride põhjal. Siinkohal tuleb arvestada järgmiste aspektidega.

Faili või kausta andmeteel (path) põhinevad reeglid

Kui defineeritakse reegel, mis lubab asukohas „C:\Programms" käivitada mis tahes tarkvara, saab turbemehhanismist möödahiilimiseks tõsta keelatud tarkvara käitusfaili ümber eelnimetatud kausta. Selle eelduseks on lokaalsete lõppkasutajate haldamist võimaldavad administraatorivolitused. Sellist olukorda tuleks asjakohaste meetmetega vältida (vt M 2.32z Piiratud kasutajakeskkonna loomine).

Faili räsiväärtusel (file hash) põhinevad reeglid

Faili räsiväärtust võib käsitleda kui faili krüptograafilist sõrmejälge. Seda tüüpi reegleid saab kasutada juhtudel, kus käitusfail ei ole digitaalselt signeeritud. Pärast igat tarkvaravärskendust tuleb koostada uus räsi ja kohandada kehtivaid reegleid. Selle tagajärjel võib haldustööde maht paisuda väga suureks. Seetõttu tuleks räsil põhinevatele reeglitele eelistada kas faili või kausta andmeteel või ka rakenduste digitaalsignatuuridel põhinevaid reegleid.

Rakenduste signatuuridel põhinevad reeglid

Kui fail on elektrooniliselt signeeritud, tuleks defineerida rakenduste digisignatuuridel põhinevad väljastajareeglid (publisher rules). Selle meetodi puhul tuleb tagada, et kliendis käivitataks rakenduse identiteeditеenus (AppIDSvc). Rakenduse signatuuride kasutamisel ei tohi turbeastmeks valida „Mis tahes väljastaja", vaid väljastaja tuleb defineerida. Reegli mõjuala saab piirata muude atribuutidega, nt versiooni numbri kasutamisega. Selliste piirangute puhul lubatakse rakendusi käivitada ainult alates teatud versioonist, eeldusel et väljastaja on selle ka signeerinud. Vanemaid versioone ei käivitata, seevastu uuemaid versioone lubatakse kasutada automaatselt. Positiivsete ja negatiivsete loetelude koostamise eest vastutavad infoturbespetsialist ja IT-juht. Nad peaksid koos osakonna juhtide ja lõppkasutajatega välja selgitama töötajate vajadused, need kokku koondama ja kontrollima, kas kõik vajadused said fikseeritud. Asjakohaseid loetelusid tuleb regulaarselt kontrollida. Vajaduse korral tuleb teha ka muudatusi.

Grupipoliitikate haldamine

Rakenduste juhtimine peaks olema kindla administraatori ülesanne. Domeenivõrgustiku puhul tuleb reegleid konfigureerida tsentraalselt grupipoliitikate haldamise mehhanismidega. Selleks läheb tarvis versioonis Windows Server 2008 R2 kasutatavaid domeenifunktsioone. Windows Server 2008 domeenifunktsioonide

puhul saab rakenduste juhtimiseks kasutada vastavaid kliendipõhiseid haldustööriistu (nt Remote Server Administration Tools for Windows 7). Grupipoliitikaobjektidega (Group Policy Objects – GPOs) tuleb defineerida erinevad reeglikomplektid ning seejärel need kasutajate ja kasutajarühmadega siduda. Näiteks saab sel viisil kindlaks määrata, et tsentraalse andmebaasi haldamiseks kasutatavat tarkvaratööriista tohib käivitada üksnes arendusosakond. Seevastu Microsofti Office Suite'i kasutuse võib vabaks anda kõikidele institutsiooni töötajatele ilma funktsioone piiramata. Vajalikud seadistused leiate grupipoliitikate haldamise redaktorprogrammist Group Policy Editor asukohas „Computer Configuration I Policies I Windows settings I Security settings I Application Control Policies I AppLocker ".

Logimine

Kui kasutaja üritab käivitada mõnda AppLockeris defineeritud reeglitele mittevastavat rakendust, katkestab AppLocker selle programmi käivitamise ja dokumenteerib aset leidnud protsessi, tehes selleks süsteemilogisse sissekande. Manipuleerimiskatsete avastamiseks ja nende tagamaade selgitamiseks tuleb süsteemilogis kajastuvaid AppLockeri sissekandeid regulaarselt analüüsida. Ideaaljuhul tuleks süsteemilogid selleks mõnda tsentraalsesse logiserverisse kokku koondada ja automaatselt läbi analüüsida. Juhul, kui AppLocker võetakse kasutusele tootmissüsteemis, saab seda üleminekuperioodil käitada ka seirerežiimil. Seirerežiimi korral programmide käivitamist reeglite vastu eksimisel ei tõkestata, kuid logisse tehakse selle kohta siiski sissekanne. Logide analüüsimisega saab välja selgitada programmid, mille suhtes reeglid õigesti veel ei toimi.

Kontrollküsimused:

- Kas klientides kasutatakse tarkvara volitamata installimise ja käivitamise tõkestamiseks AppLockerit?
- Kas AppLockeri kasutamisel lähtutakse positiivse loetelu põhimõttest „kõik, mis ei ole otseselt lubatud, on keelatud"?
- Kas AppLockeri kasutamiseks mõeldud reeglite defineerimisel eelistatakse rakenduste signatuuridel ja kindlaksmääratud väljastajatel põhinevaid reegleid?
- Kas domeenipõhises võrgus rakendatakse AppLockeri reeglistike haldamiseks kasutajatel/kasutajarühmadel põhinevaid grupipoliitikaobjekte?
- Kas süsteemilogide analüüsimisel pööratakse piisavalt tähelepanu ka sissekannetele, mis kajastavad AppLockeri reeglite rikkumise katseid?
- Kas AppLockeri reeglite toimimist katsetatakse esmalt mõnes katsesüsteemis või AppLockeri käitamisega seirere?iimis ning alles seejärel võetakse need tootmissüsteemides kasutusele?

M 4.420 Windows 7 tegevuskeskuse turvaline kasutamine

Algatamise eest vastutavad: administraator, infoturbespetsialist
Rakendamise eest vastutab: administraator

Windows 7 tegevuskeskus (Action Center) on turvakeskuse (Security Center) edasiarendus. Seevastu tegevuskeskus on täiesti ühesuguste funktsioonidega olemas kõikides Windows 7 redaktsioonides. Tegevuskeskuses saab tsentraalselt jälgida ja konfigureerida turva- ja hooldusseadistusi ning kõrvaldada tõrkeid.

Tegevuskeskuse nõuetekohane töö sõltub järgmistest Windowsi teenustest, mis hoolitsevad tõrgete automaatse diagnostika eest ja edastavad tegevuskeskuse vahendusel kasutajatele tõrketeate:

- Diagnostikapoliitikateenus (Diagnostic Policy Service – DPS) - See Windowsi teenus võimaldab tuvastada ja lahendada Windowsi probleeme. Probleemide põhjused võivad olla erinevad, nt mälu, kõvaketas või võrk. Teenus käivitab probleemide diagnostika ja teavitab seejärel tegevuskeskuse kaudu kasutajat diagnostika tulemustest.
- Diagnostikateenuse host (Diagnostic Service Host – WDiSvcHost) - Seda Windowsi teenust kasutatakse analüüsides, mis peavad töötama lokaalse teenusena. Teenuse töö sõltub otseselt diagnostikapoliitikateenuse tööst.
- Diagnostikasüsteemi host (Diagnostic Service Host – WDiSystemHost) - See Windowsi teenus diagnoosib, käsitleb ja lahendab otseselt Windowsi komponentidega seotud probleeme. Teenuse töö sõltub otseselt diagnostikapoliitikateenuse tööst.
- Windowsi veateavitusteenus (Windows Error Reporting Service – WerSvc) - Veateavitusteenus kogub tekkinud probleemide kohta teavet ja esitab lahendusettepanekuid. Samuti koostab see teenus probleemide kohta aruandeid, mille võib vajaduse korral edasi saata Microsoftile, et saada nende käest muid lahendusettepanekuid.

Probleemilahenduse aplett (Troubleshooting) on rakenduste pakett, mis kogub Windows 7-ga töötavates IT-süsteemides tekkinud probleemide kohta nii teavet kui ka lahendusettepanekuid. Lahendusettepanekute hankimiseks Microsofti käest on tarvis internetiühendust. Lisaks külastab aplett regulaarselt Microsofti servereid ning laadib alla uusi lahendusettepanekuid ja komponente. Kui institutsiooni või selle arvutite eripära kajastavaid konfiguratsioone ei soovita Microsoftile edasi saata, tuleks see funktsioon välja lülitada. Kui mõne konkreetse probleemi tekkimisel on tarvis väga spetsiifilisi lahendusettepanekuid, kogutakse Windowsi kliendis probleemi kohta andmed kokku ja saadetakse edasi Microsoftile. Sellega, mis andmed täpselt edastatakse, saab tutvuda probleemi kohta koostatud aruannetes.

Probleemi aruanne sisaldab teavet nii operatsioonisüsteemi kui ka IT-süsteemi riist- ja tarkvara kohta. See võib muu hulgas sisaldada ka isikuandmeid. Probleemi tuvastamisel võib probleemilahenduse funktsioon (Troubleshooting) püüda

seda iseseisvalt lahendada. Selleks muudab see funktsioon süsteemi konfiguratsiooni.

Tegevuskeskuse ja selle funktsioonide turvalise kasutamise huvides tuleks arvestada alltoodud aspektidega.

Kuna Windowsi teenused avaldavad teistele teenustele mõju ja vastupidi, tuleks kindlasti tagada, et Windowsi teenuste standardseadistus ei muutuks. Vastasel korral ei õnnestu Windowsi teenuseid enam korrektselt käitada.

Windowsi teenus	Standardne käivitamistüüp
Diagnostikapoliitikateenus (DPS)	Automaatne
Diagnostikateenuse host (WDiSvcHost)	Käsitsi
Diagnostikasüsteemi host (WDiSystemHost)	Käsitsi
Windowsi veateavitusteenus (WerSvc)	Automaatne

Lisameetmena tuleks grupipoliitikate abil igas Windows 7-ga töötavas IT-süsteemis teha järgmised seadistused:

- Seadistus: hankige Windowsi online -teenuse kaudu uusimaid probleemilahendusi (troubleshootings).
- Juhtpaneeli andmetee: Control Panel I All Control Panel items I Troubleshooting
- Grupipoliitikate andmeteed:
- Computer Configuration I Policies I Administrative templates I System I

Troubleshooting and Diagnostics I Microsoft Support Diagnostic Tool I restrict Tooldownloadi

- Computer Configuration I Policies I Administrative templates I System I

Troubleshooting and Diagnostics I Microsoft Support Diagnostic Tool I Execution Level Configuration

- Soovitus: seadistused desaktiveerida. Põhjendus: see tagab, et tõrkekäsitluseks vajalik andmevahetus Microsoft Supportiga läbi interneti leiab aset üksnes kasutaja teadmisel ja nõusolekul.
- Seadistus: probleemiaruannete saatmine
- Juhtpaneeli andmetee: puudub
- Grupipoliitikate andmeteed:
- Computer Configuration I Policies I Administrative templates I Windows

Componenets I Windows Error reporting I Configure Error Reporting

- Computer Configuration I Policies I Administrative templates I System I Internet

Communication Management I Internet Communication Settings I Turn off Error Reporting

- Soovitus: seadistused desaktiveerida. Põhjendus: seadistused tuleks desaktiveerida, sest muidu saadetakse Microsoftile edasi institutsiooni või selle arvutite eripära kajastavad konfiguratsioonid.
- Seadistus: arvutikonfiguratsiooni regulaarne saatmine Microsoftile
- Juhtpaneeli andmetee: puudub
- Grupipoliitikate andmetee:
- Computer Configuration I Administrative Templates I Windows Componenets

I Application Compatibility I

- Soovitus: seadistused desaktiveerida. Põhjendus: kui selle seadistuse mõju ei ole grupipoliitikatega tõkestatud, võib juhtuda, et installitud tarkvaratooted saadavad Microsoftile andmeid edasi kasutaja teadmata ja nõusolekuta.

Turvet ohustavate lisafunktsioonide tõkestamiseks tuleks kasutada järgmisi seadistusi:

- Seadistus: Windows Backup
- Juhtpaneeli andmetee: Control Panel I All Control Panel items I Action Center I Change Action Center settings. Soovitus: seadistus desaktiveerida. Põhjendus: ilmuva teate põhjal võivad lokaalsete volitustega kasutajad teha IT-süsteemis andmetest varukoopia ja salvestada selle teadmatusest mõnda lokaalsesse andmekandjasse. Selline tegevus jääb IT-osakonnale märkamata, millest tekivad omakorda muud turvariskid.
- Seadistus: kasutajasõbralikkuse programm
- Juhtpaneeli andmetee: Control Panel I All Control Panel items I Action Center I Change Action Center settings I Customer Experience Improvement Program Configuration. Soovitus: seadistus desaktiveerida. Põhjendus: seadistus takistab kasutaja harjumusi kirjeldavate andmete edastamist Microsoftile.
- Seadistus: arvuti hooldamine
- Juhtpaneeli andmetee: Control Panel I All Control Panel items I Action Center I Troubleshooting I Change settings. Soovitus: seadistus aktiveerida. Põhjendus: seadistus tuleks aktiveerida, et arvutis oleks võimalik probleeme tuvastada ja kasutajat leitud probleemidest teavitada.
- Seadistus: tõrkekäsitluse muud seadistused
- Juhtpaneeli andmetee: Control Panel I All Control Panel items I Action Center I Troubleshooting I Change settings. Soovitus: seadistused desaktiveerida. Põhjendus: seadistused tuleks desaktiveerida, et tõkestada uute

probleemilahenduste allalaadimine Microsofti käest, probleemide automaatne edastamine Microsoftile ja probleemide automaatne lahendamine. Seda seadistust ei ole soovitatav kasutada, sest see muudab automaatselt IT-süsteemi konfiguratsiooni.

Tegevuskeskuse (Action Center) kasutamise kohta ja seadistuste rakendamise järel kasutajatele kuvatavate dialoogikastide jaoks tuleks vastu võtta kohustuslikud nõuded, mida kasutaja peab järgima. Reeglid peaksid kindlaks määrama ka selle, kas ja millal tohib kasutaja tegevuskeskuse komponente iseseisvalt käsitsi käivitada (vt M 2.4 Hooldus- ja remonditööde reeglid). Tavajuhul peaks IT-süsteemi käitamise ajal tekkivate probleemide eskaleerimisega tegelema mõni vastavate töökohustustega töötaja (vt M 2.1 IT kasutajate vastutuse ja reeglite kehtestamine).

Kontrollküsimused:

- Kas Windows 7 tegevuskeskuse rakendamise jaoks on kasutajatele välja töötatud kohustuslikud reeglid?
- Kas Windows 7 keskkonnas töötavas DPS-, WDiSvcHost- ja WerSvcteenuses kasutatakse standardseadistusi?
- Kas funktsioonide „Hangi Windowsi online -teenuse kaudu uusimaid probleemilahendusi (troubleshootings)”, „Probleemiaruannete saatmine”, „Arvutikonfiguratsiooni regulaarne saatmine Microsoftile”, „Windows Backup”, „Kasutajasõbralikkuse programm” ja „Muud tõrkekäsitluse seadistused” seadistused on Windows 7-s desaktiveeritud?
- Kas Windows 7-s on arvuti hooldamise funktsioon aktiveeritud?

M 4.421 Windows PowerShelli turve

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

Windows PowerShell (WPS) on süsteemi interaktiivseks haldamiseks loodud skriptikeskkond, mis põhineb.NET-il. WPS suudab käivitada ka haldusskripte.

Skriptid kujutavad endast käsujadasid, mis salvestatakse tekstifailina ja käivitatakse käsuviibaga.

Kui WPS-i ei kasutata, tuleks see desaktiveerida. Alates Windows 7-st saab PowerShelli skriptimiskeskkonda eemaldada üksnes .NET Frameworki desinstallimisega. Seevastu juhtudel, kus rakendustel on seda siiski tarvis, tuleb PowerShelli keskkonna puhul arvestada järgmiste turbeaspektidega.

64-bitistes süsteemides eksisteerivad paralleelselt nii 32-bitine kui ka 64-bitine PowerShell. 32-bitine keskkond kasutab 32-bitist SysWOW64 emulatsioonikihti failisüsteemile juurdepääsuks ja registreerimiseks. Kui SysWOW64 kasutatakse süsteemiosadele juurdepääsuks, võib see põhjustada väärfunktsioone.

Samuti võib esineda probleeme 32-bitiste skriptide ühildumisel 64-bitiste keskkondadega ja ka vastupidi. Seetõttu tuleks 64-bitistes süsteemides kasutada üksnes 64-bitist PowerShelli. Skripte, mis koostati ja mida katsetati 32-bitistes süsteemides, ei tohiks 64-bitistes süsteemides kasutada.

Failitasandi turve

Ainult administraatoritel peaks olema õigus käivitada programmifaile, mis paiknevad asukohtades „C:\Windows \WindowsPowerShell\powershell.exe” ja „powershell_ise.exe”. Seetõttu peavad turbeseadistused tagama, et selliste failide käivitamise õigus oleks ainult administraatorite kasutajarühma liikmetel. 32-bitiste versioonide asukoht 64-bitistes süsteemides on „C:\Windows\SysWOW64” ning selle kaitseks tuleb vajaduse korral võtta täiendavaid turbemeetmeid. Tuleks kaaluda, kas anda juurdepääs üksnes kindlatele administraatorikontodele, nt kui skriptide puhul on tarvis kasutada ka automaatkäivitust või kui skripte soovitakse käivitada võrgu kaudu. Selleks on soovitatav koostada kas lokaalne või domeenipõhine eraldi turvarühm ja anda sellele programmifailide kasutamiseks vajaminevad volitused. WPS-i käivitamise volitustega programmide puhul ei tohi Systemi ega ka TrustedInstalleri turvarühma eemaldada!

PowerShelli profiili turve

Kasutajapõhine PowerShelli profiil, mis laaditakse süsteemi WPS-i käivitamisel, peab olema kaitstud. Seda, mis fail sisaldab praegu sisse logitud kasutaja profiili, saab WPS-is välja selgitada käsuga $profile. Profiil asub tavaliselt mõnes Windowsi kasutajaprofiili kaustas, millele on juurdepääs üksnes kasutajal ja administraatoril. Volitamata juurdepääsukatsete välistamiseks tuleks profiilifailide jaoks sisse lülitada objektiseire (vt M 4.344 Windows 7 ja Windows Server 2008 süsteemi seire). Profiilifailide puhul on eriti oluline, et iga rühm, millele on antud üldised

muutmisõigused, lisataks kindlasti ka SACL-loendisse (System Access Control List) (Properties I Security I Advanced I Auditing). Seirega seotud sündmusi tuleks pisteliselt analüüsida ka sündmuste kuvas.

Skriptide käivitamise turve

Ka käivitatud skripte tuleb kindlasti turvata. Erilist kaitset vajab siinkohal PowerShelli profiil, sest WPS-i käivitamisel käivitatakse profiil kasutajapõhiselt. Skriptide käivitamine võib ohustada nii operatsioonisüsteemi kui ka rakenduste stabiilsust ja terviklust ka siis, kui selle käigus ei tehta administraatorivolitustega pöördusi operatsioonisüsteemi komponentidele.

Seetõttu tuleks järgmised käivitatavad skripti- ja abifailid failisüsteemi tasandil varustada asjakohaste piiratud volitustega:

- .ps1-failid: Windows PowerShell Shell-Skript;
- .ps1xml-failid: Windows PowerShell Format and Type Definitions;
- .psc1-failid: Windows PowerShell Console File (eksporditud Shellkonfiguratsioon);
- .psd1-failid: Windows PowerShell Data File;
- .psm1-failid: Windows PowerShell Module File.

Skriptide muutmise volitused tuleks anda ainult teatud rühmadele, et tagada skriptide terviklus. PowerShelli skriptide käivitamise võimalusi tuleks piirata ka käsuga Set-ExecutionPolicy. Selle käsuga määratakse kindlaks, mis tingimustele peavad skriptid vastama, et neid käivitataks.

Võimalikud on järgmised valikud:

- Restricted: kõikide skriptide käivitamine on täielikult keelatud;
- AllSigned:.ps1- ja.ps1xml-failid peavad käivitamiseks olema digitaalselt signeeritud;
- RemoteSigned: lokaalselt koostatud skripte tohib käivitada ka siis, kui neil puudub signatuur;.
- Unrestricted: kõiki skripte tohib piiramatult käivitada.

PowerShelli skriptide käivitamise seadistuses tuleks lubada üksnes signeeritud skriptide käivitamine. Selleks tuleb PowerShelli keskkonnas käivitada järgmine käsk: Set-ExecutionPolicy AllSigned

PowerShelli skriptide signeerimine

Skriptide signeerimiseks läheb tarvis kolmanda klassi Authenticode'i koodisignatuuri sertifikaati, mida on võimalik hankida kolmel viisil:

- Institutsioonidel, kellel on olemas enda valiku võtme taristu (PKI), saavad vajamineva sertifikaadi ise koostada, eeldusel et taristusisene sertifitseerimisüksus on liigitatud kõikide PKI külge ühendatud infokooslusse kuuluvate IT-süsteemide jaoks usaldusväärseks.
- Teine võimalus on kasutada mõnda välist sertifitseerimiskeskust (Certification Authority – CA). Windows 7 konfiguratsioonis on juba ette nähtud, et need usaldavad juhtivate väliste CA-de sertifikaate.

- Kolmas võimalus seisneb enda signeeritud sertifikaadi koostamises tööriistaga Makecert.exe. See tasuta tööriist on olemas Windowsi SDK-platvormis ning osa Microsoft Office'i tarkvarapakettide puhul installitakse see automaatselt.

Selle lahenduse puudus on asjaolu, et sel moel koostatud sertifikaati saab kasutada üksnes selles IT-süsteemis, milles see koostati.

PowerShelli skriptide käivitamiseks võrgu kaudu, nt sisselogimisskriptina (vt M 2.326 Windows Vista ja Windows 7 grupeerimissuuniste planeerimine), on soovitatav kasutada kas sisemist või välist sertifitseerimiskeskust.

Kontrollküsimused:

- Kas Windows PowerShelli failide käivitamise õigus on antud üksnes administraatoritele, st nende lokaalsetele ja domeenipõhistele kasutajarühmadele?
- Kas Windows PowerShelli profiili jaoks on sisse seatud kirjutamise ja lugemisega seotud pöörduste logimine ning kas neid logisid analüüsitakse regulaarselt?
- Kas Windows PowerShelli skriptide käivitamist piiratakse käsuga Set-ExecutionPolicy AllSigned?

M 4.422z BitLocker To Go kasutamine alates Windows 7-st

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: kasutajad, infoturbespetsialist, administraator

BitLocker To Go abil saavad Windows 7 versioonide Enterprise ja Ultimate kasutajad krüpteerida vahetatavatele andmekandjatele, nt USB-mälupulkadele, välistesse kõvakettaajamitesse ja virtuaalsetesse ajamitesse (Virtual Hard Drives – VHD), salvestatud partitsioone. Kui juhtub, et vahetatav andmekandja läheb kaduma või see varastatakse ära, on sellele salvestatud andmed jätkuvalt kaitstud, sest krüpteeritud andmete dekrüpteerimine on võimalik üksnes kas parooli, smartcard 'i või andmetaastusinfoga. BitLocker To Go sisselülitamiseks tuleb liikuda ajamisümboli kontekstimenüüsse ja märgistada suvand „Enable BitLocker". Administraatorivolitusi ei ole selleks tarvis. Krüpteerimisfunktsiooniga kaitstud vahetatavaid andmekandjaid hallatakse juhtpaneeli valikus „BitLocker Drive Encryption".

Enne BitLocker To Go kasutuselevõttu on soovitatav rakendada moodulit B 1.7 Krüptokontseptsioon . Samuti tuleks täiendada nii turvapoliitikat kui ka teisi reegleid meetmetes M 2.309 Mobiilse IT-kasutuse turvapoliitika ja eeskirjad ja M 2.401 Mobiilsete andmekandjate ja seadmete kasutamine esitatud soovituste kohaselt ning määrata kindlaks, millistel juhtudel on töötajatele krüpteerimine kohustuslik, vabatahtlik ja keelatud. Siinkohal tuleb arvestada, et BitLocker To Go'ga ei saa faile ühekaupa krüpteerida, vaid krüpteerida saab üksnes andmekandja partitsiooni. Kõige keerulisem on aga tagada, et kasutajad oleksid krüptograafilise võtmematerjaliga võimalikult hoolikad (vt M 2.46 Krüpteerimise õige korraldus). Kui see peaks sattuma võõrastesse kätesse, pole andmete konfidentsiaalsus enam tagatud. Krüptovõtmete turbevajadus konfidentsiaalsuse ja käideldavuse tagamisel tuleb hinnata vähemalt võrdväärseks krüpteerimata andmete omaga. Niipea kui BitLocker To Go'd kasutavaid inimesi on juba mitu, tuleks kohe kasutusele võtta ka tsentraalselt juhitav võtmehaldus, nt Active Directory baasil.

Standardseadistuses on BitLocker To Go aktiveeritud. Seevastu kui BitLocker To Go rakendamisest on teadlikult loobutud (vt M 2.325 Windows 7 turvapoliitika kavandamine), tuleks selle kasutus grupipoliitikaga desaktiveerida, sest muidu võib see endaga kaasa tuua eri tüüpi ohte, mida on kirjeldatud ohukataloogides G 3.97 Konfidentsiaalsuse kadu vaatamata draivide krüpteerimisele BitLockeriga ja G 3.98 BitLockeriga krüpteeritud andmete kadu. Järgmises kirjelduses mainitavad BitLocker To Go seadistusvõimalused asuvad grupipoliitikas: Computer Configuration | Administrative Templates | Windows Components | BitLocker Drive Encryption | Removable Drives

Võtme liik

Pärast käsu „Enable BitLocker" käivitamist on kasutajal võimalik valida, kas sisestada krüpteerimisparool või asetada seadmesse krüpteerimissertifikaati sisaldav smartcard. Sertifikaadi avalik osa salvestatakse krüpteerimata kujul otse kaasaskantavale andmekandjale, mis tähendab, et andmekandja kaotsimineku korral on võimalik sertifikaadist välja lugeda teavet kasutatud sertifikaaditaristu (PKI) kohta. Kui PKI turbevajadus on konfidentsiaalsuse tagamisel suur, tuleks

kaaluda, kas lubada andmekandjate krüpteerimist üksnes parooliga või kasutada spetsiaalseid sertifikaate. Seevastu juhtudel, kus konfidentsiaalsusnõuded on tavapärasest suuremad, tuleb arvestada, et paroolist krüpteeritavate andmete kaitseks ei piisa.

Kasutusele tuleb võtta smartcard -süsteemid ja rakendada mitmefaktorilist autentimist. Krüpteerimiseks kasutatava parooli pikkusele tuleb kehtestada vajalikud miinimumnõuded, nagu meede M 2.11 Paroolide kasutamise reeglid seda ette näeb. Samuti tuleb kehtestada parooli keerukuse nõuded.

Krüpteerimise tugevus

Väga suurte konfidentsiaalsusnõuete korral tuleks 128-bitise AES-i ja difuusori asemel kasutada 256-bitist AES-i ja difuusorit (grupipoliitika „Choose drive encryption method and cipher strength"). Samas tuleb arvestada, et see muudab arvutusprotsessi märkimisväärselt pikemaks, mistõttu võib aeglastes arvutites sellise krüpteerimisviisi kasutamine ka ebaõnnestuda.

Krüpteeritud andmekandjate sisu avamine ilma BitLocker To Go'ta

Tarkvaratööriistaga Bitlockertogo.exe suudavad krüpteeritud andmekandjate sisu lugeda ka sellised Windowsi versioonid, millel BitLocker puudub, eeldusel et need on vormindatud tööks FAT-failisüsteemiga. Kirjutamisõigusega juurdepääs andmekandjale ei ole võimalik. Teistes operatsioonisüsteemides, nt Mac OS-is või Linuxis, BitLocker To Go'ga krüpteeritud andmekandjate sisu lugeda ei saa, sest sellist programmi ei eksisteeri. Grupipoliitikaga saab kindlaks määrata, et Bitlockertogo. exe salvestataks igale uuesti krüpteeritavale FAT-andmekandjale automaatselt krüpteerimata kujul. Kuna see rakendus ei toeta ei pääsuõiguste kontrollimist ega ka smartcard 'iga autentimist, siis sisekasutuseks selline lahendus enamasti ei sobi. Turvapoliitikas, mis käsitleb krüpteeritud andmevahetust kolmandate osalistega, tuleks kindlaks määrata, kes töötajatest tohib andmeid edastada ja millistes IT-süsteemides tohib neid krüpteeritud FAT-andmekandjatele salvestada.

Ilma krüpteerimata kirjutamise tõkestamine

Krüptokontseptsiooni põhjal on tarvis otsustada, kas ja milliste IT-süsteemide jaoks tuleks grupipoliitikaga ära keelata andmete kirjutamine välistele krüpteerimata andmekandjatele. Vastav GPO kannab nime „Deny write access to fixed drives not protected by BitLocker". Selle seadistusega on võimalik tagada, et välistele andmekandjatele salvestatud andmed on alati krüpteeritud. Seda seadistust kasutades tuleb praktikas sageli konfigureerida ka erandid ja need kasutajatele teatavaks teha, et krüpteerimisstrateegiaga kehtestatud nõuded oleksid täidetud ka keeruliste kasutusjuhtude puhul. Kõige sagedam põhjus, miks erandeid üldse tarvis läheb, on näiteks mälupulgalt andmeid lugevate esitlusseadmete kasutamine ja väliste andmekandjate planeeritud edasiandmine kolmandatele, organisatsioonivälistele isikutele. Üks võimalus, kuidas USB-mälupulki mitte krüpteerida, on need väliselt arusaadavalt ära märgistada, nt sildiga „avalik".

Krüpteerimata andmekandjate edasiandmist ja kasutamist tuleks lubada üksnes selleks volitatud töötajatele. USB-mälupulkadel hoitavate andmete konfidentsiaalsusnõuetest olenevalt tuleks vajaduse korral kaaluda ka piiravate töökorralduslike lisameetmete võtmist, nt USB-mälupulkade väljastamise kirjalikku fikseerimist. Kõik tööks vajalikud erandid peavad olema reguleeritud kas andmevahetust käsitlevas turvapoliitikas või krüptokontseptsioonis. Tehnilise poole pealt saab teatud andmekandjate jaoks erandeid luua ka eelnimetatud grupipoliitikaga, kuid selleks peab andmekandjatele olema antud spetsiaalne ID. Täpsed juhised, kuidas ID-sid konfigureerida, on kirjas sellessamas grupipoliitikas. Töötajatele tuleb õpetada, kuidas krüpteeritud ja krüpteerimata andmekandjatega õigesti ümber käia.

Vahetatavate krüpteeritud andmekandjate sisu taastamine hädaolukorras Taastamisparoolid ja -võtmed võimaldavad administraatoril või kasutajal hädaolukorras, st kui kasutaja on enda krüpteerimisparooli või smartcard 'i ära kaotanud, krüpteeritud andmeid taastada. Andmekandja esimese krüpteerimise käigus genereerib viisard 48-kohalise juhuandmetel põhineva taastamisparooli. See tuleks kas välja printida või tekstifailina kuhugi turvalisse kohta salvestada. Taastamisparoolidega ümberkäimise kohta tuleb kasutajatele välja töötada kindlad reeglid (vt M 2.22z Paroolide deponeerimine). Taastamisparoolid peavad olema sama konfidentsiaalsed ja nendega tuleb sama hoolikalt ümber käia nagu krüpteerimisparooli ja smartcard 'iga. Näiteks tuleb meetme M 4.86 Krüptomoodulite kindel rollijaotus ja konfigureerimine kohaselt kindlaks määrata, kas ja kuidas taastamisparoole ja -võtmeid tsentraalselt deponeeritakse ning kes tohivad nendele andmetele taastamise eesmärgil juurde pääseda. Et tagada taastamiseks vajaliku info parem kaitse ja kiirendada andmete taastamist hädaolukorras, on soovitatav need andmed ilma kasutaja sekkumata automaatselt Active Directorysse salvestada.

Kõikidel juhtudel tuleb tagada sobiv ümberkäimine taastamisparoolide ja -võtmetega. Selleks saab grupipoliitikaga kindlaks määrata, kuidas BitLockeriga kaitstud vahetatavate andmekandjate sisu taastada. Samuti tuleb täpselt defineerida, millised on taastamiseks vajalikud tööetapid, kes tohib andmeid taastada ja mis ressursse tohib selleks kasutada. Kui taastamisparool valitakse käsitsi või kui seda muudetakse tagantjärele, tuleb kindlasti vältida lihtlabaseid järjestusi. Kui mitme andmekandja jaoks valitakse tõhususe kaalutlustel ühesugune taastamisparool, on lihtlabaste järjestuste vältimine veelgi olulisem.

Parooli, smartcard 'i või võtme kompromiteerimise kahtluse korral tuleb kasutusele võtta uus võti. Sama kehtib ka taastamisparooli ja -võtme kohta. Grupipoliitikaga saab iga krüpteeritud andmekandja jaoks koostada 256-bitise taastamisvõtme.

Taastamisvõti võimaldab andmekandja sisule juurde pääseda ka näiteks siis, kui algsed autentimisvahendid ei ole enam kättesaadavad. Taastamisvõtit ei saa välja printida ning seda ei ole võimalik suuliselt, nt telefonitsi, edasi öelda. Nii

suureneb küll andmete konfidentsiaalsus, kuid hädaolukorras kulub andmete taastamiseks palju rohkem aega. Taastamisvõtmeid võib salvestada kas üksnes mõnele muule USB-mälupulgale või Active Directorysse. Seevastu süsteemide puhul, milles töödeldakse väga suurte konfidentsiaalsusnõuetega andmeid, tohib lubada üksnes taastamisvõtmeid, seevastu taastamisparoolidest tuleb loobuda.

Lisameetmena saab administraator installida andmetaastusviisardi (Group Policy snap-in | Computer configuration | Windows settings | Security settings | Public Key Policies | Bitlocker). See on universaalse taastamisvõtme avalik osa ja see installitakse ühtmoodi kõikidesse BitLockeri klientidesse. Selle juurde kuuluva privaatvõtmega saab krüpteeritud andmekandja sisu dekrüpteerida. Privaatvõti ei tohiks olla administraatori valduses. Üldjuhul kaasneb andmetaastusviisardite rakendamisega vajadus tagada väga suur kaitse nende väärkasutuse vastu ning viisardi väljavahetamine on kompromiteerimise korral väga töömahukas. Andmetaastusviisard ei asenda taastamisparoole ega -võtmeid, vaid pakub üksnes andmekadudevastast lisakaitset sellistele kasutajatele, kes ei ole liidetud tsentraalselt toimivasse võtmehaldusse. Andmetaastusviisardi plusse ja miinuseid tuleb hoolikalt kaaluda juba enne selle kasutuselevõttu.

Võtmematerjali hävitamine

Niipea kui krüpteeritud andmekandja eemaldatakse kasutuselt või kui see on kaotsi läinud, tuleb kõik sellega seotud võtmed ja paroolid viivitamata hävitada. Tsentraalselt salvestatud võtmete korral tuleks võtmete hävitamist, juhul kui võtmega krüpteeritud andmed on jätkuvalt konfidentsiaalsed, kajastada revisjonikindlas protokollis.

Kasutajate koolitamine

Kuna BitLocker To Go krüpteerimisfunktsiooni on lihtne rakendada ja see on kasutajale hästi näha, tekib sageli väärkasutuse oht, mida kirjeldatakse ohukataloogis G 3.44 Teabe hooletu kasutamine. Kasutajaid tuleb piisavalt koolitada, et nad oskaksid taastamisparoole ja -võtmeid turvaliselt deponeerida ning teaksid, kuidas paroolide, võtmete ja krüpteeritud andmekandjate kaotamisel õigesti toimida ja kelle poole pöörduda. Kasutajad, kes rakendavad BitLocker To Go krüpteerimisfunktsiooni ilma tsentraalse võtmehalduseta, on sageli kas juhttöötajad või usaldusisikud, kes haldavad salajast teavet. Nendele töötajatele tuleks regulaarselt vestluste käigus meelde tuletada võimalikke ohte. Siia alla kuulub ka nende koolitamine, et nad teaksid, kuidas andmekandjaid ja võtmeid nõuetekohaselt koostada ja hoida ning kuidas toimida nende kaotuse ja kasutusest kõrvaldamise korral.

BitLocker To Go kasutusvaldkonna piirid

BitLocker To Go krüpteerimisfunktsioonid kaitsevad kaasaskantavatesse ja virtuaalsüsteemidesse salvestatud andmeid üksnes nende kaotsimineku ja varguse korral. Need kaitsefunktsioonid ei toimi, kui andmekandja on süsteemiga ühendatud ja kasutaja on end edukalt süsteemis autentinud. BitLocker To Go ei kaitse andmeid volitamata kopeerimise eest ega IT-süsteemi andmekandjasse salvestatud kahjurvara eest. Selliste kaasaskantavate andmekandjate puhul, mille kaitsemehhanismid on integreeritud otse riistvaraga, on krüpteerimis- ja autentimis-

protseduuride väärkasutuse risk seoses operatsioonisüsteemi manipuleerimisega tavapärasest väiksem. Neid on soovitatav kasutada eriti suurte konfidentsiaalsusnõuetega kasutusvaldkondades.

BitLockeri tööriistad

- Recovery Password Viewer võimaldab hallata Active Directory taastamisparoole (vt Knowledge Base, artikkel 958830).
- Käsuviibatööriist repair-bde.exe on mõeldud andmete varundamiseks kahjustatud köidetest (volumes), mis on krüpteeritud BitLockeriga.
- Tööriist Bitlockertogo.exe kopeeritakse olenevalt konfiguratsioonist automaatselt BitLocker To Go'ga krüpteeritud andmekandjasse. See tööriist võimaldab krüpteeritud andmekandjale Windowsi keskkonnas lugemisõigusega juurde pääseda, eeldusel et andmekandja kasutab FATfailisüsteemi.

Kontrollküsimused:

- Kas Windows 7 kasutajad rakendavad enda töös sobivat krüpteerimisparooli või -sertifikaati?
- Kas on tagatud, et Windows BitLocker To Go taastamisparoolile või -võtmele pääsevad juurde üksnes volitatud isikud?
- Kas BitLocker To Go kasutamine on reguleeritud Windowsi kasutust sätestavas turvapoliitikas?
- Kas need kasutajad, kes krüpteerivad enda vahetatavaid andmekandjaid, kuid ei osale tsentraalses võtmehalduses, osalevad regulaarselt BitLocker To Go koolitustel?
- Kas BitLockeri ja BitLocker To Go kasutamine on krüptokontseptsioonis kajastatud?
- Kas olukorras, kus andmekandja läheb kaduma või kõrvaldatakse kasutuselt, hävitatakse Windows BitLocker To Go võtmematerjal?

M 4.423 Kodugrupi funktsiooni kasutamine Windows 7-s

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator, kasutaja

Windows 7-s võeti kasutusele uus funktsioon kodugrupp (Homegroup). See võimaldab kohtvõrgus hõlpsasti juurde pääseda teiste IT-süsteemide failidele ja printeritele. Juurdepääs andmetele on korraldatud gruppide põhjal ning selleks kasutatakse Windows 7 teegifunktsiooni (eri kaustades paiknevad sama tüüpi failid, nt muusikafailid, dokumendid, pildi- või videofailid, koondatakse kokku). Kui kodugrupp on sisse seatud, saab sellele juurde pääseda kõikide Windows 7 versioonidega. Seevastu uue kodugrupi koostamise võimalust pakutakse alates versioonist Home Premium.

Kodugrupi sisseseadmisel genereeritakse parool, mis tuleb sisestada kõikidesse IT-süsteemidesse, mida soovitakse kodugrupiga liita. Seejärel saab hakata kasutama ühiskasutusse antud ressursse. Kodugrupi parooli on võimalik tagantjärele muuta. Parooli muutmise ajal peavad kõik kodugruppi kuuluvad IT-süsteemid olema sisse lülitatud. Parooli muutmisel tuleb uus parool samuti sisestada kõikidesse kodugruppi kuuluvatesse IT-süsteemidesse. Alternatiivina saab rakendada ka IT-süsteemi kasutajakontodel põhinevat autentimist. Kodugrupp on loodud IPv6 baasil ja kasutab Microsoft Peer Name Resolution Protocoli (PNRP) ning operatsioonisüsteemil põhinevaid ühiskasutusse lubamise ja kasutajate haldamise funktsioone. Igal kodugruppi kuuluval IT-süsteemil on juurdepääs kõikides teistes IT-süsteemides ühiskasutusse antud ressurssidele ning ta saab ka ise andmeid ühiskasutusse anda.

Kodugrupi funktsioon töötab siis, kui võrgutüübi seadistuses on valitud koduvõrk. Kodugruppi kuuluvates IT-süsteemides võetakse standardselt kasutusele uus kasutajagrupp kodukasutajad (HomeUsers), mis sisaldab kõiki arvuti lokaalseid kasutajaid, ja seadistatakse tööle kasutajad, mida nimetatakse kodugrupikasutajateks (HomeGroupUser$).

Domeeniga ühendatud IT-süsteemid

Kui IT-süsteem (nt sülearvuti) on ühendatud domeeniga, siis sellise IT-süsteemiga kodugruppi tööle seadistada ei saa. Seda tüüpi IT-süsteemid võivad küll liituda juba olemasoleva kodugrupiga, kuid juurdepääs koduvõrgus ühiskasutusse antud andmetele on nende IT-süsteemide jaoks tõkestatud. Nii tagatakse, et kodugrupi liikmeks saamine ei võimalda kõrvalistel isikutel konfidentsiaalseid andmeid volitamata lugeda ega muuta. Juhtudel, kus tööandjale kuuluvate IT-süsteemide kasutamine kodukeskkonnas on ära keelatud, tuleks kodugrupi funktsioonide kasutamine IT-süsteemis grupipoliitikaga blokeerida.

Kodugrupi kasutamine institutsioonides

Enne kodugrupi funktsioonide kasutuselevõttu institutsioonis tuleks analüüsida, kas need funktsioonid on institutsiooni tööülesannete täitmiseks ilmtingimata vajalikud ning kas nende kasutamine kaalub üles võimalikud riskid. Juurdepääsu andmetele saab vajaduse korral tagada ka teistsuguste tehniliste lahendustega

(nt failiserveri ja kataloogiteenusega). Funktsioonide kasutuselevõtu või nendest loobumise otsus tuleks sõnastada eraldi poliitikana. Siinkohal on oluline kindlaks määrata, kas failide ja printerite lubamiseks ühiskasutusse tohib kasutada Peerto-Peer-funktsioone (vt M 5.152 Info ja ressursside vahetamine võrdõigusteenuste (p2p) kaudu). Grupipoliitikaobjektide redaktorprogrammis saab kodugrupiga liitumist seadistada asukohas „Computer configuration | Administrative templates | Windows components | HomeGroup". Kodugrupi liikmeks saamist tõkestavas grupipoliitikas „Prevent the computer from joining a homegroup" saab kasutada kolme seadistust: konfigureerimata, desaktiveeritud ja aktiveeritud. Kahe esimese seadistusvaliku korral on kodugrupiga liitumine võimalik.

Kui kodugrupi kasutamist soovitakse poliitikaga lubada, tuleb see hoolikalt läbi mõelda ja tagada, et kasutus oleks piisavalt turvaline. Kaasaskantavate IT-süsteemide puhul tuleb arvestada ka meetmega B 3.203 Sülearvuti ja M 2.442 Windows 7 kasutamine kaasaskantavates arvutites . Kuna juurdepääs ühiskasutusse antud ressurssidele võimaldab sisse imbuda ka kahjurvaral, tuleb terves institutsioonis ja eriti kodugrupiga liidetud arvutite puhul võtta moodulis B 1.6 Viirusetõrje kontseptsioon nimetatud meetmeid.

Samuti tuleb koolitada kasutajaid, et nad teaksid, kuidas kodugrupi funktsioone õigesti rakendada, ega tõstaks näiteks konfidentsiaalseid andmeid enda sülearvutis kodugrupi jaoks ühiskasutusse antud ressursside kausta. Kui kodugrupi kasutamist soovitakse lõpetada, tuleb kodugrupist lahkuda. Selleks on vaja avada juhtpaneel, sisestada otsingureale „Kodugrupp" ja klõpsata seejärel vastaval lingil.

Kodugrupi dialoogiaknas tuleb valida „Kodugrupist lahkumine" (Leave the homegroup) ning järgmises aknas klõpsata valikul „Lõpeta" (Finish). Seejärel muudab Windows volitused taas endiseks, st taastab enne kodugrupiga liitumist kehtinud seisundi ning kustutab ära nii HomeGroupUser$-kasutaja kui ka HomeUserskasutajagrupi.

Kodugrupi funktsioonide rakendamise koolitused kasutajatele

Kui institutsioon otsustab kodugrupi funktsioonide kasuks, tuleb kasutajaid ilmtingimata teavitada nende funktsioonidega kaasnevatest ohtudest ja õpetada neile, kuidas kodugruppi turvaliselt kasutada (vt M 3.28 Windowsi klientoperatsioonisüsteemide turvamehhanismide koolitus kasutajatele).

Kontrollküsimused:

- Kas Windows 7 kodugrupi funktsioonide kasutamise jaoks on koostatud poliitika?
- Kas kodugrupi liikmeks saamist tõkestav grupipoliitika „Prevent the computer from joining a homegroup" on konfigureeritud kooskõlas poliitikaga?
- Kas kasutajatele on õpetatud, kuidas Windows 7 kodugrupi sees ressursse turvaliselt ühiskasutusse anda?

M 4.424z Vanemate tarkvarade turvaline kasutamine alates Windows 7-st

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator, IT-juht

Kogu tarkvara, mis eales Windowsi süsteemidele on kirjutatud, ei ühildu Windows 7-ga.

Vanema tarkvara kasutamiseks on olemas kolm tööriista:

- ühilduvusreziim (Compatibility Mode) üksikute käitusfailide jaoks;
- Application Compatibility Toolkit (ACT);
- Windows XP Mode.

Kui Windows 7 keskkonnas soovitakse kasutada sellega mitteühilduvat tarkvara, on väga oluline, et tarkvara töölesaamise nimel ei tehtaks liigseid järeleandmisi terve süsteemi turvalisuse arvelt. Seepärast ei tule vanema tarkvara töölesaamiseks kohandada mitte kõiki, vaid üksnes selliseid seadistusi, mida läheb ka reaalselt tarvis. Vajaminevate seadistuste väljaselgitamiseks ja dokumenteerimiseks tuleb kasutada muudest süsteemidest isoleeritud testkeskkonda. Testkeskkond peab koosnema vähemalt ühest Windows 7-ga ja ühest Windows XP-ga töötavast arvutist. Testimisega tegelev töötaja peab olema piisavalt koolitatud ning oskama Windows 7 kliente kohandada ja tööle seada. Enne testimist tuleb kontrollida, kas tarkvara tootja pakub ka asjakohast tugiteenust. Kui tugiteenust (Windows 7 Support) ei osutata, isegi kui see tarkvara Windows 7 Compatibility Mode'i režiimis võib-olla töötaks, saab tarkvara siiski katsetada VirtualPC XP Mode'i töörežiimis (edaspidi: XP režiim). XP režiimi pakutakse alates versioonist Windows 7 Professional tasuta lisapaketina. See põhineb VirtualPC tarkvaral ning koosneb kliendist, virtuaalsest kõvakettakujutisest ja litsentseeritud Windows XP installatsioonist.

XP režiimi saab kasutada ka siis, kui tarkvara ei hakka Windows 7 keskkonnas tööle, olgugi et seda on allkirjeldatud viisil kohandatud. Kui võimalik, tuleks seda tarkvara siiski käitada kas otse Windows 7 keskkonnas või jätta see olemasoleva Windows XP keskkonna piiresse. Virtualiseerimistarkvara tekitab uusi ründevektoreid ning sellel puuduvad nii haldus-, turbe- kui ka seiretööriistad. Testkeskkonnas tuleb välja selgitada, kas tarkvara hakkab tööle ka sellises kasutajaseansis, millel puuduvad administraatorivolitused ja mille suhtes on tööle rakendatud kasutajakontode haldusfunktsioon (vt M 4.340 Windows kasutajakonto haldamise (UAC) kasutamine). Kui vanemat tüüpi riistvara soovitakse edasi kasutada, tuleb katsetada, kas selle draiverid töötavad. Testid peavad hõlmama tarkvara ja draiverite, installimisvõimaluste ja värskendusmehhanismide tööfunktsioonide kontrollimist.

Programmi ühilduvusassistent (PCA)

Kui Windows 7-ga töötavates arvutites soovitakse käivitada vanemat tarkvara, tuleb esimese asjana käivitada programmi ühilduvusassistent (Program Compatibility Assistant – PCA) asukohas „Control Panel | All Control Panel items| Troubleshooting | Programs". See assistent hangib süsteemiühilduvuse andmebaasist

(System Compatibility Database) vajaminevad ühilduvusparandused (compatibility fixes) ja rakendab programmifailidele individuaalseid ühilduvus-töörežiime. Administraator saab tundmatuid programmifaile PSA-ga analüüsida ning seejärel failide jaoks välja valida mõne esitatud eeldefineeritud ühilduvus-töörežiimi. Uue teabe ja paranduste (fixes) hankimiseks kasutab süsteemiühilduvuse andmebaas Windows Update'i funktsiooni. Teabe ja ühilduvusparanduste värskendamine võib olla otseselt seotud turbe tagamisega ning seetõttu tuleks assistendi testimisel alati seda ka värskendada.

Selleks, et PCA saaks programme analüüsida ja parandusi paigaldada, peab PCA funktsioonide kasutamine olema süsteemis lubatud. Standardina ongi need lubatud ning kui neid on tarvis veel seadistada, saab seda teha grupipoliitikate snap-in 'i administratiivsete mallidega: „Computer Configuration | Windows Components | Application Compatibility". Analüüsi tarbeks läheb tarvis järgmist seadistust: „Computer Configuration | System | Troubleshooting and Diagnostics | Configure Scenario Execution Level | Detection, Troubleshooting".

Application Compatibility Toolkit (ACT)

Kui PCA-st ei piisa, tuleb tarkvara installida Windows XP katsetamisarvutisse koos Application Compatibility Toolkitiga (ACT). Kehtiva Windowsi litsentsi korral on ACT saadaval tasuta lisapaketina ning see sisaldab erinevaid viisardeid ja tööriistu. Viisarditega saab administraator süsteemi analüüsida ajal, mil tarkvara on juba käivitatud. Viisardite kõrval tuleks kasutada ka tarkvaratööriista Standard User Analyser. See on eraldi graafilise kasutajaliidesega interaktiivne analüüsilahendus.

Läbi katsetatud tarkvara analüüsitulemustest saab välja lugeda, millised süsteemipöördused põhjustaksid Windows 7-ga töötavas arvutis vigu.

Vigade kõrvaldamiseks on kaks meetodit:

- vajalikud kohandamised saab analüüsitulemuste põhjal teha kas Windows 7-ga töötavas katsetamisarvutis;
- Windows 7-ga töötava katsetamisarvuti System Compatibility Database'i andmebaas eraldatakse ACT seest, kasutades käsuviiba käsku sdbinst ja tööriista Compatibility Administrator.

Palju vigu on võimalik kõrvaldada esimesena mainitud meetodiga. Näiteks saab sellega kindlaks määrata volitusi, muuta installimise andmeteid ja töökatalooge, koostada UAC manifeste, kohandada süsteemiprivileege ja -volitusi ning rakendada täiendavaid, tavapärasest suuremate volitustega kasutajakontosid. Registriandmebaasi süsteemikaustade ja -võtmete volitusi ei tohi mitte mingil juhul muuta.

Programmikaustade volitusi tohib muuta üksnes väga sihipäraselt ja läbimõeldult, lisaks tuleb katsetada, kas muudatused ei pärsi Windows 7 keskkonnas Windowsi ressursikaitse (Windows Resource Protection – WRP) ega ka turvatsoonide tööd.

Samuti tuleb arvestada, et muuta ei tohi selliste kaustade ja registrivõtmete volitusi, mis on seotud UAC abil tehtud virtualiseerimisega (vt M 4.338 Windows 7 failide ja registri virtualiseerimise kasutamine) või mis suunatakse ümber WoW64 tüüpi emulatsioonirežiimiga (puudutab üksnes Windowsi 64-bitiseid versioone). Teise meetodi kasutamiseks läheb tarvis ühilduvusadministraatorit Compatibility Administrator. See tööriist sisaldab mitmeid ühilduvusparandusi (fixes). Täpsed tööjuhised tuleks hankida tootja dokumentatsioonist. Kõige värskemad ühilduvusparandused teeb kättesaadavaks Microsoft, kuid neid saab vajaduse korral ka individuaalselt programmeerida. Olukorras, kus teatud kohandamised lähevad vastuollu Windows 7 turvapoliitikaga, tuleks katsetada tarkvaratööriista Compatibility Administrator või töörežiimi VirtualPC XP Mode. Kahtluse korral tuleks koostada ja dokumenteerida erandjuhtude reeglid või kaaluda teisi võimalusi, kuidas mitteühilduvat tarkvara isoleerida.

Kõik ühilduvuse tagamiseks tehtud kohandamised tuleb iga tarkvara jaoks dokumenteerida.

Näitlik tabel:

Analüüsitud viga	Raskus-aste	Kohan-damine	Ühilduvust tagav parandus
Keeldub käivitumast Windowsi vale versiooni tõttu	Suur		PCA Compatibility Mode
.ini-faili ei õnnestu kirjutada	Suur	UAC-ga tehtud virtualiseerimise kohandamine PCA-ga	
Faktura program-mimoodul ei käivitu	Ei lähe tarvis		

VirtualPC XP Mode

Olukordades, kus PCA ja ACT kasutamisest ei piisa, saab Windows 7-ga töötavasse testsarvutisse installida XP režiimi. Seejärel tuleb mitteühilduv tarkvara installida virtuaalsesse Windows XP süsteemi. Windows 7 stardimenüüsse ilmub asukohas „Microsoft VirtualPC I Windows XP Mode Applications” automaatselt

nähtavale käivitussümbol, kui rakendused installiti kõikide kasutajate jaoks XP režiimis.

Tarkvara käivitamisel suunab XP režiim programmi edasi taustal töötavasse virtuaalsesse Windows XP keskkonda ning hakkab programmiakent kuvama Windows 7 graafilises kasutajaliideses. Selle asemel saab kasutaja endale kuvada ka täielikku Windows XP programmiakent, milleks tuleb valida Windows XP Mode.

Kord juba laaditud virtuaalne Windows XP keskkond jääb tööle seni, kuni Windows 7 välja lülitatakse (shut down). Virtuaalsüsteemiga ühenduse loomiseks kasutatakse Remote Desktopi teenust, mis ühendab ka vahemälu, heliväljundi, printeri draiveri, smartcard 'id jms. Võrguside ning juurdepääs andmekandjatele ja ühendustele leiab aset taustal ning selleks kasutatakse VirtualPC tarkvara.

Seadmeid, millel puudub USB- ja jadaühendus, kasutada ei saa. Testkeskkonnas tuleb välja selgitada, kas tarkvara ja selle draiverid töötavad võrguside, tarkvaratoe, andmejuurdepääsu ja Remote Desktopi funktsioonide valdkonnas korralikult. Samuti tuleb kontrollida värskendusmehhanismide toimimist.

Seejärel tuleb katsetuste käigus analüüsida tarkvara käivitamisele kuluvat aega ja tarkvara töökiirust ning muude Windowsi rakenduste kasutusvõimalusi. Eriti hoolikalt tuleb välja valida XP režiimi väljalülitamise mehhanism ja katsetada, kas see töötab õigesti. Kui XP režiimi väljalülitamisel esineb vigu, võivad need kahjustada nii tarkvarainstallatsiooni kui ka poolelioleva seansi andmeid.

Juhul kui Windows 7 kliendis kasutatakse mõnda andmevarunduse lahendust, tuleb selle tööd VirtualPC-ga katsetada ning tagada, et selle lahenduse varukoopiad sisaldaksid ka virtuaalses instantsis tekkinud muudatusi. Pärast seda, kui XP režiim on arvutisse installitud, saab virtuaalkeskkonna seadistusvalikud avada stardimenüü alajaotises „Microsoft VirtualPC | Windows Virtual PC sümbol | XP režiimi kontekstimenüü „Settings"".

XP režiimi piirangud

VirtualPC kasutamisel tuleb rakendada moodulit B 3.304 Virtualiseerimine . Nende moodulite kõrval kehtib jätkuvalt ka Windows 7 meetmete võtmise nõue, nt kohustus rakendada keerukaid paroole, turvata võrgukeskkonna andmesidet ja kasutada BitLockerit. XP režiimi töö tuleb võimalikult hästi Windows 7-ga töötava süsteemi tööst isoleerida.

Selleks tuleb arvestada järgmiste põhimõtetega:

- XP reziimi ei tohi tootmissüsteemides kasutada alternatiivse Desktopsüsteemina. Kasutajad tohivad enda töös rakendada vaid sellist vanemat tark-

vara, st üksnes selliseid XP süsteemi tarkvarakomponente, mille kasutus on konkreetselt ette nähtud; mis ei tohi hoida kasutajaandmeid;
- andmete isoleerimine: virtuaalses Windows XP süsteemis ei tohi hoida kasutajaandmeid;
- võrgu isoleerimine: virtuaalse Windows XP süsteemi jaoks ei tohi lubada piiramatut võrgusidet.

Esimese punkti jaoks tuleks kehtestada seni kasutusse lubamata virtualiseeritud tarkvara kasutamise keeld ning vajaduse korral kaaluda ka meetme M 2.32z Piiratud kasutajakeskkonna loomine võtmist Windows XP süsteemi jaoks. Kasutajaandmete salvestamiseks tuleks kasutada host-arvutis VirtualPC-ga ühendatud ajameid. Seevastu virtualiseeritud operatsioonisüsteemi ajamite kasutamisest tuleb loobuda.

Juhul, kui tarkvara toodab kasutuse käigus ka kaitset vajavaid seansiandmeid ja logifaile, tuleb need iga päev virtualiseeritud Windows XP süsteemist mujale ümber salvestada. Selleks saab kasutada näiteks Windows XP süsteemi vastavat shutdown -skripti või mõnda VirtualPC-ga ühilduvat andmevarundustarkvara.

Kuna võrk peab olema isoleeritud, tuleb tagada, et otsejuurdepääs arvuti võrguadapterile oleks tõkestatud („Windows XP Mode | Settings | Network"). Lubada tohib üksnes järgmisi juurdepääsuliike: ühendamata, sisemine võrk ja ühiselt kasutatav võrk (NAT). Lisaks tuleks Windows Firewallis koostada %SystemRoot%\System32\vpc.exe programmifaili jaoks nii sisendi- kui ka väljundireegel, mis blokeeriks võrgu andmeside. Reeglite puhul tuleb konfigureerida ka erandid, mis tagavad, et nende virtuaalse XP süsteemi rakenduste jaoks, millel on andmesidet siiski tarvis, oleks andmeside spetsiaalselt tööle lülitatud.

Valmis ühilduvusseadistused tootmissüsteemide klientides

Katsetulemused tuleb dokumenteerida ja integreerida vanema tarkvara kasutuselevõttu ettevalmistava kontseptsiooniga (vt M 2.324 Windows 7 kasutuselevõtu planeerimine).

Tootja dokumentatsiooni kasutamine

PCA ja ACT tootjadokumentatsioon on kättesaadav nii Microsoft Techneti levituskanali kaudu kui ka internetis. Katsetulemusi kajastav dokumentatsioon peab sisaldama ka tootja dokumentatsiooni asjakohaseid osi.

Kontrollküsimused:

- Kas Windows 7 keskkonnas kasutatavate rakenduste puhul on selge, millised on nende garantii- ja kasutajatoe tingimused?
- Kas Windows 7 keskkonnas töötamiseks vajalikud tarkvarakohandamised on täies mahus dokumenteeritud?
- Kas XP reziim on Windows 7 süsteemist piisavalt isoleeritud?
- Kas Windows 7 keskkonnas XP reziimiga käitatavate rakenduste andmevarundused salvestatakse väljapoole virtuaalset XP süsteemi?

M 4.425 Vaulti ja Cardspace'i funktsiooni kasutamine Windows 7-s

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: kasutaja, administraator

Windows 7 sisaldab erinevaid peamiselt erakasutajale suunatud võrgufunktsioone, mis on standardseadistuse korral sisse lülitatud. Näiteks saab Windows 7-ga hallata erinevate ressursside, nt väliste arvutisüsteemide ja veebilehtede pääsuandmeid (Credential Manager) ning veebilehtedes ja online -teenustes registreerimiseks ja autentimiseks kasutatavaid isiklikke andmeid (Windows Cardspace). Selleks, et nimetatud funktsioonide kasutamine ei kujuneks institutsiooni turbele ohtlikuks, tuleb esmalt analüüsida, kas nende rakendamisest saadav kasu kaalub üles võimaliku turvariski. Kui leitakse, et neid funktsioone on siiski tarvis, tuleb nende rakendamine kindlasti enne kasutuselevõttu hoolikalt planeerida.

Credential Manager (Vault)

Alates versioonist Windows 7 on Windowsi operatsioonisüsteemis kasutusele võetud tsentraalselt toimiv lahendus, kuhu saab salvestada erinevate võrguressursside, nt teiste Windowsi süsteemide, online -teenuste ja veebilehtede kasutamiseks vajalikud pääsuandmed. Salvestatud pääsuandmete puhul tehakse Windowsi sisselogimisandmete põhjal vahet, kas need on sertifikaadipõhised või geneerilised sisselogimisandmed. Logimisandmete tsentraalne salvestamine kätkeb endas muu hulgas riski, et volitamata kolmandad isikud võivad hankida andmetele juurdepääsu, nt kui ekraanilukk on jäänud sisse lülitamata. Seifi sisu andmevarundusfunktsiooniga „Back up vault" saavad volitamata isikud kõik sisselogimisandmed varukoopiana näiteks mõnele välisele andmekandjale salvestada, sest kui kasutaja on ennast juba autentinud, siis süsteem kordusautentimist ei nõua ja andmevarundusfunktsioon käsib kasutajal sisestada vabalt valitava parooli. Seejärel saab kurikael pääsuandmed funktsiooniga „Restore vault" mõnda teise süsteemi enda seifi sisse kirjutada. Seetõttu tuleb hoolikalt mõelda, kas funktsioonidest saadav kasu ja aja kokkuhoid, mis tuleneb sellest, et iga kord ei pea enam pääsuandmeid uuesti sisestama, kaaluvad üles eelkirjeldatud ohud. Institutsioon peaks koostama asjakohase poliitika, milles on kirjas, kas pääsuandmete salvestamine nn seifidesse on lubatud või keelatud. Keeldu saab tehniliselt realiseerida asjakohase grupipoliitikaga. Selleks tuleb Credential Manageri teenus grupipoliitikaobjektide redaktorprogrammis „Computer Configuration | Policies | Windows Settings | Security Settigs | System Services" desaktiveerida. Kui see teenus jääb käivitamata, siis pääsuandmeid tsentraalselt seifi (Vault) salvestada enam ei saa.

Windows Cardspace (ainult Windows 7)

Seifi saab salvestada üksnes teenustesse sisselogimiseks vajalikud andmed (kasutajanime, parooli või sertifikaadi). Seevastu Windows Cardspace pakub nn kaartidega võimalust salvestada tsentraalselt ka veebilehtedes ja online -teenustes registreerimiseks vajalikke andmeid. Kui andmeid soovitakse Windows Cardspace'i salvestada, tuleb selle kasutamiseks välja töötada asjakohane poliitika. Kasutada on võimalik kahte liiki kaarte: isiklikke ja hallatavaid kaarte. Isiklikke kaarte saavad kasutajad ise luua ning neid isiklike andmetega, nt eesnime, perenime ja meiliaadressiga, täiendada. Seevastu hallatavaid kaarte saab luua üksnes institutsioon ja need sisaldavad valideeritud andmeid, nt isikuandmeid ja kontonumbrit. Kasutaja peab valideeritud kaardi installima. Kaardil sisalduvad andmed salvestatakse lokaalselt institutsiooni IT-süsteemi ning vajaduse korral edastatakse need süsteemist teenusepakkujale, nt kui töötaja asub kasutama online- raa-

matupoe teenuseid. Funktsiooni toimimiseks peab teenusepakkuja juures olema mõni Cardspace'i andmete töötlemist võimaldav mehhanism, nt .NET-Framework. Igat kaarti saab kasutada erinevates online -teenustes ja erinevatel veebilehtedel. Igasse kaarti salvestatakse selle kasutamise ajalugu ja kaardi kehtivusaeg.

Kaardid salvestatakse kasutaja IT-süsteemi krüpteeritult. Andmeid on võimalik krüpteeritult ka välistele andmekandjatele salvestada. Sellega on ühelt poolt tagatud kaartidest varukoopiate tegemise võimalus ning teisalt saab krüpteeritud kaarte teistes Windowsi süsteemides dekrüpteerida ja kasutada. Volitamata juurdepääsude tõkestamiseks peaks institutsioon või õigemini kasutaja valima kaardi jaoks PIN-koodi ja kaardi varundamise parooli. Kui need andmed lähevad kaotsi, ei saa kaarte enam edasi kasutada ning nende asemele tuleb kas ise koostada uued kaardid või tellida need kaarte väljastava institutsiooni käest. Ka siin tuleb tähelepanu pöörata sellele, et volitamata isikute juurdepääs kaartidele ja kaartide väärkasutus oleks tõkestatud. Näiteks võidakse kaartide PIN-koode üritada välja nuhkida kas Keyloggeri või Social Engineeringu tüüpi rünnetega. Seetõttu tuleb Windows Cardspace'i salvestusfunktsiooni kasutuselevõttu hoolega kaaluda. Asutustes, kus Windows Cardspace'i salvestusfunktsioone ei lähe tarvis või kus selle kasutamine on Windows 7 poliitikaga ära keelatud, tuleks Windows Cardspace'i teenus desaktiveerida. Windows Cardspace'i saab desaktiveerida grupipoliitika-objektide redaktorprogrammis asukohas „Computer Configuration | Policies | Windows Settings | Security Settings | System Services".

Windows 7 funktsioonide rakendamise koolitused kasutajatele

Kui institutsioon otsustab kas või ühe siin meetmes mainitud salvestusfunktsiooni kasutusele võtta, tuleb kasutajaid ilmtingimata teavitada nende funktsioonidega kaasnevatest ohtudest ja õpetada, kuidas neid turvaliselt kasutada (vt M 3.28 Windowsi klientoperatsioonisüsteemide turvamehhanismide koolitus kasutajatele).

Kontrollküsimused:

- Kas Windows 7 jaoks on koostatud poliitika, mis käsitleb pääsuandmete salvestamist seifi (Vault)?
- Kas Windows 7 jaoks on nõuetekohaselt tööle konfigureeritud Credential Manageri teenuse kasutamist reguleeriv grupipoliitika?
- Kas Windows 7 keskkonnas rakendatava Windows Cardspace'i jaoks on koostatud asjakohane poliitika?
- Kas Windows 7 jaoks on nõuetekohaselt tööle konfigureeritud Windows Cardspace'i teenuse kasutamist reguleeriv grupipoliitika?

M 4.426 Lotus Notesi/Domino keskkonna arhiveerimine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

Lotus Notesi/Domino keskkonna teenused toetavad väga paljusid tööprotsesse. Nende tööprotsesside hulgas võib leiduda ka selliseid, mis kehtestavad erinõuded elektrooniliselt töödeldud, välja saadetud ja vastu võetud ning salvestatud andmete arhiveerimisele. Erinõuded tuleb integreerida meetmes M 2.207 Lotus Notesi/Domino turvakontseptsioon kirjeldatud arhiveerimiskontseptsiooniga. Arvestada tuleb nii seadustest tulenevate ettekirjutuste kui ka valdkonda reguleerivate ja kontrollivate ametiasutuste ettekirjutustega. Arhiveerimiskontseptsiooni nõuded peavad olema Lotus Notesi/Domino keskkonna käitamisel täidetud. Selleks tuleb rakendada moodulit B 1.12 Arhiveerimine . Lotus Notesi/Domino käitamisel tuleb arvestada järgmiste arhiveerimist puudutavate aspektidega:

- Arhiveerimisprotsessis tuleb järgida andmekaitsenõudeid. Isikuandmed tuleb nende säilitamise jaoks kindlaks määratud aja möödudes tehniliste lahendustega kustutada. Andmete liigist olenevalt võivad eelnevatele lisaks kehtida veel ka teised seadustest või sõlmitud lepingutest tulenevad nõuded.
- Arhiveerimisprotsesside töö planeerimisel tuleb arvestada signatuuride kehtivusajaga (kehtivus ette nähtud arhiveerimisaja jooksul). Arhiveerimisprotseduuris peab olema võimalik signatuure vajaduse korral ka uuendada.
- Arhiivide turbevajadus, mis puudutab andmete konfidentsiaalsust ja terviklust, võib tootmissüsteemides hoitavate andmete omast olla isegi suurem, sest arhiivis tekib kumulatsioon. Arhiivide turbemeetmed peavad nende nõuetega toime tulema.
- Lotus Notesi/Domino andmed arhiveeritakse tootjafirma andmevormingutes. Arhiivi kasutamine eeldab ka Lotus Notesi/Domino vanemate programmiversioonide säilitamist või arhiveerimisel kasutatud ODS-andmevormingute perioodilist migreerimist. Kõikidel juhtudel tuleb tagada, et litsentsid kehtiksid, seda ka siis, kui kasutatakse piiratud kehtivusajaga litsentse (vt M 2.493 Litsentsihaldus ja litsentsiaspektid Lotus Notesi/Domino soetamisel). Arhiveerimisnõuetes defineeritud ajavahemike vältel peab olema tagatud, et arhiivile on võimalik tehniliselt juurde pääseda ning juurdepääsu võimaldamine ei riku litsentsiõigust.

Olukorras, kus osa teiste elektrooniliste dokumentide ja andmete jaoks juba kasutatakse eraldi arhiveerimissüsteeme, võib olla mõistlik Lotus Notesi/Domino süsteem (või vastav Domino rakendus või teenused) juba otse arhiveerimissüsteemiga ühendada. Lotus Notesis/Dominos on arhiveerimise lihtsustamiseks olemas nii serveri- kui ka kliendipõhised arhiveerimisfunktsioonid ja meilide arhiveerimiseks loodud konfigureeritav administraatoripoliitika, st abivahendid, millest peaks enamasti täiesti piisama. Siinkohal tuleb siiski alati üksikasjalikult järele kontrollida, kas nende funktsioonidega saavutatavad arhiveerimislahendused vastavad täpselt seadustele ja muudele nõuetele (nt meilide arhiveerimise valdkond). DAOS-i kasutuselevõtul (Domino Attachment and Object Service, saadaval alates versioonist 8.5) tuleb senist arhiveerimiskontseptsiooni ja selle protseduure kontrollida ning vajaduse korral kohandada, sest DAOS-i puhul ei säilitata arhiveeritud andmeid enam mitmes eksemplaris.

Kontrollküsimused:

- Kas elektrooniliste andmete ja meilide arhiveerimisele kehtivad seadustest tulenevad nõuded on teada ning kas nendega on Lotus Notesi/Domino arhiveerimiskontseptsioonis piisavalt arvestatud?
- Kas rakendatavad arhiveerimisprotseduurid tagavad arhiveerimiskontseptsiooni nõuete piisava täitmise käitamise ajal?
- Kas juhul, kui kasutusele võeti DAOS (Domino Attachment and Object Service), töötati arhiveerimiskontseptsioon uuesti läbi ja kohandati seda?

M 4.427 Lotus Notesi/Domino turbe seisukohalt oluline logimine ja analüüs

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: andmekaitsespetsialist, infoturbespetsialist, töötajate esindus, administraator

Lotus Notesi/Domino platvormil töötavate rakenduste ja teenuste turbe tagamiseks on tarvis turbe seisukohalt olulisi sündmusi pidevalt logida ning logisid perioodiliselt ja sündmustepõhiselt analüüsida. Selleks saab Lotus Notesi/Domino keskkonnas kasutada haldus- ja turvahaldusfunktsioone. Turvet kajastavate logide platvormiülese automaatse analüüsimise parandamiseks saab kasutada SIEM-tarkvaratööriistu (Security Information Event Management) või Log Analyzerit. Samas eeldab nende kasutamine siiski ka platvormide logimisfunktsioonide asjakohast konfigureerimist.

Kuna logid võivad sisaldada ka kaitset vajavaid andmeid ja logide analüüsimisel võib töötajatel omakorda tekkida juurdepääs võõrastele isikuandmetele ning ilmneda teave kaastöötajate käitumisharjumuste ja nende töö tootlikkuse kohta, tuleb selliste protsesside puhul täpselt andmekaitseseadusi järgida. Seetõttu tuleb meetmes M 2.207 Lotus Notesi/Domino turvakontseptsioon kirjeldatud Lotus Notesi/Domino logimiskontseptsiooni ja logide analüüsimise kontseptsiooni koostamise ja rakendamise meetme väljatöötamisse kaasata ka andmekaitsespetsialist ja töötajate esindus.

Kui Lotus Notesi/Domino keskkonna teenuste (nt meiliteenuse, töötajatele mõeldud internetijuurdepääsu) kasutamine on konkreetselt lubatud või kui seda sallitakse, tuleb eriti hoolikalt välja töötada nii kasutamist reguleerivad piirangud kui ka institutsiooni ja töötajate vahelised lepingud, millega sätestatakse täpselt logimine ja logide analüüsimine.

Logiandmete hindamiseks võib kasutada nn SIEM-Tools'e (Security Information Event Management) või Log Analyzer'it. Ka need eeldavad siiski logimise sobivat konfigureerimist seotud platvormidel.

Kontrollküsimused

- Kas Lotus Notes / Domino keskkonna jaoks on olemas ja rakendatud protokollimis- ja hindamiskontseptsioon?
- Kas on olemas eeskirjad, et käsitleda eraviisilist kasutamist?

M 4.428 Lotus Notesi/Domino keskkonna audit

Algatamise eest vastutavad: administraator, infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: andmekaitsespetsialist, erialaspetsialist, audiitor, administraator, infoturbespetsialist

Selleks, et tuvastada, kas Lotus Notesi/Domino keskkonna turvalisuse tegelik seisund vastab nõuetele ja kas süsteemis võib esineda puudusi, tuleb Lotus Notesi/Domino keskkonna turvalisust auditite ja turvakontrollidega regulaarselt hinnata. Siinkohal eristatakse organisatsiooni sees ja väljaspool organisatsiooni algatatud auditeid ja turvakontrolle. Esimese variandi puhul algatatakse ja tehakse kontrolle tavaliselt infoturbe haldusprotsessi või revisjoni raames, seevastu teise variandi alla kuulub sageli väliste kontrolliorganite, nt järelevalveameti, audiitori või ka litsentseerija tegevus (vt M 2.493 Litsentsihaldus ja litsentsiaspektid Lotus Notesi/Domino soetamisel).

Väliste auditite eesmärk on tavaliselt kontrollida seaduste ja ettekirjutuste või lepingusätete järgimist. Kontrollide tõendamine võib olla ka elektroonilises andmevahetuses, makseprotsessides või kaubandussüsteemides osalemise, eritingimuste täitmise või IT-d puudutavate kindlustuslepete sõlmimise eeldus. Andmekaitse eriline roll õigustab sageli auditeid, mille põhieesmärk on kontrollida mõnda spetsiifilist andmekaitseaspekti. Need auditid võivad hõlmata ka Lotus Notesi/Domino keskkonna andmekaitseauditit, sest Lotus Notesi/Dominoga töödeldakse ja salvestatakse paljudel juhtudel ka isikuandmeid. Auditite planeerimisel tuleb võimaluse korral lähtuda kindlast protseduurist. Auditite õigusaspektid tuleb välja selgitada ja mõjusid hinnata enne auditiga alustamist. Teatud auditid võivad vajada kooskõlastamist andmekaitsespetsialistidega ja töötajate esindajaga. Audititesse (eriti organisatsioonivälistesse) peab alati kaasama infoturbeosakonna. Nimetatud osakonna kaasamise ulatus ja sisulised üksikasjad tuleb esmalt kindlaks määrata ja dokumenteerida (nt osalemine litsentsiauditites, sertifitseerimisauditites ja vastutavate kontrolliametite korraldatud kontrollide raames tehtavates auditites). Tuleb tagada, et auditite tulemusi kasutataks infoturbehalduse tööprotsessi optimeerimiseks. Auditi käigus tuvastatud puudujääkidest ja nendega seotud IT-riskidest tuleb vastutavaid isikuid (juhtkonda, IT-juhti, infoturbespetsialisti, erialaspetsialisti) teavitada kohe.

Auditid tuleb teha läbipaistvalt ja arusaadavalt. Auditeid ja turvakontrolle (nt penetratsiooniteste), mille tegemine võib ohustada IT-protsesse või organisatsiooni teabekogumit, tuleb põhjalikult kavandada. Enne töödega alustamist tuleb teha riskianalüüs ja tööde käigus arvestada õigusaspektidega. Lotus Notesi/Domino keskkonna auditite raames võidakse vaadelda terviksüsteemi, kuid kontrollida ka üksnes turbe jaoks eriti olulisi valdkondi. Tervikkäsitluse korral saab näiteks Notesi/Domino toetatud tööprotseduuridest olenevalt hinnata turbehaldust Lotus Notesi/Domino keskkonnas nii protsessi kui ka tehnilisel tasandil. Turbe seisukohalt eriti oluliste komponentide või teenuste konfiguratsioone ja protseduure (nt sertifikaatide haldamist või Lotus Notesi/Domino turbemehhanismide seadistamist) saab üksikasjalikumalt kontrollida sihtauditite.

Täiendavad kontrollküsimused:

- Kas Lotus Notesi/Domino keskkonna auditi jaoks on olemas dokumenteeritud töökava?
- Kas infoturbeosakonna kaasamiseks väljastpoolt institutsiooni algatatud audititesse on vastutusalad kindlaks määratud?

- Kas on täpselt määratud, kuidas peab infoturbeosakond väljastpoolt algatatud auditites osalema?

M 4.429 Lotus Notesi/Domino turvaline konfiguratsioon

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

Installitud, kohandatud või migreeritud komponentide konfiguratsiooni tuleb muuta kohe pärast nende installimist, kohandamist või migreerimist. Ainult nii saab tagada, et installimise ja konfigureerimise vahele jäävas ajavahemikus ei kasutata standardkonfiguratsiooni puudujääke ründe-eesmärgil ära.

Turvaline aluskonfiguratsioon

Lotus Domino serveri turvaline aluskonfiguratsioon peab sisaldama eelseadistatud ebaturvaliste süsteemiparameetrite korrektuuri:

- Anonüümne juurdepääs Domino serverile peab standardseadistuses olema tõkestatud. xACL-i mittekasutamisel (anonüümne juurdepääs keelatakse xACL-ide kasutuselevõtuga) tuleb Domino installimisel määrata grupile ANONYMOUS standardina väärtus NO ACCESS. Kui Lotus Notesi kasutajate pöörduste sertifikaadid on väljastanud tundmatu sertifitseerimisüksus ja nende jaoks pole olemas Cross-sertifikaati, käsitleb Domino neid pöördusi anonüümsetena. Olukorras, kus mõnele andmebaasile on tarvis siiski anonüümset juurdepääsu lubada, tuleb see funktsioon eraldi andmebaasi tasandil tööle lülitada. Kui anonüümne juurdepääs eraldiseisvatele serveritele on vajalik, tuleb sellega üldarhitektuuri planeerimisel arvestada ja võtta teistsuguseid turvameetmeid. Eriti oluline on, et need serverid ei pakuks suure turbeastmega teenuseid.
- HTTP-paroolide räsiväärtuste jaoks tuleb valida turvaline salt -väärtusega räsivorming (saadaval alates versioonist Notes 4.6). Selleks tuleb siseneda menüüsse „Actions” -> „Edit Directory Profile” ja valida kastikese „Use more secure Internet password format” seadistuseks „Yes”. Vaadake ka tootja tehnilist teavet (Technote 1244808).

Lisaks tuleb turvalise aluskonfigureerimise raames määrata kindlaks juurdepääsu turvaseadistused, mis töötavad Lotus Notesi/Domino serveri tasandil (ja mitte Domino teenuste tasandil):

- Sisselogimise jaoks tuleb standardina aktiveerida kasutaja Notes-ID avaliku võtme ning nime- ja aadressiraamatusse salvestatud avaliku võtme koopia võrdlemine.
- Juurdepääs serverile peab piirduma kasutajatega, kes on kirjas serveri nime- ja aadressiraamatus.
- Aktiveerida tuleb Notes-ID parooli serveripõhine kontrollimine räsiväärtuse põhjal. Sellega kaasneb risk, et ID koopia korral ja Notesi parooli kompromiteerimisel ründaja poolt võib pärast seda, kui ründaja parooli ära muudab, süsteem ainukeseks legitiimseks ID-ks pidada üksnes ründaja ID-d.

- Access/Deny nimekirjad tuleb kasutusele võtta nii serveri kui ka kasutajate jaoks ja neid nimekirju tuleb hooldada. Seeläbi saab soovimatutest ühendustest juba serveri poole pöördumisel keelduda (nt endiste töötajate ID-ga tehtud pöördused või juurdepääsukatsed pärast juurdepääsu lubatud kestuse ületamist).
- Vahendusserverite (Pass-Through) kasutamist tuleb vältida. Nende asemel tuleks kasutada Lotus Notesi/Domino platvormi turbearhitektuuri ja võrgu topoloogiat ning piirata Pass-Through-juurdepääs defineeritud kasutajagruppidele. Kõikide pöördusi esitavate serverite üldist marsruutimist (Routing through Server = *) tuleb kindlasti vältida.
- Mõningaid serverioperatsioone saab piirata kasutajate või kasutajagruppide nimekirjade alusel. Selliste operatsioonide näideteks on andmebaaside ja replikatsioonide loomine, seireprogrammide (monitors) kasutamine, haldamine veebiliidese kaudu ning agentide ja skriptide käivitamine. Juhtudel, kus konkreetsete nimekirjade kasutamisest loobutakse, tuleb võimalustest olenevalt rakendada erinevaid nõudeid. Näiteks on uute andmebaaside loomine kõikidele kasutajatele standardina lubatud.
- Õigused juurdepääsuks nime- ja aadressiraamatule (lühend: NAB, failinimi: names.nsf) peavad olema võimalikult piiravad ja seda isegi siis, kui see tähendab kasutajate jaoks kompromisse erinevate funktsioonide kasutamisel.
- Haldusalased pääsuõigused tuleb kindlaks määrata haldusrollidega [GroupCreator], [GroupModifier], [ServerCreator], [ServerModifier], [UserCreator], [UserModifier], [NetCreator] ja [NetModifier], nagu Lotus Notesi/Domino haldamise kontseptsioon seda ette näeb.

Andmeside serveriseadistuste turvaline konfigureerimine

Andmeside turvalisuse tagamiseks saab kasutada SSL-krüpteeringuga ühendust ja sidepartnerite sertifikaadipõhist autentimist. Domino serveri saab SSL-i kasutamiseks sobivaks seadistada serveri sertifitseerimise haldamise (certsrv.nsf) kasutuselevõtuga. See eeldab domeeni- ja sertifikaadihierarhia kontseptsiooni rakendamist meetme M 2.207 Lotus Notesi/Domino turvakontseptsioon kohaselt. Seejärel saab protokolle (nt meiliprotokolle IMAP, POP3, SMTP) individuaalselt konfigureerida, st määrata kindlaks, kas SSL-i kasutamine tuleb protokolli jaoks aktiveerida või mitte. Siinkohal tuleks lähtuda kasutatud teenuste turbevajadusest. Veebipöördustele saab kehtestada sunniviisilised SSL-ühendused ka andmebaasi tasandil (Web: Request SSL Connection). Võimaluse korral ei tohiks SSL-ühenduse konfiguratsioonis autentimismeetodina kasutada mitte valikut „Ainult serveriga autentimine”, vaid valikut „Kliendisertifikaadiga autentimine”, sest osa protokolle ei toeta kliendisertifikaadiga autentimist. Järgmised serveriparameetrid tuleb konfigureerida kooskõlas organisatsiooni krüpteerimispoliitikaga:

- SSL-i protokolli versioon (võimaluse korral ainult SSL 3.0, sest Dominos ei saa SSL 2.0 krüpteerimismeetodit seadistada);
- SSL-Site'i sertifikaatide vastuvõtmine (seadistus „NO”, et keelata juurdepääsu internetiserveritele, millel pole ühiseid sertifikaate);
- aegunud SSL-i sertifikaatide vastuvõtmine (tavaliselt valida „YES”, et vältida probleeme aegunud kliendisertifikaatidega, suure ja väga suure kaitsevajaduse korral siiski „NO”);
- SSL-i krüpteerimiskoodid (kooskõlas organisatsiooni krüpteerimiskontseptsiooniga, üldjuhul tuleb vältida valikuid „No encryption with MD5 MAC”,

„No encryption with SHA-1 MAC” ning 40-bitist RC4 ja 56-bitist DES-krüpteeringut).

Teenuste turvaline konfiguratsioon
Domino pakub muu hulgas järgmisi teenuseid:

- meiliteenused (Notes Mail, POP3-Mail, SMTP-Mail, IMAP-Mail);
- veebiteenused (Webserver, Instant Messaging ja Presence, News (NNTP), W3C standardiga SOAP 1.1 ühilduvad veebiteenused, WebDAV);
- andmebaasiteenused (sh andmebaasi replikeerimine ja DB2 ühendamine);
- DAOS (Domino Attachment and Object Service);
- Groupware'i teenused;
- Directory ja CA teenused (sertifikaadihierarhia teenused) koos LDAP liidesega.

Teenuste turvaline konfiguratsioon peab arvestama nii teenuste turbeparameetreid kajastavate levinud standardite kui ka turbearhitektuuri kontekstiga, mille raames teenuseid käitatakse. Näiteks võib organisatsioonis ainult sisekasutuseks mõeldud ja Domino serveris käitatav välisühendusteta meili- või kiirsõnumiteenus olla oluliselt erineva konfiguratsiooniga kui samasuguse meili- ja kiirsõnumside jaoks kasutatav teenus, mida käitatakse demilitariseeritud tsooni serveris koos internetiühendusega. Seepärast pole iga teenuse puhul vaja vaadelda turvalisust mitte ainult teenuse, vaid ka Domino serveri kaitsevajaduse seisukohalt (ja arvestada seega teiste teenustega, mis samas Domino serveris töötavad). Selleks tuleb rakendada meetmes M 2.207 Lotus Notesi/Domino turvakontseptsioon kirjeldatud soovitusi, esmajoones aga seal sisalduvat kontseptsiooni, mis käsitleb kasutatud Domino teenuste turvet. Iga teenuse jaoks tuleb koostada turbekontseptsioon ja teenusele juurdepääsu tagavate volituste kontseptsioon (juurdepääsukontseptsioon), samuti tuleb tagada teenusepõhiste parameetrite turvaline konfiguratsioon. Eriti tähtis on tarkvara eelseadistuste puudujääkide kõrvaldamine. See kontseptsioon tuleb iga Domino teenuse puhul ellu viia vahetult pärast teenuse installimist. Tarbetute teenuste installimisest tuleb võimaluse korral hoiduda, kasutades sobivat alusinstallatsiooni. Kui see pole võimalik, tuleb vastavad serveriülesanded (server tasks) desaktiveerida.

Klientide turvaline konfiguratsioon

Lotus Notesi/Domino platvormis saab kasutada erinevaid kliente. Seejuures tuleb kasutusotstarbest olenevalt eristada järgmisi variante:

- administraatorikliendid;
- arendajakliendid;
- lõppkasutajakliendid.

Tehnoloogilisest vaatepunktist tuleb eristada järgmisi:

- tootjapõhised Notesi kliendid;
- Eclipse'il põhinevad kliendid (alates Notes 8-st);
- brauserid klientidena;
- tootjapõhised kliendid pihuarvutites ja nutitelefonides;
- võõrad meilikliendid, mis pöörduvad IMAP ja POP3 kaudu Domino serverisse.

Kasutatavate klienditüüpide valik tuleb kindlaks määrata juba arhitektuuri planeerimisel. Seejuures tuleb arvestada, et kasutusotstarbest ja kliendi kaitsevajadusest olenevalt võib tarvis minna erinevaid konfiguratsioone. Haldamisklientide ja teiste suure kaitsevajadusega klientide puhul tuleb kasutada tavapärasest rangemaid turbeseadistusi. Klientide konfiguratsiooni ebaturvalisest algseadistusest tulenevad puudujäägid tuleb kõrvaldada. Lisaks tuleb arvestada turvalise ühenduse loomiseks vajalike parameetritega, replikeerimisparameetritega ning kliendis hoitavate andmete Notesi-põhiste krüpteerimisparameetritega. Siinkohal on olulised meetmes M 2.206 Lotus Notesi/Domino kasutuselevõtu planeerimine esitatud sideturvalisuse planeerimise nõuded ja meetmes M 2.207 Lotus Notesi/Domino turvakontseptsioon esitatud Domino teenuste turvakontseptsioon ja Notesi/Domino enda turvamehhanismide kasutamise kontseptsioon (sh kliendis hoitavate andmete krüpteerimiseks). Kui Full Clienti kasutatakse esimest korda, tuleb arvestada varasemast suurema keerukusega ja valmistada evitamise jaoks ette detailsed konfigureerimisjuhised (ideaaljuhul koos kasutajate koolitamise võimalusega).

Täiendavad kontrollküsimused:

- Kas kõikide kasutatavate teenuste jaoks on olemas ja ellu viidud konfigureerimisjuhised, mis järgivad teenuste turvakontseptsioone?
- Kas kõikide kasutatavate klientide jaoks on olemas konfigureerimisjuhised?
- Kas kliendid, mis sisaldavad (nt replikeerimise tagajärjel) eriti suure kaitsevajadusega infot (kaitsevajadus „väga suur"), on sobivalt krüpteeritud?

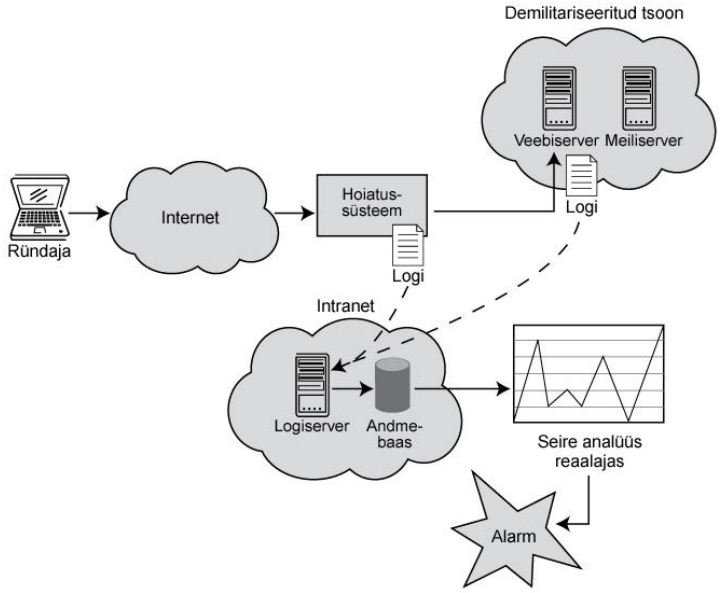
M 4.430 Logiandmete analüüs

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

Infokoosluses tekib tavaliselt suur hulk logiandmeid. Enne logisissekannete analüüsimist tuleb andmeid normeerida. Normeerimisega konverditakse logisid loovate süsteemide erinevad andmevormingud ühtseks vorminguks. Enne analüüsi tuleks sorteerida välja olulised andmed, et vähendada logiandmete hulka. Seda saab teha andmete filtreerimise, koondamise ja korreleerimisega (vt M 4.431 Logimise jaoks oluliste andmete valik ja töötlemine). Need meetmed on eriti vajalikud siis, kui kasutatakse tsentraalselt töötavat logimislahendust. Logiandmete analüüsi jaoks on kindlasti väga tähtis ka aja sünkroniseerimine. Selleks, et tuvastada korraga mitmes IT-süsteemis ja rakenduses esinevaid ründeid ja tõrkeid, peab kellaaeg igas süsteemis olema sama. Kõikide suures infokoosluses olevate süsteemide aegade sünkroniseerimiseks saab kasutada keskset ajaserverit (vt M 5.172 Turvaline aja sünkroniseerimine keskse logimise korral). Need pakuvad süsteemiaega näiteks Network Time'i protokolli (NTP) kaudu (vt M 4.227 Lokaalse NTP -serveri kasutamine aja sünkroniseerimiseks). Kõiki teisi infokoosluse süsteeme saab sünkroniseerida selle põhjal.

Teavitusfunktsiooni kasutamine nõuab logitud info kiiret analüüsimist. Analüüsi käigus vaadeldakse turvalisuse seisukohalt kriitilisi sündmusi ilma viivituseta. Lisaks võetakse juba olemasolevatest logifailidest asjakohast infot ja kasutatakse seda analüüsi jaoks. Analüüsis tuleb suurt tähelepanu pöörata kõrvalekalletele normkäitumisest, konfiguratsioonivigadele ja veateadetele, et saada ülevaadet kõikidest infokoosluse tähtsatest sündmustest. Olulise logisissekande õigeaegseks tuvastamiseks saab kasutada sobivaid algoritme ja analüüsimetoodikaid, nt signatuuride tuvastamist ja piirväärtuse analüüsi. Neid tehnoloogiaid kasutavad sageli IT-hoiatussüsteemid. Ründe tuvastamisele peaks viivitamatult järgnema hoiatus, et ohule saaks kiirelt reageerida.



Joonis. IT-hoiatussüsteemi üldine protseduur

Selleks, et tulemusi ja logisissekandeid saaks kasutada hiljem ka tõenditena, tuleks pärast analüüsi koostada aruanne. Paljudes logimisrakendustes on olemas ka veebiliidesed, millega saab analüüsi tulemuse kuvada graafikuna. See aitab paremini märgata võimalikke arengusuundumusi. Veebiliidesega saab defineerida ka sobivaid analüüsivaateid (views) ja filtreid. Kui logiandmeid analüüsitakse tsentraalselt, on infokoosluses võimalik näha ka tavapärasest keerukamaid seoseid või neid pärast käitus- või turvaintsidentide toimumist kooslusest otsida. Seega tuleks logiandmed hilisema analüüsi tarbeks arhiveerida. Enne logifailide arhiveerimist tuleb säilitusaja pikkust reguleerivate organisatsioonisiseste nõuete kõrval kontrollida ka seda, millised nõuded võivad logifailide säilitamisele kohalduda seaduste ja sõlmitud lepingute alusel. Sündmuste tagamaade väljaselgitamiseks võib andmetele olla kehtestatud minimaalne säilitusaeg, kuid andmekaitsenõuete tõttu võib kehtida ka kustutamiskohustus (vt M 2.110 Andmeprivaatsuse suunised logimisprotseduurides).

Täiendavad kontrollküsimused:

- Kas andmeid normeeritakse enne analüüsi?
- Kas infokooslus kasutab sünkroniseeritud aega?
- Kas pärast logiandmete analüüsi koostatakse aruanne?
- Kas logiandmed arhiveeritakse tulevaste analüüside jaoks?
- Kas logiandmete arhiveerimisel võetakse arvesse seadustest tulenevaid ettekirjutusi?

M 4.431 Logimise jaoks oluliste andmete valik ja töötlemine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

Logiandmed peavad sisaldama sisukat infot. Seejuures pole tähtis, kas need on kogutud lokaalselt, tsentraalselt või hoopis IT-hoiatussüsteemi jaoks. Valik, milliseid sündmusi logitakse, oleneb muu hulgas IT-süsteemide kaitsevajadusest ning see peab olema organisatsioonis kooskõlastatud ja kindlaks määratud.

Kõige muu kõrval tuleb kindlasti tähelepanu pöörata järgmistele sündmustele:

- kasutajatunnusega kokku sobimatu ehk vale parooli sisestamine;
- kasutajatunnuse blokeerimine;
- volitamata juurdepääsukatsed;
- riistvara töö katkemine ja tõrked;
- andmed võrgu koormuse ja ülekoormuse kohta;
- ründetuvastussüsteemide (Intrusion Detection System) teated ja hoiatused.

IT-hoiatussüsteem saab kõikidest nendest sündmustest teateid välja võtta, määrata neile tähtsusastme ja need ülevaatlikult esitada. Selleks rakendatakse logiandmete filtreerimist, normeerimist, kokkukoondamist ja kategoriseerimist.

Filtreerimine

Kogutud logiandmete filtreerimisel jäetakse kõrvale ebaolulised logiteated. See on vajalik, sest tekkivate logiandmete hulk on kogu info töötlemiseks liiga suur. Filtrit saab seadistada tavaliselt tsentraalses logiserveris või IT-hoiatussüsteemis. Seadistusi tuleb kohandada infokoosluse omaduste järgi ja seda tohivad teha ainult korraliku väljaõppega administraatorid. Väljasorteeritud logisündmusi ei tohi olla liiga palju, kuid ka mitte liiga vähe. Lisaks tuleb filtreid regulaarselt kontrollida ja uuendada, nt kui tsentraalsesse logimissüsteemi või IT-hoiatussüsteemi lisatakse uusi servereid või kui vanu servereid eemaldatakse käitusest.

Normeerimine

Andmete edasise töötlemise ja näiteks andmebaasi salvestamise jaoks tuleb kõik tekkivad logiteated konvertida ühtsesse andmevormingusse. Seda protseduuri nimetatakse normeerimiseks. Teadete vorming sõltub tootjast. Kuid ka operatsioonisüsteemide ja rakenduste logiandmete vahel esineb suuri erinevusi.

Kokkukoondamine

Edasise töötlemise jaoks koondatakse andmed kokku. Selles etapis liidetakse identse sisuga logiteated üheks andmepaketiks. Üks ja sama süsteem võib väga sageli üksteise järel genereerida mitmeid identseid logiteateid, mis tähendab, et nendele teadetele järgnevates teadetes muutub uue teabe hulk järjest väiksemaks. Seetõttu kaasatakse andmetöötlusse ainult esimene logifail. Siiski peab esimese teate kõrval kajastuma info hulgas ka see, kui palju tekkis selle järel liiasusega teateid, et teha kindlaks selliste identsete teadete tekkimise sagedus.

Kategooriate ja prioriteetide kindlaksmääramine

Kui andmed on filtreeritud, normeeritud ja kokku koondatud, tuleb nende jaoks kindlaks määrata kategooriad ja prioriteedid. Seeläbi saab suurendada teates kajastuva info sisukust. Prioriteedi kindlaksmääramisel võib teadete puhul lähtuda tsooniinfost (nt teateid, mis kannavad demilitariseeritud tsooni või üliturvalisuse tsooni tähistust, tuleks analüüsida eelisjärjekorras). Lisaks saab teateid liigitada süsteemi tüübi põhjal, nt turvalüüs, operatsioonisüsteem või rakendused.

Andmetevahelised seosed

Logiserverile ja IT-hoiatussüsteemile esitatav põhinõue on see, et süsteem peab suutma erinevatest allikatest saadud logiteateid kokku siduda, et selle põhjal tuleksid ilmsiks ka seosed erinevate sündmuste vahel. Infokoosluse eraldiasetsevad turvakomponendid, nt turvalüüsid, sissetungimise tuvastamise/ennetamise süsteemid ja viirusetõrjelüüsid, suudavad oma funktsioonide toimimist analüüsida üksnes piiratult. Seepärast on tarvis asjakohaseid logiandmeid omavahel seostada.

Seostatud logisissekannete näide on turvalüüsi ja marsruutri logiandmete sidumine kompromiteeritud süsteemi accounting -infoga.

Seoseid võidakse luua eri tasanditel:

- Seos sama seadmeklassi piires (nt turvalüüsid): võimaldab analüüsida, kas seadmeklassi piires on esinenud ebatavalist koormust või käitumist. Selle alusel koostatakse näiteks arenguraporteid.
- Seos sarnaste andmeväljadega seadmeklasside vahel (nt turvalüüsid ja marsruutrid): võimaldab põhjalikumalt analüüsida ründe toimepanekut.
- Seos erinevate seadmeklasside vahel: ainult see võimaldab täielikku ülevaade transpordi ja rakenduse tasandil. Näiteks edastab töökohaarvuti viirusetõrjeprogramm teate, et avastatud on ussviirus ja viirus on karantiini pandud.

Seejärel annab IDS kahjurvaraga nakatunud süsteemist teate, et ühes eraldi pordis on suurenenud võrguliiklus. Kui seoseid ei looda, on oht, et neid kaht teadet peetakse ebaoluliseks ja need võivad teiste logiteadete hulgas tähelepanuta jääda.

Kontrollküsimused:

- Kas kõik turvalisust puudutavad sündmused logitakse organisatsiooni nõuete kohaselt?
- Kas filtreid seadistavad ainult piisava koolituse läbinud administraatorid, kes arvestavad infokoosluse eripäradega?
- Kas filtrite seadistusi kontrollitakse ja uuendatakse regulaarselt?

M 4.432 Serveriteenuste turvaline konfiguratsioon

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

Pärast serveri operatsioonisüsteemi installimist (vt M 2.318 Serveri turvaline installeerimine) ja konfigureerimist tuleb tööle seadistada serveriteenus. Serveriteenused on käivitatud protsessid, mis pakuvad klientidele teatud funktsioone. Need võivad olla näiteks veebi-, meili- ja kataloogiteenused.

Serveriteenuseid saab jaotada kahte kategooriasse. Esimese kategooria serveriteenused pakuvad võrgus oma funktsioone piiramatult, st kasutaja ei pea end autentima. Selle näiteks on DNS-, DHCP- ja NTP-serverid. Teine kategooria nõuab aga kasutajalt enne teenuse kasutamist enda autentimist, nt selleks, et kaitsta konfidentsiaalset infot volitamata juurdepääsu eest. Selle näiteks on faili-, meili-, SSH- ja RDPserverid.

See, kas serveriteenuse kasutamine nõuab autentimist ja milline peab see autentimine olema, sõltub teenuse liigist ja konfiguratsioonist ning andmete kaitsevajadusest. Üldiselt tuleks kõik olemasolevad, kuid ebavajalikud serveriteenused desinstallida. Server peaks pakkuma ainult hädavajalikke teenuseid.

Põhilise serveriteenuse kõrval läheb tavaliselt vaja veel üht serveriteenust IT-süsteemi haldamiseks (vt M 4.97z Ainult üks teenus serveri kohta). Enne uue serveriteenuse installimist näiteks paketihaldusest või mõnest muust allikast, tuleks selle dokumentatsiooni lugeda, juhul kui seda pole veel tehtud. Seejuures tuleb kindlaks teha, millised failid on teenuse käitamiseks vajalikud ja millised protsessid käivitatakse. Alles seejärel tuleb alustada põhilise serveriteenuse konfigureerimisega.

Õiguste piirav andmine

Selleks, et server suudaks klientidele pakkuda infot või funktsioone, vajab serveriteenus tavaliselt mitmesugust infot, mida tuleb hoida serveri failisüsteemis.

Siia alla kuuluvad:

- käitusfailid, mille abil saab serveriteenust käivitada või hallata, samuti mitmed abirakendused, millest võib serveri käitamisel kasu olla;
- konfiguratsioonifailid või -sissekanded, mis juhivad serveriteenuse käitumist;
- logifailid, millesse serveriteenus salvestab toimunud sündmusi;
- tööandmed serveriteenuses reaalselt pakutava infoga.

Õigusi pääseda juurde sellele infole tuleb anda võimalikult piiravalt. Juurdepääs tohib olla ainult sellistel kasutajatel, kes seda infot tõesti vajavad. Juurdepääs peab olema piiratud miinimumini. Selleks, et pääsuõiguste määramine ei kulutaks suure hulga kasutajate korral liigselt ressursse, tuleks sisse seada rühmad või

rollid.

Autentimiseks vajalikke õigusi saab siiski anda ka üksikutele kasutajakontodele või eeldefineeritud IP-aadresside või -aadressivahemike alusel. Et serveriteenus saaks funktsioone pakkuda, tuleb käivitada protsess, mis pääseb ligi vajalikule infole ja muudele ressurssidele. Protsessi pääsuõigused tulenevad tavaliselt protsessi käivitajaks olnud kasutaja pääsuõigustest. Tavaliselt ei vaja protsess operatsioonisüsteemi kataloogide jaoks kirjutamisõigust ja seega ei tohiks seda ka omada.

Samas esineb sageli olukordi, kus privileegidega kasutaja, kellel on operatsioonisüsteemi kataloogide jaoks kirjutamisõigus, peab käivitama protsessi, et avada näiteks kas TCP- või UDP-pordid. Kui võimalik, tuleks sel juhul tagada, et protsess antaks pärast käivitamist üle privileegideta kasutajale. Kui protsessi ja seega serveriteenust saab käivitada ainult privileegidega kasutaja, tuleks protsess võimaluse korral sulgeda chroot -keskkonda, sandbox 'i või mõnda teise sarnasesse keskkonda. Chroot -keskkond kujutab endast arvutisüsteemi eraldatud ala, mis raskendab pärast serveriteenuse kompromiteerimist ründaja ligipääsu terviksüsteemile.

Kuid chroot -keskkond eeldab, et kõik serveriteenuse jaoks vajalikud failid oleksid samuti olemas serveriteenuse kataloogis ja seega eraldatud alas (vt M 4.198z Rakenduse installeerimine chroot -puuri).

Sõltuvused teekidest, operatsioonisüsteemi poole pöördumistest ja välistest ressurssidest

Serveriteenuste installipaketid sisaldavad arvukalt faile, mis kopeeritakse installimisel sihtsüsteemi.

Peale nende läheb serveriteenuse käitamiseks tavaliselt tarvis ka lisafaile. Nende hulka kuuluvad näiteks kolmanda osalise või operatsioonisüsteemi rakendused ja teegid. Kuigi tavaliselt kontrollitakse juba serveriteenuse installimisel automaatselt, kas kõik vajalikud failid on olemas, tuleks esmalt siiski ka käsitsi üle kontrollida, kas need on ikka tõepoolest olemas.

Näiteks kui olemasolev serveriteenus asendatakse uuema versiooniga, tuleb jälgida, et jätkuvalt oleksid olemas ka kõik selle kasutamiseks vajalikud failid. Uuendamise tagajärjel võib serveriteenus vajada juurdepääsu lisafailidele, mis polnud enne uuendust vajalikud. Vaja võib minna ka mõne teegi uuemaid versioone. Üldiselt ei tohiks uuendamise käigus piirduda ainult serveriteenuse uuendamisega, vaid uuendada tuleks kõiki asjakohaseid rakendusi ja teeke. Näiteks kui serveriteenus kasutab teeki, milles on teadaolevalt turvaauke, võidakse seda teeki serveriteenuse ründamiseks ära kasutada. Serveriteenuse pöördumisi

operatsioonisüsteemi poole tuleks võimaluse korral vältida. Kui need on siiski vajalikud, tuleb jälgida, et näiteks Command-Injection-rünnetega ei saaks serveris anda kompromiteerivaid korraldusi. Need korraldused tuleb filtreerida võimalikult piiravalt. Sageli ei kasutata serveriteenuseid sõltumatult, vaid koostöös väliste ressurssidega.

Siia alla kuuluvad näiteks:

- serveriteenused, mis sõltuvad autentimisserveritest, veebiserveritest või veebirakenduste serveritest;
- veebirakenduste serverid, mis sõltuvad andmebaasiserveritest;
- failiserverid, mis sõltuvad salvestivõrkudest.

Selliste serveriteenuste või ühenduste tõrke korral võib ka seda kasutav serveriteenus lakata töötamast. Kui käideldavuse kaitsevajadus on suur, võib osutuda iseäranis vajalikuks kasutada liiasusega ühendust või liiasusega järgasetusega serveriteenuseid.

Kättesaadavuse piiramine

Paljusid serveriteenuseid, mis pakuvad võrgus infot, saab seadistada nii, et need oleksid korraga tööootel kas ainult ühe või väheste võrguliideste jaoks, st neid peab saama liideste külge fikseerida. Võrguliidesed võivad olla füüsilised võrgukaardid või loogilised ühendused, nt virtuaalsed võrgukaardid või loopback -liidesed. Kui IT-süsteemil on mitu liidest ja kui võrgu serveriteenus on seotud ainult ühega, ei võta võrgu serveriteenus mõnele muule võrguliidesele esitatud ühenduspäringuid vastu seni, kuni neid ei edastata portidesse vms. Seeläbi saab juurdepääsu võrgu serveriteenusele piirata nii, et teenuste kasutamine võimaldatakse ainult teatud võrgupiirkondades paiknevatele kasutajatele. Seega peaks iga võrgupõhine serveriteenus olema seotud võimalikult väheste võrguliidestega. Kui võrgu serveriteenust tuleks kasutada ainult kohaliku IT-süsteemi piires, tohib seda siduda vaid loopback -liidesega. Kohalike võrguteenuste näideteks on Super- (nt inetd), X-, printimis- või ajaserver. Juurdepääsu võrguteenusele saab piirata ka paketifiltriga. Üldjuhul peaks juurdepääs võrguteenusele olema ainult volitatud IT-süsteemidel.

Selleks, et IT-süsteem, milles võrguteenust käitatakse, võtaks vastu ainult kindlate pordinumbritega IT-süsteemide ühenduspäringuid, saab ühenduse loomist reguleerida paketifiltritega. Näiteks võimaldavad paketifiltrite reeglid juurdepääsu backend -serverile piirata nii, et serverit saavad kasutada üksnes sellega kokku kuuluvad rakendusserverid. Paketifiltreid on tavaliselt võimalik seadistada ka viisil, mis sunniks neid logima kõiki või üksnes valitud ühenduspäringuid (vt M 2.74 Sobiva paketifiltri valimine ja M 4.98 Side piiramine miinimumini paketifiltritega).

Autentimise ja kasutajaandmete krüpteerimine

Olenevalt serveriteenusest ja ressurssidest, mille kasutamist teenus võimaldab, saab eristada, kas need peaksid olema kättesaadavad kõikidele või ainult valitud

kasutajatele. Selleks saab kasutada kaitsevajadusele vastavaid autentimismeetodeid. Tavalised autentimismeetodid on muu hulgas (võltsitavad) IP-aadressid, kasutajatunnus ja parool või sertifikaadid. Üldjuhul tuleb kogu info, mida läheb serveriteenuses autentimiseks tarvis, edastada krüpteeritult. Kui kasutajaandmeid edastatakse ebaturvaliste võrkude kaudu, tuleb kontrollida, kas neid saaks edastada krüpteeritult. DNS-, marsruutimis- ja NTP-info edastatakse tavaliselt ilma krüpteerimata, seevastu HTTP- või IMAP/POP3-info sageli krüpteeritult, et kaitsta selle konfidentsiaalsust. Seega tuleb otsustada, millised kasutajaandmed vajavad krüpteerimist. Üldiselt soovitatakse võimaluse korral alati krüpteerida, sest sellest tulenev täiendav töökoormus on sageli tühine 8vt M 5.68z Krüpteerimisprotseduuride kasutamine võrgusuhtluses).

Versiooniinfo piiramine

Standardsed veateated võivad sageli sisaldada liiga palju infot. Näiteks võib ründaja versiooniinfo alusel otsida turvaaukudega serveriteenuseid ja neid enda huvides ära kasutada. Sel põhjusel tuleks võimaluse korral kõiki süsteemiteateid seadistada selliselt, et nendest ei saaks teha järeldusi tarkvara versiooni või konfiguratsiooni kohta. Ka ise koostatud veateadete puhul tuleb arvestada, et need peavad kasutajaid vigadest teavitama, kuid edastatav teave ei tohi olla liiga detailiderohke.

Andmevarundus

Kogu teavet, mida läheb tarvis andmete taastamiseks, tuleb regulaarselt varundada, nt selleks, et riistvaratõrke või juhtfailide juhusliku kustutamise korral saaks kiirelt serveriteenuse kasutamisega jätkata.

Selle alla kuuluvad vähemalt:

- konfiguratsioonifailid,
- kasutajaandmed,
- logiandmed.

Paljude serveriteenuste puhul on eriti oluline kasutajaandmete käideldavus. Faili-, meili- või veebiserverite puhul on tegu infoga, mida ei saa erinevalt konfiguratsioonifailidest niisama lihtsalt uuesti koostada. Teatud serveriteenuste puhul ei piisa varundatavate failide kopeerimisest. Eriti just olukorras, kus varundatavat infot hoitakse ka andmebaasides, tuleb kasutada alternatiivseid varundamismeetodeid.

Üks selline näide on Samba TDB-failid, mille sisu talletab serveriteenus sageli pikemaks ajaks, ilma et seda salvestataks alati töö ajal kõvakettale (vt M 6.135 Samba serveri tähtsate süsteemikomponentide regulaarne varundamine).

Seepärast tuleb andmete õige varundamise tagamiseks serveriteenuse dokumentatsiooni konsolideerida.

Värskendused (updates)

Kasutatud serveriteenus peab olema alati värske. Kui kasutatud tarkvaras on leitud turvaauke ja kui nende kõrvaldamiseks on välja lastud uuem versioon, tuleks aegsasti võtta kasutusele vigadest puhastatud versioon. Enne uue versiooni kasutuselevõttu tuleb seda katsetada. Tegeliku serveriteenuse kõrval vajavad värskendamist ka järgasetusega serveriteenused, operatsioonisüsteem ja kõik muud installitud rakendused (vt M 2.273 Turvalisust mõjutavate paikade ja värskenduste kiire paigaldamine).

Logimine

Serveriteenustes esinevaid turbega seotud sündmusi tuleb mitmel põhjusel logida. Ühest küljest aitab sisselülitatud logifunktsioon varakult tuvastada ja seeläbi ka kõrvaldada potentsiaalseid kitsaskohti. Teisalt saab logide põhjal leida turbenõuete rikkumisi ja uurida tagantjärele turvaintsidendi võimalikke tekkepõhjusi. Serveriteenuse logimine tuleb integreerida logimiskontseptsiooniga (vt M 2.500 IT-süsteemide logimine).

Serveriteenusest olenevalt tuleb logides kajastada vähemalt järgmisi sündmusi:

- ebaõnnestunud sisselogimiskatsed;
- ressurssidele tehtud pöörduste ebaõnnestumine järgmistel põhjustel:
- ebapiisavad õigused,
- olematud ressursid,
- serveri vead,
- riistvara puudujäägid ja tõrked;
- muud veateated.

Kontrollküsimused:

- Kas käivitus-, konfiguratsiooni- ja logifailide ning kasutajaandmete pääsuõigused, mida läheb tarvis serveriteenuse tööks, on antud piiravalt?
- Kas kõik ressursid, mida läheb tarvis serveriteenuse tööks, on olemas kõige uuemas versioonis?
- Kas võrgu serveriteenus saab ühendustele reageerida ainult hädavajalike võrguliideste kaudu?
- Kas serveriteenuste autentimise info edastatakse alati krüpteeritult?
- Kas kogu serveriteenuse jaoks olulist infot varundatakse regulaarselt?
- Kas serveriteenuse turvalisuse seisukohalt olulisi sündmusi logitakse?

M 4.433z Serveriteenuste turvaline konfiguratsioon

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: IT-juht, infoturbespetsialist

Ülekirjutatavates andmekandjates hoitavat konfidentsiaalset infot saab krüpteerida mitmel viisil ja kaitsta seeläbi volitamata juurdepääsu eest. Krüpteerida saab kas kogu andmekandja, kindla partitsiooni või üksnes väljavalitud failid. Turvalisuse seisukohalt on parim lahendus kogu andmekandja krüpteerimine, sest nii peab kasutaja kõige vähem protsessi sekkuma ja kõik failid on volitamata juurdepääsu eest kaitstud. Tervikliku andmekandja või partitsiooni krüpteerimine on kasutaja jaoks peaaegu läbipaistev.

Kasutajad peavad end autentima ainult alglaadimisel või partitsiooni esmakordsel kasutamisel. Kui krüpteeritakse ainult kindlaid faile või failikonteinereid, on oht, et kaitsevajadusega failid võidakse kogemata salvestada kõvaketta krüpteerimata alasse. Lisaks peab sellise lahenduse korral kasutaja krüpteerimisprogrammi eraldi käivitama. Ka väljavalitud partitsioonide täieliku krüpteerimise korral on oht, et konfidentsiaalne info satub mingil põhjusel krüpteerimata partitsioonile. Seetõttu on parim ja tõhusaim meetod konfidentsiaalsete andmete kaitsmiseks volitusteta juurdepääsu eest siiski andmekandjate täielik krüpteerimine.

Andmekandjaid saab krüpteerida nii tarkvara- kui ka riistvarapõhiste lahendustega. Tarkvaral põhinevate lahenduste hulka kuulub näiteks Microsofti BitLocker (vt M 4.337z BitLockeri Drive Encryption kasutamine) või avatud lähtekoodiga programm TrueCrypt. Mobiilsed andmekandjad, nt USB mälupulgad ja sülearvutid, tuleb võimaluse korral alati täielikult krüpteerida, isegi kui need ei pruugi konfidentsiaalset infot sisaldada. Statsionaarsete IT-süsteemide puhul on suure konfidentsiaalsusvajaduse korral vaja andmekandjad samuti alati täielikult krüpteerida.

Serveri kõvaketaste krüpteerimisel tuleb analüüsida ka seda, kas valitud krüpteering on piisava jõudlusega ja sobib kasutajapöörduste hulgaga.

Lisaks krüpteerimisprogrammile läheb andmekandja krüpteerimiseks vaja krüptograafilisi võtmeid. Krüptograafilised võtmed tuleb genereerida turvaliselt meetme M 2.46 Krüpteerimise õige korraldus kohaselt ja hoida neid krüpteeritud andmekandjatest eraldi. Selleks saab kasutada näiteks kiipkaarte või USB-pääsmikke (tokens). Selline eraldamine pole USB mälupulkade krüpteerimisel tavaliselt võimalik ja turvaanalüüsis tuleb selle asjaoluga arvestada. Muidugi tuleb krüpteeritud andmekandjatesse salvestatud andmeid ka regulaarselt varundada (vt M 6.56 Andmevarundus krüptoprotseduuride kasutamisel). Mõned andmekandja või partitsiooni krüpteerimise programmid või krüpteeritud failikonteinerite kasutamise programmid pakuvad ka võimalust krüpteeritud alad n-ö ära peita. Kuna selliseid

funktsioone on keeruline kasutada ja vale kasutamise tagajärjel võib tekkida täielik andmekadu, tuleks neist hoiduda.

Kontrollküsimused:

- Kas mobiilsete klientide ja andmekandjate krüpteerimiseks on valitud ja installeeritud sobiv lahendus?
- Kas kõikide statsionaarsete IT-süsteemide jaoks, mis töötlevad konfidentsiaalset infot, mille kaitsevajaduse klass on vähemalt suur, on valitud sobiv andmekandjate krüpteerimise lahendus?

M 4.434 Eraldiseisvate seadmete kasutamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

Eraldiseisvate seadmete (appliances) all peetakse silmas spetsiaalseks kasutusotstarbeks konstrueeritud seadmeid, nt tulemüüre, marsruutreid, paketifiltreid, NAS- või VoIP-süsteeme. Nende eelis seisneb optimaalselt kokku sobitatud riist- ja tarkvaras ning mõningate keerukate protseduuride lihtsustamises kasutaja jaoks. Ka konfigureerimise on tootja kasutaja jaoks üldjuhul juba suures osas ära teinud. Seadmed on tarnimisel sageli kasutusvalmis ja neid võib rakendada pärast mõne lihtsa sisestuse tegemist. Seetõttu on eraldiseisvaid seadmeid enamasti lihtne installeerida ja kasutada. Samas on eraldiseisva seadme konfiguratsioon vähem paindlik ja pakub seetõttu ka vähem võimalusi erinevatest, ükskõik kas organisatsiooni enda või teenusepakkuja valitud individuaalsetest IT-komponentidest koosneva süsteemiga kohandamiseks. Isekoostatud lahendusi, nt tulemüüre, saab sageli installeerida ka tavapärasesse standardoperatsioonisüsteemiga töötavasse riistvarasse ja kohandada sobivate tarkvarakomponentidega. Seetõttu on need väga paindlikud ja neid saab edukalt kasutada väga erineval otstarbel. Samas võib vajalike komponentide paigaldamise ja integreerimise käigus tekkida ka palju vigu.

Veel üks puudus on asjaolu, et eri komponentide (nt riistvara, operatsioonisüsteemi, tarkvara) tugiteenuse saamiseks tuleb sageli pöörduda erinevate kontaktisikute poole.

Alljärgnevalt on võrreldud eraldiseisvate seadmete mõningaid eeliseid ja puudusi.

Eelised

Puudused

Lihtne installida, kasutuselevõtuks kulub vähe aega.

Lihtsus, konfigureerimine pole liiga töömahukas.

Käitamiseks pole tarvis laialdasi eriteadmisi.

Konfigureerimine on lihtsustatud, sest eraldiseisvates seadmetes on sageli olemas administreerimisliidesed.

Eraldiseisvad seadmed toetavad sageli funktsioonide automaatset värskendamist (update).

Erinevalt lahendustest, mis koosnevad kasutusvajaduse alusel kokkupandud IT-komponentidest, on väiksem tõrgete oht, sest eraldiseisvatel seadmetel on sageli tavaarvutist vähem liikuvaid komponente (nt kõvakettad või ventilaatorid).

Tootjapõhise riist- ja tarkvara laiendamise võimalused on väiksemad.

Defektide korral võib tekkida terviksüsteemi väljavahetamise vajadus.

Pikad tööseisakud, kui seade tuleb tõrke korral tootjale saata. Seetõttu tuleks vajadusel muretseda asendusseade, mida hoitakse Cold Standby reþiimis.

Seadmetes kasutatavate turvamehhanismide kvaliteeti on keeruline kontrollida.

Spetsiaalsete toodete turvalise konfigureerimise ja kasutamise kohta on vähe teavet (muud peale tootjainfo). Eriti problemaatiliseks muutuvad need juhud, kus tootja lõpetab tugiteenuse osutamise.

Osa eraldiseisvatest seadmetest pole eriti levinud. Sellistel juhtudel leidub väga vähe nõustajaid või teenusepakkujaid.

Eraldiseisvate seadmete rakendamise kasuks otsustamise ja kindlate seadmete väljavalimise põhjused tuleb dokumenteerida.

Installeerimine, konfigureerimine ja andmevarundus

Eraldiseisvad seadmed tarnitakse sageli eelinstalleeritud operatsioonisüsteemi ehk püsivaraga (firmware). See asub tavaliselt kohakindlas flash-andmekandjas või osa seadmete puhul ka kõvaketastel või vahetatavatel mälukaartidel. Kuna eelinstalleeritud püsivara kopeeritakse seadmele juba tootmise ajal ning tootmise ja kasutuselevõtu vahele võib jääda pikk ajavahemik, on eelinstalleeritud püsivara kasutuselevõtu ajaks tavaliselt juba vananenud ning vahepeal on avaldatud juba uued püsivara versioonid. Seega tuleks enne eraldiseisva seadme kasutuselevõttu püsivara tootja juhiste kohaselt värskendada (firmware update). Installeeritav püsivara peab pärinema usaldusväärsest allikast (vt M 4.177 Tarkvarapakettide tervikluse ja autentsuse tagamine).

Konfiguratsioon

Tavaliselt konfigureeritakse eraldiseisvaid seadmeid veebiliidese, Telneti/SSH, SNMP või tootjapõhiste protokollidega. Tootest ja tootjast olenevalt pakutakse ka konfigureerimistööriistu, mida saab installeerida teistesse IT-süsteemidesse ja mis võimaldavad konfigureerida ühte või mitut eraldiseisvat seadet. Iga sellise konfigureerimisvõimaluse puhul tuleb jälgida, et võrgu kaudu konfigureerimisel ei saaks kolmas osaline sidet pealt kuulata ega seda muuta. Seepärast tohib konfigureerimiseks kasutada üksnes turvalisi ühendusi, nt krüpteeritud ühendusi või eraldi konfigureerimisvõrku.

Eelseadistatud paroolid tuleb ära muuta

Eraldiseisvatel seadmetel on tarnimisel tavaliselt eelseadistatud paroolid. Paroolid tuleb kohe ära muuta (vt M 4.7 Algparoolide muutmine) ja sobivasse kohta hoiule panna (vt M 2.22z Paroolide deponeerimine). Pärast konfigureerimist tuleb konfiguratsioon varundada, et tõrke korral saaks samaväärse seadme kiirelt asendusena tööle võtta. Kui eraldiseisva seadme konfiguratsiooni käitamise ajal muudetakse, tuleb need konfiguratsioonimuudatused samuti varundada ja dokumenteerida.

Logimine

Eraldiseisvate seadmete kasutamise käigus esineb sageli sündmusi, mida tuleb logida. Kahjuks pole eraldiseisvates seadmetes logifailide salvestamiseks piisavalt mäluruumi või ei sobi kasutatava mälu liik pideva kirjutamise jaoks. Seetõttu on soovitatav salvestada sündmused eraldi IT-süsteemi, tavaliselt eraldi logiserverisse (vt B 5.22 Logimine).

Turvaline kasutusest kõrvaldamine

Eraldiseisvate seadmete kasutusest kõrvaldamisel või vahetamisel tuleb seadmetest kustutada kogu turvalisust puudutav info.

Kasutusotstarbest olenevalt võivad seda infot sisaldada näiteks

- konfiguratsioonifailid, mis annavad infot organisatsiooni võrgustruktuuri kohta;

- paroolifailid;
- logifailid, mis võivad sisaldada turbeinfot või isikuandmeid;
- sertifikaadid ja krüptograafilised võtmed (nt juurdepääs teistesse IT-süsteemidesse).

Sellise info kustutamine võib eraldiseisvate seadmete puhul olla keerulisem kui tavalistes IT-süsteemides. Eraldiseisvatel seadmetel hoitava info kustutamise metoodika sõltub sellest, kuhu ja kuidas on andmeid salvestatud, nt kas integreeritud kõvakettale või püsimällu. Paljud seadmed on varustatud tehaseseadete taastamise funktsiooniga, mille abil on võimalik kõik konfiguratsiooni puudutavad seadistused taastada väärtustele, mis on seadmel tehasest väljudes. Pärast tehaseseadete taastamise funktsiooni kasutamist tuleb siiski üle kontrollida, kas andmed on tõepoolest kustutatud ehk tarneseisundisse tagasi muudetud või on teatud andmed või failid siiski alles jäänud.

Vajaduse korral tuleb salvesti muuta kasutuskõlbmatuks

Kui seadmetele on salvestatud eriti tundlikku turbeinfot ning kui ei olda piisavalt kindel, kas andmed said turvaliselt kustutatud, tuleb mälukiibid või kõvakettad muuta vajaduse korral füüsiliselt kasutuskõlbmatuks.

Tähistused tuleb eemaldada

Sageli on eraldiseisvatele seadmetele paigaldatud kirjad IP-aadresside, hostinimede või muu tehnilise teabega. Ka need tähistused tuleb enne seadme kõrvaldamist eemaldada.

Kontrollküsimused:

- Kas eraldiseisva seadme valimise põhjused on dokumenteeritud?
- Kas eraldiseisvaid seadmeid värskendatakse enne kasutuselevõttu ja kas eelseadistatud paroolid muudetakse ära?
- Kas eraldiseisvaid seadmeid konfigureeritakse ainult kaitstud ühenduste kaudu (või otse seadmes)?
- Kas eraldiseisvate seadmete konfiguratsioone varundatakse regulaarselt?
- Kas eraldiseisvate seadmete kasutusest kõrvaldamine on turvaline ja kas kogu konfidentsiaalne teave kustutatakse?

M 4.435z Isekrüpteerivad kõvakettad

Algatamise eest vastutab: infoturbespetsialist

Rakendamise eest vastutab: administraator

Selleks, et volitamata isikud ei pääseks ligi kõvaketastel asuvatele konfidentsiaalsetele andmetele, tuleks need võimaluse korral alati täielikult krüpteerida (vt M 1.1 Vastavus normidele ja eeskirjadele).

Krüpteerimiseks saab kasutada nii riist- kui ka tarkvarapõhiseid meetodeid. Selles meetmes käsitletakse isekrüpteerivatel kõvaketastel põhinevat riistvarapõhist krüpteerimist (self-encrypting device, SED). SED-d kasutavad krüpteerimiseks spetsiaalset riistvaralist krüptokontrollerit ja on seetõttu väga tõhusad.

Kasutatavad krüpteerimislahendused lähtuvad ainult ühest kasutajast, st mitme kasutajaga lahendused pole üldjuhul ette nähtud.

Isekrüpteeriva kõvaketta kasutamisel võib juhtuda, et IT-süsteemi ei saa enam töömällu puhkeseisundisse jätta, sest kõvaketta väljalülitamisel krüpteeritakse kõik andmed ja töömällu (RAM) salvestatud võti kujutaks endast turvariski. Sellele tuleb mõelda enne kasutamist.

Isekrüpteerivaid kõvakettaid ei tohi kombineerida TPM-mooduliga, sest sellise kombinatsiooni puhul pole tavaliselt võimalik kõvaketast mõnes muus IT-süsteemis alusvõtmega (master key) dekrüpteerida. Sellises olukorras tekkinud IT-süsteemi kahjustuse korral ei ole kõvakettal asuvad andmed enam dekrüpteeritavad, sest kõvaketas on TPM-mooduli kaudu püsivalt IT-süsteemiga seotud. Isekrüpteerivad kõvakettad kasutavad tavaliselt 128- kuni 256-bitise võtmepikkusega AES-i. Andmete krüpteerimiseks kasutatav võti on data encryption key (DEK). DEK asub krüptokontrolleris, mis on manipuleerimise eest väga hästi kaitstud. See võti genereeritakse juhuslike riistvarasündmuste alusel. DEK krüpteeritakse autentimisvõtmega authentication key (AK). AK genereeritakse tavaliselt siis, kui kasutaja valib endale parooli. Teatud isekrüpteerivate kõvaketaste puhul saab AK salvestada ka pääsmikule, nt kiipkaardile või USB mälupulgale ja lisaks parooliga krüpteerida. See võimaldab kasutada kahefaktorilist autentimist.

Alusvõti

Lisaks DEK-le ja AK-le on tavaliselt olemas alusvõti (master key), mis võimaldab andmeid dekrüpteerida ka parooli või pääsmiku kaotamisel. See võti tuleb genereerida installeerimisel ja seda tuleb hoida parooli või pääsmiku kaotamise juhuks turvalises kohas. Organisatsiooni töökorralduses peab olema reguleeritud, mida tuleb teha, kui kasutaja on krüpteeritud kõvaketta parooli ära unustanud. Sellisel juhul tuleb parool alusvõtmega lähtestada ja kasutaja peab valima uue parooli. Kui kasutaja on end edukalt autentinud, toimub DEK dekrüpteerimine. DEK abil dekrüpteeritakse ja krüpteeritakse kõik kõvakettal asuvad andmed,

ilma et kasutaja töö käigus seda märkaks. Kui arvuti lülitatakse välja või kui SED kettaühendus lahutatakse, krüpteeritakse kõik andmed DEK-ga ja DEK krüpteeritakse omakorda AK-ga. Kõvaketta krüpteerimise meetodi puhul peaks alati kasutama piisavalt pikka võtit. Lisateavet krüptograafiliste meetodite jaoks sobivate võtmepikkuste kohta saate meetmest M 2.164 Sobiva krüptoprotseduuri valimine .

Enne isekrüpteeriva kõvaketta soetamist tuleb kontrollida, kas sellised kõvakettad ühilduvad IT-süsteemi ülejäänud riistvaraga. Lisaks tuleb kontrollida, kas valitud kõvaketta kirjutamis- ja lugemiskiirused on piisavad. Kontrollida tuleb ka seda, kas IT-süsteemi kasutusvaldkond seab mõningaid muid raamtingimusi. Näiteks ei leidu palju isekrüpteerivaid kõvakettaid, mida saaks integreerida olemasoleva ainulogimisega arhitektuuriga. Samuti tuleb kontrollida, kas ja kuidas saab tavaliste kõvaketastega IT-süsteeme migreerida isekrüpteerivateks kõvaketasteks (nt kaasasoleva programmiga või uuesti installeerides). Isekrüpteeriva kõvaketta installeerimine on organisatsioonis koolitatud administraatorite ülesanne. Selleks peavad nad genereerima esmalt uue DEK ning määrama parooli ja alusvõtme, mida tuleb hoida turvalises kohas (vt M 2.22z Paroolide deponeerimine ja M 6.56 Andmevarundus krüptoprotseduuride kasutamisel). Esimese asjana peab kliendi kasutaja asendama DEK algparooli turvalise parooliga (vt M 2.11 Paroolide kasutamise reeglid).

Isekrüpteeriva kõvaketta parandamise, müümise või utiliseerimise korral peab olema tagatud, et sellest ei oleks võimalik kätte saada konfidentsiaalset infot. Seega tuleb enne parandamist, müümist või utiliseerimist genereerida uus DEK või kasutada kustutuskäsku ATA Secure Erase.

Kontrollküsimused:

- Kas isekrüpteerivate kõvaketaste installeerimisel genereeritakse uus DEK ja koostatakse alusvõti, mis pannakse turvalisse kohta hoiule?
- Kas enne parandamist, müümist või utiliseerimist kustutatakse DEK või kasutatakse käsku ATA Secure Erase?

M 4.444 XXX

M 4.445 XXX

M 4.446 XXX

M 4.447 SAN-Fabricu tervikluse tagamine

Algatamise eest vastutavad: IT-juht, infoturbeametnik

Rakendamise eest vastutab: administraator

SAN-Fabric'u terviklus tähendab selles meetmes, et plaanitud ja käitaja poolt ettenähtud komponendid töötavad SAN-Fabric'us ning et tähelepanematu töötaja ega sihilikult tegutsev ründe toimepanija ei too SAN-Fabric'usse komponente ega sega seeläbi SAN-Fabric'u tööd või mõjuta andmete leket. SAN-Fabric'u tervikluse tagamiseks tuleks rakendada täiendavate turbefunktsioonidega protokolle, mida kirjeldatakse käesolevas meetmes.

American National Standards Institute (ANSI) on sellega seoses välja arendanud standardi, mis kirjeldab erinevaid turvalisuse tõstmise protokolle Fibre-Channel-võrkudes.

Fibre Channel Secure Protocol (FC-SP)

FC-SP kirjeldab turvalise autentimise võimalikke struktuure kahe kommutaatori, lõppseadme ja kommutaatori vahel ning kahe lõppseadme vahel. FC-SPP-s kirjeldatud protokollide abil võib kommutaator autentida uusi lõppseadmeid SAN-il lokaalselt või tsentraalselt installeeritud serveri kaudu, kasutades sageli juba olemasolevat autentimise taristut.

Kasutaja käsutuses on kolm erinevat protokolli, mille abil saab Fibre-Channel-SAN-is rakendada autentimismehhanisme.

Diffie Hellman Challenge Handshake Authentication Protocol (DH-CHAP):

- DH-CHAP pakub kahesuunalist, paroolil põhinevat autentimist (CHAP), mis on täiendavalt kaitstud Diffie-Hellmann-meetodiga võtmete vahetamiseks.

Fibre Channel Authentication Protocol (FCAP):

- FCAP realiseerib FC-komponentide mõlemapoolse autentimise digitaalsete sertifikaatide alusel.

Fibre Channel Password Authentication Protocol (FCPAP):

- FCPAP kujutab endast paroolil põhinevat meetodit, mis kasutab ära Secure Remote Password'i (SRP).

Nende protokollide võimalusi tuleks kasutada komponentide vastastikuseks autentimiseks. Nende protokollide kasutamisega saab kindlustada, et liita ei saa ühtegi FC-Fabric'u komponenti, omamata vastavaid sertifikaate või paroole. Tänu sellele ei saa Fabric'u konfiguratsiooni ei lugeda ega ka manipuleerida. Isegi

võõraste komponentide eduka füüsilise ühendamise korral SANFabric'uga puudub juurdepääs, mis võimaldaks näiteks lugeda andmeliiklust. WWN-Spoofing jääb sel moel edutuks.

Kontrollküsimused:

- Kas SAN-Fabric'u tervikluse tagamist toetatakse täiendavate turbefunktsioonidega protokollide kasutamisega?
- Kas protokollide DH-CHAP, FCAP ja FCPAP kasutamisega võetakse arvesse nende protokollide turbefunktsioone ja kasutatakse vastavaid konfiguratsioone?

M 4.448z Krüpteeringu kasutamine salvestisüsteemides

Algatamise eest vastutavad: IT-juht, infoturbeametnik

Rakendamise eest vastutavad: administraator, IT-juht

Andmete puhul, millel on salvestisüsteemis konfidentsiaalsust puudutav kõrge kaitsevajadus, tuleks kontrollida krüpteerimise kasutamise võimalusi.

Kui salvestisüsteemi andmed krüpteeritakse, peavad asutused järgima edaspidi meetmeid M 2.46 Krüpteerimise õige korraldus ja M 5.68 Krüpteerimisprotseduuride kasutamine võrgusuhtluses .

Vahet tuleb teha andmete krüpteerimisel nende edastuskanalis (Data-in-Motion) või andmete krüpteerimisel vahetult salvestiüksuses (Data-at-Rest). Krüpteerimine edastuskanalis on kohane ka replikatsioonide ja Backup-Traffic'u korral, samal ajal kui loodud Backup- või arhiiviandmed tuleb krüpteerida salvestiüksuses.

Konfidentsiaalsuse suhtes kõrge või väga kõrge kaitsevajadusega andmete krüpteerimine peaks olema esmajärjekorras tagatud rakenduse kaudu, mis vastutab ka andmete töötlemise eest.

Krüpteerimistehnika peaks olema integreeritud kas otse salvestisüsteemi komponentidesse või tuleks krüpteerida täiendava toote abil. Lihtsalt rakendatav lahendus pakub hetkeseisuga isekrüpteerivate kõvaketaste kasutamist salvestisüsteemi sees.

Fibre-Channel-Frames'ide edastamine peaks ka siis toimuma krüpteeritud ühenduse kaudu, kui andmed arvutuskeskusest ei välju.

SAN-ühenduse kaitsmine IP kaudu nõuab täiendavaid kaitsemeetmeid, sest IP-ühendust on märksa lihtsam kahjustada kui eraldi olevat Fibre-Channel-ühendust. Kui rakendus ei paku ühenduse krüpteerimist, tuleb krüpteeritud ühendus kaasata ja seda kasutada muul moel (nt operatsioonisüsteemi või edastusvõrgu funktsioonide kaudu), et säilitada andmete konfidentsiaalsus.

Kontrollküsimused

- Kas kõrge kaitsevajadusega andmed krüpteeritakse?
- Kas on kindlaks määratud, millistel tasanditel (Data-in-Motion ja Data-in-Rest) peab krüpteerimine toimuma?

- Kas IP kaudu teostatava SAN-ühenduse kaitsmiseks võetakse täiendavaid kaitsemeetmeid?

M 4.449z Tsoonide kontseptsiooni juurutamine

Algatamise eest vastutavad: infoturbeametnik, IT-juht

Rakendamise eest vastutavad: infoturbeametnik, IT-juht

Sageli rajatakse asutustesse suured, aga lihtsad võrgud, mis saavad hakkama ilma täiendavate turvatsoonideta. Seejuures liidetakse kõik IT-süsteemid ühtsesse võrku, mille interneti-liidesel vastutab teabeturbe eest tsentraalne turvalüüsi lahendus (vt moodulit B 3.301 Turvalüüs (tulemüür)). Selline lihtne turvastruktuur pakub siiski ründe toimepanijate või kahjurvaraprogrammide suhtes liiga väikest turvalisust, sest pärast turvalüüsist läbipääsemist on kogu võrk koos kõikide komponentide ja andmetega avatud.

Nende ohtude taustal peaksid asutused võtma meetmeid, et kaitsta oma võrku ja koos sellega ka ühendatud IT-süsteeme nagu server, kliendid, võrk (IP ja FC), ja salvestikomponente. Üks võimalik lahendus on tsoonide moodustamine. Selleks jaotatakse võrk eraldi aladeks, mis kõik kaitstakse näiteks oma turvalüüsi või paketifiltriga.

Tsoonide kontseptsioon eristab selle tulemusel erinevaid turvatsoone, millel on erinevad turbefunktsioonid. Sellise turbekontseptsiooni juurutamine põhineb säilitatud andmete erineval kaitsevajadusel ja vajab seetõttu hoolikat planeerimist.

Lisaks kaitsevajaduse analüüsile tuleb kindlaks teha samal ajal võrgus olevad sideühendused ja võrrelda neid tegelikult vajalike ühendustega. See protseduur aitab kaasa võrguliikluse vähendamisele mõistliku ja vajaliku mahuni ning sõltuvussuhete minimeerimisele IT-süsteemide vahel. Vahendatavad andmed moodustavad aluse turvatsoonide jaotamiseks.

Turvatsoonid erinevad üksteisest tavaliselt alljärgneva poolest:

- protsesside ja andmete omanik,
- töödeldavate teabeobjektide klassifitseerimine ja kaitsevajadus,
- kasutajarühmad ja komponendid, mis tohivad nendele teabeobjektidele ligi pääseda,
- ohud ja rakendatavad turvameetmed.

Kõik ühe asutuse IT-süsteemid määratakse täpselt ühele tsoonide kontseptsiooni tsoonile. Turvatsoon kujutab endast selle süsteemi jaoks keskkonda, mille jaoks on kindlaks määratud turbefunktsioonid, mis puudutavad tsoonidevaheliste sideühenduste kaitset. Kooskõlas õiguste ja rollide kontseptsiooni rakendamisega, mille kaudu antakse luba juurdepääsuks IT-süsteemidele kõikides piirnevates tsoonides või lahutatakse nendest, kaitstakse kõrgema kaitsevajadusega andmeid väliskeskkonna eest.

Tsooniüleste juurdepääsude keelamise põhimõte hoolitseb seejuures täiendavalt turbeastme tõstmise eest, sest see takistab ründe toimepanijal kasutada vähem tugevate kaitsemeetmetega, kahjustatud süsteemi hüppelauana kogu võrgu jaoks. Kui IT-süsteem on kahjustatud, saab rünnata kõiki sama tsooni IT-süsteeme.

Puudutatud tsoonist väljapoole jäävate muude tsoonide IT-süsteemid on kaitstud tsoonide eraldamise meetmetega.

Tsoonide kontseptsioon sõnastab kasutuskeskkondade turbeastme, mis tuleb teostada konkreetse võrgu-, rakendus- ja turvastruktuuri kaudu. Olenevalt IT-süsteemide kaitsevajadusest on võimalikud erinevad vormid, mis tagavad kas madala, keskmise või kõrge kaitsetaseme.

Kontrollküsimused:

- Kas on teostatud asutuse võrgu olemasolevate sideühenduste analüüs?
- Kas iga IT-süsteem määrati eraldi turvatsooni?
- Kas on olemas turvastruktuur, mis kirjeldab nõudeid vajalikele turvalisusega seotud teenustele ja nende liidestele üksikute turvatsoonide jaoks?

M 4.450 Veebiteenuste andmeside turve

Algatamise eest vastutavad: IT-rakenduste eest vastutavad töötajad, IT-juht
Rakendamise eest vastutavad: administraator, IT-juht

Kuna veebiteenuste andmeside ei kulge alati tingimata sisemiste, vaid ka välimiste, võõraste võrkude ja muude osalevate objektide kaudu, tuleb tagada, et andmed oleksid edastatud turvalise kanali kaudu. Seejuures on eesmärk tagada edastatavate andmete konfidentsiaalsus ja terviklus.

Veebiteenuste andmeside kaitseks võib rakendada erinevaid meetodeid ja standardeid, mida võib jaotada kahte põhistrateegiasse:

- edastamisel põhinev krüpteerimine ja
- sõnumitel põhinev krüpteerimine.

Edastamisel põhinev krüpteerimine SSL-i/TLS-i abil

SSL-/TLS-protokollide rakendamise abil saab kaitsta veebiteenuste andmesidekanaleid edastamistasemel. Tänu andmevoo krüpteerimisele kahe lõpp-punkti vahel on tagatud, et andmed on ülekandmise ajal kaitstud ja neid ei saa lugeda. Krüpteerimisega tagatakse ka sõnumi terviklus.

Lisaks krüpteerimisele peitub SSL-i/TLS-i kasutamises eelis, et selle kaudu on võimalik suhteliselt probleemivabalt rakendada rohkem autentimise vorme.

- Serveri autentimine: server autendib end veebiteenuste kliendi suhtes krüptograafilise sertifikaadi alusel.
- Kliendi autentimine: lisaks serverile autendib end ka klient serveri suhtes masinsertifikaadiga.
- Kasutaja autentimine: kliendipoolne autentimine võib toimuda ka kasutajaga seotud sertifikaatidega ja seda võib samaaegselt kasutada kõikide kasutajate autentimiseks.

SSL-/TLS-iga krüpteerimise eelis seisneb eelkõige selles, et rakendamine võib suurel määral toimuda olenemata veebiteenuste enda realiseerimisest, lihtsamal juhul veebi- või rakenduste serveri vastava konfiguratsiooni kaudu.

SSL-i/TLS-i kasutamise puudus seisneb selles, et krüpteeritakse üksnes ühendus kahe lõpp-punkti vahel. Keerulised olukorrad, mil näiteks ühte sõnumit tuleb saata läbi mitmete vahejaamade ja iga vastuvõtja tohib lugeda ainult üht kindlat osa sõnumist, ebaõnnestuvad.

Krüpteerimise korral SSL-/TLS-iga on andmed ainult ülekandel krüpteeritud.

Sel ajal, kui andmed on serveris ja ootavad näiteks järjekorras sõnumite töötlemist, on need süsteemis krüpteerimata. SSL-i/TLS-i kasutamine tuleb seetõttu varem konkreetse rakendusolukorra taustal üle kontrollida. Täiendavat teavet SSL-i/TLS-i kasutamise kohta leiate meetmetest M 5.66z SSL-i/TLS-i kasutamine kliendis ja M 5.177 SSL-i/TLS-i kasutamine serveris .

Sõnumil põhinev krüpteerimine WS-standardi abil

Kuna veebiteenuste korral võivad sõnumid liikuda üle paljude vahendajate ja otseühendus ei ole alati võimalik, saab vahendaja tõenäoliselt andmeid, mis ei ole tema jaoks mõeldud. Selleks et tagada sõnumite turvalisus, tuleb neid käsitleda nii, et osasõnumeid saavad lugeda ainult selleks volitatud vastuvõtjad, mille tõttu tuleb sellisel juhul kasutada sõnumil põhinevat krüpteeringut, näiteks XMLtasandil.

Selleks saab kasutada erinevaid standardeid:

- XML-Encryption (XMLEnc),
- XML-allkirjad (XMLSig),
- WS-Security,
- WS-SecureConversation.

Standardi ja selle kasutusvõimaluste täpsem kirjeldus on toodud meetmes M 4.451w Veebiteenuste värsked standardid .

Krüptograafiliste mehhanismide rakendamiseks tuleks kasutada loodud tarkvara teeki (Framework) ja olemasolevaid krüptoteeke (nt Java jaoks krüptoteegid IAIK-JCE või Bouncy Castle, viimane on kättesaadav ka C#/Microsoft.NET-i jaoks), sest iseseisev krüptorakendus on vastuvõtlik vigadele ja sisaldab teadaolevalt kitsaskohti.

Kättesaadavus

Kuna veebiteenused võimaldavad äriprotsesse teostada organisatsiooniüleselt, tuleb siinjuures pöörata erilist tähelepanu ka kättesaadavusele. Ühe komponendi tõrge võib kaasa tuua kogu äriprotsessi töö katkemise, mis võib mõjutada paljusid osapooli. Sel põhjusel tuleb süsteemide kättesaadavust silmas pidades vaadelda meetmeid nagu koormuse jaotus või kasutatava rakenduste serveri liiasused, et saavutada piisavalt suur kättesaadavus. Eesmärk peab olema vältida kättesaadavuse kaotust ühe komponendi tõrke korral (single point of failure). Olenemata süsteemis töödeldavate sõnumite hulgast, peab süsteem olema niimoodi laiendatav, et see saab hakkama ka päringute suurenenud hulgaga.

Lisaks tuleb kasutusele võtta turvameetmed, et minimeerida veebiteenuse töö katkemise riski sihilike rünnete tõttu (Denial of Service). Lisateavet leiate selle kohta meetmes M 4.405 Ressursside blokeerimise (DoS-rünnete) tõkestamine veebirakendustesja veebiteenustes .

Kontrollküsimused:

- Kas sõnumivahetuse kaitseks kasutatakse sobivat edastamisel põhinevat või sõnumil põhinevat krüpteerimismeetodit?

- Kas krüptograafiliste funktsioonide rakendamisel kasutati loodud tarkvara teeki?
- Kas veebiteenuse sideliideste jaoks võeti arvesse kättesaadavusnõudeid ja rakendati vastavalt?

M 4.451w Veebiteenuste värsked standardid

Algatamise eest vastutavad: IT-rakenduste eest vastutavad töötajad, IT-juht

Rakendamise eest vastutavad: administraator, IT-juht

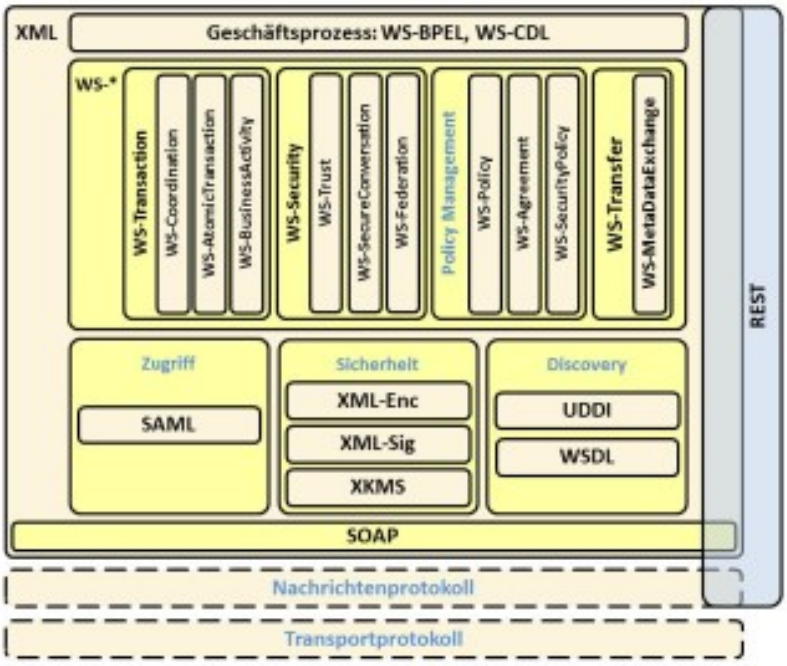
Veebiteenused on tarkvararakendused, mida saab kasutada võrgu kaudu. Need pakuvad mitmesuguseid infotehnoloogial põhinevaid teenuseid kasutamiseks peaaegu mis tahes kliendi kaudu. Keeruliste infotehnoloogiamaastike kooskõlas mängivad veebiteenused järjest tähtsamat rolli. Seejuures on nende teenuste kasutamise juures väga suure tähtsusega turvalisusega seotud aspektid.

Selleks, et tagada veebiteenuste laitmatu integreerimine teenustele suunatud struktuuri (SOA), arendati välja erinevad standardid, mis vaatlevad veebiteenuste kõige erinevamaid aspekte. Eelkõige Organization for the Advancement of Structured Information Standards (OASIS) ja World Wide Web Consortium (WC3) pakuvad selle teema kohta üksteist täiendavaid ja üksteisele üles ehitatud standardeid.

Põhinedes heakskiidetud interneti transpordiprotokollidel, üldistatakse standardites lisaks tehnilistele ja organisatoorsetele teemadele ka turvalisusega seotud aspekte, et arvestada tööprotsessi modelleerimise komplekssete nõuetega.

Turvalisuse seisukohalt kõige tähtsamad standardid on kujutatud järgmises graafikus ja neid esitletakse järgmistes lõikudes. Arvestades teema keerukust ja standardite pidevat edasiarenemist, võib siin esitatu kujutada endast üksnes valikut, mis ei ole kindlasti täielik.

XML-Encryption



Joonis. Encryption on XML-dokumentide krüpteerimise standard. Seda haldab WC3.

XML-Encryption-standard määratleb krüpteerimise erinevad võimalused. Krüpteerida on võimalik terveid XML-dokumente, nende alamelementidega üksikuid elemente või üksikute XML-elementide sisu. Seega on võimalik XML-andmete väga peen krüpteerimine. Krüpteeritud andmed on omakorda XML-dokumendid või nende osad.

Üksikute elementide krüpteerimiseks sobib XML-Encryption eriti siis, kui mitmed mitteusaldusväärsed asutused osalevad teabevahetuses, kuid nad ei tohi teada saada muude vastuvõtjate sõnumeid.

Järgmine näide illustreerib krediitkaardiandmete krüpteerimist sõnumi sees:

<?xml version='1.0'?>
<PaymentInfo xmlns='http://example.org/paymentv2'>
<Name>John Smith</Name>
<EncryptedData Type='http://www.w3.org/2001/04/xmlenc#Element'
xmlns='http://www.w3.org/2001/04/xmlenc#'>
<CipherData>
<CipherValue>A23B45C56</CipherValue>
<CipherData>
</EncryptedData>
</PaymentInfo>

Krüpteeritavad andmed asendatakse XML-Encryption'i rakendamisega alati kõrgemal oleva elemendi EncyptedData kaudu.

Krüpteeritud andmete kõrval võidakse sisestada ka andmeid kasutatavate krüpteerimisalgoritmide, võtme ja plaanitava vastuvõtja kohta. Seega on ka krüpteerimine võimalik mitmete vastuvõtjate jaoks (nt asümmeetrilise krüpteeringuga

Public-Key-taristu raames).

Krüpteeringut saab teostada nii sümmeetriliste kui ka asümmeetriliste meetoditega.

XML-Encryption'i kasutamisel tuleb tähele panna, et kasutada tuleb turvalisemaid krüptograafilisi algoritme. Täiendavad suunised krüptograafiliste algoritmide ja võtmepikkuste kohta sisalduvad BSI tehnilises suunises Krüptograafilised meetodid: soovitused ja võtmepikkused – 2. osa. TLS-i rakendamine (TR-02102-2) ja meetmes M 2.164 Sobiva krüptoprotseduuri valimine .

XML-Signature

XML-Signature määratleb XML-süntaksi elektrooniliste allkirjade jaoks. Funktsioonide poolest sarnaneb XML-allkiri krüpto-standardile PKCS#7, on aga lihtsamalt laiendatav ja sobiv XML-dokumentide jaoks.

XML-allkirjadega võib allkirjastada mis tahes ressursse. Tavaliselt on need XML-dokumendid või nende osad, aga allkirjastada on võimalik ka mis tahes andmeid, mis on adresseeritavad URL-i kaudu.

Kui XML-allkirja kasutatakse, et allkirjastada ressursse, mis jäävad väljapoole ümbritsevat XML-dokumenti, tähistatakse seda kui detached signature, kui allkirjastatakse ümbritseva dokumendi osi, on see enveloped signature, kui allkirjastatavad andmed sisalduvad XML-allkirjas, on see enveloping signature.

Kuna loogilisel XML-struktuuril võivad olenevalt keskkonnast olla erinevad, ühtviisi kehtivad vormid, tuleb usaldusväärseks allkirjastamiseks läbi viia standardne üleminek kanooniliseks vormiks (Canonical XML).

XML-allkirja kasutamisel tuleb nagu ka XML-Encryption'i rakendamisel pöörata tähelepanu tugevate krüptograafiliste meetodite valikule.

XML Key Management Specification

XML Key Management Specification (XKMS) põhineb SOAP-l, XML-allkirjal ja XML-Encryption'il ning lubab XML-i alusel valideerida ja hallata asümmeetrilisi krüptograafilisi võtmeid. Sellega võimaldatakse PKI (Public-Key-Infrastrukture) lihtsat sisestamist SOA-sse.

XML Key Registration Service Specification'i (X-KRSS) abil kirjeldatakse võtmete kasutusaega (registreerimine, tühistamine, uus versioon) ja sinna juurde kuuluvate privaatsete võtmete taastamist.

XML Key Information Service Specification (X-KISS) määratleb juurdepääsu avalike võtmete ja sinna juurde kuuluvate sertifikaatide kinnitamisele.

Usaldusväärne vaheinstants (TrustPoint, mis on samuti veebiteenus) töötleb klientide päringuid ja moodustab liidese olemasolevatele Public-Key-taristutele.

Seejuures saab teostada tsentraalset Trust Management'i, et rakendada vastavaid nõudeid, mis puudutavad juurdepääsukaitset, osavõtjate ringi ja konfidentsiaalsust.

SAML

Security Assertion Markup Language (lühendatult SAML) on XML-il põhinev andmevorming autentimis- ja autoriseerimisandmete vahetamiseks. Sellega saab kirjeldada ja edastada turvalisusega seotud andmeid.

Selle vormingu arendas välja OASIS-konsortsium, võttes arvesse turbenõudeid jagatud IT-keskkondades. Erinevate, ühekordsetel kasutaja sisselogimistel (Single Sign-On) põhinevate rakenduste kasutamise kõrval võib kirjeldada ka jagatud toiminguid paljude osavõtjate ja autoriseerimisteenustega.

SAML Assertion sisaldab kapseldatud turbeinfot, mis väga üldiselt lihtsustatult ütleb järgmist: „Kinnitust A kontrolliti hetkel t kontrollija R poolt subjekti S suhtes tingimusel B". Seega võib lisaks autentimisandmetele edastada ka kinnituse objektide omaduste kohta, mis mängivad juurdepääsuõiguste ja tehingute kulgemise kontrollimisel olulist rolli.

SOAP

SOAP (Simple Object Access Protocol) on võrguprotokoll struktureeritud andmete vahetuseks süsteemide vahel ja protsessisiseseks suhtluseks. See on üles ehitatud tuntud interneti-protokollidele nagu näiteks HTTP või SMTP ning põhineb W3C-standardil XML Information Set andmete esitamiseks. See on World Wide Web Consortium'i (W3C) tööstuslik standard.

SOAP kujutab endast raamistikku, mis kirjeldab sõnumite struktuuri ja teeb kindlaks, kuidas on andmed sõnumitesse sisestatud ja kuidas neid saab lugeda. Kuna kasutajaandmete semantikale ei ole nõudeid määratud, võib üle kanda mis tahes rakendusekohaseid sisusid. Seega võib XML-i kõrval kasutada ka muid andmevorminguid (nagu nt CSV).

SOAP-ga ei saa küll suhelda mis tahes transpordiprotokollide kaudu, kuid praktikas kasutatakse tavaliste võrgustruktuuride ühilduvuse põhjal HTTP-d ja HTTPS-

i.

REST

Representational State Transfer (REST) kirjeldab projekti paradigma veebirakenduste jaoks ja seda saab suures plaanis kasutada veebiteenustel. REST põhineb lihtsatel põhimõtetel, mida tuleb arvesse võtta REST-le vastava veebirakenduse projekteerimisel ja rakendamisel.

Varem projekteeriti REST HTTP-protokolli arvesse võttes, see ei määra aga kindlaks rakendamise üksikasju. Seega ei ole ka nõutavaid protokolle ega standardeid.

REST-d saab hästi rakendada koos HTTP-l või SOAP-l põhinevate veebiteenustega.

Tähelepanu keskpunktis on REST korral lisaks ressurssidele, mida veebirakendus pakub, suhtlusliidese ühtlus. Sinna võib lisaks projekteerida võrgusuhtluse lihtsustatud struktuuri, et tõsta komponentide sõltumatust, laiendatavust ja võrgustatavust.

Täpsemalt kehtivad järgmised põhimõtted.

- Client-Server: serveri ja kliendivahelised vastutusalad on täpselt ära jaotatud (Separation of Concerns). See kehtib eriti just andmetalletuse kohta.
- Oleku puudumine: suhtlus on ilma olekuta. Iga REST-päring sisaldab kõiki andmeid, mida server vajab päringu korrakohaseks töötlemiseks. Tuleviku päringute töötlemiseks ei pea server salvestama klienti puudutavaid andmeid suhtlusprotsessidest.
- Vahemälusobilik: server võib ressursse tähistada vastavalt sellele, kas need sobivad vahemällu. Sellisel juhul saavad kõik võrgusuhtluse jaamad kuni kliendini välja salvestada serveri vastuse vahemälusse ja kasutada seda koostalitluse jaoks.
- Ühtne liides: kliendi ja serveri vahelisele liidesele rakendatakse tarkvaraarendusest tuttavat üldistamise põhimõtet. Seeläbi muutub adresseerimise, suhtluse, andmestruktuuride ja tehingute standardiseerimine REST-le vastava veebirakenduse jaoks kohustuslikuks.
- Mitmekihilisus: kihilise veebistruktuuri sisseviimisega tõstetakse laiendatavust ja paindlikkust. Seejuures tunneb iga komponent ainult enda vahetut suhtluspartnerit ja sellel puudub teave terviksüsteemi muu struktuuri kohta.

Lisaks saab vahekihtide ja prokside kaudu kapseldada ka teenuseid, sisestada vanemaid süsteeme, rakendada turvanõudeid ning jagada ülesandeid ja koormusi.

- Code on Demand: serveril on võimalus anda klientide käsutusse tarkvaraosi, millega laiendatakse kliendi funktsioone. Sellega võimaldatakse kliendile serverist sõltumatuid tegevusi edastatavate andmete alusel.

Liidese standardiseerimise ühtse liidese sobiv põhimõte sisaldab järgmisi nõudeid.

- Adresseerimine: kasutada antud ressursid peavad olema üheselt identifitseeritavad. Selleks pakuvad end URI-d (Uniform Resource Identifier) või URL-id (Uniform Resource Locator).
- Ressursside manipuleerimine esitluste kaudu: tegevused seoses ressurssidega (rakendamine, taastamine, muutmine, kustutamine) viiakse läbi ressursside esitluste kaudu. Seejuures võib soovitud andmeid edastada erinevates esitlusvormides (Media Type) (nt HTML, XML, JSON, PDF).

Soovitud tegevus määratakse kindlaks operatsioonide kaudu, nagu näiteks POST (ressursside loomine), GET (ressursside taastamine), PUT (ressursside värskendamine), DELETE (ressursside kustutamine). Võimalikud on ka oleku, pääsuõiguste, ressursside ajaloo või muude funktsioonidega seotud operatsioonid.

- Isekirjutavad sõnumid: kliendi iga päring ja serveri iga vastus on sõnum ning see peab olema isekirjutav, st et sõnum sisaldab kõiki andmeid, mida vastuvõtjal on vaja, et oma ülesannet korrakohaselt täita.
- Hüpermeedia kasutamine: hüpermeedia on veebirakenduse käiviti. Iga rakenduse oleku manipulatsioon ja iga ressursi taastamine toimub hüpermeedia kaudu. Hüpermeedia tähendab selles seoses, et kõik kliendi jaoks vajalikud veebiteenusesisesed viited muudele ressursside esitlustele ning kõik pakutud tegevused tuleb kasutusse anda veebiteenuse enda kaudu, mis tähendab, et klient ei vaja teadmisi veebistruktuurist, et seda kasutada. Nende andmete kasutamine võib toimuda näiteks XML-struktuuri seotud URL-ina.

Veebiteenuste jaoks tulenevad REST kasutamisest järgmised eelised.
Range ülesannete jaotusega võivad klient ja server olla lihtsalt kujundatud, et võimaldada suuremat koostalitlusvõimet, ja kõiki komponente saab arendada või isegi välja vahetada üksteisest sõltumatult. Suhtluse oleku puudumine lihtsustab mõlemapoolset andmetalletust. Hüpermeedia võimaldab veebiteenuste kasutamist ilma aluseks oleva rakenduse täpse tundmiseta ja lihtsustab SOA-keskkonna orkestreerimist. Liideste ühtsus vajab suurel määral standardiseerimist, mis on süsteemiülese SOA-integratsiooni eeldus. Mitmekihilisus võimaldab läbipaistvat suhtlust ka keerulistes süsteemikeskkondades, millel on kõrged nõudmised kättesaadavuse suhtes.

Web Services Description Language (WSDL)
WSDL on XML-il põhinev metakeel XML-il põhinevate veebiteenuste kirjeldamiseks. WSDL-fail kujutab endast veebiteenuse käivitamiste, parameetrite, andmestruktuuride ja tagastusväärtuste kirjeldust. Lisaks liideste kirjeldusele ja juurdepääsulogidele on olemas kõik vajalikud andmed veebiteenusele ligipääsu tagamiseks. WSDL-i rakendatakse sageli SOAP- ja XML-skeemiga, et orkestreerida XML-il põhinevaid veebiteenuseid jagatud IT-keskkonnas. Klient võib WSDL-failist kindlaks teha, millised funktsioonid on serveris saadaval. Teenuse WSDL-standardist saab automaatselt genereerida lähtekoodi veebiteenuse kasutamiseks SOAPsõnumitega.

UDDI (Universal Description, Discovery and Integration)
UDDI tähistab SOA-keskkonnas standardset kataloogiteenust veebiteenuste jaoks. See mängib tsentraalset rolli kliendinõuete dünaamilisel sidumisel

veebiteenustega. Vajalikke andmeid pakutakse kolmes kataloogis. Valgetel lehekülgedel hoitakse põhiandmeid, need kirjeldavad teenuseosutaja identiteeti. Kollased leheküljed liigitavad pakutavad teenused standardse taksonoomia järgi. Seejuures võib kasutada rahvusvaheliselt tunnustatud standardeid (nt UNSPSC – United Nations Standard Products and Services Code). Rohelised leheküljed säilitavad veebiteenuste liidesekirjeldusi.

Teenuse tehnilised aspektid salvestatakse struktureeritult nn tModel'isse. Selleks et määrata nõuet konkreetsele teenusele, võrreldakse kliendi ja veebiteenuse tModel-kirjeldusi (tModel-Keys) omavahel. Kohustuslikud andmed (binding Template) lisatakse seejärel kliendile dünaamiliselt.

WS-*

Üks tööstuslike standardite omaette rühm on WS-*-standardid. Neid haldavad põhiliselt W3C ja OASIS ja sulgevad lõhe pigem tehnilise iseloomuga veebiteenuse standardite ja tööprotsessi taseme kõrgete nõudmiste vahel. Need on suhteliselt täpselt suunatud rakendusalale, on osaliselt üksteise peale üles ehitatud ja neid võib kombineerida, et luua keerulisi nõudmisi. Siia kuuluvad adresseerimine, kontekst, koordineerimine, töökindlus, metaandmed ja tehing, eriti veel ka konfidentsiaalsus, terviklus ja kättesaadavus, aga ka juurdepääsu juhtimine ja õiguste haldus.

Standardiseerimine võimaldab platvormist sõltumatut ja süsteemiülest keeruliste tööprotsesside moodustamist SOAP ja WSDL alusel. Järgneb WS-*-standardite valik, mis on eriti asjakohased veebiteenuste turvalisuse jaoks.

WS-Policy

WS-Policy on standard, mis lubab veebiteenusel anda teavet oma suuniste kohta, mis puudutavad turvalisust, kvaliteeti ja muid nõudmisi. See on põhistandard raamistiku jaoks, mis võimaldab vajalike ja valikuliste suuniste määratlemise teenuste ja teenusekasutajate jaoks.

WS-PolicyAssertions'i abil kirjeldatakse tervet hulka standardi kinnitusi, mida võib Policy piires kasutada. Policy Assertion kirjeldab käitumisomadust, kohustust või võimalust. Suure hulga neid suuniseid võib omistada veebiteenuse olemile (operatsioon, sõnum, lõpp-punkt) WSDL-is. WS-Policy-standardis ei määrata kindlaks, millised suunised olemas on, see toimub spetsiaalsetes domeenile omastes standardites (turvalisus, tehing ja muud).

WS-PolicyAttachment standardiseerib poliitikate ühendamise WSDL-i ja UDDIga, valikuliselt kirjeldavate elementide piires või väliselt ning osutavalt.

WS-Security

Web Services Security Language (WS-Security, WSS) põhinebXML-allkirjal ja XML-Encryption'il. WS-Security eesmärk on tagada SOAP-sõnumite turvalisem vahetus ning tagada sellega ka sõnumite konfidentsiaalsus ja terviklus.

SOAP täiendusena määrab see täpselt kindlaks, millisel viisil sisestada sõnumitesse krüpteerimisandmeid, allkirju, autentimistõendeid. Seejuures toetatakse autentimistõendite erinevaid mudeleid, muu hulgas X.509-sertifikaate, Kerberos-Ticket'eid, kasutajanime/parooli kombinatsioone ja SAML-Assertion'eid. Sõnum on seega üldiselt kaitstud, kui edastamine toimub läbi mitmete instantside.

Lihtne autentimistõend kasutajanime ja parooliga autentimiseks näeb WS-Security korral välja järgmine:

<wsse:UsernameToken>
<wsse:Username>manfred.testheimer</wsse:Username>
<wsse:Password Type="wsse:PasswordDigest">
59xi0qBCwKxwgmMxU38nOouyqDA=
</wsse:Password>
<wsse:Nonce>Sd7rTLv5W/mLa9eX2a0+rk==</wsse:Nonce>
<wsu:Created xmlns:wsu=
"http://schemas.xmlsoap.org/ws/2002/07/utility">
2013-07-12T14:12:45Z
</wsu:Created>
</wsse:UsernameToken>

Juhuarv (Nonce) ja genereerimise ajahetk, mis mõlemad kuuluvad parooli-hash'i, on valikulised. Kasutada tuleks üht nendest valikutest, sest sellega tõstetakse vastupanu rünnete vastu.

Kerberos-Ticket näeb seevastu WS-Security's välja näiteks selline:

<wsse:BinarySecurityToken
ValueType="wsse:Kerberosv5ST"
EncodingType="wsse:Base64Binary">
SGllciBrb2VubnRlIElocmUgV2VyYnVuZyBzdGVoZW4hCg==
</wsse:BinarySecurityToken>

WS-Transfer

WS-Transfer on SOAP-l põhineva protokolli standard XML-il põhinevate olemite esitluste vahetamiseks veebiteenuse taristu kaudu.

Olemid on seejuures järgmised:

- ressursid, mis on adresseeritavad veebiteenuse kaudu ja millel on XML-i esitlus;
- veebiteenused, mis genereerivad vastavalt XML-esitlusele uusi ressursse (Resource Factories).

Seejuures kantakse ühe toimingu päring ja vastus alati üle XMLdokumentidena.

Võimalik on XML-esitluse otsene manustamine.
Ressursside operatsioonidena on ette nähtud GET (kohustav), PUT ja DELETE (alati valikulised). Resource Factories jaoks on ette nähtud operatsioon CREATE (valikuline).

WS-MetaDataExchange
Veebiteenused kasutavad metaandmeid, et kirjeldada, millisel viisil saab ligi pääseda muudele lõpp-punktidele ja mida tuleb seejuures tähele panna. Selleks kasutatakse eelkõige XML-skeemi, WSDL'i, WS-Policy't ja WS-PolicyAttachment'i.

Selleks, et lihtsustada automaatset juurdepääsu nendele metaandmetele, määratleb WS-MetaDataExchange Metadata Resources, mis võimaldavad tarbijatel teha päringuid veebiteenuse õigeks kasutamiseks vajalike metaandmete suhtes.

Selleks kasutatakse ressursse WS-Transfer-standardi kohaselt, mis sisaldavad vastavaid andmeid pakituna XML-is.

WS-Agreement
SOA-keskkonnas on väited kättesaadavuse, kvaliteedi ja veebiteenuste muude omaduste kohta tarbijate jaoks otsustava tähendusega. WS-Agreement kirjeldab protokolle ja andmestruktuure Service Level Agreement'ide esitlemiseks veebiteenuste jaoks.

Muu hulgas võidakse pakkuda, aktsepteerida, tagasi lükata või lõpetada kokkuleppeid ning võimalik on teha päring kokkuleppe oleku kohta.
Suurem väärtus on pandud paindlikkusele ja laiendamisvõimalusele, et luua erinevates keskkondades domeenile omaseid nõudmisi.

WS-ReliableMessaging
WS-ReliableMessaging on pühendatud usaldusväärsele sõnumite edastamisele. Sellega saab tagada, et sõnumid jõuavad ka üksikute komponentide ülesütlemise korral usaldusväärselt vastuvõtjani. Tänu sellele saab rakendus ühelt poolt reageerida suhtluses esinevatele vigadele ja probleemidele, teiselt poolt saab edastatavaid sõnumeid kontrollida, kas need on jõudnud vastuvõtjani (mittesalgamise kaitse-eesmärk).

See saavutatakse, kui saatja ja vastuvõtja vahele on sisestatud vahenduskiht, mida suhtluses osalejad kasutavad praktiliselt läbipaistvalt. Sõnum edastatakse Reliable Messaging Source'i kaudu vahekihti, antakse vastavate mehhanismide kaudu kaitstult üle ja edastatakse Reliable Messaging Destination'i kaudu tegeli-

kule vastuvõtjale. Suhtlus põhineb SOAP-l ja WSDL-il. Edastamisele võib esitada erinevaid nõudmisi: AtLeastOnce (vähemalt üks kord), AtMostOnce (kõige enam üks kord), ExactlyOnce (täpselt üks kord) ja kombineeritult üksteisega, InOrder (esialgses järjekorras). Kui nõutav edastamine ei ole võimalik, teavitatakse saatjat veast.

WS-ReliableMessaging'i juurde kuulub ka WS-Reliable Messaging Policy Assertion, millega on võimalik kirjeldada suuniseid ümber usaldusväärse sõnumiedastuse, mida saab siduda WS-Policy'ga.

WS-Transaction

WS-Transaction on standard, mis pakub andmebaasimaailmast tuttavat tehingu kontseptsiooni veebiteenuste jaoks. Eesmärk on koordineerida keerulistes keskkondades operatsioonide teostamisel ühiseid tegevusi ning tagada kõikide osalevate teenuste läbipaistev ja järjepidev käitumine.

Selleks on olemas kolm alamstandardit: WS-Coordination tegevuste koordineerimiseks, WS-AtomicTransaction lühikese kestusega tehinguteks ja WS-BusinessActivity pikema kestusega tehinguteks.

WS-Coordination

WS-Coordination pakub laiendamisvõimalusega raami, mis kirjeldab protokolle, mis võimaldavad veebiteenuste koordineerimist jagatud süsteemides. Sellega saab paljude osalejate vahel koostada kokkuleppe, kuidas peaks nende üksikutest tegevustest koosneva tehingu tulemus välja nägema. See pakub ka üldistamisvõimalust olemasolevate koordineerimissüsteemide, näiteks töövoogude (Workflows) jaoks.

Keskse koha (Coordination Service) võtab endale koordineerimine ja võimaldab osalejate registreerimist koordineerimise konteksti piires.

WS-AtomicTransaction

WS-Atomic Transaction põhineb WS-koordineerimisel ja määrab kindlaks ainult lühikese kestusega tehingute protokolli, mille jaoks on olulised ACID-omadused:

Atomicity (eraldatus), Consistency (järjepidevuse säilitamine), Isolation (isoleerimine), Durability (kestvus).

Selleks on ette nähtud järgmised protokollid: Completion (tehingu algataja jaoks), Volatile Two-Phase Commit (lühiajaliste ressurssidega osalejad, nt vahemälud) ja Durable Two-Phase Commit (mittelühiajaliste ressurssidega osalejad, nt andmebaasid).

Atomic Transaction'i saab edukalt lõpetada üksnes siis, kui kõik osaülesanded on edukalt lõpetatud. Kuna eeldatakse, et kõik osalejad tegutsevad ühiselt, tuleks Atomic Transactions'it kasutada ainult usaldusväärses keskkonnas.

WS-BusinessActivity

WS-BusinessActivity põhineb samuti WS-Coordination'il ja määratleb Business Activity koordineerimistüübi. See koordineerimistüüp on mõeldud kasutamiseks pikaajaliste tegevuste korral, millest võtavad osa erineva usaldusväärsusega osalejad (Trust Domains).

Business Activity võimaldab osalejatele vastastikust lepingut, mis puudutab jagatult teostatavaid operatsioone. Oluline tunnus on, et operatsioone võib pesastada suvaliselt (Nested Scopes). Seejuures võib kasutada ka Atomic Transaction'eid.

Erinevalt Atomic Transaction'ist võib Business Activity ka siis edukalt lõpetada, kui üksikud, alluvad tegevused ebaõnnestuvad. Otsuse võtab selle kohta vastu tegevuse algataja. Sellega saab kujutada ka keerulisi töö- ja otsustamisprotsesse ning kaasatud võivad olla erineva koostöövõimega osalejad.

WS-Trust

WS-Trust on WS-Security laiendus ja võimaldab teatud subjektide kokkulepitud omadusi domeenide sees ja vahel (Trust-domeenid). Seejuures on tegemist Security Token'ite väljaandmise, uuendamise ja valideerimisega ning turvalise sõnumivahetuse vahendamise, ülesehituse ja hindamisega WS-Trust hõlmab veebiteenuse kirjeldust, mis annab välja WS-Security'ga ühilduvaid Security Tokens'eid (Security Token Services, STS). Lisaks sellele määratakse kindlaks sõnumite vorming, mida kasutatakse suhtluseks ümber Security Tokens'ite, samuti mehhanismid krüptovõtme vahetamiseks.

WS-SecureConversation

WS-SecureConversation järgib sessioonipõhise turvalisuse lahendust. Sellega toetab WS-SecureConversation turbekonteksti, mis genereeritakse pärast esimest autentimist. Turbekontekst võimaldab kestvat kaitstud suhtlust paljude sõnumite või tehingutega ja vähendab seejärel suhtluse kaitset. Seda standardit tuleks kasutada eriti siis, kui veebiteenuste vahel tuleb vahetada iseäranis suurt hulka sõnumeid.

WS-Secure-Conversation'i kaudu genereeritud turbekontekst koosneb ühisest sessioonivõtmest, mida tähistatakse ka kui SecurityContextToken-Element'i.

Pääsmike vahetus osapoolte vahel toimub Diffie-Hellmann-meetodiga ja seda kasutatakse krüpteerimiseks ja dekrüpteerimiseks.

Turbekonteksti genereerimiseks on olemas järgmised võimalused:

- Security Token Service'ite (STS) kasutamine koos WS-Trust'iga: suhtluspartnerid usaldavad välist teenust, mis on vastutav pääsmike genereerimise eest;

- genereerimine ja jaotamine suhtluspartneri kaudu: suhtluspartner vastutab pääsmiku genereerimise ja jaotamise eest. See eeldab, et kõik osalised usaldavad väljastajat;
- genereerimine Challenge/Response-meetodiga.

Täiendavalt on olemas mehhanismid turbekonteksti uuendamiseks, muutmiseks, laiendamiseks või lõpetamiseks.

WS-Federation

WS-Federation on tihedalt seotud WS-Security'ga ja kirjeldab paindlikku taristut liit-identiteetide jaoks. Selle kontseptsiooni korral ei hallata identiteete ühest tsentraalsest instantsist, vaid jagatud instantsidest, mis vastutavad alati teatud rühma identiteetide eest (nt asutuse töötajate jaoks). Üksikud identiteedi haldamise instantsid on omavahel seotud ja usaldavad vastastikku üksteist.

WS-Federation võimaldab identiteetide, atribuutide ja autentimisprotseduuride vahetamist erinevate turbekontekstide vahel. Seejuures kasutatakse WS-Trust'i ja WS-MetadataExchange'i.

WS-SecurityPolicy

Web Service Security Policy Language (WS-SecurityPolicy) kirjeldab turvalisusel põhinevat Policy Assertions'it. Sellega mõeldakse spetsiaalseid tagatisi, mida veebiteenused peavad täitma, et oleks täidetud turvalisusega seotud aspektid.

Standard laiendab põhilisi turbeprotokolle, mis on määratletud WS-Security's, WS-Trust'is ja WS-SecureConversation'is, mis seisneb selles, et pakutakse mehhanisme, mis kujutavad endast veebiteenuste nõudeid ja omadusi kui tagatisi (Policies).

Web Single Sign-On

Web Single Sign-On Interoperability Profile ja Web Single Sign-On Metadata Exchange Protocol on identiteedi halduse standardid, mis peavad tagama koostalitluse WS-Federation'i ja Liberty Alliance'i protokollidega. Need põhinevad muu hulgas SAML-il ja WS-MetadataExchange'il.

Eesmärk on integreerida veebiteenuse lahenduste identiteedi haldus ja võimaldada juurdepääs koondatud identiteetide omadustele. Sellega saab võimalikuks platvormiülene, tsentraliseeritud identiteedi haldus, millega kaasneb veebiteenuste juurdepääsu juhtimine.

WS-BPEL

Web Services Business Process Execution Language (WS-BPEL) on keeleline määratlus veebiteenuse tegevuste määratlemiseks tööprotsesside sees. Seda kasutatakse veebiteenuste orkestreerimise kirjeldamiseks ja see põhineb WSDL-il.

Kirjeldust ennast kasutatakse teisalt kui veebiteenust.

Basic Activities (põhitegevused) ja Structured Activities (tegevuste keerulised protsessid) kõrval on ette nähtud ka Scopes (seotud tegevused), mis võimaldavad ka veakäsitlust, sündmuste käsitlust, lõpetamise käsitlust ja kompenseerimise käsitlust.

Seoses sellega on võimalikud ka pikaajalised tehingud.

Veebiteenuste funktsionaalse hargnemise ja kompositsiooni kaudu on tagatud kõrgetasemeline paindlikkus.

Laiendustega WS-BPEL4People ja WS-Human Task käsitletakse ka inimsekkumist tööprotsessidesse.

WS-CDL

Web Services Choreography Description Language'i (WS-CDL või ka WSC-horeography) kasutatakse ka veebiteenuste koreograafiaks. XML-il põhinev keel kirjeldab vahetut suhtlust veebiteenuses osalejate vahel vaatlusperspektiivist, mille abil defineeritakse osaliste käitumist. Seejuures kirjeldatakse suhtlemisstruktuuriga veebiteenuse mittefunktsionaalseid omadusi. Eesmärk on kirjeldada ülemaailmset olukorda, mida osalejad omad käitumisega jäljendavad, mis ei tunne aga tsentraalset kontrollinstantsi. Koreograafia defineerib korduvkasutatavad üldised reeglid, mis juhivad osalistevahelist sõnumivahetust, ja ühise käitumise võimalikke mustreid, mis on kokku lepitud kahe või enama koos tegutseva osaleja vahel. Eeskirjade korduvkasutus võimaldab ka keeruliste koreograafiate puhul lihtsustatud kompositsiooni. Oluliste suhtlusele esitatavate nõudmistena tuvastati ja rakendati viis turvalisusega seotud aspekti: autentsus, terviklus ja konfidentsiaalsus ning mittesalgamine ja aruandekohustus. Seejuures arvestati ka nõudmistega vastavalt allkirjaseadusele. Seega on allkirjaseaduse kohaselt võimalik valida edasijõudnud ja kvalifitseeritud elektroonilise allkirja vahel koos pakkuja akrediteerimisega või ilma. Standardi teise versiooniga väärtustati eriti nõudmisi veebiteenuste kasutamisel. Laiendus võttis selle kohaselt arvesse eelkõige rahvusvaheliselt tunnustatud WS-standardeid.

M 4.452 Veebiteenuse seire

Algatamise eest vastutavad: IT-juht, üksikute IT-rakenduste eest vastutavad töötajad

Rakendamise eest vastutab: administraator

Süsteemi turbeseisundi mõistmiseks on hädavajalik rakendada pidevat järelevalvet. Niisuguse seire eesmärk on tuvastada kehtivate turvaeeskirjade rikkumisi, avastada võimalikke olemasolevaid turvaauke ja tuvastada turvaauke tekitavaid väärkonfiguratsioone. Veebiteenuse turbekontseptsiooni ühe osana tuleb seepärast välja arendada seire kontseptsioon. Keerukamate süsteemide nagu nt veebiteenuste puhul ei ole mõeldav, et seirega tegelevad vaid mõned üksikud administraatorid, st kontroll peab aset leidma automaatselt vastavate süsteemikomponentide või toodete poolt. Veebiteenuste seire tuleb kohandada vastavalt muudatustele. Lisaks tuleb veebiteenuse seire planeerimisel arvesse võtta põhimõtteliselt kõiki vastavaid komponente. Seetõttu peaksid seire kontseptsioonis sisalduma näiteks ka andmebaasid ja kataloogiteenused, sõltuvad ja kasutatud veebiteenused ning vastavad IT-süsteemid.

Sellel on eriline tähtsus siis, kui erinevad teenused on omavahel ühendatud Enterprise Service Bus'i (ESB) kaudu.

Kättesaadavuse ja jõudluse järelevalve

Kui teenused langevad rivist välja, nende liidesed muutuvad või reaktsiooniajad halvenevad, võivad sellel olla kaugeleulatuvad tagajärjed mitmetele sõltuvatele süsteemidele. Seepärast tuleb veebiteenuste kättesaadavuse ja jõudluse üle teostada nõuetekohast järelevalvet.

Lisaks veebiteenuse üldisele kättesaadavusele ja aktiivsusele ning vastavalt liideste teenustele ja sõltuvussuhetele tuleks seetõttu jälgida ka jõudluse parameetreid.

Siia kuuluvad näiteks:

- päringute reaktsiooniajad,
- päringute või taotluste arv,
- taotluste ja vastuste suurus või
- salvestite täituvuse tasemed (nt JVM salvesti, Message-Queues).

Seepärast tuleb ühelt poolt väärkonfiguratsioonid või tehniliste põhjustega kitsaskohad ning teiselt poolt denial-of-service-tüüpi ründed varakult tuvastada ja neid kiirest käsitleda. Eriti, kui on tegemist kõrgete nõudmistega kättesaadavusele ja veebiteenuse jagamisel mitmetele süsteemidele, tuleb jälgida koormuse jaotumist.

Teated

Lisaks tuleks pidevalt hinnata logifaile ja süsteemiteateid (Notifications), mis puudutavad vastavaid teateid. Selle jaoks tuleks vastavas veebiteenuses konfigureerida kaitsevajadusele suunatud logitasand (vt ka M 4.397 Veebirakenduste

turvet puudutavate sündmuste logimine).

Järelevalve alla võivad kuuluda näiteks järgmised teated:

- vea- või hoiatusteated,
- volituste rikkumist või muutmist puudutavad teated (nt administraatori volituste andmine),
- turvalisusega seotud seadistuste muutmist puudutavad teated,
- kehtetuid XML-sõnumeid puudutavad teated või
- veateated, mis puudutavad liideste sobimatust.

Kõrgema kriitilisusega teated peaksid äratama vastutava töötaja tähelepanu, et tagada reageerimine sobiva aja jooksul. Selle jaoks soovitatakse kasutada alarmeerimissüsteemi.

Poliitikate järelevalve
Sellega seoses tuleks arvesse võtta ka erinevaid teateid, mis puudutavad eksimist kehtestatud poliitikate vastu (nt WS-Policies, WS-SecurityPolicies).

Need võivad sisaldada näiteks järgmist:

- eksimine kindlaksmääratud sõnumisuuruse vastu,
- eksimine sõnumitele kehtestatud krüpteerimisnõude vastu,
- vead sõnumisisude krüpteerimisel või dekrüpteerimisel,
- vead sõnumisisude allkirjas või
- väär autentimine.

Teenuse krüpteerimise seire
Kui kõrgemate konfidentsiaalsusnõuete tõttu kasutatakse krüpteerimismeetmeid (nt TLS), tuleks teostada järelevalvet nende funktsioonide üle. Just veebiteenuse automaatse funktsiooni tõttu on olemas oht, et krüpteerimisel esinevaid vigu ei märgata õigeaegselt.

Krüpteerimise seire lähtepunktid on näiteks järgmised:

- veebiteenuse sertifikaadi ajakohasus ja kehtivus,
- päringuid tegevate teenuste sertifikaatide ajakohasus ja kehtivus,
- vea- või hoiatusteated krüpteeritud ühenduste ülesehitamisel (nt vananenud SSL-versioonide hoiatusteated)

Hindamine piirväärtuste ja trendide kaudu
Ohtude ja kitsaskohtade õigeaegseks tuvastamiseks tuleb kindlaks määrata piirväärtused ning tuletada jälgitavatest väärtustest trendid, näiteks hõivatud mäluruum, süsteemi koormus või kasutatud ribalaius. Piirväärtuste ja kõikide kriitiliste trendide abil tuleks seire kontseptsiooni raames kindlaks määrata tegevussuunised.

Kontrollküsimused:

- Kas veebiteenuste jaoks on olemas seire kontseptsioon?
- Kas teostatakse asjakohast kättesaadavuse ja jõudluse seiret?
- Kas operatsioonisüsteemide ja teenuste teateid jälgitakse asjakohaselt?
- Kas on tagatud kiire reageerimine kriitilistele teadetele?
- Kas rakendatud poliitikate üle teostatakse nendest kinnipidamise suhtes järelevalvet?
- Kas krüpteerimisfunktsioonide üle teostatakse asjakohast järelevalvet?
- Kas on määratletud piirväärused ja trendid ning kas neid toetavad tegevussuunised?

M 4.453z Pääsmikuteenuse (Security Token Service) kasutamine

Algatamise eest vastutab: IT-juht

Rakendamise eest vastutab: administraator

Pääsmikuteenus (Security Token Service (STS)) on veebiteenus, mille kaudu saab taotleda, uuendada ja kontrollida identiteedi- ja volitustega seotud andmeid. Selle printsiip seisneb identiteedimudeli nõudepõhises (claimes-based) põhimõttes, kusjuures nõue (claim) tähendab olemi väidet teise olemi või enda kohta, kas näiteks kasutajatunnuse või teatud õiguse kohta. STS-i võib kasutada, et kanda üle autentimist ja autoriseerimist või kui STS-i kasutavad paljud rakendused ja teenused, siis et teostada Single Sign-on'i. Põhimõtteliselt viiakse läbi teenuste ja nende käivitajate eraldamine, mille järel ei pea teenus usaldama iga üksikut käitajat seoses edastatavate identiteediandmetega enam otse, vaid ainult STS-i. Sealjuures võib käitaja olla samuti veebiteenus (Web-Service-autentimine), aga ka kliendirakendus või veebilehitseja (passive client), kusjuures viimasel juhul esineb STS kui veebirakendus (Web-SSO).

Lihtsustamine seisneb selles, et mitte iga rakendus või teenus ei pea juhtima kasutajate autentimist, kasutajakontode haldamist ja paroole, kataloogiteenuste ühendamist ja integreerimist asutuse järgmistesse identiteedi ja juurdepääsu kontrollimise süsteemidesse. Oma olemuselt on sellel struktuurivahetusel siiski tähelepanuväärsed tagajärjed turvalisusega seotud küsimustele.

Kuna STS kujutab endast samuti veebiteenust, tuleb selle kohta rakendada mooduli B 5.24 Veebiteenused . See meede hõlmab edaspidi lisaks STS-i kasutamise aspekte muu veebiteenuse kaudu, vajaduse korral ka teise asutuse kaudu. Praktikas on STS sageli juba olemas. Kui ei kasutata enda käitatavat STS-i, on tegemist autentimisfunktsioonide väljasttellimisega. Seetõttu tuleb järgida ka mooduli B 1.11 Väljasttellimine (Outsourcing) . Individuaalse kokkuleppe korral STS-pakkujaga tuleb lepingutingimused kokku leppida nii, et oleks tagatud juurdepääsukontrolliga kaitstud andmete kaitse. Vastasel juhul tuleb pakkuja lepingutingimusi kontrollida selles osas, kas need vastavad kaitsevajadusele.

See, kas teatud STS-i võib kasutada rakenduse jaoks, sõltub rakenduse kaitsevajadusest ja muude meetmete võimalusest tugevdada veelgi juurdepääsukontrolli kaitset, näiteks kahefaktorilise autentimisega. Usaldust pakkuja suhtes tuleb põhjendada selgete kriteeriumidega ja nendest kinnipidamise kehtivusega. Aga ka siis, kui STS-i käitatakse oma asutuse sees, leiab autentimise väljasttellimise korral kaitsevajaduse ülevõtmine aset STS-il, millega kaasnevad kumulatsioonimõjud, kui paljud rakendused ja teenused esinevad tarbijatena. Tuleb lähtuda selles, et STS võtab üle oma kaitsevajaduse konfidentsiaalsuse ja tervikluse osas nende andmete maksimumpõhimõtte järgi, millele pääseb ligi nende kasutamise kaudu. Kättesaadavuse osas võib samuti tekkida olukord, kus STS on ainule kasutamiseks tõhus autentimise võimalus. Lisaks tuleb arvesse

võtta kumulatsioonimõjusid, juhul kui STS võtab üle autentimise suure hulga teenuste ja asutuste jaoks.

Siia lisandub asjaolu, et STS-il ei hoita ainult andmeid selle kohta, millisel kasutajal on millised nõuded, vaid et pääsmike päringutega kogunevad ka andmed selle kohta, milline kasutaja millist teenust, kui sageli ja millises kontekstis kasutab. Kui kasutajad on inimesed, tuleb arvestada privaatsfääriga (pöörates tähelepanu moodulile B 1.5 Andmekaitse), kui kasutajad on masinad, tuleb arvestada metaandmete konfidentsiaalsusega.

STS-i teostamine on võimalik erinevate tehnoloogiate (nt REST) abil, praktiliselt rakendatakse STS-i ometi sageli SOAP abil. Siinjuures kasutatakse üldiselt WS-*-perekonna standardeid, et tagada funktsionaalsus ja koostalitlus.

Security Tokens'i termin on Standard WS-Security's defineeritud kui mis tahes andmeobjekt, mis sisaldab üht või enamat nõuet, st kinnitatud väidet olemi kohta ja selle võib lisada SOAP-sõnumile. Sageli on Security Token'id digitaalselt allkirjastatud, et tõestada väite kindlust krüptograafiliselt.

WS-Security toetab erinevat tüüpi Security Token'eid, isegi Username Token'it autentimiseks kasutajatunnuse ja parooli abil. Parool kantakse sealjuures üle kui räsiväärtus, mille arvutusse on kaasatud Nonce (juhuslik väärtus) ja ajatempel, et takistada Replay-tüüpi ründeid. Teine ettenähtud pääsmikutüüp on BinarySecurityToken mitte XML-il põhinevate vormingute jaoks nagu X.509-sertifikaat.

Järgmised pääsmikutüübid on ette nähtud kasutamiseks laiendusmehhanismi kaudu.

Enamik STS-e kasutab tänapäeval pääsmikke, mida kirjeldatakse Security

Assertion Markup Language'is (SAML). Seejuures on tegemist laiendatud standardiga nõude kirjeldamiseks. SAML Security Token (täpsemalt SAML Assertion, standard, mis sisaldab peale selle veel muid elemente, mida vajab siiski eelkõige Web-SSO) on identiteediandmete, atribuutide, autentimis- ja autoriseerimisotsuste kirjeldus XML-is, mis on laiendatav asjakohastel eesmärkidel.

SAML-standard on alates versioonist 1.1 versioonini 2.0 oluliselt laienenud ja hõlmab nüüd täiendavaid protokolle ja kasutusstsenaariume (profiles), mis põhiliselt keerlevad Web-SSO ümber. Igal juhul tuleb vastu võtta põhjapanev otsus toimivates ja koostalitlevates rakendustes olemasoleva standardite kogumi kohta, mis ühilduvad omavahel ja plaanitud suhtluspartneritega ning vastavad kõikidele turbenõuetele.

Standardis WS-Trust, mis rajatakse WS-Security'le, defineeritakse STS-i selle tegevustega. Kui server nõuab autentimist, saadab klient Request for Security Token'i (RST), näiteks oma kasutajanime ja parooliga Username Token'i kujul STS-ile. Siinjuures võib kindlaks määrata, millist pääsmikutüüpi vajatakse, milline nõue peab pääsmikus sisalduma ja kuidas väljastatavat pääsmikku kaitsta. STS saadab tagasi Request for Security Token Response'i (RSTR), mis sisaldab Security Token'it, mille klient saab nüüd esitada serverile. Seda saab ta vastavalt olukorrale kas allkirja abil ise kontrollida või esitada uuesti kontrollimiseks STS-ile.

Selleks et turvapääsmik oleks usaldusväärne, tuleks see kas sel moel allkirjastada, et seda oleks võimalik kontrollida või tuleb ülekannet muul moel järjekindlalt kaitsta, näiteks edastamistasandil. Kuna STS-i allkiri kehtib siiski ka nõude kinnitusena Security Token'is, peaks selle puudumise kompenseerima muude meetmete nagu näiteks turvalise autentimisega andmevahetuse ajal.

Konfidentsiaalseid andmeid nagu näiteks paroole ei tohi kunagi STS-ile või sealt tarbijatele kaitsmata üle kanda. Siin tuleb alati kasutada turvalist räsimeetodit juhusliku komponendiga (Salt, nt koos Nonce'iga). Lisaks tuleb Replay-tüüpi ründeid takistada nõuetekohaste meetoditega, näiteks ajatemplite kasutamisega, kui edastuskanal neid juba ise usaldusväärselt ei tõrju.

Kui Security Token ei võta ette otsest, krüpteeritud teed STS-ist serverisse, tuleb ka selle sisu krüpteerimisega kaitsta, et hoida ära olukord, kus volitamata kolmas isik saab pääsmikku kasutada autentimiseks. Piisab, kui krüpteerida krüptograafiline osa, st STS-i allkiri. Kui Assertion sisaldab siiski muid konfidentsiaalseid andmeid, tuleb ka neid kaitsta. Põhimõtteliselt tuleb aga vajalikku konfidentsiaalsust minimeerida andmete kokkuhoiu põhimõttega, küsides alati võimalikult üldisi nõudeid (nt „Kasutaja on täisealine").

Järgmine kaitsemeede on kehtestada pääsmikule vastavalt kaitsevajadusele lühiajaline kasutusaeg, et vähendada kahju väära kasutamise korral. Enamik Framework'e annab siin standardid, mida võiks võimaluse korral lühendada.

Paljud omavahel seotud standardid koos nende erinevate versioonide ja standardiseerimisastmega tõid minevikus sageli esile rakendusi, mille turvalisus oli oluliselt kahjustatud või puudus üldse. Kuna aluseks olevate turbefunktsioonide puhul on tegemist XML-Encryption'i, XML-allkirjade ja sageli TLS/SSL-iga, on vastavatel rünnetel ka siin oma roll, mis on seda olulisem, mida rohkem kriitilisi autoriseerimisotsuseid STS-id teevad.

Ründed nagu XML Signature Wrapping, st sõnumi pahatahtlik muutmine, ilma et allkiri muutuks kehtetuks, on võimalikud eelkõige tänu sellele, et allkirjade genereerimist ja kontrollimist ei kooskõlastata üksteisega. Siin tuleks kasutada kas sama tarkvarabaasi või, kui see ei ole võimalik (nt väline STS, XML-Gateways), viiakse pärast iga kohandamist läbi liideste põhjalikud testid. Põhimõtteliselt tuleb STS-i funktsioonide teostamiseks valida välja juurdunud, hästi testitud teegid ja raamistikud, mille kohta on andmed kitsaskohtade ja turvapaikade suhtes ajakohaselt saadaval ning mis tuleb sisse kanda. Sidekanalite kaitsmisel tuleb tähelepanu pöörata meetmele M 4.450 Veebiteenuste andmeside turve . Igal juhul tuleb keerulise teema puhul kasutada tingimata oskusteavet, mis puudutab STS-i turvalist rakendamist kontseptsioonifaasi jooksul.

Kontrollküsimused:

- Kas STS on ka ise modelleeritud kui veebiteenus ja kas sellele vastavalt rakendatakse asjakohaseid meetmeid moodulist B 5.24 Veebiteenused ?
- Kas võõra STS-i kasutamisel järgiti moodulite B 1.1 Organisatsioon ?
- Kas SSL/TLS-i konfiguratsiooni kontrolliti enne kasutamiseks loa andmist vigade osas ja kas olekut valideeritakse korrapäraste ajavahemike järel?
- Kas lepingutingimused STS-käitajaga vastavad STS-i kaudu ligipääsetavate andmete ja rakenduste kaitsevajadusele?
- Kas arvesse võeti STS-il kogunenud andmete konfidentsiaalsust?
- Kas andmete kokkuhoidu teostatakse pidevalt võimalikult üldiste nõuete kaudu?
- Kas STS-funktsioonide kasutamiseks valiti välja väljatöötatud teegid ja raamistikud, mille jaoks on saadaval ka ajakohased andmed kitsaskohtade ja turvapaikade kohta?
- Kas pääsmikud allkirjastatakse või krüpteeritakse edastuskanalil järjepidevalt ning autenditakse?
- Kas kõik paroolid kantakse üle kui räsiväärtus kaitsega brute-force-tüüpi ja replay-tüüpi rünnete vastu?
- Kas Security Token'i jaoks valiti võimalikult lühike kasutusaeg?

M 4.454 Veebiteenuste kaitsmine keelatud kasutuse eest

Algatamise eest vastutavad: IT-rakenduste eest vastutavad töötajad, IT-juht

Rakendamise eest vastutavad: administraator, IT-juht

Tagamaks, et veebiteenuseid kasutavad üksnes selleks volitatud osapooled, tuleb esitada konkreetsed nõuded üksikute kasutajate või klientide autentimisele ja volitamisele. Need nõuded tuleb realiseerida hoolikalt valitud autentimis- ja volitamismudeli raames ühe või mitme saadaoleva WS-Standard'i kombinatsiooni abil. See tagab veebiteenuse üksikute juurdepääsude piiramise ja kontrolli. Seda, milliseid veebiteenuse standardeid võib nõuetekohase autentimise ja volitamise rakendamiseks kasutada, on kirjeldatud meetmetes M 4.455 Volitamine veebiteenustes ja M 4.456 Autentimine veebiteenustes .

Selleks, et raskendada ründeid veebiteenustele, mis halvimal juhul toovad kaasa volituste süsteemi tühistamise ja võimaldavad koos sellega volitamata juurdepääsu konfidentsiaalsetele andmetele või kaitsmist vajavatele funktsioonidele, tuleks kasutada täiendavaid meetmeid veebiteenustele tehtavate brute-forcetüüpi rünnete või muude automatiseeritud rünnete vastu. Automatiseeritud ründed eristuvad suure arvu juurdepääsukatsete poolest lühikese ajavahemiku jooksul. Suure külastatavusega päringud (näiteks paroolide äraarvamiseks) tuleks tuvastada kindlaksmääratud piirväärtuste järgi ja see peaks kaasa tooma nõuetekohased reageeringud (vastutavate isikute alarmeerimine, juurdepääsu lukustamine). Sellised piirväärtused võivad olla seotud näiteks juurdepääsude arvu, veateadete, ülekantava andmehulga või ülekantavate XML-sõnumite suurusega. Tuvastatud ründekatse korral võib juurdepääsu ajutiselt lukustada. Alternatiiviks juurdepääsu lukustamisele on vastuste lisanduv viivitus (st iga valekatsega kasvav ooteaeg), mis pidurdab tõhusalt automatiseeritud ründeid.

Piirväärtuste kindlaksmääramisel tuleb tähelepanu pöörata sellele, et seadusliku teenuse kasutaja (kliendid ja nende kasutajad, teised veebiteenused) jaoks ei piirataks veebiteenuse funktsioone ja teenindust. Põhimõtteliselt tuleks alati tagada, et veebiteenusele tohivad ligi pääseda ainult volitatud süsteemid või kasutajad. Tulemüüri kaudu võib kindlaks määrata, kas veebiteenusele pääsevad ligi üksnes volitatud IP-aadressid või IP-aadressiplokid. Suletud keskkondades saab kasutada Whitelisting-lahendust. Kui käitatakse veebiteenust, mis peaks olema internetist kättesaadav (nt API-d vabaks kasutamiseks kolmandale isikule), on soovitatav kasutada Blacklisting-lahendust.

Tuntud IP-aadresside lukustamisega, mida võib määrata näiteks rämpsposti serveriteks, võib kindlaks teha, et süsteemide, mida tuleb käsitleda pahatahtlikena, juurdepääsud on välistatud. Selliste lukustusnimekirjadega saab takistada ka

volitamata juurdepääse kindlatest piirkondadest või riikidest. Alternatiivselt võib IP-aadressiplokkide lukustamist teostada ka teenuseosutaja. Tulemüüri vastava konfiguratsiooniga saab tagada, et silmatorkavalt sagedased käivitamised ühelt IP-aadressialalt või üksikult IP-aadressilt piiratakse, et osutada vastupanu võimalikule denial-of-service-tüüpi ründele.

Teist võimalust, et piirata juurdepääsu veebiteenusele ainult volitatud kasutajatele, pakub VPN-i kasutamine. Näiteks saab asukoht-asukohta-VPN-iga tagada, et ainult valitud ring äripartnereid saab konfidentsiaalsust ja terviklust säilitades veebiteenusele ligi pääseda. Täiendavad juhised VPN-ide kasutamise kohta leiduvad moodulis B 4.4 Virtuaalne privaatvõrk (VPN) . VPN aitab kaasa veebiteenuse kaitsmisele, sest veebiteenuse suhtes ei saa läbi viia brute-force-tüüpi ründeid, sest need on teostatavad ainult sisevõrgust ja ei ole seega internetis nähtavad.

Veebiteenused on tihti rajatud sellele, et neid võib käivitada nii siseselt kui ka väliselt (nt äripartneri kaudu), mille korral saab alati toimuda üks juurdepääs erinevatele funktsioonidele. Välistel kasutajatel võib olla võimalus ainult tellimuse esitamiseks, samal ajal kui sisekasutajatel on olemas ka võimalus sissetulnud tellimusi hallata ja töödelda. Sageli pakutakse neid erinevaid funktsioone sama veebiteenuse lõpp-punkti kaudu. Kuna kõik funktsioonid on siiski käivitatavad sama lõpp-punkti kaudu, võib väline ründe toimepanija WSDL-failide lugemise või muude andmete hankimise meetoditega kindlaks teha sisemiste funktsioonide käivituspunktid, et manipuleerida või lugeda andmeid. Sel põhjusel tuleks veebiteenuse teostamisel pöörata tähelepanu sellele, et funktsioonide andmine sisemiste ja väliste käivitajate käsutusse ei toimu samal lõpp-punktil.

Ideaaljuhul asuvad erinevad veebiteenuse lõpp-punktid erinevatel süsteemidel.

Juurdekuuluvate URL-ide eraldamisega saab siis teostada tulemüüri kaudu ka ülitäpse kontrolli veebiteenusel, sest veebiteenus on käivitatav erinevate URL-ide ja portide kaudu, või isegi ainult kindlatest võrkudest.

Kui ei soovita, et teatud operatsioonidele juurde pääsetakse, võib ka XMLstruktuuri (skeemi) kirjeldus teenuse käivitamiseks olla muudetud nii, et soovimatud operatsioonid eemaldatakse. Kui esitatakse päring, mis sisaldab skeemist eemaldatud operatsiooni, tuvastatakse see XML-päringu valideerimise raames skeemi suhtes kui mittekehtiv ja lükatakse tagasi.

Juurdepääsu piirang veebiteenusele teenuse kasutajate autentimise ja volitamise kaudu võib osutuda kasutuks, kui rünne saavutab mõju enne, kui pääsukontrolli mehhanismid maksvusele pääsevad. Sel põhjusel peab eel-

nevalt toimuma kogu sõnumi asjakohane valideerimine, enne kui veebiteenus seda edasi töödelda tohib. Seda protsessi nimetatakse ka skeemi valideerimiseks.

Skeemi valideerimisega tagatakse, et tõrjutakse sõnumid ja ründed, mis kalduvad defineeritud skeemist kõrvale. See tähendab, et skeem peab olema kujundatud nii suurte piirangutega kui võimalik, mis tähendab, et ainult piiratud kogus XMLvorminguid võib olla teenuse kasutamiseks kättesaadav. Skeemi valideerimisel on seejuures vajalik piirata skeemi nii, et välistatakse tuntud ründemustritega sõnumid. Lisaks tuleb sõnum kindlas järjekorras läbi uurida, mida saab kasutada injektsiooni rünnete jaoks (vt G 5.174 Injektsiooniründed).

Lisaks tuleb veebiteenuse skeemid sobitada nii, et töödeldakse ainult kuni teatud suurusega sõnumeid. Ülisuure sõnumi töötlemine võib töötleva süsteemi ressursid üle koormata ja tuua seega kaasa jõudlusekaod või katkestused töös.

Sõnumi suuruse piiramisel tuleb tähelepanu pöörata sellele, et töödelda ei tohi piiranguteta sõnumiosi, millel on järgmised tunnused:

- xsd:any,
- xsd:anyType,
- xsd:anySimpleType,
- elementide või tüüpide rekursiivne määratlus,
- piiramatud loendid.

Skeemi valideerimine võib toimuda kas juba XML-lüüsil või otse süsteemil, mis veebiteenust pakub. Otsuse, kus valideerimine peab toimuma, peab tegema juba planeerimisfaasis, sest sellel võivad olla mõjud ka üldstruktuuri jaoks.

Kontrollküsimused:

- Kas autentimise ja volitamise jaoks on valitud ja rakendatud nõuetekohased standardid?
- Kas on rakendatud meetmed, mis võivad tuvastada automatiseeritud ründed ja neid tõrjuda, näiteks piirväärtuste järelevalvega päringute jaoks?
- Kas sellega on tagatud, et veebiteenusele pääsevad ligi ainult volitatud osalised?
- Kas toimub sisemiste ja väliste operatsioonide eraldamine ja kas on tagatud, et ainult vastavad kasutajad tohivad enda jaoks vajalikke operatsioone käivitada?
- Kas XML-skeem on üles ehitatud vastavate piirangutega ja kas skeemist kinnipidamist kontrollitakse?

M 4.455 Volitamine veebiteenustes

Algatamise eest vastutavad: IT-juht, infoturbeametnik, üksikute IT-rakenduste eest vastutavad töötajad

Rakendamise eest vastutavad: administraator, arendaja

Volitused

Samal ajal, kui autentimise eesmärk on kinnitada väidetavat identiteeti, on volituste eesmärk kontrollida, kas eelnevalt autenditud olem on volitatud ligi pääsema teatud ressurssidele. Mõlemad terminid täiendavad teineteist seega identiteedi- ja juurdepääsuhalduse koostisosade poolest (Identity and Access Management, IAM) ja enne iga volitamist peab olema toimunud vastav autentimine. Volitamise kõige tähtsam põhimõte on, et igal juurdepääsul ressursile tuleb kontrollida, kas volitused seda päringut tegelevale olemile lubavad – ja nimelt iga tegevuse juures, st iga üksiku päringu korral veebiteenuses.

Rollid ja õigused

Üksikute õiguste määramist ja haldamist iga üksiku kasutaja jaoks pole keeruliste rakenduste juures mõistlik rakendada. Seetõttu tuleb arendada nõuetekohane rollimudel, mille korral määratakse kasutajatele nende ülesannetele vastavad rollid, mille jaoks nad saavad vajalikud volitused.

Erilised väljakutsed veebiteenuste kasutamisel

Veebiteenustel ja eriti teenusele suunatud struktuuridel (SOA) on vastupidiselt monoliitsetele rakendustele mitte ainult üks, vaid mitu punkti, kus peab toimuma kontrollimine, sest pääsueeskirjade (policies) elluviimine peab toimuma iga teenuse juurdepääsupunkti juures. Neid kontrollipunkte nimetatakse ka Policy Enforcement Point'ideks (PEP). Nii selliste reeglistike planeerimine kui ka praktiline haldamine on keeruline väljakutse ja peaks olema teostatav tsentraalses tööriistas. Volituste kontrollimise instants peab olema võimeline lugema veebiteenuse sõnumeid. Sageli realiseeritakse sellised kontrollinstantsid ka ise kui veebiteenused ja need kasutavad veebiteenuse standardeid rollide ja õiguste loomiseks.

Organisatsiooni üleminekud

Erilised väljakutsed tekivad, kui veebiteenuse kasutamine ületab organisatsiooni piirid. Sel juhul tuleb leida kontseptsioonid ja reeglid, kuidas käsitleda volitamisega seotud otsuseid päringute korral väljaspool organisatsioone ja teistele organisatsioonidele. Vastavaid usaldussuhteid tuleb alati täpsustada formaalsete tingimuste ja õiguste mudelitega.

Kihid

Kuna moodsad rakendused ja seega ka veebiteenused on tavaliselt üles ehitatud paljudes kihtides (vähemalt kaks, parem kolm, näiteks esitlus, talitlusloogika ja andmetalletus), tõuseb küsimus volitamisest mitte ainult üks kord, juurdepääsul esitluskihile, vaid lisaks sellele ka iga kihi juurdepääsul vastavalt selle all olevale kihile.

Järgmine, selle kohal olev kiht võib SOA-s moodustada kataloogid (Repositories), st andmebaasid, mis pakuvad andmeid teenuste kohta näiteks standardi UDDI kohaselt.

Minimaalsed õigused

Põhimõtteliselt tuleb igal kihil järgida põhimõtet „Minimaalne juurdepääs" (Least Privilege): väljastada tohib alati üksnes nii palju õigusi, kui tegelikus kontekstis erialaste ülesannete täitmiseks vaja. See toob kaasa, et administratiivseid õigusi võivad teostada vaid erilised kasutajad ja halduse eesmärgil. Minimaalsete volituste põhimõte kehtib ka juurdepääsul kataloogidele, kui need ei ole täielikult avalikud. Minimaalsete volituste põhimõte kehtib ka süsteemi volituste kohta, millega töötavad rakenduste serveri, andmebaasi, XML-tulemüüri ja muude komponentide protsessid.

Avaliku juurdepääsuga veebiteenused

Eriti siis, kui veebiteenuseid pakutakse suurtele, võimalik, et anonüümsetele kasutajakihtidele (teenusena internetis), tuleb arvestada juhuslike ja süstemaatiliste rünnetega volitustele kõikidel kihtidel. Sel puhul tuleb rakendada erilisi arhitektuurseid meetmeid. Väljastpoolt kättesaadavad liidesed tuleks seejuures paigutada isoleeritud piirvõrkudesse (DMZ) ja eraldada sisemistest teenustest ja andmekogudest. DMZ-sse võib paigutada ka täiendava Security-Service'i, mis kõik veebiteenusele tehtavad päringud üle kontrollib. Seejuures võib see üle võtta ka päringute autentimise ja volitamise, nt juurdepääsu abil kataloogiteenusel sisevõrgus. Tegelikud andmed asuvad rakendusserveris, samuti sisevõrgus, millele veebiteenus lubab esitada üksnes kindlaid päringuid.

Turvalüüsid

Kuna veebiteenuse suhtlus toimub sageli erinevate võrgualade vahel, mängivad klassikalised tulemüürikontseptsioonid võrkude turvaliseks eraldamiseks suurt rolli. Siia lisandub tõsiasi, et SOAP-sõnumite sees võidakse edastada mis tahes andmeid, käske ja faile (manustena), millele tulemüür, mis filtreerib ainult aadressi- ja porditasandit, ei saa eesmärgipäraselt reageerida. Eesmärgikohased veebiteenuse tulemüürid peavad olema teostatud kui Application Level Gateways (ALG). Sellisel juhul tähistatakse neid sageli ka kui XML-Firewall või XML-Security-Gateway. Sellised süsteemid võivad filtreerida XML-i, analüüsida, kontrollida kahjurvara ja uurida SOAP-sõnumeid, et blokeerida näiteks teatud tegevusi või osalisi. Ka volitamise jaoks võib kasutada XML-Firewall'i. Sellisel juhul teeb see otsuse, kas autenditud kasutajal on õigus teatud tegevust teostada, mis seisneb sõnumis sisalduva Security Token'i uurimises, hindamises ja krüptograafilises kontrollimises.

Standardid

Olemasolevatel IT-süsteemidel on sageli suletud juurdepääsumehhanismid. Andmed olemite ja atribuutide kohta salvestatakse tavaliselt pääsuloendites (Access Control Lists, ACL), mis võivad väga erinevad välja näha. Sellega raskendatakse liigselt andmevahetust ja ühist kasutamist erinevate süsteemide kaudu. Veebiteenuste alal, kus liidesed, andmemudelid ja autentimismeetodid on juba ühtlustatud, tuleks seetõttu rakendada ka juurdepääsukontrolli jaoks asjakohaseid standardeid.

Vastupidiselt muudele spetsiifilistele teemadele ei ole volitamine siiski siiani sulandunud WS-*-perekonna eraldi standardisse. 2014. aasta alguseks ei olnud standardit WS-Authorization avalikustatud. Selle asemel on olemas erinevad XML-standardid, mis kohati kattuvad, osaliselt üksteist täiendavad ja käsitlevad volitamise teemat alati teatud tähelepanuga.

SAML-is (Security Assertion Markup Language), standardiseeritud XMLraamistikus olemi autentimise, volitamise ja atribuutidega seotud andmete kirjeldamise ja päringu jaoks näiteks SOAP kaudu saab niinimetatud Assertions'is (ütlustes) muu hulgas kodeerida ja vahetada volitamist puudutavaid otsuseid.

Teisest küljest kujutab XACML (eXtensible Access Control Markup Language) endast keelt, mis XML-il põhinedes kirjeldab, kuidas tuleb luua reeglid ja sinna juurde kuuluvad päringud ja vastused, et võimaldada kontekstil ja atribuutidel põhinevat ressurssidele juurdepääsukontrolli volitamist. Tegevuste lihtsate tagatiste ja keeldude kõrval on siin võimalus enne või pärast volitamisotsust sundida tegema lisategevusi. XACML-i tugevus seisneb eelkõige ülitäpses kirjelduses ja pääsuõiguste ülekandmises.

XACML ja SAML kattuvad küll osaliselt kui autentimise ja volitamise standardid, täiendavad üksteist aga erineva fookuse alusel ja neid kasutatakse seetõttu sageli kombineeritult. Samal ajal kui SAML võimaldab autentimist ja autentimis- ja volitamisotsuste ülekandmist olemite vahel, hõlmab XACML eelkõige volitamisotsuseid, st seda, kuidas neid PEP-is töödeldakse.

Etapiviisiline kaitse

Eriti siis, kui andmetel või operatsioonidel on kõrge kaitsevajadus, ei tuleks volitamist kontrollida ainult ühes kohas, vaid aset peaks leidma etapiviisiline kaitse (Defense in Depth). Nii saab turvalüüs kontrollida juba päringu ja teenuse enda volitust enne väljastamist veelkord, et kätte saada võimalikud valekonfiguratsioonid või lüüsi tarkvara kitsaskohad.

Lõpuks tuleks vea korral alati vastu võtta kindel otsus (Fail Securely): kui tegemist on konfidentsiaalsuse või terviklusega, tuleb ebaõnnestunud volitamise korral juurdepääsust keelduda. Ainult juhul, kui kättesaadavuse nõuded on märgatavalt suuremad kui muud turvanõuded, tohib vea korral anda loa juurdepääsuks. Selline otsus tuleb siiski igal juhul dokumenteerida riskianalüüsis.

Kontrollküsimused:

- Kas välja on arendatud nõuetekohane rollide ja õiguste mudel?

- Kas juurdepääsuõigusi kontrollitakse iga üksiku juurdepääsu korral igale ressursile alati uuesti?
- Kas SOA juures on olemas tsentraalne tööriist rollide ja õiguste haldamiseks?
- Kas minimaalsete volituste põhimõttele jäädakse järjepidevalt kindlaks, eriti ka administratiivsete juurdepääsude ja osaleva tarkvara teenusekontode puhul?
- Kas avalikult kättesaadavate veebiteenuste korral kasutatakse turvalist arhitektuuri, näiteks DMZ-i kujul koos Security-Service'iga või XML-Security-Gateway'ga?
- Kas ebaõnnestunud volitamise korral naaseb süsteem turvalisse olekusse, mis vastab kaitsevajadusele?

M 4.456 Autentimine veebiteenustes

Algatamise eest vastutavad: IT-rakenduste eest vastutavad töötajad, IT-juht, infoturbeametnik

Rakendamise eest vastutavad: administraator, arendaja

Selleks, et piirata juurdepääsu veebiteenusele volitatud isikute ringile või et realiseerida erinevaid volitusi veebiteenuse sees (vrdl M 4.455 Volitamine veebiteenustes), tuleb teenusele ligipääsevaid kasutajaid üheselt identifitseerida ja autentida. Samuti peab kasutajal olema võimalus kindlaks teha, kas ta suhtleb tõesti soovitud teenusega.

Autentimine peab seejuures toimuma enne kaitsmist vajavate andmete ülekandmist.

See tähendab, et veebiteenuse kasutaja peab kindlaks tegema, et ta tõesti suhtleb soovitud teenusega, enne kui ta saadab teenusele konfidentsiaalsete andmetega päringu. Samuti peab veebiteenus kontrollima päringut tegeva kasutaja või veebiteenuse identiteeti, enne kui see saadab tagasi konfidentsiaalsed andmed või annab kasutajale volitused funktsioonide käivitamiseks (vt M 4.455 Volitamine veebiteenustes).

Suhtluspartnerite autentimist tuleb rakendada erinevatel tasanditel. Üks võimalus on autentimine edastustasandil SSL-i/TLS-i abil. Seda nimetatakse sageli ka Transport Layer Authentication'iks. Teine võimalus on autentimine sõnumitasandil, näiteks WS-Security-standardi mehhanismidega. Kui lisaks üksikutele sõnumitele tuleb autentida hoopis keerulist sõnumivahetust, soovitatakse sisse seada vastav seansihaldus (vrdl M 4.394 Seansihaldus veebirakendustes).

Identiteedihaldus

Veebiteenuse kasutajate autentimiseks on vaja koguda kasutajaandmeid ja salvestada sinna juurde kuuluvad identifitseerimistunnused. Need protseduurid on osa nn identiteedihaldusest (Identity Management). Klassikaline rakendus on selline, kui iga veebiteenuse osutaja kasutab oma isiklikku kasutajahaldust ja viib autentimise läbi ise. Sel puhul räägitakse isoleeritud identiteedihaldusest. Selle mudeli korral suhtleb kasutaja ainult soovitud veebiteenusega. Muude veebiteenuste kasutamiseks tuleb tema identiteeti hallata seal alati sõltumatult. Kui veebiteenuseid kasutatakse teenusele suunatud arhitektuurides (SOA), on enamasti tegemist keeruliste süsteemidega, mis sageli ei allu ühe üksiku asutuse kontrollile. Seetõttu ei ole sageli võimalik lasta identiteete hallata üksikute teenuste käitajatel. Selle ülesande võtavad endale spetsialiseerunud organisatsioonid või organisatsiooniüksused, identiteeditеenuse osutajad (Identity Providers). Tsentraalse identiteedihalduse korral eksisteerib selline identiteeditеenuse osutaja, kes osutab identiteedihaldust paljudele teenuseosutajatele. Sellist liiki identiteedihalduse näited on teenuseosutajate nagu Microsoft, Facebook või Google teenused, aga

ka tsentraalse autentimissüsteemi kasutamine ettevõtte sees. Tsentraalsed identiteedihaldussüsteemid pakuvad sageli single-sign-onfunktsiooni. Kasutaja peab end autentima ainult ühe identiteeditenuse osutaja juures, selleks et kasutada erinevate teenuseosutajate teenuseid. Kolmas identiteedihalduse variant on liitidentiteedihaldus (Federated Identity Management). Selles variandis on olemas mitu identiteeditenuse osutajat. Kasutajate autentimine toimub standardsete liideste ja protokollide kaudu. Veebiteenuste jaoks omab siin tähtsust eelkõige standard WS-Federation. Konkreetsed tehnoloogiad, mida selle standardi rakendamiseks kasutada saab, on Security Assertion Markup Language (SAML) ja OpenID.

Kasutatavate näitajate liik

Osalejate autentimine veebiteenuse suhtluses toimub üheselt identiteedile määratud tunnuste, nn identifikaatorite tõendamise kaudu. Tavalised identifikaatorid on seejuures kasutajanimed koos paroolidega, sertifikaadid ja allkirjad ning identiteeditenuse osutaja või Security-Token-Service'i krüptograafiliselt kaitstud andmehulgad (Token), nagu see on kindlaks määratud WS-Trust'is (vrdl M 4.453z Pääsmikuteenuse (Security Token Service) kasutamine). Järgnevalt on esitatud erinevad autentimismeetodid. Veebiteenuse jaoks tuleb välja valida meetod, mille turvalisus vastab kaitsevajadusele.

Väga lihtsa autentimise näide kasutajanimede ja paroolidega on HTTP Basic Authentication. Seda saab kasutada nii REST-l põhinevate veebiteenuste kui ka SOAP-l põhinevate veebiteenuste jaoks. See pakub siiski ainult vähesel määral kaitset autentimisandmetele ja seetõttu tuleb sellele lisada täiendavad turvameetmed nagu edastamise krüpteering. Teine näide on Username Token'i kasutamine WS-Security rakendamisel.

Parimat kaitset pakuvad erinevad võimalused, et autentida veebiteenuse sõnumeid sertifikaatide ja allkirjadega. Enamasti kasutatakse XML-allkirju vastavalt XMLDSIG-standardile. Allkirjade autentimiseks kasutamise eelised on, et autentimine toimub sõnumitasandil. Tänu sellele saab vajaduse korral loobuda seansihaldusest (Session Management), sest iga sõnum autenditakse allkirjaga.

Selle meetodi puudus on jõudlusekadu seoses igale sõnumile allkirja genereerimise, ülekandmise ja kinnitamisega. Seetõttu nõuab allkirjade kasutamine Public Key taristu (PKI) kasutamist.

XML-allkirjade puhul tuleb kindlaks teha, et allkiri on tõesti seotud teenuse poolt töödeldavate andmetega. Kui see nii ei ole, saavad võimalikuks nn XMLsignature-wrapping-tüüpi ründed (vt G 5.183 XML-i vastu suunatud ründed). Selle ründe korral sisestatakse kehtivad, allkirjastatud XML-andmed ründe toimepanija

poolt manipuleeritud XML-i dokumenti. Kui allkirja kinnitamise funktsioonid ja tegelik rakendusloogika töötlevad nüüd XML-andmeid erineval moel, võib tekkida olukord, et kontrollitakse eelnevalt sisestatud andmete allkirja, rakendustasandil töödeldakse aga manipuleeritud andmeid.

Järgmine võimalus veebiteenuse suhtluses osalejate autentimiseks on autentimine pääsmikuga, mis on väljastatud usaldusväärse kolmanda isiku poolt. Pääsmikuna tähistatakse siinjuures andmestruktuuri, mis kinnitab pääsmiku omaniku identiteeti. Pääsmiku enda terviklus ja autentsus tuleb omakorda kindlaks määrata krüptograafiliste meetmetega. Veebiteenuste suhtluses sageli kasutatavate pääsmike näited on SAML või OAuth-Token.

Kasutajate juurdepääsul suurendatud kaitsevajadusega veebiteenustele võib olla nõutav teostada tugevat autentimist, kasutades mitmeid autentimisfunktsioone (nt kiipkaardi omamine ja selle juurde kuuluva PIN-koodi teadmine). Kui niisuguse mitmefaktorilise autentimise jaoks kasutatakse üksteisest sõltumatuid autentimisfunktsioone, väheneb võimalus, et ründe toimepanijad saavad kõik nõutavad funktsioonid oma kontrolli alla.

Kui autentimiseks kasutatakse krüptograafilisi algoritme, näiteks Hashingmeetodit või allkirju, tuleb kindlaks teha, et need vastavad tehnikatasemele. Siinjuures tuleks võtta vastavaid mooduli B 1.7 Krüptokontseptsioon .

Autentimisandmete turvaline edastamine

Identifikaatorite edastamine peab olema asjakohasel moel kaitstud, nii et ründe toimepanija ei saa kasutada identifikaatoreid, et esitleda end seadusliku kasutaja või veebiteenuste osutajana. Vajalikud kaitsemehhanismid sõltuvad kasutatava identifikaatori liigist. Kasutajanimede ja paroolide edastamisel peab olema tagatud konfidentsiaalsus, näiteks edastamise krüpteeringu või erinevate veebiteenuse sõnumite krüpteeringuga.

Seetõttu tuleb autentimisandmeid kaitsta taastamise (Replay-tüüpi ründed) ja edastamise (Relay-tüüpi ründed) eest. See toimub tavaliselt sõnumis oleva ajatempli abil, näiteks wsu:Timestamp- element WS-Security rakendamisel, või ühekordsete juhuslike arvude (Nonce) kasutamisega, näiteks wsse:Nonce- elemendi kujul. Nonce'ide kasutamisel tuleb tagada, et juhuslikke arve ei kasutataks mingil juhul mitu korda. Kaitse Relay-tüüpi rünnete eest tuleb ellu viia täpsete, sõnumi vastuvõtja manipulatsioonide eest kaitstud andmetega.

Kontrollküsimused:

- Kas veebiteenuse ja veebiteenuse kasutaja vahelises suhtluses toimub vas-

tastikune autentimine, enne kui vastaspoolele edastatakse konfidentsiaalseid andmeid või enne kui võimaldatakse juurdepääs funktsioonidele?

- Kas autentimiseks kasutatakse piisavalt tugevaid meetmeid?
- Kas paroole edastatakse ainult krüpteeritult?
- Kas XML-allkirjade kasutamisel on tagatud, et allkiri on tõesti seotud rakendustasandil töödeldavate andmetega, et takistada signature-wrapping-tüüpi ründeid?
- Kas asutuse krüptokontseptsioonis on arvesse võetud autentimiseks kasutatavaid krüptograafilisi meetodeid?
- Kas on võetud kaitsemeetmed identifikaatorite taastamiseks ja edastamiseks?

M 4.457 Teenusetarbijate turvaline lahutamine veebirakendustes ja veebiteenustes

Algatamise eest vastutavad: IT-juht, üksikute IT-rakenduste eest vastutavad töötajad

Rakendamise eest vastutab: administraator, arendaja

Kui veebiteenust kasutavad paljud, üksteisest sõltumatud kasutajad (teenusetarbijad), tuleb võtta meetmeid, mis takistavad, et kasutajad pääsevad kogemata või pahatahtlikult ligi teise teenusetarbija andmetele (vt G 4.94 Volitamata juurdepääs teise teenusetarbija andmetele veebirakendustes ja veebiteenustes). Andmekogude eraldamiseks on olemas erinevad meetodid, mida võib kasutada nii eraldi kui ka kombineeritult.

Rakenduspõhine lahutamine

Rakenduse programmikood otsustab programmifunktsiooni teostamisel, millised andmed on milliste kasutajate jaoks kättesaadavad, kuvades näiteks ainult kasutaja enda poolt salvestatud andmekogusid või on andmetel kindel teenusetarbija tähis, mida rakendus kontrollib. Siin on oht tahtmatuks ligipääsuks teiste teenusetarbijate andmetele eriti suur, sest juba rakendusviga koodis või puuduv kontroll funktsioonide otsesel käivitamisel võib avalikustada vastavad andmed.

Lahutamine andmetalletuses

Selle teostusvariandi puhul hoitakse erinevate teenusetarbijate andmeid eraldi kasutatavates andmesalvestussüsteemides (nt erinevates loogilistes andmebaasides, erinevates tabelites või erinevates harudes kataloogiteenuste skeemis). Vastavate teenustarbijatele omaste kontode kasutamisega andmetele juurdepääsul ja sobiva volituste kontseptsiooni abil saab tagada, et loetakse või muudetakse ainult teenusetarbija andmeid. Selles olukorras on liigitamisviga ainult veel siis võimalik, kui viga toob kaasa ka kasutatava andmebaasi / kataloogiteenuse konto vale liigitamise.

Keskkondade lahutamine

Erinevate teenusetarbijate teenuseid pakutakse erinevatel virtuaalsetel või füüsilistel süsteemidel. Kasutaja juurdepääsul tehakse kindlaks, et saadaval on ainult teenusetarbija enda süsteemide teenused. Seda on võimalik saavutada näiteks vastava autentimismeetodiga või võrgupõhiste meetmetega, mis muudavad erinevad süsteemid kättesaadavaks üksnes vastava teenusetarbija võrgust.

Kliendispetsiifiline krüpteering

Täiendavat kaitset lubamatute juurdepääsude eest saab teostada andmete krüpteeritud salvestamisega. Krüpteering hõlmab sellisel juhul terveid andmebaasi sisusid, alternatiivselt aga ka ainult üksikuid tundlikke andmevälju. Vajalike krüptograafiliste võtmete genereerimise, kasutamise ja säilitamisega kasutaja süsteemides välistatakse kolmandate isikute juurdepääs oma andmetele. See meetod tagab kaitse ka selle eest, et administraatorid ja teenuse töötajad ei pääseks volitamata nägema andmeid, mis nõuab aga ka vastavat nõuetekohast strateegiat võtmehalduseks, eriti võtmete kaotuse või vahetamise puhul. Lisaks piiravad krüpteerimismeetmed tugevalt ka andmete töötlemist serveril ja nii ei ole enam näiteks võimalik otsimine ja sorteerimine andmebaasi haldussüsteemi vahenditega.

Teenusetarbijate lahutamise turvaliseks ja tõhusaks rakendamiseks tuleb järgida järgmisi punkte:

- erinevate teenusetarbijate andmekogude lahutamine ei tohi olla rakendatud puhtalt rakendusepõhiselt, vaid seda peab võimaluse korral toetama ka loogiliselt eraldatud andmetalletus eraldi andmebaasi juurdepääsu kontodega ja vastavalt piiratud volitustele;
- suurendatud kaitsevajaduse korral tuleb täiendavalt kontrollida ja vajaduse korral rakendada võimalusi kliendispetsiifiliseks krüpteerimiseks. Seejuures tuleb tagada, et juurdepääs vajalikele krüptograafilistele võtmetele on võimalik üksnes selleks volitatud isikutel (kliendipõhine krüpteering). Selline lahendus on just siis vajalik, kui tuleb välistada turvaliselt teenuseosutaja administraatorite juurdepääs andmekogudele;
- kasutajate liigitamine oma teenusetarbijateks peab toimuma manipuleerimise suhtes turvaliselt (vastava, teenusetarbijate järgi eraldatud kasutajahalduse või nõuetekohaste kriteeriumide järgi kasutajate automaatseks liigitamiseks teenusetarbijateks, näiteks sertifikaatide alusel);
- teenusetarbijate lahutamist tuleb läbi viia järjepidevalt. See puudutab väliseid liideseid, aga ka andmevarunduse protseduuri (võimalus kliendiandmete eraldatud taastamiseks). Ka logimismehhanismid peavad olema loodud nii, et oleks võimalik logiandmete kliendispetsiifiline hindamine või kättesaadavaks tegemine;
- valitud teenusetarbijate lahutamise kontseptsioon peab olema dokumentides kirjeldatud nii, et seda oleks võimalik kontrollida. Korrapäraste auditite ja penetratsioonitestide käigus tuleb arvesse võtta teenusetarbijate lahutamise tõhusust rakendusalas.

Kontrollküsimused:

- Kas kontseptsioon näeb ette meetmeid, mis lähtuvad puhtalt rakendusepõhiselt realiseeritud teenusetarbijate liigitamiseks, et välistada olukorda, kus lihtsad tarkvaravead toovad kaasa juurdepääsu teiste teenusetarbijate andmetele?
- Kas teenusekasutajate liigitamine teenusetarbijateks toimub usaldusväärse ja manipuleerimise suhtes turvalise meetodi abil?
- Kas teenusetarbijate eraldamise kontseptsioon võtab arvesse kõiki vastavaid aspekte (teenuse kasutamine, liidesed, andmevarundus, logimine)?
- Kas kasutatav, erinevate teenusetarbijate andmete eraldamise kontseptsioon on kontrollitavalt dokumenteeritud? Kas rakendamine vastab dokumentatsioonile?
- Kas teenusetarbijate lahutamise tõhusust kontrollitakse korrapäraselt turvaauditite või penetratsioonitestide käigus?

M 4.458 Veebiteenuste kasutuselevõtu planeerimine

Algatamise eest vastutab: IT-juht

Rakendamise eest vastutavad: administraator, vastutav spetsialist

Enne veebiteenuse kasutuselevõtmist tuleb määrata kindel eesmärk, mida veebiteenus peab täitma. Veebiteenused kujutavad endast ainult suhtlemise liiki masinate vahel ja toovad kaasa spetsiifilisi eeliseid ja puudusi rakenduste ja teenuste muude vormide integreerimise vormingute suhtes. Mitte iga rakendus ei sobi veebiteenuste teostamiseks. Ka kulu-tulu-kaalutlustel on siin oma osa.

Nii on andmete läbilaskevõime just järjepideva veebiteenuse turvastandardite kasutamisel regulaarselt silmnähtavalt halvem kui klassikaliste massandmete edastamismeetodite korral. Teiselt poolt on olemas eelised teenuste ja funktsioonide korduvkasutamiseks ning rakenduste laiendatavuses ülesannete jaotamisega erinevatele teenustele.

Alguses teostatakse nõuete analüüs, mis tuleks ka dokumenteerida. Siinjuures soovitatakse seotud protsesside loomisel alustada kõrgel abstraktsioonitasemel, visandada sinna tööprotsessid tegeliku ja soovituna ning selle peale projekteerida üksikasjalikult sisestused, väljastused, liidesed ja andmed. Samuti tuleb identifitseerida teenuseosutajad, tarbijad, sideühendused ja vajalikud teenusekataloogid.

Lõpuks tuleb otsustada, kas ja milliseid veebiteenuseid selles avalikustada tuleb.

Põhiline otsus tuleb langetada REST-l või SOAP-l põhineva veebiteenuse osas.

Kui SOAP on siseselt käitatavate rakenduste puhul oluliselt levinum ning rajatud paljudele tööriistadele ja standarditele, võib REST-d kohata peamiselt liikuvates veebikeskkondades. Lõpuks sõltub otsus põhilises osas muudest teenustest ja rakendustest, mis on juba olemas või mis tuleb ühendada. Igal juhul tuleb alguses arvesse võtta aluseks oleva arhitektuuriga seotud otsuse tagajärjed ja need läbi mängida.

See on eriti kohane siis, kui tuleb luua teenusele suunatud arhitektuur (SOA) või kui teenus tuleb integreerida olemasolevasse SOA-sse. Siinjuures tuleb selgitada SOA-kasutusmudeliga seotud teemasid. Kes vastutab asutuse erialaste

funktsioonide ja töödeldavate andmete eest? Rollid ja vastutusalad tuleb hiljemalt nüüd kindlaks määrata ja dokumenteerida.

See, kas arhitektuur tuleb teenuseorientatsiooni suunas ümber kujundada, on strateegiline otsus, mis peaks käima veebiteenuste kasutamise strateegia ja platvormi strateegiaga käsikäes. Kui veebiteenused tuleb omavahel integreerida erineval, võimalik, et vahelduval moel (siin räägitakse orkestreerimisest), võib äriprotsesside koostalitluse juhtimiseks rakendada modelleerimis- ja kirjelduskeeli nagu BPMN või BPEL. Seda on kõige varem mõtet teha siis, kui olemas on piisavalt suur arv veebiteenuseid, mida tuleb uute teenuste loomiseks liita erineval moel.

Eriti hästi sobivad veebiteenuste teostamiseks teenused, mida vajavad paljud rakendused või muud teenused. Seejuures tuleks arvesse võtta, et teenuseid ei kasutata ainult asutusesiseselt. Kui need antakse muude asutuste käsutusse, tuleb tingimata selgitada, kes otsustab kolmandale isikule vahendatavate teenuste ja andmete kasutusse andmise üle. Lisaks sellele tuleb arvesse võtta võrguüleminekute ja sideliideste kaitsmist, et veebiteenustele oleks võimalik väljastpoolt päringuid esitada, ilma et kahjustataks asjatult asutuse sisevõrku. Seejuures edastatakse ettevõtte andmed sageli läbi tulemüüride võrgusegmentidest välja ja nende kaudu sisselülitatud portidele nagu 80 (HTTP) või 443 (HTTPS). Sel moel võib integreeritud faili kujul asutusse sattuda ka kahjurvara. Siin tuleb üle kontrollida ja vajaduse korral kohandada kaitsekontseptsioonid ja tehnilised kaitsemeetmed nagu Application Level Gateways (ALG).

Veebiteenuste kaitsmiseks rünnete vastu tuleb ka rakendamisel ette näha nõuetekohased kaitsemeetmed, näiteks sisestus- ja väljastusandmete järjepidev valideerimine ning töödeldavate XML-andmete ühilduvuskontrollid. Ka selle jaoks tuleb planeerimisetapis välja töötada vastavad nõuded ning need dokumenteerida.

Selleks, et oleks võimalik informeeritult otsustada veebiteenuste juurutamise, sellega seotud riskide ja vajaliku kaitse üle, on oluline dokumenteerida veebiteenuse kõik funktsioonid ja hoida need dokumendid ajakohased. See toimub kõige paremini kõikide veebiteenuste jaoks tsentraalses paigas. Kui veebiteenust kasutavad mitmed osapooled, peaks kõikidel pooltel olema juurdepääs nendele andmetele.

Paralleelsel kasutamisel on oma mõju ka veebiteenuse kasutusajale. Tuleb selgitada ja kirjeldada, kuidas võib läbi viia paljude rakenduste või organisatsioo-

nide poolt kasutatava veebiteenuse muudatusi. Sama asi kehtib ka väljalülitamise kohta kasutusaja lõpus.

Veebiteenuse funktsioonide elluviimiseks soovitatakse kaasata hinnatud ja hästi testitud komponente, sest teema on keeruline ja iseseisvalt loodavate programmide korral võivad sageli esineda programmivead. Nii rakenduste serveri kui ka veebiteenuse teekide või raamistike korral tuleks valida tooted, mida aktiivselt edasi hooldatakse ning mille puhul on olemas ajakohased andmed nende kitsaskohtade ja paikade kohta.

Kui kasutusele võetakse keerulised standardid nagu WS-Security, WS-Trust või WS-Federation, tuleb täpselt planeerida ja katsetada erinevate turbefunktsioonide vastastikust sõltuvust ja mõju. Turvalisuse säilitamiseks terves SOA-s on lõpuks vajalik standardite, kontseptsioonide ja mehhanismide kooskõla, mis väljub puhta klient-server-suhte kaitse piiridest. Siin tuleb küsida nõu spetsialistidelt.

Muude turvalisusega seotud eesmärkide kõrval, mis mängivad oma osa vastavalt kasutamise eesmärgile, on otsustavaks peaaegu alati teenuse kasutaja ja teenuse osutaja vahelise suhtluse kaitse. See võib toimuda kas edastustasandil, kui sõnumite edastuskanal seda võimaldab (nt SSL-i/TLS-i kaudu HTTP korral), või sõnumitasandil. Viimane võimaldab lisaks lõpp-punktist lõpp-punkti kaitse kõrval valida ja hinnata turvaparameetreid ka üksikasjalikumalt, näiteks allkiri või krüpteering ainult sõnumi kindlate osade jaoks. Seejuures on vajalik kasutatavate mehhanismide põhjalik tundmine, et mitte saada ründe ohvriks logides või rakenduses olevate kitsaskohtade kaudu, nt XML signature-wrapping-tüüpi rünnete kaudu (vt G 5.183 XML-i vastu suunatud ründed). Lisaks sellele raskendab lõpp-punktist lõpp-punkti krüpteering pahatahtlike sõnumite filtreerimist. Siin võib aidata, kui ajastada krüpteerimine Application-Level-Gateway'le.

Selleks et täielikult ära kasutada veebiteenuste eeliseid, eriti nende korduvkasutatavust ja laiendatavust, on otsustava tähtsusega, et identiteedi- ja juurdepääsuhaldust ei realiseeritaks igas teenuses eraldi. Veebiteenuse keskkonna planeerimine hõlmab seetõttu kasutajate ja õiguste kõikehõlmava halduse planeerimist. Täpsemat teavet leiate selle kohta meetmetest M 4.455 Volitamine veebiteenustes ja M 4.456 Autentimine veebiteenustes .

Eespool nimetatud, veebiteenuse planeerimise jaoks olulised aspektid kehtivad sarnasel kujul ka klassikaliste IT-rakenduste korral. Võimaliku paralleelse kasutamise ja orkestreerimise tõttu liiga ulatuslike ülesannete ning standardite ja logide tehnilise keerukuse tõttu on planeerimispuuduste mõju projekti edukusele võrrel-

des teiste tehnoloogiatega siiski kõrgem.

Kontrollküsimused:

- Kas on kirjeldatud veebiteenuse kasutamise eesmärki ja kas tarbijate nõudeid on analüüsitud ning kas need on dokumenteeritud?
- Kas on dokumenteeritud, kes vastutab erialaste funktsioonide ja töödeldavate andmete eest?
- Kas võrguüleminekute kaitse kontseptsioonid ja meetmed on kohandatud silmas pidades veebiteenuste kasutamist?
- Kas veebiteenuse sõnumites on olemas kaitse kahjurvara eest, ja kas turvameetmed nagu sisestuse ja väljastuse valideerimine tarkvara rakendamise jaoks on kinnitatud?
- Kas veebiteenuse teostamiseks valiti välja hinnatud, hästi testitud komponendid, teegid ja raamistikud?
- Kas tarbija ja teenuseosutaja vaheline suhtlus on asjakohaselt kaitstud edastus- või sõnumitasandil?

M 4.459 Krüpteeringu kasutamine pilvteenustes

Algatamise eest vastutavad: infoturbeametnik, IT-juht

Rakendamise eest vastutavad: administraator, infoturbeametnik

Põhimõtteliselt tuleb pilvteenuste kasutamisel teha vahet andmete krüpteerimisel edastuskanalis (liikvel andmed) ja andmete krüpteerimisel nende salvestuskohas (jõudeolekus andmed). Edastuskanalis krüpteerimine on seejuures seoses pilvteenuste kasutamisega alati kohustuslik, välja arvatud siis, kui on tegemist privaatse pilve pilvteenusega, mida kasutatakse kaitstud kohaliku võrgu kaudu. Pilvteenusesse logimine peab igal juhul toimuma krüpteeritult, ka privaatse pilve kasutamise korral. Sellekohased nõuded ja soovitused on toodud meetmetes, mis puudutavad teenuse definitsiooni (vt M 2.536 Tarbitavate pilvteenuste määratlemine teenuste tarbija poolt) ja lepingu koostamist pilvteenuseosutajaga (vt M 2.541 Pilvteenuseosutajaga sõlmitava lepingu koostamine). Seepärast ei süveneta selles meetmes lähemalt edastuskanalis toimuva krüpteerimise kasutamise võimalustesse ja viidatakse meetmetele M 5.66z SSL-i/TLS-i kasutamine kliendis ja M 5.177 SSL-i/TLS-i kasutamine serveris .

Andmete krüpteerimisel nende salvestus- või töötlemiskohas tuleb eristada kaht varianti. Ühelt poolt saab krüpteerimist teostada enne andmete ülekandmist pilvteenuseosutajale otse teenust tarbiva asutuse kaudu. Teisel juhul toimub edastatavate andmete krüpteerimine kõigepealt pilvteenuseosutaja süsteemides. Kui krüpteerimist teostab pilvteenuseosutaja, tuleb täita sellekohaseid lepingutingimusi, mis sisaldavad muu hulgas nõudeid turvaliste krüpteerimismehhanismide valikuks ja sobivate võtmepikkuste kasutamiseks. Seetõttu tuleb kokku leppida, et vajaduse korral võib pilvteenuste kasutaja algatada uute võtmete andmise ning ta võib mõjutada võtmete kasutusaegasid. Tähelepanu tuleb pöörata sellele, et krüpteerimisel pilvteenuseosutaja kaudu lasub vastutus võtmehalduse eest samuti temal. Pilvteenuseosutaja töötajad, kes teavad vastavatest võtmetest, võivad sel moel juurde pääseda asutuse andmetele.

Alternatiivina andmete krüpteerimisele pilvteenuseosutaja kaudu võib olenevalt pilvteenusest olla asutusel võimalus rakendada oma krüpteerimismehhanisme. Turvaline võtmehaldus on seega tema kätes. Sellega seoses on osutunud kasulikuks niinimetatud füüsilise turvamooduli (hardware security module, HSM) kasutamine võtmete turvaliseks genereerimiseks ja salvestamiseks. HSM-i kasutamise korral ei ole oluline, kus krüpteerimine aset leiab, kas pilves või asutuse süsteemides, sest pilvteenuseosutaja ei saa võtmele ligi pääseda.

Tuleb tähele panna, et asutuse kaudu krüpteerimine ei ole alati teostatav. Pilvteenuste kasutamise eripära seisneb asjaolus, et arvestada tuleb kasutatud tee-

nusemudeli sõltumatust. Nii ei ole näiteks tarkvara kasutamisel teenusena paljudel juhtudel oma krüpteering võimalik, kuna rakendusi kasutatakse API kaudu (nt CRM-andmebaasi krüpteering). Kui aga krüpteering on kohustuslik ja pilvteenuseosutaja ei saa seda pakkuda, võib olenevalt pilvteenusest kasutada ka kolmandaid tootjaid, kes sellist krüpteeringut pakuvad. Kui asutus plaanib oma krüpteerimismehhanismide kasutuselevõtmist või kasutab kolmandat tootjat, soovitatakse tihedat koostööd pilvteenuseosutajaga, et välistada võimalikult varakult võimalikke probleeme töö käigus.

Selle meetme rakendamisel tuleb lisaks arvesse võtta moodulit B 1.7 Krüptokontseptsioon .

Kontrollküsimused:

- Kas krüpteerimisel pilvteenuseosutaja kaudu on olemas lepingutingimused, mis esitavad nõuded turvaliste krüpteerimismehhanismide valimiseks ja nõuetekohaste võtmepikkuste rakendamiseks?
- Kas oma krüpteerimismehhanismide kasutamisel tagatakse nõuetekohase võtmehalduse rakendamine?
- Kas krüpteeringu rakendamisel võetakse arvesse pilvteenuste kasutamise eripärasid valitud teenuse puhul?

M 4.460 XXX

M 4.461 XXX

M 4.462z Sissejuhatus pilveteenuse kasutamisse

Algatamise eest vastutavad: infoturbeametnik, IT-juht

Rakendamise eest vastutavad: administraator, infoturbeametnik, IT-juht

Pilvteenuste kasutamise definitsioonid ja põhimõisted

Pilvteenust iseloomustatakse tavaliselt alljärgnevalt toodud omaduste kaudu (Cloud Security Alliance'i ehk CSA järgi). Kirjeldus ei ole seejuures jäik, vaid seda võib alati tõlgendada, täiendada või ka vähendada.

Nõudeselve (on-demand self-service)

Vahendamine, see tähendab IT-ressursside kasutusseandmine, nagu näiteks arvutusvõimsus või salvestivõimsused, toimub automaatselt ilma pilvteenuseosutaja sekkumiseta (pilvteenusetarnija, cloud service provider, lühidalt CSP).

Broad network access

Pilvteenuseid pakutakse võrgu kaudu ja neile pääseb ligi standardmehhanismide või standardlogide kaudu.

Ressursside ühendamine (resource pooling)

Pilvteenuseosutaja IT-ressursid on koondatud nn seadmete kogudesse. Võttes aluseks kliendipõhise mudeli, on pilvteenuseosutajal võimalik olla vajadusepõhises vastavuses paljude kasutajate nõuetega. Pilvteenuste kasutamisel ei tea tellija pilvteenuseosutaja IT-ressursside täpset asukohta. Selliste ressursside näited võivad olla salvestisüsteemid, protsessorivõimsus, töömälud või ka rakenduse tarkvara.

Rapid elasticity

Pilvteenuseid saab kohandada (automaatselt) kiiresti ja paindlikult, et oleks võimalik reageerida teenust tarbiva asutuse kiiresti muutuvate vajadustega.

Mõõdetav teenus (measured service)

Pilvteenused kasutavad sageli tööriistu, mis valvavad automaatselt ressursside kasutamist ja optimeerivad seda olenevalt kasutatavatest teenustest (nt salvestisüsteemid, protsessorivõimsus või aktiivsed kasutajakontod). Läbipaistvuse loomiseks nii teenust tarbiva asutuse kui ka teenuseosutaja juures saab ressursside kasutamist mõõta ja edastada tulemused kasutajale.

Pay per use

Arveldamine toimub pilvteenuste kasutamisel tavaliselt teenuste või ressursside alusel, mida kasutaja tegelikult tarbis.

BSI definitsioon

Selleks, et kõikide pilvtehnoloogia tööde jaoks oleks olemas ühtne alus, määras BSI termini „pilvtehnoloogia" jaoks kindlaks järgmise definitsiooni:

pilvtehnoloogia puhul on tegemist võrgukeskkonnas toimivate IT-teenustega, mille puhul saab pakkumist, kasutamist ja arveldamist kohandada dünaamiliselt vajadust mööda. Selliste teenuste pakkumiseks ja kasutamiseks rakendatakse eranditult asjakohaseid tehnilisi liideseid ja protokolle. Pilvteenuste raames pakutavate teenuste ulatus hõlmab infotehnoloogia täielikku spektrit ja sisaldab muu hulgas taristut (nt arvutusvõimsus, mäluruum), platvorme ja tarkvara. Siinses dokumendis kasutatakse pilvtehnoloogia mõistet just selles tähenduses, kusjuures

eespool nimetatud omadusi tuleb pidevalt meeles pidada. Seega ei ole lihtne veebirakendus tavaliselt pilvtehnoloogia, kuigi tootjate reklaamiosakonnad seda sageli nii nimetavad.

Pilvteenuste kasutamine erinevate pilvteenuste mudelite abil

Pilvteenuste kasutamisel võib eristada kolme teenusemudeli kategooriat. Paremaks arusaamiseks kirjeldatakse neid alljärgnevalt lähemalt.

Taristu teenusena (infrastructure as a service, IaaS)

IaaS-i puhul pakutakse teenusena IT-ressursse, nagu arvutusvõimsus, andmesalvesti või võrgud. Pilvteenuste kasutaja ostab need virtualiseeritud ja suures osas standardiseeritud põhiteenused ning ehitab nendele üles oma teenused siseseks või väliseks kasutamiseks. Nii saab pilvteenuste kasutaja rentida näiteks arvutusvõimsust, töömälu ja andmesalvestit ning lasta neil töötada oma valitud operatsioonisüsteemil koos enda valitud rakendustega. IT-ressursside haldamine allub teenust tarbivale asutusele ja seda teostab tavaliselt kliendi pilvteenuste administraator (customer cloud service administrator).

Platvorm teenusena (platform as a service, PaaS)

PaaS-teenuste osutaja annab kasutada täieliku taristu ja pakub kasutajale sellel platvormil standardiseeritud liideseid, mida kasutavad kliendi teenused. Nii võib platvorm teha teenusena kättesaadavaks näiteks simultaanteeninduse, laiendatavuse, juurdepääsukontrolli, juurdepääsud andmebaasile jne. Teenust tarbival asutusel ei ole juurdepääsu aluseks olevatele kihtidele (operatsioonisüsteem, riistvara). Ta saab aga platvormil tööle panna oma rakendused, mille arendamiseks pakub pilvteenuste osutaja tavaliselt oma tööriistu.

Tarkvara teenusena (software as a service, SaaS)

Kõik rakenduste pakkumised, mis vastavad pilvtehnoloogia kriteeriumidele, asuvad selles kategoorias. Pakkumiste valikul ei ole siinjuures piire. Näidetena võib nimetada kontaktandmete halduse, finantsraamatupidamise, tekstitöötluse või koostöörakendused. Asutuse töötajad kasutavad tarkvararakendusi otse läbi interneti. Paigaldus oma arvutil või asutuse arvutuskeskuses ei ole sageli vajalik. Osaliselt rakendatakse siiski ka arhitektuure, mille puhul on vajalik või võimalik spetsiaalse klienditarkvara kasutamine (veebilehitseja ja/või klienditarkvara kaudu).

Pilvteenuste kasutamine erinevate pilvteenuste mudelite abil

Asutused, kes otsustavad hakata kasutama pilvteenuseid, saavad tavaliselt valida järgmiste kasutusmudelite vahel.

Avalik pilv

Pilvteenuste pakkumine mis tahes kasutajatele üle interneti.

Privaatpilv

Pilvteenuste pakkumine ainult oma asutuse jaoks. Privaatpilve korral on võimalik täiendav eristamine:

- On-premise: pilvtaristut käitatakse asutuse arvutuskeskuses;
- Off-premise: pilvtaristut käitatakse võõras arvutuskeskuses.

Juhis probleemide korral kasutusmudelite liigitamisel:

Kontsernides, kus on palju ettevõtteid, käitatakse IT-tütarettevõtte seisukohast privaatpilve kogu kontserni jaoks. Teenust tarbiv kontserni ettevõte seda seisukohta teatud tingimustel siiski ei jaga, sest ta jagab seda pilve oma silmis „võõrastega". Seepärast käsitleb kontserni ettevõte seda kui avalikku pilve.

Hübriidpilv

Hübriidpilv kujutab endast tavaliselt avaliku pilve ja privaatpilve segu. Teenuseosad luuakse seejuures on-premise-süsteemi kaudu, samal ajal kui muud teenuseosad luuakse avaliku pilve süsteemide kaudu pilvteenuseosutaja juures. Teenused, mis luuakse pilvteenuseosutaja kaudu, võivad olla ka privaatpilve off-premise- või ühispilve lahendused. Hübriidpilv pakub võimalust teenuste jagamiseks avaliku pilve ja privaatpilve vahel.

Näide:

Kontoriteenuste kasutuselevõtmiseks hallatakse e-posti kontosid asutuse privaatpilves, veebikonverentside ja andmete kasutusseandmiseks kasutatakse siiski teenuseosutaja avaliku pilve taristut. Pilvteenuseosutaja käitab oma arvutuskeskuses eraldi klientide jaoks virtuaalset privaatpilve. Kliendi seisukohast näeb pilv välja nagu privaatpilv, teenuseosutaja annab selle aga tavaliselt kasutusse simultaanteeninduses ehk jagatud taristus. Hallatud privaatpilve korral võib pilvtaristu seevastu olla paigutatud ka oma arvutuskeskusesse. Seda käitab ja haldab siiski väline teenuseosutaja.

Ühispilv

Ühispilve koonduvad sarnaste tööstusharude või huvidega asutused ja kasutavad koos pilve keskkonda, mille pilvteenuseosutaja annab spetsiaalselt selle kooskonna käsutusse. Ühispilvi kasutatakse ka avalikus halduses. Siin annab kasutajarühma pilvteenuseosutaja rakenduse kasutada eraldi pilvteenusena, nt personalihaldus või e-posti teenus.

M 4.463 Rakenduse turvaline installeerimine

Algatamise eest vastutavad: IT-juht, vastutav spetsialist
Rakendamise eest vastutab: administraator

Pärast testide ja rakendusloa väljastamise edukat lõpetamist tuleb planeerida rakenduse Roll-Out või installeerimine. Siinkohal on kasulik koostada installeerimisjuhend (vt M 2.84 Tüüptarkvara installeerimisjuhendite otsustamine ja koostamine). Enne tarkvara installeerimist tuleb üle kontrollida tarkvarataarne täielikkus ja korrektsus (vt M 2.90 Kohaletoimetuse kontroll) ning kindlaks teha kasutatava tarkvara terviklus (vt M 2.86 Tarkvara tervikluse tagamine). Installeerimisel tuleb rakendada meedet M 2.87 Tüüptarkvara installeerimine ja konfigureerimine , mis on rakendatav ka individuaaltarkvara korral.

Selleks, et hiljem jooksva töö käigus kontrollida, kas rakendus on õigesti konfigureeritud ja et lihtsustada rakenduse uuesti installeerimist, tuleks rakenduse installeerimine dokumenteerida kõikides selle etappides. See võib toimuda näiteks üksteisele järgnevate installeerimisekraanide kuvatõmmiste vormis, milles teostatakse alati vastavad seadistused.

Hilisemate konfiguratsioonimuudatuste läbiviimisel või rakenduse värskenduste korral tuleb tähelepanu pöörata sellele, et see dokumentatsioon oleks ajakohastatud. Hilisemate konfiguratsioonimuudatuste ainuke dokumentatsioon Ticket-süsteemis või Change-Tool'is toob tavaliselt kaasa selle, et nõutud konfiguratsiooni ei ole ilma suure töömahuta võimalik kontrollida. Seega ei ole rakenduse konfiguratsioon hiljem enam kergesti kontrollitav (vt ka M 2.34 IT-süsteemi muutuste dokumenteerimine).

Kontrollküsimused:

- Kas rakenduste installeerimine on dokumenteeritud nii, et algse installeerimisega mitte kursis olev administraator saab selle dokumentatsiooni abil edukalt läbi viia?

M 4.464 Turbe tagamine rakenduste igapäevatöös

Algatamise eest vastutavad: erialaspetsialist, infoturbeametnik
Rakendamise eest vastutab: administraator, infoturbeametnik, IT-juht

Rakenduse või spetsiaalse protseduuri käitamise ajal tuleks tagada, et kasutajat toetatakse piisavalt küsimuste ja probleemide korral. See võib toimuda IT-süsteemi, nt IT-kontaktisiku kasutamise või nn Service- või User-Help-Desk'i (SD/UHD) kaudu. Lisaks tuleks kasutajaid asjakohaselt toetada ka erialaste aspektide osas. See võib toimuda näiteks Key-User'i või nn erialase juhtimiskeskuse kaudu. Need korraldavad uute kasutajate algse juhendamise ja koolituse, toetavad rakenduse õigel kasutamisel ja võtavad vastu nõudeid rakenduse järgmistele versioonidele.

Rakenduse turvalisusega seotud oluline aspekt jooksva töö käigus on nõuetekohane pääsuõiguste andmine (vt M 2.8 IT-rakendustele ja andmetele pääsuõiguste andmine) ja pidevalt ajakohane dokumentatsioon volitatud kasutajate ja õiguste profiilide kohta (vt M 2.31 Volitatud kasutajate ja õiguste profiilide dokumenteerimine). Antud volituste õigsust tuleb regulaarselt kontrollida. Tähelepanu tuleb pöörata sellele, kas rakenduse logiandmeid hinnatakse regulaarselt (vt M 2.64 Logifailide kontroll). Siin tuleb tähelepanu pöörata kõikidele kehtivatele spetsiifilistele seadusest tulenevatele ja lepingulistele nõuetele, mis puudutavad logifailide säilitamise aega, nende kättesaadavust kolmanda isiku kaudu (nt järelevalveametid) ja hindamisnõuetele.

Tavaliselt tekib rakenduse jooksva kasutamise käigus vajadus rakenduse funktsionaalseks sobitamiseks, tuleb kõrvaldada vigu või sulgeda turvaauke. Turvapaikade ja muudatuste halduse läbiviimisel tuleb arvesse võtta mooduli B 1.14 Turvapaikade ja muudatuste haldus . Erilist tähelepanu tuleb pöörata sellele, et:

- turvalisuse seisukohalt kriitilised turvapaigad ja värskendused tuleb paigaldada kiirelt (vt M 2.273 Turvalisust mõjutavate paikade ja värskenduste kiire paigaldamine),
- konfigureerimismuudatused, sh turvapaigad ja värskendused on eelnevalt nõuetekohaselt testitud ja väljastatud (vt M 2.556 Rakenduste katsetamine ja kasutusloa väljastamine) ning teostatakse hoolikalt (vt M 4.78 Konfiguratsioonimuudatuste hoolikas teostamine) ja
- konfiguratsioonimuudatused on nõuetekohaselt dokumenteeritud (vt M 4.463 Rakenduse turvaline installeerimine).

Lisaks tuleb kindlaks teha, kas andmevarundusi viiakse läbi nõuetekohaselt (vt M 6.33 Andmevarunduskontseptsiooni loomine) ja kas olemasolevate andmevarunduste alusel on võimalik rakenduse taastamine (vt M 6.41 Andmete taastamise harjutamine). Kindlaks tuleb määrata andmevarunduste liik ja maht ning seejuures võib erinevate komponentide jaoks olemas olla andmevarunduse

erinevaid protseduure, nt lähtekoodi, konfigureerimisandmete, logiandmete ja sisuandmete jaoks.

Kolmanda isiku poolt arendatud rakenduste korral on teatud juhtudel autoriõigusega seotud rikkumiste ennetamiseks vajalik litsentsihaldus. Samuti on tõrgeteta töö tagamiseks kasulik, et kõikidel asutuse töökohtadel kasutatakse rakenduste ühtseid versioone (vt M 2.88 Tüüptarkvara litsentsi- ja versioonihaldus).

Kontrollküsimused:

- Kas kasutajaid toetatakse rakenduse jooksva kasutamise käigus piisavalt?
- Kas rakenduste juures teostatakse regulaarseid logiandmete analüüse ja kontrolle väljastatud volituste osas?
- Kas on tagatud, et rakendustes olevad turvaaugud suletakse kiirelt?

M 4.465 Mobiil- ja nutitelefonide ning tahvel- ja pihuarvutite kasutuselt kõrvaldamine

Algatamise eest vastutab: infoturbeametnik

Rakendamise eest vastutab: IT-juht

Ikka ja jälle avastatakse kasutatud mobiil- ja nutitelefonidel, tahvel- ja pihuarvutitel eelnevate omanike konfidentsiaalseid andmeid ja nii kahjustatakse asutuse, kes on seadme müünud või mittekohaselt kõrvaldanud, infoturvet. Asutuste seadmeid ostetakse kokku ka suunatud rünnete jaoks ja otsitakse tundlikke andmeid.

Kõrvaldatud mobiil- ja nutitelefonidel, tahvel- ja pihuarvutitel peavad kõik kaitset vajavad andmed olema nõuetekohasel moel hävitatud. Selleks tuleks seadme mälu ja vajaduse korral olemasolev mälukaart kustutada spetsiaalse tarkvaraga.

Seade tuleb lähtestada tehaseseadetele. Lisaks sellele tuleb kontrollida, kas kõik andmed on tõesti kustutatud, selleks võib vastutav isik kasutada spetsiaalset Computer-Forensic-tarkvara ja seadmeid. Kui ekspertiisi abiga leitakse ikkagi vastavaid kriitilisi andmeid ja teatud mobiiltelefoni jaoks ei ole olemas ühtki meetodit andmete turvaliseks kustutamiseks, soovitatakse seade hävitada. Kui kõrvaldatakse ainult väline mälukaart, tuleks järgida meedet M 2.13 Tundlike ressursside jäljetu hävitamine .

Kui ära tuleb müüa nutitelefon, tahvel- või pihuarvuti, mille operatsioonisüsteemi tuuma või operatsioonisüsteemi muudeti infoturbe meetmete tõttu, tuleb arvestada sellega, et antud meetme kasutamisega kustub tavaliselt tootja garantii või tugi. Seetõttu tuleb kaaluda, kas need meetmed tuleb enne müüki tühistada.

Mobiil- ja nutitelefone, tahvel- ja pihuarvuteid ei tohi tavaliselt visata olemprügi hulka. Järgida ja kontrollida tuleb vastavaid kõrvaldamise eeskirju.

Kontrollküsimused:

- Kas töökorralduslikult on tagatud, et kaasaskantavaid seadmeid kontrollitakse ja need kõrvaldatakse eraldi?
- Kas andmete turvaliseks kustutamiseks ja tulemuse kontrollimiseks on olemas abivahendid?

M 4.466 Viirusetõrjeprogrammide kasutamine nutitelefonides ning tahvel- ja pihuarvutites

Algatamise eest vastutavad: IT-juht, infoturbeametnik

Rakendamise eest vastutavad: administraator, kasutaja

Viirustõrjeprogrammidel nutitelefonide, tahvel- ja pihuarvutite jaoks on tavaliselt muud kaitsefunktsioonid kui nende vastetel teistele klientidele (vt G 5.193 Nutitelefonide, tahvel- ja pihuarvutite ebapiisav kaitse pahavara eest).

Kahjurvaravastased kaitseprogrammid tuleb välja valida vastavalt asutuse kaitsevajadusele ja võttes arvesse nõudeid, mis on esitatud kaitsele lõppseadmete kaotuse või varguse korral (vt M 6.159 Nutitelefonide ning tahvel- ja pihuarvutite kaotuste ja varguste ennetamine). Need peavad olema tsentraalselt installeeritud ja seadistatud.

Programmid peavad igapäevaselt uuendama allkirjade andmebaasi ja vähemalt üks kord nädalas läbi viima täieliku skaneerimise. Seoses sellega, et selline skaneerimine võtab lõppseadme protsessori ressursid teatud ajaks oma käsutusse, peaks need toimuma ajal, mil lõppseadet kasutatakse vähe või ei kasutata üldse. Kaitseprogramm peaks seejuures läbi uurima kõik failitüübid ja nakatunud failid hilisemaks analüüsiks karantiinikausta panema. Kui karantiinifunktsiooni ei ole või kahjurvara edasine analüüs ei ole võimalik muudel põhjustel, peaks programm olema seadistatud nii, et see kustutab nakatunud failid kohe. Igal juhul tuleb sellise sündmuse korral teavitada IT-kasutajatuge või infoturbe juhtkonda. Nakatunud lõppseade tuleks nii kiiresti kui võimalik IT-süsteemide kaudu täpsemalt muude kahjurvaraprogrammide suhtes läbi uurida.

Kui nutitelefon, tahvel- või pihuarvuti ühendatakse PC-ga ja andmed salvestatakse kaasaskantavale lõppseadmele, peaks kaitseprogramm uued andmed nii kiiresti kui võimalik üle kontrollima. Lisaks tuleks ka kõik äsja installeeritud rakendused kahjurvara osas üle kontrollida ja viiruse leidmisel tuleks see eemaldada. Tuleks leida selline viirusetõrjeprogramm, mis testib võrguliiklust internetis surfamisel lokaalselt kahjurvaraprogrammide osas. Kasutajate tähelepanu tuleb juhtida sellele, et nad tohivad internetis surfata ainult selle kaitsega. Kui lõppseadmed on asutuse võrguga ühendatud VPN-i kaudu ja kui asutus juba kontrollib kogu võrguliiklust kahjurvaraprogrammide suhtes, ei pea võrguliiklust lokaalselt enam kontrollima.

Kontrollküsimused:

- Kas lõppseadmele installeeriti viirusetõrjeprogramm, mis vähemalt üks kord nädalas kontrollib kõiki kasutajaandmeid kahjurvara suhtes ja värskendab iga päev oma viiruste andmebaasi?
- Kas viirusetõrjeprogramm on konfigureeritud nii, et see kontrollib veebiliiklust kahjurvara suhtes ja tõrjub nakkusi?
- Kas viirusetõrjeprogramm on konfigureeritud nii, et uusi andmeid ja rakendusi kontrollitakse kohe kahjurvara suhtes ja need kustutakse või eemaldatakse viiruse leidmisel?

M 4.467 Nutitelefonide, tahvel- ja pihuarvutite rakenduste valimine

Algatamise eest vastutavad: IT-juht, infoturbeametnik

Rakendamise eest vastutavad: administraator, kasutaja

Nutitelefonide, tahvel- ja pihuarvutite rakendusi müüvad tavaliselt lõppseadmete või operatsioonisüsteemide tootjate veebipoed. Tavalistes poodides pakuvad rakendusi nii suured ettevõtted kui ka üksikud arendajad. Rakenduste hinnad on väga erinevad ja ulatuvad tasuta rakendustest kuni mitmekohaliste summadega rakendusteni. Tavaliselt on tööalaseks kasutamiseks saadaval väga palju rakendusi.

Lisaks sellele on veel mõningaid veebipoode, millele pääseb tavaliselt ligi üksnes ringiga, nii et viiakse läbi kas „Jailbreak" (iPhone'i või iPad'i korral) või lubatakse Androidi puhul seadistustesse tundmatust allikast pärinev installatsioon. Jailbreak'i ei tohiks mingil juhul teostada ja tundmatutest allikatest pärit installatsiooni tohiks kasutada üksnes pärast allika põhjalikku kontrollimist üksikute rakenduste jaoks.

Nutitelefonide, tahvel- ja pihuarvutite rakendused tuleb välja valida vastavalt nende lõppseadmete kasutuseesmärgile ja lõppseadmetel olevate andmete kaitsevajadusele ning neid tuleb enne kasutamist testida. Seepärast peaks IT-süsteem enne installeerimist koostama nimekirja soovitud funktsioonidest ja omadustest. Lisaks sellele tuleb määratleda kriteeriumid, mis rakendustel mingil juhul olemas olla ei tohi. Siia alla kuulub näiteks aadressiraamatu volitamata saatmine aadresside edasimüüjale. Nende nõuete alusel tuleks kõne alla tulevad rakendused üle kontrollida kasutajakommentaaride ja teiste asutuste testide alusel, et teha kindaks, kas need töötavad usaldusväärselt ja kas turvavärskendused on kiiresti saadaval. Seejärel tuleks kõiki rakendusi IT-süsteemiga testida ja kontrollida ning alles siis võib need kasutajale kasutada anda. Tuleb kaaluda rakenduste asutusesisese poe loomist, mille kaudu saaks soetada rakendusi.

Kui selliseid rakendusi ei ole, mis vastavad kvaliteedi- või turbenõuetele, tuleb rakendused ise arendada. Selleks tuleb arvesse võtta moodulit B 5.25 Rakendused . Vastavalt rakenduse litsentsile on võimalik neid kohandada oma vajadustele ja lülitada näiteks välja kriitilised programmide käivitamised, nagu näiteks veebiserveritele, aadressiraamatu laialisaatmine või alusetu GPS-positsioneerimine. See võib olla hinnaline alternatiiv asutuse enda rakendustele.

Kui kasutajad soovivad lisarakendusi, mida ei kasutata tööalastel eesmärkidel või mitte ainult tööalastel eesmärkidel, peaksid ka selle jaoks olema ühtsed eeskirjad. Kui need programmid, nt kaardimängud või Sudoku, ei kahjusta infoturvet ja kui töötajad tasuvad nende eest ise, võib rakendust tavaliselt lubada. Kui see nii

ei ole, tuleb töötajale otsust põhjendatult selgitada, et seda ei välditaks.

Kontrollküsimused

- Kas lõppseadmete rakendused valitakse välja kindla eesmärgiga, kohandatakse ja testitakse enne kasutusse võtmist?

M 4.468 Isikliku ja tööalase kasutamise lahutamine nutitelefonides ning tahvel- ja pihuarvutites

Algatamise eest vastutab: infoturbeametnik

Rakendamise eest vastutab: IT-juht

Kui nutitelefone, tahvel- või pihuarvuteid kasutatakse tööalaselt ja isiklikult, tuleb mõlemad kasutused lahutada. See on võimalik mitmel moel.

- Kõige lihtsamal juhul installeeritakse seadmetele rakendus, mis haldab kõikide tööalaste andmete ja juurdepääsudega andmemahutit. See rakendus peab olema kasutamiseks kõikide tööalaste tegevuste jaoks, nagu e-post, tähtajad, kontaktid, ülesanded, sisaldama oma veebilehitsejat ja rajama iseseisvalt krüpteeritud ühenduse asutusega. Erinevate rakenduste lahutamine toimub siiski ainult operatsioonisüsteemi kaudu. Seetõttu on selle lahutamise tõhusus sõltuv kasutatavatest operatsioonisüsteemidest ja nende juurdepääsu kontrollimise võimalustest (Mandatory Access Control, MAC) ja seega süsteemiti erinev. Andmemahuti variandi jaoks ei pea reeglina sekkuma operatsioonisüsteemi endasse. See on olemas erinevate operatsioonisüsteemide jaoks. Olenemata sellest, millise tootja isiklike ja tööalaste andmete lahutamise rakendust kasutatakse, peaks see tööalased andmed mahutis krüpteerima ja takistama seadme kasutamisel isiklikul eesmärgil juurdepääsu andmetele muude, mõeldavalt pahatahtlike rakenduste poolt. Lisaks võib olla kasulik, et IT-süsteem koostab koos turvahaldusega keelunimekirja (Blacklist) rakendustest, millel on funktsioonid või õigused, mille tõttu võidakse ohustada tööalaste rakenduste infoturvet. Lisaks peaksid kasutajad end enne juurdepääsu mahutile edukalt autentima. Ühendused asutuse võrguga peavad olema kaitstud krüptograafiliselt. Lahendused, mis seda ei toeta, ei paku piisavat kaitset ja neid ei tohiks seetõttu kasutada.
- Teine võimalus isiklike ja tööalaste kasutamiste lahutamiseks lõppseadmetel on jätta andmed ka töötlemisel asutuse serveritele. Sellisel juhul antakse kliendi kasutusse ainult pind, millega kaitstud võrguühenduse kaudu asutuse serveri rakendust kasutatakse. Vastav lõppseadmel olev programm tuleb seejuures konfigureerida nii, et andmeid ei saa salvestada lokaalselt. Selliseid Thin-Client'e või serveril põhinevaid lahedusi kasutatakse pikemat aega juba ka sülearvutitel. Selleks, et serveril põhinev lahendus saaks töötada, peab siiski igal kasutushetkel olema saadaval piisavalt dimensioneeritud internetiühendus. Lisaks tuleb teenus kohandada nutitelefoni või tahvelarvuti raamtingimustele, nt puutetundlik ekraan hiire ja klaviatuuri asemel.
- Veel üks võimalus seisneb selles, et mõlemaid kasutusalasid kasutatakse kui erinevaid virtuaalmasinaid samal seadmel. Vastupidiselt andmemahuti variandile ei lahutata virtualiseerimisel isiklikku ja tööalast kasutamist mitte rakendustasandil, vaid operatsioonisüsteemi tasandil. Seeläbi lahutatakse liidesed, mida muidu kasutatakse rakenduste vahel operatsioonisüsteemi kaudu koos selle olemasoleva juurdepääsukontrolli mehhanismidega. Virtuaalmasinate vaheline andmevahetus on võimalik ainult sügavamal asuva virtualiseerimiskihi kaudu Hypervisor'i vormis (ka Virtual Machine Monitor, VMM). Lisaks sellele võib üksikutele virtuaalaladele alati installeerida oma rakendusi ja kasutada neid üksteisest eraldatuna. Nii arvestatakse ka kasutaja vajadustega, et installeerida oma rakendusi ja neid kasutada. Keelunimekiri ei ole sellisel juhul tavaliselt vajalik, sest rakendused töötavad

ainult virtuaalmasinates ja seega ei pääse isiklikud rakendused ligi tööalastele andmetele ja rakendustele.

Iga asutus peab kontrollima, millised esitatud lahendustest vastavad levitatud andmete kaitsevajadusele ja on kohased asutuse turvastrateegiale. Üldiselt võivad otsuselangetamist mõjutada veel järgmised eelised või puudused:

- virtualiseerimislahendus pakub Hypervisor'i vastava kvaliteedi juures rohkem turvalisust kui Container-lahendus;
- virtualiseerimislahenduse korral peab sekkuma väga sügavale operatsioonisüsteemi või see tuleb isegi välja vahetada. Paljud seadmetootjad on selle keelanud ja ennetavad seda tehniliste meetmetega. Samuti lõpeb tavaliselt selliste sekkumistega operatsioonisüsteemi lõppseadme garantii;
- sageli tõstab virtualiseerimislahendus oluliselt voolu tarbimist, nii et aku, võrreldes seadmega, kus ei toimu virtualiseerimist, läheb kiiremini tühjaks;
- virtualiseerimislahendust ei saa realiseerida kõikidel seadmetel, sest mõned seadmedraiverid ei ole saadaval;
- Container-lahendus pakub küll vähemal määral turvalisust kui virtualiseerimine, kuid sellega ei sekkuta ka nii sügavale operatsioonisüsteemi, nii et seadme garantii tavaliselt sellega ei kao;
- nii Container- kui ka virtualiseerimislahenduse korral võivad asutuse kaudu teostatavad andmevarundused kogemata kaasata ka isiklikke andmeid. Seetõttu tuleb selle meetme rakendamise jaoks tavaliselt kaasata ka andmekaitseametnik. Virtualiseerimislahenduse korral on isikuandmete ettevaatamatu kogumine selgelt ebatõenäolisem, sest siin on isiklike ja tööalaste kasutamiste lahutamist rakendatud rangemalt. Thin-Client-lahenduse korral on see aga seevastu välistatud, sest tööalaseid andmeid ei salvestata lõppseadmele ja seetõttu ei pea neid ka kaitsma;
- Thin-Client-lahendus eeldab pidevalt saadaval olevat ja piisavalt dimensioneeritud internetiühendust. Lühiajalised ühenduste katkestused võivad kahjustada serveril olevaid rakendusi ja võivad andmed isegi hävitada. Lisaks sellele tõuseb pideva andmeühenduse puhul voolu tarbimine märgatavalt, mille tõttu on kasutusaeg kuni järgmise laadimiseni lühem.

Kontrollküsimused

- Kas kaasaskantavatel lõppseadmetel lahutatakse tööalased ja isiklikud andmed üksteisest kaitstud Container'i või virtualiseerimislahendusega?
- Kas tööalaste ja isiklike andmete lahutamise meetme võtmisel kaasatakse ka andmekaitseametnik?

M 4.469 GSM-koodide sissesmugeldamise tõkestamine telefonifunktsioonidega lõppseadmetes

Algatamise eest vastutab: infoturbeametnik

Rakendamise eest vastutab: IT-juht

GSM-koodide hulk ja nende funktsioon on tootjaspetsiifiliselt iga lõppseadme jaoks erinev. Tavaliselt ei saa aga GSM-koode üldiselt välja lülitada. Selleks, et GSM-koode ei smugeldataks telefonifunktsiooniga lõppseadmetesse, tuleb rakendada järgmisi soovitusi.

Selleks, et takistada, et ründe toimepanija ei sisestaks GSM-koode otse lõppseadmesse, ei tohiks seadet jätta kunagi järelevalveta. Lisaks sellele peab koodilukk olema aktiveeritud.

Selleks, et takistada GSM-koodide lõppseadmesse sisestamist interneti veebilehtedelt, tuleb installeerida programmid, mis kontrollivad lokaalselt külastatud internetilehti ja filtreerivad vastavad GSM-koodid välja. Selleks on turul vastavaid rakendusi. See filtreerimisfunktsioon on sageli integreeritud ka nutitelefonide, tahvel- ja pihuarvutite viirusetõrjeprogrammidesse.

Selleks, et takistada GSM-koodide smugeldamist Near-Field-Communication-(NFC)-liidese või QR-Code'i kaudu, peavad rakendused olema lõppseadmel konfigureeritud nii, et need ei tõlgenda ega ekspordi NFC kaudu või QR-Code'ist vastuvõetud andmeid kohe, vaid teavitavad kõigepealt kasutajat vastuvõetud andmete sisust ja lasevad eksportimise kasutajal kinnitada. Kasutajaid peab olema selles osas teavitatud, et nad iga päringut ka tõesti kontrollivad ja GSM-koodid alati tagasi lükkavad. Selleks tuleb neile teada anda, et GSM-kood algab tel:-iga ja URL HTTP://-ga või HTTPS://-iga.

Kontrollküsimused

- Kas lõppseadmel on seadistatud koodilukk?
- Kas lõppseadmel on rakendus, mis kontrollib veebiliiklust GSM-koodide osas ja filtreerib need koodid välja?
- Kas lõppseadmel on NFC või QR-koodide jaoks installeeritud ainult sellised programmid, mis teavitavad kasutajaid vastuvõetud andmete sisust ja nõuavad eksportimiseks kinnitust?

M 4.471 Windows 8 uute turbefunktsioonide ülevaade

Algatamise eest vastutavad: infoturbametnik, IT-juht

Rakendamise eest vastutavad: administraator

Windows 8 kujutab endast ühelt poolt turvalisusega seotud aspektide kohaselt Windows 7 operatsioonisüsteemide järjepidevat edasiarendust, peale selle viidi aga sisse ka täiesti uued turvafunktsioonid. See on osaliselt tingitud süsteemi ülesehitusest: nii saab uusi rakendusi installeerida üksnes App-Store'i kaudu, x86-protsessorite buutimisprotsessi kaitsmine UEFI-süsteemidel toimub Secure Boot'i kaudu. Osaliselt on süsteemi sisse toodud ka täiesti uued funktsioonid (nt Windows To Go koos oma turvalisusega seotud konfigureerimisvõimalustega). Alljärgnev ülevaade näitab Windows 8 turvalisusega seotud olulisi uuendusi ja viitab vastavatele täpsemaid üksikasju sisaldavatele meetmetele. Arvesse võetakse vahepeal Microsofti poolt väljatoodud Windows 8 värskendusi Windows 8.1 kujul.

Buutimiseelse ja buutimisetapi kaitse

Üks tähtsamaid Windows 8 operatsioonisüsteemi uuendusi on süsteemi käivitamisprotseduuri kaitsmine. Kaitsmine toimub süsteemi käivitamise erinevates etappides. Buutimisprotsessi kaitsmise eeldus on senise harjumuspärase BIOS-i asemel UEFI (Unified Extensible Firmware Interface) (vt M 2.559 Windows 8 soetamine).

Järgmised funktsioonid kaitsevad süsteemi käivitamist:

Secure Boot Windows 8-s

Secure Boot määratleti Unified Extensible Firmware Interface'i (UEFI) versiooni 2.3.1 järgi. Sellega soovitakse vältida soovimatu tarkvara (nt kahjurvara) käitamist. Secure-Boot-režiimis laadib süsteemi riistvara eranditult üksnes UEFIBootloader'eid, mille digitaalne allkiri või räsi on eelnevalt salvestatud. Samas ei tohi operatsioonisüsteemi selleks installeerida BIOS-režiimis.

ELAM (Early Launch Antimalware)

ELAM-draiver (Early Launch Anti Malware) on esimene draiver, mis käivitatakse Windowsi tuuma järgi. Seeläbi on võimalik kontrollida kõiki teisi draivereid seoses juurkrattidega. Kontrollimine toimub samas siiski vaid tuntud juurkrattide või buutimiskomplektide räsiväärtuste alusel. Uued ja tundmatud juurkratid võivad seega jääda tuvastamata.

Measured Boot

Measured Boot protokollib kõik laaditud tarkvara komponendid (riistvara ja draiver) süsteemi käivitamisel. Seejärel võib järgmine tarkvara, nt viirusetõrjetarkvara, või võrguteenus kasutada loodud protokolli süsteemi oleku kontrollimiseks.

Kaitse kahjurvara eest ja muud turvafunktsioonid

Windows Defender kui täielik Security-Suite on nüüd Windows 8 süsteemi lahutamatu koostisosa.

Vaatamata integreeritud turvafunktsioonile, tuleks asutuses Windows Defender'i kaudu kontrollida eraldi Security-Suite'i vajadust.

Muud uued turvafunktsioonid on järgmised:

Malicious Software Removal Tool

SmartScreen: see programmikäivitusi kontrolliv funktsioon on nüüd olemas kogu süsteemi ulatuses. SmartScreen'i rakendamise korral tuleb arvestada andmekaitsenõuetega (vt meede M 4.472 Andmete kokkuhoid Windows 8 puhul).

Võimalus kasutada funktsiooni „Family Safety" piiratud õigustega töökohtade jaoks (nt kioski režiim). See funktsioon võimaldab piirangut veebifiltri kasutamisega või rakenduste käitamise piirangut.

Windows To Go

Asutuse mobiilsed teenusekasutajad saavad värskelt loodud Windows-To-Goinstallatsiooni kaudu installeerida oma isikliku keskkonna USB-mälupulgale.

Turvalisuse tagamiseks on Windows To Go's juurdepääs USB-mälupulkadele või kõvaketastele standardina inaktiveeritud. Sellega vähendatakse oluliselt ohtu nakatuda väliste lisaseadmete kaudu kahjurvaraga.

Failid või rakendused on kasutaja jaoks siiski saadaval.

Uuendused rühmasuunistes

Windows 8 ja vastava Windows 2012 serveri juurutamisega loodi uued rühmasuuniste objektid (GPO), ja laiendati oluliselt olemasolevaid. Tuleb tähele panna, et uusi GPO-sid saab Windows 2012 serveril kasutada reeglina üksnes koos Active Directory'ga. Olulised uued GPO-d Windows 8 jaoks on muu hulgas võimalus kasutada või lukustada suvandeid „PIN Logon" ja „Picture Password" logimismeetoditena. Peale selle laiendati biomeetrilist turvet (Windows Biometric Framework). Dynamic Access Control'i (DAC) kaudu saab andmeid liigitada automaatselt või käsitsi. See võimaldab kontrollida pöördusi. Näiteks saab kontrollida juurdepääsu konfidentsiaalsetele andmetele.

Uuendused turvaseires

Uue turvafunktsiooni „Dünaamiline juurdepääsu juhtimine" (ingl DAC – Dynamic Access Control) tulemusel saab kasutaja kasutada erinevaid volitusi, olenevalt sellest, kas ta pääseb VPN-võrgu kaudu asutuse ressurssidele ligi töölaualt või sülearvutist. Selle uue funktsiooni kontrollimiseks saab Windows 8-s ja Windows serveris 2012 kasutada alljärgnevaid uusi või täiendatud kontrollimissuvandeid.

Failikasutuse seire

Failikasutuse seire kasutamise korral protokollitakse nüüd ka kasutatud failide atribuutide kohta käivaid andmeid. Täiendatud kasutajate sisselogimiste seire Windowsi serveri ja Windowsi klientsüsteemid pakuvad võimalusi kontrollida kasu-

tajate sisselogimisi. Niipea kui kasutaja sisse logib lokaalselt või võrgu kaudu, loob Windowsi operatsioonisüsteem kontrollimise kohta sündmuse. Alates Windowsi serverist 2012 ja Windows 8-st tuvastatakse täiendatud andmed lisaks sisselogimissündmusele uue sündmuse ID kaudu. Nii protokollitakse nt failile juurdepääsu korral kasutatud faili atribuudid.

Sõnastusel põhinevad seirepoliitikad

Faili või kausta jaoks saab nüüd koostada ka sõnastusel põhinevaid seirepoliitikaid. Selle jaoks võib valida ja koostada erinevaid sündmusi, mille esinemisel luuakse protokollis vastav kirje. Sellise sõnastusel põhineva seirepoliitika näide on andmekasutuse protokollimine, kui asutusevälised isikud pääsevad ligi andmetele, mille jaoks neil puuduvad volitused.

Vahetatavate andmekandjate seire

Juurdepääsu korral vahetatavale andmekandjale luuakse nüüd seiresündmus.

DirectAccess

Siiani oli DirectAccess'i kasutamiseks VPN-juurdepääsu jaoks sisevõrgus vaja tingimata kasutada IPv6. Alates Windows 8-st on nüüd võimalik DirectAccess'i kasutamine sisevõrgus ka IPv4-ga.

Virtuaalsed kiipkaardid

Windows 8-ga saab nüüd kasutada virtuaalseid kiipkaarte. Need emuleerivad füüsiliste kiipkaartide funktsioone, kasutavad aga siiski süsteemi TPM-kiipi.

M 4.472 Andmete kokkuhoid Windows 8 puhul

Algatamise eest vastutavad: andmekaitseametnik, infoturbeametnik
Rakendamise eest vastutavad: administraator, infoturbeametnik

Windows 8 hiljuti kasutusele võetud funktsioonid toovad osaliselt kaasa ulatuslikuma juurdepääsu süsteemi- või kasutajaandmetele. Näitena võib tuua andmete otsese salvestamise pilves rakendusprogrammide abil ja Windows 8 laiendatud turvafunktsiooni SmartScreen (vt G 2.203 Integreeritud pilve-funktsioon).

Andmed, mida operatsioonisüsteem või rakendused ja äpid vajavad, luuakse kasutamise ajal sageli automaatselt, ilma et kasutaja seda märkaks. Seetõttu ei ole kasutajatel sageli võimalik kindlaks määrata edastatavate andmete ulatust ja sünkroniseerimisintervalli.

Täitmaks asjakohaseid konfidentsiaalsuse ja andmekaitsele esitatavaid nõudeid, tuleks enne rakendamist kontrollida, kas Windows 8 kasutatud funktsioonid, rakendused ning äpid on kooskõlas seadusest tulenevate ja organisatsioonis kehtivate nõuetega.

Alljärgnevalt on toodud mõned selliste rakenduste või süsteemifunktsioonide näited, mille puhul tuleb kinnitada nende vastavust andmekaitsele.

Sisselogimine süsteemi Microsofti kontoga

Lisaks klassikalisele sisselogimisele mõnda süsteemi lokaalse või Active Directory'l põhineva konto kaudu, on Windows 8 puhul võimalik süsteemi sisse logida ka nn Microsofti konto kaudu. Selle variandi puhul logib Windows kasutaja äppide kasutamise ja sinna juurde kuuluvate veebilehtede kasutamise korral automaatselt sisse.

Selline konto on vajalik, et installeerida äppe ja pääseda ligi Microsofti Windows Store'ile. Konto loomine ei nõua siiski, et sisselogimine Windowsisse seadistataks ümber Microsofti konto protseduurile. Töökeskkonnas ei peaks seetõttu kasutama sisselogimist Microsofti konto kaudu.

Eeldades, et Microsofti konto tuleb luua, et kasutada teatud äppe, peaksid Microsofti salvestatud andmed kasutajale olema piiratud miinimumini.

SmartScreen

Internet Exploreri kaitsmiseks on Microsoft välja töötanud SmartScreen-filtri, mis blokeerib käivitatavad veebilehed, kui neid tuntakse kalastustüüpi rünnete platvormide või kahjurvara levitajatena. Windows 8-s seda funktsiooni laiendati. Lisaks Internet Exploreri jälgimisele hoiatab filter nüüd vajaduse korral ka selliste programmide käitamise korral, mis toetuvad veebisisude esitamisel operatsiooni-

süsteemile (nt HTML-sisude äpid või esitamine Office'is või Outlook'is), või mida käitatakse asutusevälisest ajamist. Filtri kasutamise eeldus on siiski olemasolev internetiühendus, sest programme ja võimalikku kahjukoodi puudutavat olulist teavet hoitakse tsentraalsetes andmebaasides. Seetõttu kasutab Smartscreen pidevalt ajakohast teavet veebilehtede kohta, mida teatakse olevat kahjulikud. See funktsioon tähendab siiski ka seda, et märkimisväärsed andmed kasutatud IT-süsteemi kohta edastatakse tsentraalsetele teenustele ja salvestatakse vähemalt iga natukese aja järel Microsofti serveritesse. Näitena võib tuua nime ja versiooni ning arvuti käitatavate programmide krüptograafilised kontrollsummad (räsiväärtused) ja lähtesüsteemi IP-aadressid.

SmartScreen-funktsiooni saab täielikult inaktiveerida, valides juhtpaneel | süsteem ja turvalisus | hoolduskeskus | Windowsi Smartscreen-seadistuste muutmine. See peaks toimuma juhul, kui tekkivate kasutusandmete väärkasutamise eest kaitsmine kaalub üles infektsiooni ohu veebijuurdepääsu korral.

Äpid ja (mitte)teadlik pilvteenuste kasutamine

Kui luuakse Microsofti konto, määratakse sellele automaatselt tasuta mäluruum pilves.

Aluseks olevat Microsofti pilve nimetati kuni 2014. aasta veebruarini SkyDrive ja seejärel nimetati see ümber OneDrive'iks.

Vana nimi	**Uus nimi**
SkyDrive	OneDrive
SkyDrive Pro	OneDrive for Business

Sisselogimisel Microsoft konto kaudu salvestatakse OneDrive'is vähemalt järgmised andmed:

- fotod, mis on tehtud arvutiga,
- dokumendid (OneDrive valitakse salvestamisel standardseks salvestuskohaks),
- arvutiseadistuste varukoopiad.

Kui sisselogimine arvutis ei toimu Microsofti konto kaudu, võib sünkroniseerimine toimuda üksnes niinimetatud OneDrive'i äpi kaudu, see on aga alates Windows 8.1-st süsteemi lahutamatu koostisosa. Seetõttu salvestavad ka erinevad äpid andmeid pilvteenustesse. Seega ei ole seejuures osaliselt võimalik mõjutada salvestamise mahtu ega kestust.

„Koju helistamine" äppide poolt

Äppide installeerimises peitub nn „Koju helistamise" funktsiooni (ingl „Phone home") oht. See tähendab, et äpid võtavad automaatselt ühendust tootja serveritega.

Tavaliselt on see äpi soovitud ja elementaarne funktsioon, nt kui laaditakse alla ja kuvatakse ajakohaseid teateid. Siiski ei ole sageli võimalik teada saada täpset teavet pakkujale edastatavate andmete liigi ja ulatuse kohta. Tahtmatu andmeside ja sellega seotud kulude riski kõrval on olemas võimalus, et äpid pääsevad ligi süsteemi isikuandmetele ja edastavad need andmed tootjale.

Rakenduste ja äppide kontrollimine

Enne kui rakendusele või äpile antakse luba selle asutusesiseseks kasutamiseks, tuleks alljärgnevaid punkte hoolikalt kontrollida: millised andmed edastatakse asutusevälisele pilvteenuste osutajale, kuidas sünkroniseerib äpi tootja andmeid ja millised andmed edastatakse selle käigus tootjale. Neid aspekte tuleks eriti arvesse võtta kasutamiseks mõeldud alternatiivsete rakenduste või äppide valikul. Võimaluse korral tuleks loobuda äppidest, millega toimub ebasoovitav või mittevajalik ulatuslik andmete edastamine kolmandatele isikutele.

Kontrollküsimused:

- Kas Windowsi süsteemi sisselogimine toimub lokaalse või Active Directory'l põhineva konto kaudu ja mitte Microsofti konto kaudu?
- Kas kasutajate Microsofti kontod loodi ilma isikute andmeteta või üksnes tingimata vajalike andmetega?
- Kas SmartScreen'i funktsiooni usaldusväärsust kontrolliti ja hinnati asutusesiseste või asutuseväliste andmekaitse nõuete suhtes?
- Kas rakenduste ja äppide valikul võeti kriteeriumina arvesse kolmandatele isikutele andmete edastamise minimeerimist?
- Kas rakenduste vajalikud sideühendused ja edastatud andmed on teada ja dokumenteeritud? Kas rakendused on konfigureeritud nii, et edastatakse ainult vajalik minimaalne hulk andmeid?

M 4.473 XML-transpordikonteinerite pealtkuulamise kaitse SOA-s

Algatamise eest vastutavad: IT-turvaspetsialist, IT-juht

Rakendamise eest vastutavad: administraator, IT-juht

Kui teenusele suunatud arhitektuuris (SOA) edastatakse konfidentsiaalseid andmeid, tuleb nende kaitseks rakendada sobivaid krüpteerimismeetodeid. Need krüpteerivad vastavalt vajadusele kas kogu sõnumi või ainult teatud elemendid, näiteks XML-Encryption'iga (XMLENC W3C järgi). Tuleb kindlaks teha, kas kasutatava krüpteeringu liik (nt terve sõnumi, alamelemendi või XML-elemendi sisu krüpteerimine) vastab ka soovitud konfidentsiaalsuse kaitsele.

Peale selle tuleb tähelepanu pöörata sellele, et loodud sõnumid sisaldaksid üksnes nii palju metaandmeid, et võimalikele ründe toimepanijatele ei pakutaks välja ründepunkte.

Kontrollküsimused:

- Kas XML-i krüpteeritakse?
- Kas kasutatud krüpteeringuga (terve sõnum või teatud elemendid) saavutatakse soovitud konfidentsiaalsuse kaitse?

M 4.474 Turvaaukude kaitse SOA Backend-rakendustes

Algatamise eest vastutavad: infoturbametnik, IT-juht
Rakendamise eest vastutavad: arendaja, administraator

Vahelelülitatud autentimis- ja autoriseerimisvahenditega tuleks kõigepealt piirata ründevõimalusi teenusele suunatud arhitektuuri (SOA) Backend-rakendustele. Peale selle tuleb tagada, et juba autenditud ja autoriseeritud kasutajad ei viiks läbi ründeid nendele süsteemidele.

Backend-rakendusi tuleb kaitsta regulaarsete värskendustega. Lisaks sellele saab filtreerida XML-sõnumeid, et välistada kahjuliku koodi edastamine või kriitiliste käskluste käivitamine.

Seepärast tuleb XML-transpordikonteineri valimisel pöörata tähelepanu sellele, et kaitsevahendeid kasutataks sellisel viisil, millega välditakse sisu kahjustamist.

Kontrollküsimused:

- Kas Backend-rakendusi kaitstakse regulaarsete värskendustega?
- Kas XML-sõnumeid filtreeritakse kahjukoodi ja kriitiliste käskluste suhtes?

M 4.475 Kaitse identiteediteenuste teesklusrünnete vastu

Algatamise eest vastutavad: IT-turbespetsialist, IT-juht
Rakendamise eest vastutavad: kasutajad

Teesklusrünnete takistamiseks identiteediteenustele tohiks kasutaja käivitada üksnes teenuseid, mida ta saab usaldada. See võib tema jaoks olla tuvastatav kehtiva sertifikaadi näol vastava teenuse kohta või tagatud etteantud identiteedi automaatse tõendiga (Service Authentication). Kasutaja peaks iga teenusepöörduse korral kontrollima kriitiliselt esitatud usaldusväärsusele viitavaid omadusi.

Kontrollküsimused:

- Kas on tagatud, et identiteediteenuseid kasutatakse kehtiva sertifikaadiga?

M 4.476 WS-Notification-Subscription'i kaitse Broker'is

Algatamise eest vastutavad: IT-turbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator

NotificationConsumer saab kas enda või kolmanda isiku jaoks teostada Subscription'i NotificationBroker'i juures. Standardi kohaselt ei teavita maakler ka kolmandat tarbijat tema eest tehtud Subscription'i kohta. Selleks, et ründe toimepanija ei saaks seda mehhanismi ära kasutada, peab määratud tarbija end maakleri jaoks autentima. Kui seda ei toimu, peaks maakler Subscription'i põhimõtteliselt tagasi lükkama. Eduka Subscription'i korral peab maakler lisaks kas URI (Uniform Resource Identifier) või WS-Resource'i kaudu saatma vastu sõnumi teostatud määramise kohta. Selle teabega saab tarbija kontrollida oma Subscription'i olekut. Ka see vastus tuleb igal juhul autentida.

Subscription määratakse NotificationConsumer'i poolt üks kord ja see kehtib tavaliselt nii kaua, kuni seesama tarbija selle NotificationBroker'i juures ära kustutab. Olemasoleva Subscription'i korral ei teavita maakler tarbijat sellest, kas varem määratud Subscription on endiselt olemas. Seetõttu ei tuvasta tarbija, kas maakler ei reageeri üksnes selle tõttu, et ei ole andmeid sõnumite (Notification) kohta või ei eksisteeri enam Subscription'it.

Kontrollküsimused:

- Kas on tagatud, et NotificationConsumer ja NotificationBroker autendivad end üksteise suhtes?

M 4.477 WS-Notification-Subscription'i kaitse

Algatamise eest vastutavad: IT-turbespetsialist, IT-juht
Rakendamise eest vastutavad: administraator

NotificationBroker vastutab sõnumi (Notification) saatmise eest. Sellel eesmärgil hindab see ainult sõnumi teemat (Topic). Tegelik sisu maaklerit ei huvita. Seetõttu võib sõnumi sisu olla näiteks täielikult krüpteeritud, ilma et see kujutaks maakleri jaoks probleemi. Sõnumite kaitsmiseks kahjustamise eest tuleb need vähemalt allkirjastada. See võib kogu sisu osas ja XML-märgendi puhul ka märgendi atribuudi suhtes toimuda protokolli päises. Vajaduse korral võib saatja konfidentsiaalsuse kaitseks krüpteerida ka elemendid sõnumi sisus (SOAP body).

Kontrollküsimused:

- Kas SOAP-sõnumeid (vajaduse korral ka märgendi atribuuti) allkirjastatakse?
- Kas SOAP-sõnumid krüpteeritakse kõrgema kaitsevajaduse korral?

M 4.478 Võtmehaldus SOA-s

Algatamise eest vastutavad: IT-turbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator

Teenusele suunatud arhitektuuris (SOA) peab saama teenuseid samamoodi identifitseerida nagu kasutajate või rollide puhul. Selleks on vaja, et kaasnev identiteedikaitse oleks seotud automaatselt genereeritud asümmeetrilise võtmepaariga ja sellele järgneva automaatse sertifikaadi genereerimise ja avaldamisega.

Rünnete raskendamiseks sellega seotud sertifitseerimisprotsessile, tuleb sertifitseerimisprotsessid paigutada eraldatud „Trusted Key Store'i". SOA-teenuse privaatne võti ei tohi „Trusted Key Store'ist" lahkuda. Sertifitseerimisprotsessi haldamiseks määratakse SOA-teenusele alati Key-Management Service (XML Key Management Service, XKMS). SOA-teenus ja XKMS suhtlevad lokaalselt ja vähendavad seega ründevõimalust kasutatavatele võtmeelementidele. XKMS kui lokaalne sertifitseerimisasutus peab SOA-teenuse avaliku võtme (Public Key) allkirjastama ja avaldama selle kui kehtiva võtme oma infodomeenis.

Kontrollküsimused:

- Kas võtmete paremaks kaitsmiseks rünnete eest kasutatakse lokaalset võtmehaldust?
- Kas avalikustatud võtmed allkirjastatakse?
- Kas SOA-teenuse privaatne võti jääb turvaliselt salvestatuna oma süsteemi?

M 4.479 Poliitikate kaitse SOA-s

Algatamise eest vastutavad: IT-turbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator

Teenusele suunatud arhitektuurides (SOA) korraldatakse juurdepääsud teenustele ja volitused poliitikate (Policies) abil erinevate SOA-platvormide kaudu. Need peavad juba enne teenusekasutaja SOA-keskkonnas tegutsemist olemas olema või enne seda, kui teenuseosutaja teabe või teenused SOA-platvormil kättesaadavaks teeb. Ühes infodomeenis võib kasutada ainult ühte poliitikat. Teisiti väljendades – infodomeen määratleb end oma poliitika kaudu. Kui poliitikat kasutatakse infodomeeni kõikidel SOA-platvormidel, nõuab see, et iga SOA-platvormi kohta kasutatakse ühte lokaalset Policy-Enforcement-Point'i (PEP). Poliitikad peavad infodomeeni kõikide SOA-platvormide jaoks olema tsentraalselt kasutatavad, nt Service-Repository's. Need määratakse kindlaks ja antakse kasutada tavaliselt Web-Services-Description-Language-(WSDL)-Statement'is. Sellise WSDL-faili modifikatsiooniga teenuseosutaja või tarbija juures võidakse valida vale poliitika. Vältimaks poliitikaseadistuste kahjustamise võimalust, peab allkirja väärtus olema „tugevalt" seotud WSDL-failiga, nt XML Strong Binding'i kaudu.

Seeläbi saab üksteisega liita mitu infodomeeni, mille tulemusel pääseb domeeni A teenusekasutaja ligi domeeni B teenuseosutajale. Siinjuures peavad üksikute domeenide administraatorid kooskõlastama poliitikad nii, et teenusekasutaja ei koguks paljude üksteisele järgnevate pöördustega domeenidele ilma volitusteta õigusi. Protseduurist ja sellest tekkivatest poliitikatest tuleks kontrollitavalt kinni pidada.

Kontrollküsimused:

- Kas poliitikaseadistused ja eeskirjad on SOA-s kaitstud kahjustuste eest?
- Kas SOA-poliitika luuakse kontrollitavate eeskirjadega?

M 4.480 WS-Resource'i kaitse SOA-keskkondades

Algatamise eest vastutavad: IT-turbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator

OASIS-standardi „Web Services Resource" (WS-Resource) abil saab teenuseid täiendavalt kaitsta. Standard määrab kindlaks erinevad parameetrid, mis näitavad, kas teenus on kasulik või tuleb see vajaduse korral lukustada. WS-Resource'i parameetrite päritoluks võib olla kaks võimalust. Parameetrite väärtused määratakse kindlaks vahetult seoses sinna juurde kuuluva teenusega, nt teenust tohib kasutada klassifikatsiooniga „avatud", „aste 1" või võrreldavalt. Parameetrite väärtused tuletatakse muudest, väljaspool SOA-keskkonda asuvatest ressurssidest, nt sidepordi ülekandekiirus. Kui SOA-süsteemis kasutatakse ressursse, mis on määratletud madalama klassifitseerimisastmega kui SOAsüsteem, toimub üleminek „klassifitseerimisastmelt 1" „klassifitseerimisastmele 2". Seejuures imporditakse ka klassifitseerimisastme 1 andmed klassifitseerimisastme 2 keskkonda.

Tuleb kaaluda, kuidas kaitsta WS-Resource-teavet meetmes M 4.478 Võtmehaldus SOA-s .

Ülemineku korral „Klassifikatsiooniastmelt 1" „Klassifikatsiooniastmele 2" tuleb sõltuvalt madalama klassifikatsiooniga ressursi tavapärasest käitumisest integreerida täiendavad loogilisuse kontrollid.

Kontrollküsimused:

- Kas on kindlaks määratud meetmed, mis kaitsevad WS-Resource'i teabe üleminekut klassifikatsiooniastme 1 alalt klassifikatsiooniastme 2 alasse?
- Kas on olemas WS-Resource'i andmete loogilisuse kontroll nende üleminekul klassifikatsiooniastme 1 alalt klassifikatsiooniastme 2 alasse?

M 4.481 Ühendusevaba SOAP-suhtluse turvaline kasutamine

Algatamise eest vastutavad: IT-turbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator

UDP kaudu kasutatakse protokolli profiili SOAP eeskätt multiadresseerimise alusel. See kaitseb ka kitsasribaühendusega sidevahendite ressursse. SOAPsõnumid saadetakse siinjuures anonüümsele multiaadressile ja teenuseosutaja ei tea seetõttu tavaliselt, kes on vastuvõtjad.

Takistamaks sõnumite saatmist volitamata vastuvõtjatele, tuleb SOAP-sõnumites endas rakendada vastavat kaitset. Teenuseosutaja saavutab selle sobiva sisukrüpteeringuga, nii et üksnes volitatud vastuvõtjad saavad SOAP-sõnumeid lugeda.

Taasesitusrünnete ennetamiseks tuleks sõnumi krüpteeritud alas kasutada lisaks järjestuste lugejaid.

Kontrollküsimused:

- Kas on kindlaks määratud meetmed, mis takistavad SOAP-sõnumite saatmist volitamata vastuvõtjatele?
- Kas on kindlaks määratud meetmed, mis takistavad SOAP-sõnumite puhul taasesitusrünnet?

M 4.482 Integreeritud süsteemide funktsioonide riistvaraline teostamine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT-turbespetsialist, IT-juht

Rakendamise eest vastutavad: planeerija, arendaja, hankija

Integreeritud süsteemi kavandamise korral määratakse kindlaks, millised funktsioonid töötavad programmeeritaval protsessoril ja milliseid rakendatakse vahetult riistvaras. Potentsiaalne ribalaius on riistvara-tarkvara-sektsioneerimisel suur. Skaala ühes otsas on universaalselt programmeeritavad mitmeotstarbelised protsessorid (General Purpose Processor, GPP), nagu neid kasutatakse ka töökoha arvuti juures. Teises otsas on spetsialiseeritud digitaalsed riistvarasüsteemid, mis käitavad ainult üht programmi (Single Purpose Processor, SPP).

Keskteed täielikult programmeeritavate protsessorite ja puhaste riistvararakenduste vahel kujutavad endast programmeeritavad rakenduspõhise käsustikuga protsessorituumad (Application Specific Instruction set Processor, ASIP). Need on protsessorid, mille käsustik on optimeeritud teatud rakendusviiside jaoks, nt digitaalne signaalitöötlus või juhtimisfunktsioonid.

Ka riistvararakenduste puhul on erinevaid astmeid. Integreeritud lülitusskeemi rakendamise suvandite puhul piisab ribalaiusest alates kiipidest, mis kavandati ja toodeti konkreetsete klientide jaoks, (Application Specific Integrated Circuit, ASIC) kuni kiipideni, mis on küll välja töötatud konkreetsete ülesannete jaoks, kuid mida peetakse nii üldisteks, et neid võib kasutada paljudes erinevates toodetes (Application Specific Standard Product, ASSP). Siia lisanduvad mõned segavormid, nagu nt kiibid, mille tootja on kohandanud kliendi soovi kohaselt (Customer Specific Standard Product, CSSP), mõnede eelnevalt rakendatud elementidega kiibid (ingl structured ASIC) ja eelnevalt määratletud ulatusega ja kliendikonfiguratsiooni jaoks vaba ulatusega kiibid (ingl platform ASIC).

Eriti prototüüpide arenduses on laialt levinud programmeeritavad ASIC-d. Selle tehnoloogia tähtsaimad esindajad on Field Programmable Gate Array (FPGA) ja Complex Programmable Logic Device (CPLD). Mõlemad on integreeritud lülitusskeemid, kuhu saab programmeerida loogilise lülituse, kusjuures sellega on mõeldud, et määratletakse lülitusskeemi funktsioonide struktuur ja mitte, et määratakse kindlaks ajalised protsessid. CDLD-del on võrreldes FPGA-dega oluliselt lihtsam struktuur. Neil ei ole loogikaplokkide ja trigerite programmeeritavaid ventiilimaatrikseid, vaid üksnes konfigureeritav lülitusmaatriks, mis võib ühendada erinevad sisendi signaalid erinevate väljundi signaalidega. CPLD on kohe pärast sisselülitamist kasutusvalmis, samuti nagu ainult üks kord programmeeritav

FPGA. Static random-access memory'l (SRAM) põhinevate elementidega ümberkonfigureeritav FPGA vajab konfigureerimise jaoks laadimistsüklit. FPGA moodulid on suuremad kuid CPLD moodulid ja neil on suurem voolukulu.

Programmeeritavaid loogikamooduleid saab programmeerida väljaspool sihtsüsteemi või, kui on olemas vastavad liidesed, ka sihtsüsteemi sees. Neid kasutatakse tihti selleks, et töötada välja prototüüp. Tootmissüsteemis asendatakse need enamasti ASIC-dega. Edasiarendust kujutavad endast ASIC-d, mis end töötamise ajal ümber programmeerivad ja mis on tänu sellele kohandatavad tegelikele nõudmistele.

Integreeritud süsteemi kavandamisel tuleb arvesse võtta tarkvara või riistvara lahenduste erinevaid turvalisusega seotud omadusi ja kooskõlastada need vastavate turvanõuetega. Aparatuursed algoritmid, nt nagu ASIC või FPGA, panevad ühelt poolt funktsioonide manipuleerimisele vastu suuremad tõkked võrreldes tavaliste tarkvaral põhinevate rakendustega, kuid teiselt poolt on need vähem paindlikud ja ei võimalda üldiselt täiendavate turvamehhanismide hilisemat integreerimist. Kui turvamehhanismid kaasatakse aga algusest peale riistvara arendusse, on neid võimalik tõhusalt rakendada. Riistvaras saab edukalt rakendada ka paralleelseid protsesse, nt võib Java virtuaalmasinat kasutada mitte tarkvarana, vaid riistvarana Java protsessori kaudu.

Kui funktsioone otsustatakse rakendada riistvaras, tuleb arvestada, et ASIC-del ja FPGA-del on IT-turvalisuse suhtes erinevad tugevused ja nõrkused. ASIC-de puhul peituvad ohud projektis ja valmistamises. Selleks et ründe toimepanija ei saaks lisada soovimatuid funktsioone ega tagauksi või uurida välja konfidentsiaalseid andmeid, tuleks kiipe vastavalt testida ning arendus- ja tootmisahel peaks olema usaldusväärne (vt M 2.563 Usaldusväärse tarne- ja logistikaketi ning pädeva tootja valimine integreeritud süsteemide jaoks). FPGA-de korral määratakse lülitus kõigepealt kindlaks riistvara kirjelduskeeles, kusjuures kaasneda võib ka võõras intellektuaalne omand. Lülitust sünteesitakse ja rakendatakse spetsiaalsete projekteerimistööriistadega. Seejärel kantakse konfigureerimise andmed üle FPGA-le. Arvestada tuleb sellega, et võimalik kasutatav võõras intellektuaalne omand oleks usaldusväärne, et projekteerimistööriistad ei saaks kahjustatud ja et andmed kantaks FPGA-le üle kaitstud keskkonnas. Vajaduse korral tuleb ülekanne krüpteerida. Loogikamoodulite korral on erinevusi ka elektromagnetilises ühilduvuses. FPGA-d on osakeste kiirguse ja elektromagnetiliste lainete suhtes tundlikumad kui ASIC-d. Kui integreeritud süsteemi ei töötata välja ise, vaid hangitakse terviku või komponentidena, tuleb samamoodi arvesse võtta nimetatud soovitusi.

Kontrollküsimused:

- Kas riist- ja tarkvaralahenduste projekti üle otsustamisel võeti arvesse tur-

valisusega seotud aspekte?

- Kas projekti otsuse tegemisel, kuidas toimub rakendamine konkreetse riistvaratehnoloogiaga, võeti arvesse turvalisusega seotud aspekte?

M 4.483 Krüptograafiliste protsessorite ja kaasprotsessorite (Trusted Platform Module) kasutamine integreeritud süsteemides

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT-turbespetsialist, IT-juht

Rakendamise eest vastutavad: arendaja, hankija, planeerija

Integreeritud süsteemide korral võib krüptograafiliste algoritmide ja protokollide läbitöötamiseks kasutada täiendavat mikrokontrollerit, nt räsifunktsioonide ja allkirja kinnitamise kiirendamise eesmärgil. Täiendav mikrokontroller suhtleb süsteemi mikrokontrolleriga püsivara-autentimise kehtivuse üle.

Alates konfidentsiaalsuse kõrgest kaitsevajadusest või terviklusest tuleb see suhtlus muuta vastupanuvõimeliseks riistvararünnete vastu, viies

- trajektoorid trükkplaadi sisemistele kihtidele,
- kasutades dünaamilisi signaale (impulsse), et anda põhi-mikrokontrollerile teada edukast buutimisprotsessist ja
- rakendades võimaluse korral mitmeid erinevate dünaamiliste signaalidega PIN-e.

Trusted Computing'i põhimõte määratletakse Trusted Computing Group'is (TCG) rea usaldusväärsete pidepunktide abil süsteemis. Olulised pidepunktid seoses integreeritud süsteemidega on Root of Trust for Measurement (RTM), Root of Trust for Storage (RTS) ja Root of Trust for Reporting (RTR). RTM-i ülesanne on olla pidepunktiks platvormi konfiguratsiooni ülevaatamiseks. See käivitatakse veel enne operatsioonisüsteemi käivitamist. RTM-i käivitamisega mõõdab see riistvara platvormi konfiguratsiooni selle käivitamise ajal, samuti esimest käivitatud tarkvarakomponenti. Seejärel selle töö lõpetatakse ja rohkem tegevusi läbi ei viida. Seega on võimalik tuvastada kõik platvormi või kõigepealt käivitatud tarkvarakomponentide nt Bootloader'i muudatused. Seejärel käivitatud tarkvarakomponentide nagu operatsioonisüsteemi või rakenduste muudatusi sellega ei tuvastata. Sellel eesmärgil kasutatav mehhanism nõuab, et iga tarkvarakomponent mõõdaks vastavalt järgmisena käivituvat tarkvarakomponenti ja kontrolliks selle õigsust. Seega tekib nn „Trusted Chain of Measurement". RTM kujutab endast ahela algust. Mõõtetulemused vähendatakse krüptograafiliste funktsioonide abil räsiväärtusteni ja salvestatakse kaitstud mäluruumides etalonväärustena.

Root of Trust for Storage'it kasutatakse selleks, et salvestada turvaliselt andmeid ja Root of Trust for Reporting'it, et turvalisusega seotud andmeid õigesti esitada.

Integreeritud süsteemid on küll otstarbekohased seadmed, kuid vastupidiselt puhtale riistvara rakendamisele (ASIC) siiski universaalsed arvutid. Seepärast on ka integreeritud süsteemide korral kasulik ja vajalik seadmete konfiguratsioone, tarkvara ja andmeid täpsemalt kontrollida, ega neid pole muudetud. Terviklusele esitatavate kõrgete nõuetega süsteemides olevad andmed tuleks töötleva

süsteemi kaudu autentida, kasutades krüptograafilisi protsessoreid või riistvaraturvamooduleid (Trusted Platform Module). Sidefunktsioonidega integreeritud süsteemide korral peaks olema võimalik seadmeid kindlamalt tuvastada ja nende seadmetega usaldusväärselt suhelda. Lisaks tuleb olekuteave seadme kohta saada usaldusväärselt. Erilist tähelepanu tuleb pöörata sellele, et seade ei saaks duplitseerida teise seadme identiteeti või et seade ei väljastaks enda olekuteabe asemel teise seadme oma.

Usaldust pakkuvat pidepunkti ja sellel põhinevaid kontrollimisi on integreeritud süsteemide puhul enamasti lihtsam teostada kui standardarvuti puhul, näiteks kui püsivara kasutatakse koos lugemispääsuga failisüsteemiga squashfs ning kui konfiguratsioon ja olek salvestatakse tarkvarast eraldi. RTM saab siis mõõta kogu püsivara enne selle käivitamist ning keeruka usaldusahela rajamine pole vajalik. Tänu sellele ei pea kohandama operatsioonisüsteeme ja talitlusaeg ei muutu. Samuti ei ole vaja mõõta eraldi iga tarkvarakomponenti. Mõõta saab kogu püsivarapilti ja võrrelda seda etalonväärtusega.

Kontrollküsimused:

- Kui krüptograafiliste arvutuste jaoks kasutatakse täiendavat mikrokontrollerit, siis kas selle side süsteemi mikrokontrolleriga on piisavalt kaitstud?
- Kas integreeritud süsteemi jaoks on sisse viidud vajalikud usaldust pakkuvad pidepunktid?
- Kas integreeritud süsteemi jaoks on teostatud Chain of Trust?

M 4.484 Salvesti kaitse integreeritud süsteemides

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT-turbespetsialist, IT-juht

Rakendamise eest vastutavad: arendaja, hankija, planeerija

Kui integreeritud süsteemis töötab mitu tarkvarakomponenti, võib olla mõistlik need eraldada. Kui iga komponendi jaoks ei kasutata oma mikrokontrollerit, võib selle saavutada ka salvesti kaitse tehnoloogiatega. Salvesti kaitse eesmärk on struktureerida töömälu ja eraldada alad nii, et programmeerimisviga või ühe programmi tõrge ei mõjutaks teiste programmide või kogu süsteemi stabiilsust.

Takistada tuleb programmide ligipääsu teiste programmide mäluruumile. Andmete paremaks kaitsmiseks integreeritud süsteemidel, millel on kõrged nõuded terviklusele ja käideldavusele, tuleb salvesti kaitsemehhanisme arvesse võtta juba süsteemi projekteerimisel. Valida tuleb teostusvorm, mis tagab vajaliku turbeastme ja ei ole vastuolus integreeritud süsteemi kasutusvajadustega. Kaks põhimõttelist lahendust on riistvara-salvestikaitse ja tarkvara-salvestikaitse. Riistvara korral toetab salvesti kaitset salvesti haldamise üksus (Memory Management Unit, MMU) või lihtsam salvesti kaitse üksus (Memory Protection Unit, MPU). MMU-ga on võimalik ühendada mitu virtuaalset protsessorit ühel füüsilisel protsessoril, mida hallatakse operatsioonisüsteemi kaudu. Iga programm võib saada oma virtuaalse mikrokontrolleri ja füüsilise mikrokontrolleri ressursse saab määrata paindlikult. MMU on standardi kohaselt serverite, arvutite ja moodsate nutitelefonide koostisosa, väikestes integreeritud süsteemides seda tavaliselt ei ole.

MPU korral kasutavad kõik programmid füüsilise salvesti ühist aadressiruumi. MPU jälgib, millisele mäluruumile programm ligi pääseb. Kui juurdepääs ei ole lubatud, saab operatsioonisüsteem mälupöörduse enne andmete salvestis muutmist kinni püüda. Teoreetiliselt võiks iga programm saada eraldi nn kaitseruumi.

Integreeritud süsteemide enamasti nappide ressursside põhjal tuleks aga ainult nii palju kaitseruume luua kui vaja, nt kaks, et eraldada usaldusväärsete programmide käitamine mitteusaldusväärsetest.

Riistvaral põhineva salvesti kaitse korral kontrollib mälupöördusi riistvara. See lähenemine toimib ka siis, kui mitteusaldusväärsed tarkvarakomponendid programmeeriti otse masinkoodis. Jälgitavad mälupöördused ei hõlma üksnes laadimis- ja salvestamiskäskusid, vaid ka masinkäskusid, mis laaditi enne nende käitamist. Kui mälupöörduse kontrollimine ebaõnnestub, katkestab riistvara asjakohase masinaprogrammi töö ja alustab süsteemi tarkvaras katkestusprotseduuri.

Millised õigused millise mäluruumi jaoks kehtivad, seda kirjeldatakse spetsiaalses juurdepääsukaitsega registris. Riistvaral põhineva salvesti kaitse jaoks mõeldud CPU vajab riistvara, mis toetab privilegeeritud ja mitteprivilegeeritud töörežiimi.

Tarkvaral põhineva salvesti kaitse korral ei kontrolli riistvara kaudselt mälupöördusi, vaid seda teeb eelnevalt ainult tarkvara. Kontrollimine võib seejuures osaliselt toimuda ülekande ajahetkel või ka töö käigus, näiteks automaatselt genereeritud kontrollimistega.

Kontrollküsimused:

- Kas integreeritud süsteemil on meetmed salvesti kaitseks?
- Kas salvesti kaitse liik ja mäluruumi hulk ning suurus süsteemi ja kasutamise eesmärgi jaoks on asjakohased ja piisavad?

M 4.485 Turvaline operatsioonisüsteem integreeritud süsteemide jaoks

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT-turbespetsialist, IT-juht

Rakendamise eest vastutavad: planeerija, administraator, arendaja

Integreeritud süsteemide jaoks on olemas väga palju erinevaid operatsioonisüsteeme. Mõned spetsialiseeritud süsteemid ei vaja üldse operatsioonisüsteemi, teised on integreeritud süsteemid, mis on välja töötatud mitmeotstarbelistest operatsioonisüsteemidest, nt integreeritud Linux'i variandid või Windows CE. Sinna vahele jäävad paljud erinevate aspektidega integreeritud süsteemidele spetsialiseerunud (reaalajas) operatsioonisüsteemid, nagu nt RTOS või VxWorks.

Ühelt poolt vajatakse mitmeotstarbelise operatsioonisüsteemi omadustest tavaliselt ainult üht osa, nt

1. aadressiruumi deskriptorid on vajalikud üksnes nende süsteemide korral, mis vajavad aadressiruumi isoleerimist,
2. andmesüsteem ja failihaldus ei mängi mõnede kasutusvaldkondade puhul mingit rolli,
3. ROM-il põhinevad süsteemid, millel töötab automaatselt ainult üks programm, ei vaja protsessil põhinevat kasutajaõiguste haldust,
4. loobuda võib protsessiolekute töömahukast haldusest, kui protsesside töötamise plaan on eelnevalt kindlaks määratud ja enam ei muutu,
5. sündmuste haldust vajatakse üksnes sündmustepõhiste ja/või tõkestavate süsteemide korral.

Teisest küljest võivad integreeritud süsteemide jaoks olemas olla nõuded, mida ei ole võimalik mitmeotstarbeliste operatsioonisüsteemidega kasutada või see on keeruline, nt

- tugevad reaalaja-kinnitused,
- täiendavad mehhanismid vigade tuvastamiseks ja kõrvaldamiseks,
- kohustus töötada ressursisäästlikult.

Kui töötatakse välja või soetatakse integreeritud süsteem, tuleb tähelepanu pöörata sellele, et operatsioonisüsteem ja selle konfiguratsioon sobiksid ettenähtud töö jaoks etteantud tingimustes ja vastaksid turbenõuetele. Operatsioonisüsteem tuleb konfigureerida kogu süsteemi spetsiifiliste turbenõuete kohaselt. Turbenõuded peaksid olema dokumenteeritud turvapoliitikas ja tarkvara arendusprotsessis. Põhimõtteliselt peaks operatsioonisüsteemis olema üksnes ettenähtud ülesande jaoks vajalikud teenused, funktsioonid ja omadused. Ühendada võib üksnes kasutavate liideste ajameid.

Erinevates valdkondades ja kasutamise etappides tuleks järgida operatsioonisüsteemi turvalisusega seotud aspekte. Süsteem tuleks välja töötada turvalises plaanipärases protsessis. Süsteemiarhitektuur peaks eraldama pakettide tuuma, nagu vahevara, võrguprotokollid ja rakendused. Olemas peaks olema nende

komponentide täiendamise ja muutmise võimalus ilma tuuma muutmise vajaduseta. Selle võib saavutada nn mikrotuumaga. Mikrotuumal (ingl microkernel) on vastupidiselt monoliitsele tuumale ainult põhifunktsioonid salvesti- ja protsessihalduseks ning sünkroniseerimiseks ja suhtlemiseks. See on seega vähem rünnatav ja ka tõrkekindlam. Nagu soovitatakse meetmetes M 4.78 Konfiguratsioonimuudatuste hoolikas teostamine , M 4.177 Tarkvarapakettide tervikluse ja autentsuse tagamine , M 4.483 Krüptograafiliste protsessorite ja kaasprotsessorite (Trusted Platform Module) kasutamine integreeritud süsteemides ja M 4.489 Kaitstud ja autenditud buutimisprotsess integreeritud süsteemides , peab operatsioonisüsteem andma mehhanismid turvaliseks buutimiseks ja turvaliseks programmi käitamiseks. Selleks peab see olema võimeline integreerima ja kasutama Trusted Platform Module'it (TPM).

Jooksva töö käigus peaks süsteem suutma tõrjuda ründeid. Seda on võimalik saavutada ka nii, et installeeritakse täiendavad turvatooted ja kasutatakse neid. Puhkerežiimis ei tohiks ründe toimepanijal olla võimalik andmetele ligi pääseda.

Kiipkaardi operatsioonisüsteemil peaksid olema järgmised mehhanismid ja teenused:

- kasutaja identifitseerimine ja autentimine PIN-i, PUK-i või biomeetrilise meetodiga;
- juurdepääsukontroll koos õiguste haldusega;
- kiipkaartide ja teiste arvutite vastastikune autentimine;
- turvaline andmete ülekandmine („Secure Messaging"), et vältida andmete uurimist ja manipuleerimist;
- allkirjastamis- ja krüpteerimisfunktsioonid turvatud interaktsioonis krüptoterminalidega;
- kõikide liideste I/O-kontroll operatsioonisüsteemi kaudu loata pöörduste vastu.
- Üksikute rakenduste häirekindluse tagamine: erinevad rakendused ei tohi üksteist vastastikku mõjutada.
- Kiipkaartide inaktiveerimise võimalus

Kõrge või väga kõrge kaitsevajadusega süsteemide korral tuleb kontrollida, kas on vajalik operatsioonisüsteemi hinnata, nt ISO 15408 kohaselt. Kogu operatsioonisüsteemi täieliku hindamise asemel on mõistlikum järgida BSI-kaitseprofiili „Operating System Protection Profile (OSPP)".

Kontrollküsimused:

- Kas integreeritud süsteemi kontseptsiooni või soetamise planeerimise puhul analüüsiti operatsioonisüsteemile esitatavaid nõudeid?
- Kas operatsioonisüsteemi funktsioonid on ka turvamehhanisme silmas pidades ettenähtud ülesande jaoks piisavad?
- Kas olemas ja aktiveeritud on ainult vajalikud teenused ja funktsioonid ?
- Kas operatsioonisüsteem toetab Trusted Platform Module'i kasutamist?

- Kas operatsioonisüsteemi tase on hinnatud tunnustatud standardi järgi asjakohaseks?

M 4.486z Integreeritud süsteemide vastupanuvõime külgkanalrünnete vastu

Algatamise eest vastutavad: IT-turbespetsialist, IT-juht

Rakendamise eest vastutavad: arendaja, hankija

Integreeritud süsteemi tuleb selle kaitsevajaduse kohaselt tugevdada külgkanalrünnete vastu, kasutades üht või mitut alljärgnevalt kirjeldatud mehhanismi. See meede kirjeldab võimalikke ründevorme ja vastumeetmeid nende eest kaitsmiseks.

Külgkanalrünnete liigid

Kui IT-süsteemid rakendavad krüptograafiat, ei toimu see mitte abstraktses matemaatilises süsteemis, vaid saavutatakse programmeeritud integreeritud lülitusskeemi kaudu. Need suhtlevad loodusseaduste alusel oma keskkonnaga ja avaldavad seeläbi teavet töödeldavate andmete kohta. Külgkanalrünne on krüptoanalüütiline protseduur, et kahjustada krüptomuutujaid, mille korral kasutatakse ära krüptosüsteemi füüsilist rakendamist seadmes või tarkvaras. Külgkanalründed on suure ajakuluga. Need vajavad täielikku ligipääsu seadmele, mis on sageli võimalik üksnes lahtimonteeritud olekus. Külgkanalründed võib põhimõtteliselt jaotada mitteinvasiivseteks ja invasiivseteks rünneteks.

Mitteinvasiivsed ründed

Mitteinvasiivsed või passiivsed ründed jälgivad füüsikalisi parameetreid, nt voolukulu, käitusaega ja mälukasutust, ning samal ajal töötavad vastavad krüptograafilised koodiosad ja tuletavad nendest kaitstud andmeid, nagu võtmed ja paroolid.

Energiakulu analüüs

Simple Power Analysis on meetod, mille korral salvestatakse mikroprotsessori energiakulu krüptograafiliste arvutuste ajal otse. Energiakulu varieerub olenevalt vastavast teostatud mikroprotsessori käsust. See annab seega ülevaate teostatud operatsioonidest ja võtmest. Krüptoloogilise operatsiooni energiakulu mõõtmiste võrdlemisega on võimalik avastada mustrid, nagu nt DES-ringid või RSA-operatsioonid, ja tuletada nendest salajase võtme. Differential Power Analysis (DPA) kasutab täiendavalt statistilisi meetodeid. Sellega võib ründe toimepanija oma eesmärgi saavutada ka keerukamate töötlusliikide, nagu rööpsuse või otsemällupöördusega (Direct Memory Access, DMA).

Ajakasutuse analüüs

Arvutusaja-ründed kasutavad olukorda, et krüptosüsteemid vajavad olenevalt võtmest erinevate loetavate tekstide või šifreeritud tekstide jaoks pisut erinevaid teostamisaegu. Kui ründe toimepanijal on juurdepääs süsteemile, võib ta erinevate sisestuste läbiproovimisega ajakasutuse analüüsi abil võtme järk-järgult taastada. Arvutusaja-ründeid on avalikustatud nii kiipkaartide kui ka tarkvararakenduste suhtes.

Mikroarhitektuurilised ründed (nt vahemälu-ründed, instruktsioonidevahemäluründed) Need ründed on suunatud tarkvaral põhinevate krüptosüsteemide vastu. Ründe mõte seisneb selles, et krüptoloogilise tarkvara käitamise ajal

laaditakse andmeid ja rutiine võtmest sõltumatult vahemälusse ja/või käsupuhvrisse. Eesmärk on mikroarhitektuuriliste protsessori omaduste ja funktsioonide ärakasutamine ning sel moel võtmeni jõudmine. Järgmised mitteinvasiivsete külgkanalrünnete lähtepunktid on arvutusvead vigastes mikroprotsessorites, elektromagnetiline kiirgus ja müraemissioonid. Erinevaid külgkanalründeid on võimalik ka omavahel kombineerida.

(Pool-) invasiivsed ründed

Ründeid nimetatakse invasiivseteks või aktiivseteks, kui seadmesse tungitakse füüsiliselt. Pärast oluliste turvafunktsioonide lühiajalise rikke tekitamist võib vigaseid tulemusi võrrelda omavahel ja/või õige tulemusega. See on ründe toimepanija jaoks eriti huvitav, kui töötavad krüptograafilised algoritmid, nt allkirja loomisel. Saadud andmete abil saab ta tuletada salajase võtme. Rikke saab esile kutsuda kriitilise koodi teostamise momendil, nt võidakse tekitada pingekõikumised nagu spike'id (impulssliigpinge) või glitch'id (jõnksud). Süsteem võidakse jätta ka elektromagnetilise kiirguse või äärmusliku temperatuuri mõjuvälja. Neid ründeid tähistatakse erialases kirjanduses ka kui „poolinvasiivseid", sest kuigi tegemist on füüsilise sekkumisega, ei hävitata kiipi ega kahjustata seda püsivalt ega manipuleerita. Viimastel aastatel on oluliselt sagenenud vintsutusründed, mis käivitavad lühiajalise rikke.

Järgmised külgkanalrünnete meetodid on asjakohase uurimise objektiks, nt fotoonilised külgkanalründed, mis toimuvad fotoonilise emissioonianalüüsi või fotoonilise veainduktsiooni kaudu.

Külgkanalrünnete tõrjumise võimalused

Et iga füüsikaline süsteem on vastastikuses toimes oma keskkonnaga, ei ole sajaprotsendiline kaitse külgkanalrünnete eest võimalik. Seega on eesmärk vähendada selle tulemuslikkuse tõenäosust. Vastupanuvõime külgkanalrünnetele ei tähenda seega, et need või nende tulemuslikkus tehakse täiesti võimatuks, vaid et selle saavutamine muudetakse keerulisemaks. Oluline kontseptsioon seisneb selles, et suurendada mõõtmiste nõutavat hulka ründe tulemuslikkuse jaoks niivõrd, et jääkrisk muutuks võimalikult madalaks või et seda on võimalik mõnel muul viisil maandada.

Andmete maskeerimine

Eesmärk on segi ajada seos tegelike salajaste andmete ja ründe toimepanija mõõdetud külgkanalteabe vahel. Vahetulemused randomiseeritakse salajase maskiväärtusega. Sellega katkestatakse seos tegelike andmete ja mõõdetud külgkanalteabe vahel. Maskeerimine võib toimuda nii algoritmi tasemel kui ka väravatasemel.

Tarkvaratehnilise lahenduse korral määratletakse maskeerimisskeemi järgi maskid ja neid kasutatakse algoritmi kaudu kõikidel vahetulemustel. Väravatasemel võib kasutada spetsiaalseid loogikastiile, nagu nt mCMOS, MDPL või iMDPL, mis peavad krüpteerimis- ja dekrüpteerimisprotseduuri ajal taastama ühtlase het-

keprofiili. See teema on endiselt käimasolevate uuringute objekt. CMOS-i loogikal põhinev laialt levinud riistvara neid tingimusi ei täida ja nende voolutarve sõltub tugevalt töödeldavatest andmetest.

Voolutarbimise summutamine või filtreerimine

Eesmärk on peita müraga signaal, mida sisaldab külgkanalteave. Tüüpilised meetodid on suurendada olemasolevat müra mürageneraatorite rakendamisega või vähendada signaali ulatust, mida kannab külgkanalteave. Viimast on võimalik ulatuslikult saavutada võimalikult püsiva, kaitstava seadme andmetest sõltumatu voolutarbimisega. Lisada võib ka kunstlikke voolumüra allikaid ja kasutada voolu juhuslikult.

Tugevdamine käitamisrünnete vastu

Eesmärk on varjata süsteemi ajalist käitumist tundlike andmete töötlemise ajal. Selleks võib programmi töösse lisada fiktiivoperatsioone või juhuslikke hooldustsükleid, nt krüptograafilise algoritmiga. Tõhusat kaitset erinevate käitamisrünnete ja voolutarbe analüüside vastu on võimalik saavutada randomiseerimistehnoloogiatega e nn pimestamisega. Selle puhul liidetakse vahepealsele väärtusele juhuslik väärtus või korrutatakse vahepealset väärtust juhusliku väärtusega. Olenevalt sellest, milliste suurustega see krüptograafilises algoritmis toimub, on tegemist kas baaspimestamise, moodulpimestamise või eksponentpimestamisega. Need väldivad olukorda, kus ründe toimepanija võiks teada saada modulaarse astendusalgoritmi vahepealseid väärtusi, mida kasutatakse krüptograafilise protseduuri juures.

Tugevdamine (pool-) invasiivsete rünnete vastu

Erinevate veaanalüüside kaudu on võimalik tuvastada või kvalifitseeritult kahtlustada ründeid, kui arvutusetapid viiakse läbi liiasusega ja tulemused ei lange kokku. Lisada võib filtreid, et kompenseerida ebakorrapärasusi toitepinges või suurendada tolerantsi segatud taktsignaalide suhtes. Laseritega teostatavaid optilisi sekkumisi saab tuvastada või raskendada valgusdetektorite ja spetsiaalsete kaitsekihtidega. Integreeritud süsteemid võib varustada ka salvestielementidega, mille sisu igapäevatöös ei muutu. Kui tuvastatakse muutus, tekib kahtlus ründe suhtes, mis teostati diferentsiaalse veaanalüüsi abil. Selleks vajatakse täiendavat mäluruumi või täiendavat arvutusaega.

Kontrollküsimused:

- Kas võetakse kaitsevajadusele ja ohule vastavaid ennetavaid meetmeid mitteinvasiivsete külgkanalrünnete vastu?
- Kas võetakse kaitsevajadusele ja ohule vastavaid ennetavaid meetmeid (pool-) invasiivsete külgkanalrünnete vastu?

M 4.487z Urkimiskaitse (tuvastamine, takistamine, tõrje) integreeritud süsteemides

Algatamise eest vastutavad: IT-turbespetsialist, IT-juht

Rakendamise eest vastutavad: IT-turbespetsialist, administraator, planeerija

Integreeritud süsteemidele tuleb alates konfidentsiaalsuse kõrgest kaitsevajadusest ja terviklusest kavandada ja rakendada urkimiskaitse kontseptsiooni.

Põhjalik urkimiskaitse koosneb kolmest funktsionaalsest valdkonnast: „takistamine", „tuvastamine ja tõendamine" ning „reageerimine ja kaitse". Erialakirjanduses kasutatakse selle jaoks enamasti inglisekeelseid mõisteid tamper resistance, tamper evidence ja tamper response. Urkimiskaitse võib puudutada taristuelemente, riistvara ja tarkvara. Viimase korral kasutatakse mehhaanilisi mehhanisme (vt M 4.90w Krüptoprotseduuride kasutamine ISO/OSI etalonmudeli eri kihtides ja M 4.483 Krüptograafiliste protsessorite ja kaasprotsessorite (Trusted Platform Module) kasutamine integreeritud süsteemides).

Taristuelementide ja riistvara ründamise takistamiseks tuleb luua sissemurdmiskindel (tamper resistant) süsteem, mida ei ole selle ehituse põhjal võimalik volitamata muuta. Selle jaoks, et ründe toimepanija saab süsteemi vabalt kasutada, puudub täielik kaitse. Siiski on ehituslike ja tehniliste meetmete abil võimalik seada need tõkked ründe toimepanija jaoks võimalikult kõrgeks. Sellise süsteemi toestamine võib olla kulukas ning tulemuseks võib olla keeruline ja mitte eriti paindlik süsteem. Enne sellise otsuse langetamist tuleks seetõttu analüüsida ja hinnata, milline kulu on süsteemi kaitsevajadust arvesse võttes vajalik ja mõistlik. Sissemurdmiskindluse suurendamisele aitavad kaasa erinevad konstruktsioonielemendid. Näidetena võib tuua spetsiaalsed kruvid, nagu Torx-TR, mille profiili keskel on tihvt, mis takistab selle kruvi keeramist tavalise Torx- või lamepea-kruvikeerajaga, või ümbrised, kaitsekihid ja passiivsed või aktiivsed metalljuhtmed. Integreeritud süsteeme võib keskkonnaga ka ehitustehniliselt niimoodi ühendada, et neid on väga raske eraldada ning neid ei ole koos keskkonnaga võimalik transportida nt võib kasutada metalli või betooni. Palju kulukam on selliste meetodite kasutuselevõtt, mis tuvastavad ja dokumenteerivad sissemurdmisi (tamper evidence). Need võimaldavad tuvastada süsteemi modifikatsioone automatiseeritult või tagavad välise kontrollija abil süsteemi veatuse. Seda liiki mehhanismide näited on plommid ja pitsatid, aktiivselt juhitud metalljuhtmed koos anduritega, mis reageerivad valgusele, survele või vastupanu- ja võimsusemuutustele.

Reaktsioonina urkimisründele (tamper response) võidakse saata hoiatus kõrgemal olevale haldusüksusele. Lisaks tuleks süsteemi tundlikud andmed kustutada võimalikult automaatselt. Olenevalt andmete kaitsevajadusest tuleks vaadelda erinevaid võimalusi. Lihtsalt teostatav on RAM-i toite katkestamine, kuid siis jääb ründe toimepanijale siiski võimalus andmed vastava varustuse ja oskuse korral

taastada. Peale selle puudutab see ainult üht osa integreeritud süsteemi andmetest. Levinud meetod seisneb selles, et RAM kirjutatakse mitmekordselt üle. Sageli kirjutatakse see kõigepealt mitu korda üle 0-iga ja seejärel mitu korda 1-ga. Selle meetodi puudus seisneb selles, et ei ole võimalik garanteerida, et see protseduur ka tegelikult toimub, kui seadet või selle toidet mõjutatakse. Kõige kindlam on seade füüsikaliselt hävitada. Seda on võimalik teostada nt termiitreaktsiooniga.

Kontrollküsimused:

- Kas on olemas urkimiskaitse kava?
- Kas on loodud kaitsevajadusele vastavad mehhanismid, et takistada urkimisründeid?
- Kas on loodud kaitsevajadusele vastavad mehhanismid urkimisründe tuvastamiseks ja salvestamiseks?
- Kas on loodud kaitsevajadusele vastavad mehhanismid urkimisründele reageerimiseks?

M 4.488 Mittekasutatavate liideste ja teenuste inaktiveerimine integreeritud süsteemides

Algatamise eest vastutavad: IT-turbespetsialist, IT-juht
Rakendamise eest vastutavad: arendaja, administraator

Integreeritud süsteemid on sageli varustatud mitmete erinevate liidestega. Lihtsate sisendite ja väljunditega andurite ja ajamite ühenduste kõrval on olemas erineva keerukusega võrgusuhtluse, käsitlus- ja näidikuliidesed.

Füüsikalised liidesed
Põhimõtteliselt peaksid olemas olema üksnes vajalikud füüsikalised liidesed. Kui riistvara on ette antud ja kui see sisaldab mittevajalikke liideseid, tuleb juurdepääs neile takistada ehituslike meetmetega.

Loogilised liidese võrguprotokollid
Põhimõtteliselt tohib aktiveerida üksnes vajalikud teenused. Mittevajalikud protokollid, mis mõnedes konfiguratsioonides on standardi kohaselt olemas, tuleb inaktiveerida, nagu nt Appletalk, IPX või NetBios. Protokolliteenused, mis edastavad andmeid loetavas kirjas, nagu nt telnet, http või ftp, tuleb kõrgendatud kaitsevajaduse korral inaktiveerida. Vajaduse korral tuleb vastava eesmärgi saavutamiseks rakendada turvalisi protokollivariante või alternatiive. SNMP v1 ja v2 teenused tuleb inaktiveerida.

Loogiline liidese rakendustasand
Kõik rakendustes mittekasutatavad liidesed peavad olema konfigureeritud nii, et nende liideste kaudu ei oleks võimalik juurdepääs integreeritud süsteemile. Sisse võivad olla lülitatud üksnes need teenused, mida on tarvis ülesannete lahendamiseks. Keerukate rakenduste korral, mille puhul on nõutav juurdepääsu autentimine, tuleb kontrollida, milliste rakenduse valdkondade jaoks autentimine kehtib. Kui nt veebiserveri korral on HTML-leheküljed kaitstud parooliga, ei ole sellega veel tagatud, et kaitstud on ka juurdepääs konfiguratsiooniandmetele XML-i või JSON-i kaudu. Selliste lünkade leidmiseks võib veebilehti analüüsida ja objekte kontrollida HTTP-kliendi abil.

Kui integreeritud süsteemides kasutatakse operatsioonisüsteemi, mille jaoks on olemas sellele kohandatud automaatne turvaaukude skanner, nagu nt Linuxsüsteemidel, peaks sellega tuvastama nõrgad kohad ja võimaluse korral need ka kohe kõrvaldama. Kõikides süsteemides tuleb turvaauke otsida universaalsete pordiskannerite või programmidega, mis genereerivad juhuslikke või kindlaks määratud pakette, nn packet builder'eid.

Kontrollküsimused:

- Kas olemas on ainult vajalikud füüsikalised liidesed?
- Kas aktiveeritud on ainult vajalikud teenused?

- Kas juurdepääs rakendusliidestele on kaitstud turvalise autentimisega?

M 4.489 Kaitstud ja autenditud buutimisprotsess integreeritud süsteemides

Algatamise eest vastutavad: asutuse/ettevõtte juhtkond, IT-turbespetsialist
Rakendamise eest vastutab: hankija, arendaja, planeerija

Integreeritud süsteemi buutimisprotsess ei tohi olla kahjustatav. Seda ei tohi olla võimalik käivitada autentimata buutimisvahenditest ning autentimata buutimisvahend ei tohi võtta üle integreeritud süsteemi andmeid. Tuleb kindlaks teha, et kasutatav tarkvara oleks kirjutatud või välja antud pädeva asutuse poolt. Buutimisprotsess peab olema kaitstud, mis tähendab et Bootloader kontrollib operatsioonisüsteemi terviklust ja laadib selle üksnes siis, kui see on liigitatud õigeks. Operatsioonisüsteem peaks käivituma, kui Bootlaoader'i usaldusväärsus on kinnitatud pöördkontrolliga.

Seda saab kontrollida asümmeetrilise krüptograafiameetodiga. Hetkel (2015. aasta seisuga) tulevad selle jaoks kõne alla nt Elliptic Curve Digital Signature Algorithm (ECDSA) ja RSA (Rivest, Shamir ja Adleman), kombineeritud SHA-ga (secure hash algorithm). Originaaltarkvarast arvutatakse räsiväärtus ja allkirjastatakse väljaandja privaatse võtmega. Seda kontrollitakse avaliku võtmega. Avaliku võtme autentsus tuleb tagada PKI-meetodiga.

Turvaline buutimisprotsess tuleb läbi viia etapiviisiliselt. Kõigepealt peab töötama minimaalne, valmistamisel kindlalt ROM-i programmeeritud Bootloader (ROM-Loader). Sellel peab olema eelnevalt kindlalt sisseprogrammeeritud krüptograafiline võti, et omalt poolt kinnitada järgmise Bootloader'i digitaalne allkiri. Selle esimese kinnitusvõtme peab andma riistvara, see võib olla integreeritud üks kord programmeeritava varundusega ROM-i või salvestatud lokaalsesse Trusted Platform Module'isse (TPM) vt ka M 4.483 Krüptograafiliste protsessorite ja kaasprotsessorite (Trusted Platform Module) kasutamine integreeritud süsteemides .

ROM-Loader laadib järgmise, suurema arvu funktsioonidega Boot Loader'i, mis käivitab seejärel operatsioonisüsteemi või uuesti Loader'i. Allkiri peab olema salvestatud ka riistvaralise kaitsega kohas, sest allkirjavõtmega kontrollitakse, kas komponendid teises (ja vajaduse korral järgmises) buutimise etapis on ehtsad.

Käitatavat tarkvara võib laadida mitme etapi kaupa, kusjuures igas käimasolevas etapis kontrollitakse iga järgmise etapi allkirja. Kui allkirja kinnitamine ei õnnestu või kui ühendus katkestatakse, tuleb eeldada, et turvaline olek on kahjustatud.

Sageli ei kasutata integreeritud süsteemides x86-l põhinevaid, BIOS-i (Basic Input/Output System) või UEFI-ga (Unified Extensible Firmware Interface) arvuteid, vaid ARM-il põhinevaid, Universal Boot Loader'iga (U-Boot) seadmeid. TCG toetub oma standardites aga ennekõike RTM-i rakendamisele pre-BIOS-is või UEFI-s, kus RTM-i tuleb eriti kaitsta. ARM-i platvormidel on paljudel juhtudel juba ilma Trusted Computing'ita võimalus tarkvara turvaliseks käivitamiseks, nagu nt ARM-i Secure Boot või üksnes ühekordselt kirjutatav salvesti, mis on kaitstud ka füüsiliste manipulatsioonide eest.

Kontrollküsimused:

- Kas operatsioonisüsteemi terviklust kontrollitakse Bootloader'i kaudu?
- Kas Bootloader'i terviklust kontrollitakse operatsioonisüsteemi kaudu?
- Kas teostatakse mitmeetapilist buutimiskontseptsiooni üksikute sammude krüptograafiliselt turvalise kontrollimisega?
- Kas kasutatakse turvalist riistvara usaldustõendit?
- Kas ARM-il põhineva integreeritud süsteemi puhul kasutatakse ARM-i Secure Boot'i?
- Kas UEFI korral kasutatakse Secure Boot'i?

M 4.490 Seadmemoodulite funktsiooni automaatseire (BIST) integreeritud süsteemides

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT-turbespetsialist, IT-juht

Plaanilise enesetestiga (Built-In Self Test, BIST) saab ise testida lülitusskeemi, seadet või süsteemi. Selleks luuakse testsignaalid, mis on salvestatud testitavatele komponentidele ja hinnatakse vastussignaale, enamasti etteantud õigete vastussignaalide võrdlemisega. BIST korral rakendatakse testimiskeskkonna (Automatic Test Equipment, ATE) funktsioone, nagu testsignaali generaatorid või hindamisüksused, täielikult või osaliselt otse kiibil. See toob kaasa lühendatud signaaliteed, vähendatakse tahtmatuid ühendamisi ja parandatakse signaali terviklust testimisjuhtmetel.

Enesetest võib tark- ja riistvara funktsionaalse diagnostilise testina toimuda tavatöös, algatusfaasis, puhkeajal, enne väljalülitamist või väljaspool töökeskkonda.

BIST erinevate liikide näited on järgmised:

- Loogika-BIST: pseudomustri- või pseudojuhugeneraator toodab juhumustri, millega kontrollitakse loogilisi olekuid. Kui väljastusolekud ei vasta tõeväärtustabelile, töötab loogika vigaselt.
- Salvesti-BIST: katsekontuuri abil loetakse salvesti mooduleid ja võrreldakse nende väljastusolekuid etteantud mustriga.
- Signatuuri analüüs: lülituskomponentide osade signaalid kogutakse pikema ajavahemiku jooksul kokku ja sellest kogumist vahendatakse signatuur. Seda võrreldakse nimiväärtusega ja tehakse järeldus, kas tegemist on kogu skeemi õige või väära funktsiooniga.

Perimeetri skaneerimistest: täiendavate elementide, nn riividega, viiakse signaalid väljastpoolt eeldefineeritud asukohtade kaudu testitavasse skeemi.

Skeemi signaale, mis asuvad lülitusahela klemmidel, saab tuvastada skaneerimise teekonna kaudu.

Igapäevatöös on riivid passiivsed, funktsionaalne erinevus varasema lülitusskeemiga puudub.

- Analoog- ja segasignaaliga BIST: kõigepealt kinnitatakse digitaalsed komponendid täielikult digitaalse BIST-skeemi abil. Seejärel kinnitatakse Analog-Digital-Converter (ADC) ja Digital-Analog-Converter (DAC). Järgnevalt saab kinnitada muud komponendid, määrates need analoogsete multiplekseritega DAC ja ADC vahele.

Kõikidele kättesaadavusele ja terviklusele esitatavate kõrgendatud nõudmistega seadmemoodulitele peaksid olema integreeritud enesetesti seadmed. Testid

peavad käivitusprotseduuri ajal ja käitamise jooksul sobivate ajavahemike järel kontrollima süsteemi terviklust. Kui võimalik, peaksid enesetesti funktsioonid kontrollima ka seadmemooduli turvafunktsioone või turvalisusega seotud omadusi. Kõrgema kaitsevajadusega komponentide korral, nt kriitilistes juhtimissüsteemides, tuleks korrapäraselt kontrollide salvestite ja I/O-komponentide terviklust BIST raames. Olemasolevaid BIST-funktsioone tuleks võimaluse korral täiendada vajalike funktsioonidega.

Kontrollküsimused:

- Kas viidi läbi integreeritud süsteemi vajalike enesetesti mehhanismide analüüs?
- Kas integreeritud süsteemil on olemas vajalikud plaanilised enesetestid?
- Kas enesetestid hõlmavad ka turvalisusega seotud omadusi?

M 4.491 Silumisvõimaluste tõkestamine integreeritud süsteemides

Algatamise eest vastutavad: IT-turbespetsialist, IT-juht
Rakendamise eest vastutavad: administraator, arendaja

Integreeritud süsteemide levinud silumisprotseduurid on In-Circuit-Emulation (ICE) ja On-Chip-Debugging (OCD). ICE seadmed asendavad sihtsüsteemi tegeliku kontrolleri riistvaraga, kuhu on paigaldatud vajalikud analüüsifunktsioonid. Hiljem rakendatud sihtsüsteemil neid lisafunktsioone ei ole ja seega ei ole sellel ka lubamatuid silumisvõimalusi. Ajalistel, tehniliste ja majanduslikel põhjustel kasutatakse siiski rohkem OCD-d. Seejuures rakendatakse silumisvõimalusi seeriamoodulitel. OCD võib seega sekkuda programmi töösse, nt selleks, et lugeda registrite väärtusi või Trace-mälu või et käitada väikeseid seireprogramme, mis koguvad ja annavad välja silumisteavet.

Integreeritud süsteemidel ei asu uuritav tarkvara tavaliselt siluriga samal arvutil. Seetõttu kasutatakse kaugsilumist, st arendaja käivitab integreeritud süsteemis rakenduse, millega silur ühendab end arendussüsteemil nt Etherneti või RS232 kaudu. Kui kasutatakse nt GNU silureid (GDB), käitab integreeritud süsteem GDBserverit, mille puhul GDB-klient registreerib end arendussüsteemil. Klient või programmeerija annab integreeritud süsteemis olevale serverile korralduse rakenduse uurimiseks. Server teostab korraldused ja saadab tulemused arendussüsteemile tagasi.

Kui võimalik, tuleb riist- ja tarkvaraarendusest süsteemis või tarkvaras installeeritud silumise abivahendid seeria projektist täielikult eemaldada. Tarkvara tootekoodist tuleb eemaldada kõik koodielemendid, mis ei ole süsteemi funktsionaalsuse osa. Siia kuuluvad nt katkestuspunktid ja mittekasutatud kood. Kui kasutatakse On-Chip-Debugging'it, tuleb tagada, et silumisfunktsioone ei kasutaks ega aktiveeriks volitamata isikud. Riistvara valdkonnas tuleb kindlaks teha, et testsignaalide ja mõõtepunktide ühendusliidesed analüsaatorite ühendamiseks ei oleks volitamata isikute jaoks aktiveeritud ega kasutatavad.

Kontrollküsimused:

- Kas võimaluse korral on jäetud silumiskomponendid sihtsüsteemile installeerimata?
- Kui kasutatakse On-Chip-Debugging'it, kas on tagatud, et silumisfunktsioone ei kasuta ega aktiveeri volitamata isikud?
- Kas kõik riistvara silumisliidesed on inaktiveeritud?

M 4.492 Integreeritud veebiserveri turvaline konfiguratsioon ja kasutamine

Algatamise eest vastutavad: IT-turbespetsialist, IT-juht
Rakendamise eest vastutavad: arendaja, administraator

Mõnedel integreeritud süsteemidel on integreeritud veebiserver, millega saab teha teabepäringuid ja neid juhtida. Seejuures on tavaliselt tegemist nn sisseehitatud veebiserveriga, millel on piiratud funktsioonid, mis on optimeeritud enamasti vähestele olemasolevatele ressurssidele. Turul on saadaval suurel hulgal integreeritud veebiservereid, need on väikesed, koormavad CPU-d mõõdukalt ja on suures osas platvormist sõltumatud. Nende põhiülesanne on edastada veebidokumente HTTP(S)-i kaudu kliendile. Mõned valdavad peale selle ka dokumentide dünaamilist koostamist, nt Server-Side Scripting'u kaudu. Integreeritud veebiserveri jaoks peaksid olema installeeritud ja aktiveeritud üksnes vajalikud komponendid ja funktsioonid. Veebiserver peaks konto piires töötama võimalikult väikeste õigustega. Kui käivitamiseks on vaja suuremaid õigusi, tuleks järgmiseks siirduda ilma privileegideta kontosse. Kõik turvalisuse ja vigade kõrvaldamise jaoks olulised teated tuleks protokollida, nt struktureeritult edukate ja mitte-edukate pöörduste, sisemiste vigade, väärate või mittetäielike HTTP-päringute ja muude vastavate süsteemiteadete järgi. Seda protokollimist tuleks kirjeldada turvalisusega seotud dokumentides (täiendavat teavet leiate selle kohta meetmest M 2.497 Logimise turbekontseptsiooni koostamine).

Süsteemiseadistused peaksid olema võrdlemisi piiravad, nt tuleks samaaegselt võimalike ühenduste arvu piirata kasutuseesmärgile olulise määrani ja piirata tuleks sisemise vahemälu suurust. Kui seda kasutatakse, tuleks pöördust kontrollida CGI-failides CGI-Wrapper'iga nii, et käitada saaks üksnes selgesõnaliselt lubatud programme. Veebiserveriga peaks võimaluse korral suhtlema üksnes SSL-ühenduse kaudu ja juurdepääs peaks olema võimalik üksnes pärast põhjalikku autentimist.

Kontrollküsimused:

- Kas installeeritud ja aktiveeritud on ainult vajalikud teenused ja funktsioonid?
- Kas veebiserverit kasutatakse ilma privileegideta konto raames?
- Kas protokollitakse turbega seotud sündmusi?
- Kas kõik konfiguratsiooniparameetrid on seadistatud nii piiravaks kui võimalik?
- Kas juurdepääs on võimalik üksnes pärast põhjalikku autentimist ja kas ülekanne on krüpteeritud?

M 4.493z Arenduskeskkonna valimine tarkvaraarenduse jaoks

Algatamise eest vastutavad: arendusjuht

Rakendamise eest vastutavad: varumisosakonna juht

Tarkvaraprojekti teostamiseks on vaja sobivat arenduskeskkonda. Valik toimub esmajoones projekti jaoks ettenähtud programmeerimiskeele ja kavandatava rakendustüübi abil. Peale selle tuleks arvestada lisafunktsioonide ja soetamis- ning käitamiskuludega.

Sobiva arenduskeskkonna valimiseks soovitatakse tingimata nõutud ja täiendavalt soovitud kriteeriume võrrelda saadavalolevate toodetega, pannes need kirja ühte tabelisse.

Valikukriteeriume võib siinjuures vaadelda kui võrdseid või lisada neid kaalutult, ning need on järgmised:

- toetatud programmeerimiskeeled;
- toetatud operatsioonisüsteemid;
- koostöövõimalused;
- projektihalduse funktsioonid;
- refaktoreerimisfunktsioonid;
- soetamiskulud;
- hoolduskulud;
- ühilduvus olemasolevate arendussüsteemidega;
- ühilduvus olemasolevate projektidega (vajaduse korral).

Kui pärast erinevate arenduskeskkondade võrdlemist jäävad sõelale mitmed tooted, võib otsuse teha subjektiivse võrdlusega.

Siinjuures tuleb arvestada valikukriteeriumidega, mida ei iseloomusta konkreetne väärtus, näiteks:

- kasutatavus;
- intuitiivsus;
- tootja usaldusväärsus.

Kontrollküsimused:

- Kas arenduskeskkonna jaoks koostati vajalike ja täiendavate valikukriteeriumide nimekiri?
- Kas arenduskeskkond valiti välja etteantud kriteeriumide alusel?

M 4.494 Arenduskeskkonna turvaline kasutamine

Algatamise eest vastutavad: arendusjuht

Rakendamise eest vastutavad: arendaja, arendusjuht

Arendatava tarkvara turvanõuetest tulenevad turvanõuded arenduskeskkonnale, mis puudutavad terviklust, usaldusväärsust ja käideldavust. Need ja nõutavad turvameetmed tuleb dokumenteerida. Seejuures tuleb arvestada alljärgnevate aspektidega:

Arenduskeskkonna sektsioneerimine

Arendus peab toimuma kaitstult. Siinjuures peab arenduskeskkond nagu ka testimiskeskkond olema rangelt tootmiskeskkonnast eraldatud. Arenduskeskkonda tuleb kaitsta selle eest, et arendus toimuks katkestusteta, ning tuleb tagada, et arenduskeskkonna käideldavus, usaldusväärsus ega terviklus ning töödeldavad andmed ei saaks tootmiskeskkonna poolt ega vastupidi kahjustatud. Koodiarhiivide ja muude arendusega seotud andmete manipuleerimise vältimiseks peab juurdepääs neile olema piiratud. Juurdepääsud arendusega seotud andmetele peavad olema määratud üksikutele kasutajatele ning need tuleb dokumenteerida.

Tootmiskeskkond tuleb eraldada arenduskeskkonnast, näiteks võrgu eraldamise või juurdepääsukontrolliga, et neid ei oleks võimalik volitamata muuta ega manipuleerida. Eriti vajalik on tagada, et äsja loodud või muudetud tarkvara võetakse tootmiskeskkonda üle üksnes läbipaistvate ja dokumenteeritud protsesside abil ning volitatud isikute poolt. Turvalisi süsteeme saab välja töötada üksnes turvalises keskkonnas. Selle jaoks on lisaks tehnilistele meetmetele vajalikud ka taristu ja organisatsioonilised turvameetmed. Näiteks peavad kasutatavad ruumid olema kaitstud volitamata juurdepääsu eest.

Kommentaarid ja dokumendid

Kommentaarid ja muud tootmistegevuseks mittevajalikud andmed tuleb eraldada lähtetekstidest, konfiguratsioonifailidest ja käivitatavatest failidest enne, kui neid kasutatakse tootmissüsteemis. Kui arenduskeskkond seda toetab, tuleks see konfigureerida nii, et programmipakettide koostamisel eraldatakse automaatselt kõik andmed, mis ei vasta ettenähtud kasutuseesmärgile. Tagatud peab olema, et selle jaoks on täpselt dokumenteeritud, millised andmed peaksid tellija huvides valmis programmipaketis sisalduma. Arendusandmetes olevad vastavad kommentaarid, dokumendid ja lisateave peavad alaliselt alles jääma, et tagada igal ajal tarkvara kontrollimine ja hooldamine.

Töökohtade kaitsmine

Kui tarkvara arendatakse jaotatud töökohtadel ja seda teevad erinevad inimesed, peab töökohtadevaheline ühendus olema kaitstud. Suhtlemine peab toimuma krüpteeritud andmeühenduste kaudu ja juurdepääsu tähtsatele komponentidele, nagu näiteks organisatsioonivälised koodiarhiivid, tuleks täiendavalt kaitsta turvaväravatega. Kogu arendusprotsessi jooksul tuleb kõikidel IT-süsteemidel kasutada kahjulike programmide vastu ajakohast tarkvara. See kehtib ka tootmissüsteemi töö kohta (vt B 1.6 Viirusetõrje kontseptsioon).

Kontrollküsimused:

- Kas arenduskeskkonda käitatakse tootmiskeskkonnast eraldi?

- Kas kommentaarid ja muud mittevajalikud andmed eemaldatakse enne programmipakettide tootmissüsteemi rakendamist?
- Kas töökohad suhtlevad omavahel turvalise ühenduse kaudu?
- Kas arendusandmete jaoks kehtib juurdepääsukontroll?
- Kas kasutatakse ajakohast viirusetõrjetarkvara?

M 4.495 Tarkvaraarenduse turvaline süsteemikujundus

Algatamise eest vastutavad: arendusjuht

Rakendamise eest vastutavad: arendaja, arendusjuht

IT-süsteemide projekteerimisel tuleb kontrollida kõiki saadaval olevaid turvamehhanisme ja hinnata, kas need täidavad turvanõudeid, mis tulenevad kavandatava kasutuskeskkonna kaitsevajadusest. Turvamehhanisme tuleb rakendada nii, et kõik turvanõuded oleksid täidetud ja teostatud.

Iga ähvardusega tuleb tegeleda sobivate turvameetmetega. Eelkõige tuleb turvalise süsteemprojekti juures järgida järgmisi põhireegleid:

- Sisestusandmeid tuleb enne edasitöötlemist põhjalikult kontrollida ja need valideerida. Ebasobivateks liigitatud sisestusandmed tuleks kõrvale jätta ja neid mitte enam edasi kasutada.
- Klient-server-rakenduste korral tuleks andmed serveris põhjalikult valideerida. Kliendi kaudu toimuvad valideerimised suurendavad kasutusmugavust, ei paku aga turvalisust ning tuleb seetõttu serveris üle korrata.
- Süsteemikomponentide vahel tuleks andmeid edastada krüpteeritult. Erandeid tuleb põhjendada.
- Tarkvara ja süsteemi jaoks, millel tarkvara käitatakse, tuleb ette näha turvaline tüüpkonfiguratsioon. Siinjuures tuleb teostada operatsioonisüsteemi ja tarkvara kasutatavate moodulite ning rakenduste turvalised põhiseadistused.
- Vigade või süsteemi komponentide tõrke korral ei tohi avaldada andmeid (nt versiooni numbreid või failiteed).
- Tarkvara kasutamine peab olema lubatud võimalikult väheste kasutajaõigustega.
- Süsteemiprojekt tuleb dokumenteerida ja kontrollida turvanõuete täielikku täitmist. Turvanõuded peavad olema rakendatavad tarkvara tootmisprotsessis ja peavad seepärast vastama ka sealsetele keskkonnatingimustele (nt kasutatav operatsioonisüsteem).

Kontrollküsimused:

- Kas peetakse kinni turvalise süsteemiprojekti põhireeglitest?
- Kas süsteemiprojekt on dokumenteeritud ning selle täielik vastavus turvanõuetele kontrollitud?

M 4.496 Väljatöötatud tarkvara turvaline installeerimine

Algatamise eest vastutavad: arendusjuht

Rakendamise eest vastutavad: arendaja, arendusjuht

Valmis tarkvara turvalise installeerimise eeldus tootmiskeskkonnas on edukas testimine eelnevalt kindlaks määratud testimisprotseduuri järgi (vt M 2.568 Tarkvara testimisprotseduurid). Edasi tuleb käitamisprotseduure testida usaldusväärsuse suhtes, et välistada puudused tootmisprotsessis. Peale selle peavad olemas olema hädaolukorra kavad juhuks, kui tarkvara installeerimisel või käitamisel ilmnevad rikked. Need peavad sisaldama tegevusjuhiseid prognoositavate probleemide jaoks ja vähemalt üht kontaktisikut, kellega kasutaja saaks otse ühendust võtta. Peale selle peavad administraatorid olema koolitatud tarkvara hooldamiseks.

Koolitus hõlmab teadmisi sellest, kuidas tarkvara konfigureeritakse ning täiendavaid teadmisi selle kohta, kuidas kasutatakse tarkvara tootmisprotsessis, et abistada kasutajaid probleemide tekkimise korral. Lisaks tuleb kasutajaid süsteemiga tutvustada, näiteks ettevalmistavate koolituste või dokumentide abil. Installeerimisprotsessi jaoks peab olemas olema installeerimisplaan, mis kirjeldab üksikasjalikult kõiki läbiviidavaid etappe ja vaatleb seejuures ka võimalikke veaallikaid või kõrvalekaldeid erinevate sihtsüsteemide vahel. Pärast installeerimist kontrollitakse dokumenteeritud testimisplaani järgi, kas paigaldus on õige, ning antakse süsteem kasutusse.

Kontrollküsimused:

- Kas väljatöötatud tarkvara turvalise installeerimise eeldused on täidetud?
- Kas väljatöötatud tarkvara installerimine viiakse läbi olemasoleva installeerimisplaani järgi?
- Kas väljatöötatud tarkvara õiget installeerimist kontrollitakse testimisplaani järgi?

M 4.497 Võrguhaldussüsteemi turvaline installeerimine

Algatamise eest vastutavad: IT-turbespetsialist, IT-juht
Rakendamise eest vastutavad: administraator

Võrguhaldussüsteemi installeerimine nõuab ulatuslikku ja hoolikat planeerimist. Pärast süsteemi analüüsimist (vt M 2.140z Võrgu hetkeolukorra analüüsimine), halduskontseptsiooni kindlaksmääramist (vt M 2.143 Võrguhalduse kontseptsiooni väljatöötamine) ja sobiva haldussüsteemi valimist (vt M 2.171 Sobiva süsteemihaldustoote valimine) tuleb hakata hoolikalt planeerima toote installeerimist ning see vastavalt plaanile ka teoks teha. Olevalt haldustoote aluseks olevast arhitektuurist, tuleb kohtvõrgu jaoks luua selge võrguhaldussüsteemi konfiguratsioon, mis arvestaks eriti just sõnastatud võrguhalduskontseptsiooniga.

Sageli tuleb kesksetesse arvutitesse installeerida ka andmebaasisüsteemid, millesse haldustarkvara salvestab pidevalt haldusteavet. Olenevalt tootest võib osutuda võimalikuks selle ühendamine juba olemasoleva andmebaasisüsteemiga. Haldustarkvara jaoks tuleks kasutada deditseeritud, piisava jõudlusega IT-süsteemi.

Lisaks nendele kriteeriumidele, mis peavad üldjuhul tagama süsteemi reguleeritud tehnilise toimimise, tuleb turbe seisukohast turbeastme määramisse IT etalonturbe alusel (vt BSI-standardit 100-2 IT etalonturbe meetod) kaasata ka haldussüsteemi juurde kuuluv tarkvara ja vastavad andmed. Võrguhaldussüsteemi kahjustamine võib kaasa tuua kogu võrgu avarii. Süsteemi märkamatute muudatustega võib tekkida oluline kahju, mis võib ohtu seada isegi terve asutuse eksistentsi. Kui võrguhalduse andmete kaitsevajaduse aste on liigitatud „kõrgeks” või „väga kõrgeks”, tuleb läbi viia täiendav turvaanalüüs ja vajaduse korral riskianalüüs.

Installeerimisel tuleb arvestada eriti just alljärgnevate punktidega:

- Kõiki arvuteid, milles hoitakse haldusinfot, tuleb kaitsta eriti hoolikalt: lähtuvalt kasutatavast süsteemist tuleb rakendada meetmeid 3. komplekti moodulitest.
- Haldustarkvarale tohivad ligi pääseda ainult volitustega administraatorid ja revidendid.
- Juurdepääs arvutitele peab olema piiratud.
- Suhtlemine halduskomponentide vahel peab toimuma krüpteeritult, et takistada haldusteabe pealtkuulamist ja kogumist. Kui tootel puudub krüpteerimise tugi, tuleb suhtlemise kaitseks võtta erimeetmed (vt M 2.579 Kohaliku

võrgu regulaarsed auditid ja M 5.68z Krüpteerimisprotseduuride kasutamine võrgusuhtluses).

- Haldustarkvara tuleb lisada andmevarunduse kontseptsiooni.

Kontrollküsimused:

- Kas võrguhaldussüsteem on installeeritud turvaliselt?

M 4.498 Ainulogimisega pöörduse turvaline kasutamine

Algatamise eest vastutavad: IT-turbespetsialist, IT-juht

Rakendamise eest vastutavad: IT juht

Tsentraalse identiteedi- ja volituste halduse süsteemi soovitud eesmärk on, et IT-kasutajad autendivad end üks kord ja saavad seejärel pideva juurdepääsu IT-süsteemidele ja rakendustele IT-koosluses, mille jaoks neil on vastavad volitused. Sellist lahendust nimetatakse Single-Sign-On'iks (SSO). Selle kaudu on administraatoritel lihtsam hallata identiteete ja volitusi ning kasutajate jaoks muudab see IT-kasutuse hõlpsamaks, sest nad peavad end ainult üks kord sisse logima.

Turbe seisukohalt toob SSO seega kaasa palju eeliseid, kuid ka mõned ohud ja vastavad turvameetmed.

- Identiteedivarguse korral ei ole ründe toimepanijal juurdepääs mitte ainult ühele, vaid paljudele süsteemidele. Seetõttu tuleks SSO-süsteeme kasutada alati kahefaktorilise autentimisega.
- SSO-süsteemi turvalisus määrab kindlaks ühendatud süsteemide ja rakenduste turvalisuse. Seetõttu peavad Single-Sign-On'i jaoks kasutatavad turvamehhanismid ja parooli kvaliteet (moodustamise reeglid, keerukus, kehtivusaeg) olema piisavad ühendatud rakenduste või süsteemide üha suurenevate nõuete jaoks.
- Ründe toimepanija jaoks on autentimisandmed SSO puhul eriti huvitavad. Seetõttu tohib neid edastada ja salvestada üksnes krüpteeritult.
- Kui tsentraalne SSO-süsteem langeb rivist välja, võib teatud tingimustel kaduda juurdepääs sellega seotud IT-süsteemidele või rakendustele. Seetõttu on siin tingimata vaja hädaolukorra kontseptsiooni (vt M 6.166 Valmisolek hädaolukorraks identiteedi- ja volituste halduse süsteemi puhul).
- Mobiilsed IT-süsteemid on mõnikord ajutiselt vallasrežiimis. Sellest hoolimata tahavad kasutajad töötada ka väljaspool tööruume. Tuleb tagada, et sellistes olukordades oleks võimalik kaitstud juurdepääs.
- Kui kasutajad ei saa SSO-süsteemi sisse logida, näiteks selle tõttu, et nad on oma logimispääsmiku või salasõna unustanud, saavad nad oma IT-d alles siis uuesti kasutada, kui on võetud vastavad asendusmeetmed.
- Mõnikord ei vasta pääsuõiguste andmine SSO-süsteemide puhul üldse või ei vasta piisavalt konkreetsele kontekstile, mis tähendab, et arvesse ei võeta rolli, kohta, aega või tegevust, nii et kasutajad töötavad ulatuslike juurdepääsuõigustega, mis kehtivad paljude erinevate tegevuste korral. Kasutajad peavad SSO-süsteemidesse pidevalt sisse logima, sest SSO kaudu sõltub paljude süsteemide turvalisus just juurdepääsu turvalisusest. Tuleb kontrollida, kuidas toimub automaatne väljalogimine tegevusetuse korral, sest SSO kaudu võib ühendada ka süsteeme, mille puhul võivad pikemad tegevusetuse etapid olla normaalsed.
- Mitmekordse sisselogimise võimalus tuleb SSO-süsteemil inaktiveerida. Samuti on SSO-süsteemi mitmekordselt valesti sisselogimise korral soovitatav kasutajate automaatne lukustamine.

SSO-süsteemidesse võib lisada levinud IT-süsteeme ja rakendusi ilma suuremate muudatusteta, mittestandardsete lahenduste jaoks tuleb leida muud

lahendused. Seetõttu kasutatakse praktikas ühilduvusest ja majanduslikkusest tingituna pigem niinimetatud Reduced-Sign-On-lahendusi mitte kogu organisatsiooni hõlmavate volitustega.

Kasutajatel võib samaaegselt olla mitu rolli erinevate volituste profiilidega, näiteks administraator ja töötaja. Tuleb mõelda selle peale, kuidas tagada SSO puhul, et kasutajad ei teostaks erinevate turvanõuetega ülesandeid sama kasutajatunnusega maksimaalsete volitustega (rollide lahutamine).

Erinevate rollide jaoks peaksid kasutajad kasutama ka erinevaid süsteemirolle, seega töötama eraldatud kasutajatunnustega, eriti erinevate turvanõuete korral. Nii on võimalik näiteks takistada, et ründe toimepanija väärkasutab kahjustatud kasutajatunnuse abil liiga paljusid õigusi.

Töötajatele ei tohiks aga siiski määrata liiga palju kasutajatunnuseid, sest see ei ole praktiline ning seeläbi tõuseb oht, et möödaminekukatsete korral tekivad uued turvariskid. Seepärast tuleks olenevalt andmete või IT-süsteemide kaitsevajadusest kontrollida, kui palju kasutajatunnuseid on vaja.

XML-Framework Security Assertion Markup Language'i (SAML) või programmikonstruktsioonidel, nagu FastXPath, põhinevate asukohaandmete ja nimeruumiprefiksite teisendamise kasutamine võivad parandada SSO-süsteemide turvalisust XML-Signature-Wrapping-rünnete suhtes.

Kontrollküsimused:

- Kas Single-Sign-On'i puhul kasutatavad turvamehhanismid vastavad ühendatud rakenduste ja süsteemide nõuetele?
- Kas SSO puhul kasutatakse pidevalt kahefaktorilist autentimist?
- Kas autentimisandmed edastatakse ja salvestatakse SSO puhul üksnes krüpteeritult?

M 4.499 Identiteedi- ja volituste halduse süsteemide asjakohane valik

Algatamise eest vastutavad: IT turbespetsialist, IT-juht
Rakendamise eest vastutavad: IT-juht, IT turbespetsialist, varumisosakond

Asjakohaste lahenduste valimise korral identiteedi- ja volituste halduse jaoks ei ole oluline roll üksnes tehnilistel küsimustel. Praktika on näidanud, et siinjuures on olulised edu tegurid töökorralduslikud aspektid. Identiteedi- ja volituste halduse süsteem peab esmajoones sobima asutusele ja selle vastavatele äriprotsessidele, organisatsioonistruktuuridele ning protsessidele ja nende kaitsevajadusele ning alles teises järjekorras olema ühendatud olemasoleva taristuga. See peab looma asutuses kehtivad nõuded identiteetide ja volituste käsitlemiseks. Siia kuuluvad näiteks nõuded meetmest M 2.220 Pääsu reguleerimise suunised .

Identiteedi- ja volituste halduse süsteemid on keerulised süsteemid, mille juurutamine vajab väga palju teadmisi tehnikast, äriprotsessidest ja volituste mudelitest, mistõttu on sageli vaja teha koostööd organisatsioonivälistе nõustajatega. Erinevate IT-süsteemide ühendamine võib toimuda erinevate tehniliste lähenemiste kaudu, nt kataloogiteenustega. Tehnoloogiline nõue on, et heterogeensete rakenduste erinev volituste haldus integreeritakse tsentraalselt.

Muu hulgas tuleb selgeks teha järgmised punktid:

- Kas rakendatakse tsentraalset või detsentraalset lahendust?
- Kas tuleb kasutada ainulogimisega pöördust?
- Kas toimub omandi, teadmiste ja/või biomeetriliste omaduste autentimine?
- Kas tsentraalse lahenduse (reduced sign-on) korral peab rakendus põhinema sünkroniseerimisel või tsentraalsel andmepanga võrdlusel?
- Millised liidesed on vajalikud IT-süsteemide ühendamiseks identiteedi- ja volituste halduse süsteemiga?

Identiteedi- ja volituste halduse süsteemi juurutamisega tekib kiiresti soov, et kasutajad ei peaks igasse IT-süsteemi sisse logima erineva parooliga. Pigem sooviksid kasutajad ka suurte heterogeensete võrkude korral autentida end üksnes esimese kasutatava IT-süsteemi juures. Selline meetod, mida nimetatakse ainulogimisega pöörduseks, edastab seejärel autentimisandmed järgmistele IT-süsteemidele.

Praktikas on end õigustanud püüdlemine eelkõige reduced sign-on'i poole, mis tähendab et logimisprotseduure iga kasutaja kohta püütakse kahandada. Just seeläbi vähendatakse oluliselt kasutajate, aga ka administraatorite koormust.

Olemas on terve hulk erinevaid identifitseerimise ja autentimise mehhanisme. Asjakohaste mehhanismide valikul peaks esikohal olema nendega kaitstavate andmete ja äriprotsesside kaitsevajadus (vt ka M 4.133z Sobivate autentimismehhanismide valimine).

Identiteedi- ja volituste halduse süsteemi asjakohase valiku jaoks tuleb asutuse konkreetsete nõuete põhjal tuletada valikukriteeriumid (vt ka meetmeid M 2.555 Rakenduste autentimiskontseptsiooni koostamine , M 4.133z Sobivate autentimismehhanismide valimine , M 4.498 Ainulogimisega pöörduse turvaline kasutamine ja M 4.500 Identiteedi- ja volituste halduse süsteemide asjakohane kasutamine).

Alljärgnevalt on üles loetletud mõned valikukriteeriumid identiteedi- ja volituste halduse süsteemi jaoks:

- Kas on võimalik teostada tööülesannete lahutamise põhimõtet (M 2.5 Vastutuse ja ülesannete jaotamine)?
- Koostalitlusvõime: kas identiteedi- ja volituste halduse süsteemiga on võimalik tsentraalselt integreerida heterogeensete rakenduste erinevat volituste haldust?
- Kas rakendus toetab kavandatud autentimistegurite, nagu teadmised, omand ja biomeetria, kasutamist.
- Kas on võimalik autentimisvõimaluste skaleerimine kaitsevajaduse alusel?
- Kas on võimalikud järjepidevad õiguste muutmised kuni õiguste lühiajalise äravõtmiseni, kui see on väga vajalik (nt töötaja vabastatakse tähtajatult töölt)?
- Kas autentimisandmeid kaitstakse salvestamisel ja töötlemisel piisavalt (ei salvestata ega edastata loetava kirjana, vaid alati krüpteeritult)?
- Kas identiteedi- ja volituste halduse süsteemi olemasolevad krüptograafilised funktsioonid vastavad kaitsevajadusele ja kas neil on piisav mehhanismi tugevus (vt ka M 2.164 Sobiva krüptoprotseduuri valimine)?
- Kas autentimisandmeid hallatakse turvaliselt? Kas on tagatud, et näiteks paroole ei salvestata kunagi vastavatesse IT-süsteemidesse krüpteerimata kujul?
- Kui kiiresti on võimalik identiteete, volitusi või paroole muuta, nt kahjustamise kahtluse korral?
- Kas reageerimist valedele autentimiskatsetele saab juurutada turvanõuete kohaselt?
- Kas turbe seisukohalt kriitilisi parameetreid, nagu autentimisnõuded, on võimalik konfigureerida turvanõuete kohaselt?
- Kas identiteedi- ja volituste halduse süsteemi saab määratud valdkondades juurutada haldustöötajate jaoks diferentseeritud õiguste struktuure (lugemine, kirjutamine, käitamine, muutmine)?
- Kas toode salvestab õiguste haldamisega seotud andmeid nii, et neid ei oleks võimalik manipuleerida?
- Kas identiteedi- ja volituste halduse süsteemil on olemas asjakohane logimine?
- Kas on tagatud, et volitamata isikute logimist poleks võimalik inaktiveerida?

- Kas protokollid ise ei ole volitatud isikute jaoks loetavad ega muudetavad?
- Kas logimine on ülevaatlik, täielik ja õige?
- Kas identiteedi- ja volituste halduse süsteemil on olemas ülevaatlik ja lihtsalt kasutatav logiandmete analüüs?

Kontrollküsimused:

- Kas valitud identiteedi- ja volituste halduse süsteem sobib, et viia ellu töö-ülesannete lahutamise põhimõtet?
- Kas kriteeriumide nimekirja nõuded on valitud identiteedi- ja volituste halduse süsteemiga kaetud?

M 4.500 Identiteedi- ja volituste halduse süsteemide asjakohane kasutamine

Algatamise eest vastutavad: IT-turbespetsialist, IT-juht

Rakendamise eest vastutavad: IT juht

Identiteedi- ja volituste halduse süsteemid on integreeritud IT-süsteemid, millega saab digitaalseid identiteete IT-taristus kõikide süsteemide jaoks plaanija eesmärgipäraselt ulatuslikult automatiseerida. Selline süsteem peaks hõlmama kõiki protsessi toiminguid, mis on seotud õiguste ja kasutajatunnuste määramise, kustutamise ja muutmisega.

Siia kuuluvad:

- identiteedihaldus,
- rollihaldus,
- kasutajatunnuste ja -õiguste haldus ja hooldus: määramine, muutmine ja kustutamine,
- poliitikate haldus.

Tehnilise teostuse kohaselt koosneb identiteedi- ja volituste halduse süsteem andmetalletuskomponendist (andmebaas), töövoost (volituste andmine jne) ja liideste lahendusest (kataloogiteenused jne), et seadistada volitusi. Üksikud komponendid peavad olema piisavalt kaitstud, vt konkreetseid mooduleid, nt B 1.15 Andmete kustutamine ja hävitamine).

Identiteedi- ja volituste halduse süsteem võib olla üles ehitatud erinevalt, näiteks

- tsentraalselt (kõik identiteedid on koondatud ühte kohta),
- liidetult (identiteetide detsentraalne jaotamine väljapoole asutuse piire).

Selleks, et vähendada kulutusi administreerimisele ja hooldusele, on abiks asjakohased kasutaja- ja volituste halduse tööriistad. Peale selle soovitatakse õiguste juurutamiseks automaatseid taotlemise ja määramise protseduure, sest siinjuures tuleb sageli läbida mitmed kinnitamisprotseduurid, mis tuleb kokku viia ja mida tuleb järgida.

Identiteedi- ja volituste halduse tsentraalsed tööriistad on soositud ründe eesmärk, sest manipuleerimise korral oleks siin võimalus juurdepääsuks paljudele süsteemidele ja andmetele. Sageli on identiteedi- ja volituste halduse tööriistad ka nii keerulised, et edukat rünnet on raske avastada. Seetõttu on oluline kindlaks määrata reeglid, mille järgi tegeliku või kahtlustatava ründe korral toimida (vt ka B 1.8 Turvaintsidentide käsitlus). Tsentraalsete identiteedi- ja volituste halduse süsteemide korral, mille puhul on vajalik alaline juurdepääs volituste kontrollimiseks, tuleb võtta meetmed hädaolukordade haldamiseks (vt M 6.166 Valmisolek hädaolukorraks identiteedi- ja volituste halduse süsteemi puhul).

Kontrollküsimused:

- Kas on olemas asjakohased tööriistad identiteedi- ja volituste halduse süsteemi jaoks?
- Kas identiteedi- ja volituste halduse süsteem on rünnete eest piisavalt kaitstud?

M 4.501 Kiirgusturve

Algatamise eest vastutab: infoturbespetsialist

Rakendamise eest vastutab: infoturbespetsialist

Iga elektrooniline seade kiirgab rohkemal või vähemal määral tugevaid elektromagnetilisi laineid. See kiirgus on tuntud kui elektromagnetiline koormus ning selle maksimaalselt lubatud tugevus on üldjuhul seaduses reguleeritud.

Infotöötlusseadmete puhul (arvuti, printer, faksiaparaat, modem jne), võib see elektromagnetiline kiirgus endas kanda ka hetkel töödeldavat infot. Sellist infot kandvat kiirgust nimetatakse paljastavaks kiirguseks. Kui paljastav kiirgus püütakse kinni teatud kauguses, nt naabermajas või läheduses asuvas sõidukis, saab selle abil infot taastada. See ohustab andmete konfidentsiaalsust. Reeglina tuleb selleks tarvitusele võtta lisameetmed.

Paljastav kiirgus võib ruumist lahkuda mitmel erineval moel:

- Elektromagnetiliste lainetena, mis levivad vabas ruumis nagu raadiolained.
- Juhtmaterjaliga seotud kiirgusena mööda metalljuhte (kaableid, kliimašahte, küttetorusid).
- Andmekaabli ja paralleelselt jooksva kaabli kattumisel. Kiirgus levib paralleelkaablil pikalt edasi ja on veel kaugel kättesaadav.
- Akustilise kiirgusena, nt printeritel. Printimise üksikasjalik teave levib heli või ultraheli kaudu ja on mikrofonidega salvestatav.
- Akustilise kattuvuse korral teiste seadmetega. Heli muutmine elektrisignaalideks toimub heli suhtes tundlike seadmeosadega, mis võivad teatud eeldustel töötada nagu „mikrofon”. Edasi toimub levimine mööda metalljuhti või elektromagnetilise ruumikiirguse kujul.
- Paljastavat kiirgust võib tekitada ka seadmete väline manipuleerimine. Kui nt kiiritada seadet kõrgsagedusliku energiaga, võivad seadmes toimuvad elektrilised protseduurid mõjutada saabuvaid laineid nii, et need kannavad endas nüüd töödeldud infot.

Igal juhul mõjutab seadmete installeerimine ehk nende omavahelised kaablid ja ühendus vooluvõrguga olulisel määral kiirguse levikut ja seega ka ulatust. Kaitsemeetmed, mis vähendavad ohtu, ilma et sellega kaasneks olulisi lisakulusid.

Siia kuuluvad järgmised:

Tsoonimudel

- Tsoonimudel arvestab paljastava kiirguse levimistingimustega seoses vastavate hoone- ja maastikutingimustega. Seejuures mõõdetakse põhjustavast IT-seadmest potentsiaalse vastuvõtjani leviva kiirguse nõrgenemist. Olenevalt kasutuskoha omadustest võib kasutada ka seadmeid, millel on võetud tarvitusele ainult vähesed häirevähendamise meetmed või siis selliseid, millel need üldse puuduvad.

Häire piiramine allikas

- Häire piiramine allikas on eriti tõhus uute IT-toodete arendamisel. Sellisel juhul vähendatakse või muudetakse paljastavat kiirgust juba tekkekohas seadme sees selliselt, et seda ei saaks enam kasutada. Tänu sellele meetodile on nt võimalik kasutada ka soodsamat plastkorpust, mis tõstab toote hinda vaid tühisel määral.

Lühimõõtmise meetod

- Lühimõõtmise meetodi ja manipuleerimise kontrollmeetodi väljatöötamine võimaldab tagada kiirgusturvalisust vähese vaevaga ka pärast hooldust, remonti või võimalikke volitamata juurdepääse.

Vähese kiirgusega või varjestatud seadmed

- Arvutimonitoride tootjad teevad sageli reklaami mõistega „vähese kiirgusega" normide MPR II, TCO või SSI kohaselt. Need direktiivid arvestavad eranditult seadmete kiirguse võimalike tervist kahjustavate mõjudega. Seega ei sobi kiirguse mõõtmismeetodid ja piiväärtused paljastava kiirguse tõendamiseks ja sarnaselt elektromagnetilise ühilduvuse (EMC) mõõtmistele ei võimalda hinnata andmete volitamata pealtkuulamise ohtu.

Lisaks pakutakse ka spetsiaalse varjestusega IT-süsteeme. Meetmes asuv detailne kontrollikontseptsioon on mõeldud IT-seadmete või -süsteemide astmeliseks kontrolliks. Selle kontseptsiooni põhiidee seisneb kaitsemeetmete mahu võimalikult tõhusas kohandamises kasutaja poolt eeldatavale ohuastmele, et pakkuda minimeeritud kulude juures optimaalset kiirguskaitset. Nt võib tsoonimudeli järgi kontrollitud ja tsoonides 1–3 kasutusse lubatud seade (nn „1. tsooni seade") pakkuda piisavat kaitset konfidentsiaalsete andmete volitamata pealtkuulamise eest. Usaldusväärsusega seotud kõrge või väga kõrge kaitsevajaduse korral tuleks seepärast kontrollida, kas vähese kiirgusega või varjestatud seadmete kasutamine on eesmärgipärane või isegi nõutav.

Kontrollküsimused:

- Kas kiirgusturbe jaoks on kaalutud täiendavaid meetmeid, mida võiks vaja minna?

M 4.E1 ID-kaardi/PKI lahenduste turvaline seadistamine

Algatamise eest vastutavad: IT juht

Rakendamise eest vastutavad: administraator, IT juhi määratud isik

Kõik ID-kaardi/PKI lahenduste seadistamised tuleb läbi viia vastavalt väljatöötaja normdokumentatsioonile ja juhenditele. Igal tootel ja lahendusel peab olema oma kindel vastutaja (ülem), kelle vastutusalas on toote asjakohane seadistamine ja edasine haldamine. Kui toote või lahenduse seadistamine eeldab mingite dokumentatsioonis/juhendites üheselt fikseerimata probleemide lahendamist, tulevad need olukorrad reguleerida asutusesiseste juhendite ja kordadega.

Nimetatud juhendite ja kordade olemasolu ja pideva täiendamise eest vastutab IT juht või tema määratud isik. Juhendite ja kordade koostamisel peab igal juhul osalema ka turvajuht, kes peab need juhendid ka kinnitama. Turvajuhi vastutusalasse jääb nende juhendite/kordade vastavuse hindamine asutuse infoturbepoliitikaga (vt – M 2.192 Infoturbepoliitika koostamine ja M 2.337 Infoturbe integreerimine üleorganisatsioonilistesse tegevustesse ja protsessidesse). Enne ID-kaardi/PKI lahenduste evitamist läbi viia vastavad turvatestid. Lisaks tuleb neil juhtumeil, kui asutuses kasutatakse digitemplit automaatrežiimis ilma inimese vahetu osavõtuta, teha kohustuslikus korras penetratsioonitestid (vt M 5.150 Penetratsioonitestide läbiviimine). Muudel juhudel on penetratsioonitestide korraldamine vabatahtlik.

Muus osas tuleb ID-kaardi/PKI lahenduste turvalisel seadistamisel lähtuda erineva tüüptarkvaraga tehtavatele tegevustele kehtivatest turvameetmetest ja neile kehtivatest reeglitest. Eriline tähelepanu tuleb sealjuures pöörata meetmes M 2.86 Tarkvara tervikluse tagamine kirjeldatule, kuna see võimaldab ära hoida IDkaardi/PKI lahenduste kuritahtlikku manipuleerimist (vt G 2.E6 Digiallkirja andmine või autentimine ilma võtmepaari omaniku teadmata). Kõikidest kasutatud lahendustest tuleb omada varukoopiat (vt M 6.21 Kasutatava tarkvara varukoopia). Lisaks tuleks lugeda ka M 2.318 Serveri turvaline installeerimine ja M 4.239 Serveri turvaline käitus .

Kontrollküsimus:

- Kas olemasolev vastutusskeem ja juhendmaterjalid tagavad piisaval tasemel ID-kaardi/PKI komponentide asjakohase seadistuse?

M 4.E2 ID-kaardi/PKI lahenduste turvaline seadistamine

Algatamise eest vastutavad: IT juht

Rakendamise eest vastutavad: administraator, IT juhi määratud isik

Asutuse sees tuleb halduslike protsessidega tagada, et kõik arvutid, kus kasutatakse ID-kaardi/PKI lahendusi või kus võib ette tulla digiallkirjastatud dokumentide lugemise vajadust, oleksid varustatud ID-kaardi tarkvara viimase versiooniga. Vastava uuendamise korraldamise täpsema viisi määrab ära IT juht või tema määratud isik. See peab olema fikseeritud mingis kirjalikus juhendis ning kinnitatud asutuse turvajuhi poolt. Uuendatus on seetõttu oluline teema, et uuemaid digiallkirjadega varustatud dokumente võivad tarkvara vanemad versioonid kas üldse mitte lugeda või kuulutada korrektsed digiallkirjad vääralt mitteverifitseerunuteks (vt M 4.E1 ID-kaardi/PKI lahenduste turvaline seadistamine).

Kontrollküsimus:

- Kas ja kuidas on tagatud, et asutuse kõikides arvutites on seadistatud ID-kaardi tarkvara uusim stabiilne versioon?

M 4.E3 ID-kaardi, digi-ID ja mobiil-ID ning nende sertifikaatide õigeaegne uuendamine

Algatamise eest vastutavad: kasutaja
Rakendamise eest vastutavad: kasutaja

Kui asutuse töötaja kasutab tööasjus oma ID-kaarti, digi-ID-d ja/või mobiil-ID-d, peab ta õigeaegselt hoolitsema seadme uuendamise eest, et asutuse infosüsteemis ei tekiks seadme või seadmel asuva sertifikaadi kehtivusaja lõppemisest tingitud käideldavuskadusid. Arvestades võimalikke järjekordi ja muid ootamatusi seadme vahetamisel/uuendamisel, on mõistlik uut ID-kaarti ja/või digi-ID-d taotleda hiljemalt kuu kuni kaks enne kehtivusaja lõppemist. Uut mobiil-ID-d on mõistlik taotleda nädal kuni kaks enne kehtivusaja lõppemist.

Tuleb arvestada, et seadme uuendamine ja seadmel oleva sertifikaadi uuendamine on tegelikult kaks eraldiseisvat tegevust – seade võimaldab oma kasutusajal genereerida uue võtmepaari, millele saab võtta uue sertifikaadi. Kuna aga kaasajal on sertifikaadi (võtmepaari) eluiga aga seadme elueaga võrdne, läheb sertifikaatide uuendamist ilma seadme uuendamiseta praktikas tarvis üsna harva – näiteks juhtumeil, kus vastav privaatvõti on mingitel juhtumitel kompromiteerinud või on tekkinud kompromiteerumisoht. Nende viimaste olukordade üle (ja sertifikaatide uuendamisvajaduse üle) peab otsustama asutuse turvajuht (vt M 5.E1 Sertifikaatide õigeaegne peatamine). Nimetatud teemasid tuleb käsitleda ka töötajate koolitamisel (vt M 3.E2 Töötajate koolitus ID-kaardi/PKI lahenduste kasutamise osas). Nimetatud teavitustöö läbiviimise eest vastutab asutuse turvajuht.

Kontrollküsimused:

- Kas asutuses on esinenud probleeme, mille on tekitanud ootamatult kehtivuse kaotanud ID-kaart, digi-ID ja/või mobiil-ID kaart?
- Kas kasutajad on teadlikud, et ID-kaart, digi-ID ja/või mobiil-ID uuendamisele tuleb mõelda aegsasti enne kehtivusaja lõppemist?

M 4.E4 Juurdepääsutõendiga määratud signeerimisressursi seire ja uuendamine

Algatamise eest vastutavad: IT juht

Rakendamise eest vastutavad: IT juht või tema määratud isik

Eesti rahvusliku PKI vaates peamise sertifitseerimisteenuse osutaja – Sertifitseerimiskeskuse ASi – teenuste eest maksmine on suures osas koondatud digiallkirja andmisega kaasnevasse OCSP-teenusesse. Teenuste eest tasumine käib antud digiallkirjade mahu pealt, kusjuures OCSP-teenuse kasutamist digiallkirjastamise tarkvaras võimaldab selles arvutis asuv juurdepääsutõend, mille põhjal seotakse antud allkirjad ka konkreetse asutusega. Nimetatud skeem võib ebapiisava seire või järelevalve korral tekitada olukorra, kus asutuse poolt ostetud ressurss ootamatult ammendub, mistõttu ühel hetkel ei saa olemasoleva juurdepääsutõendi põhjal asutuse sees enam uusi digiallkirju anda.

Juurdepääsutõendiga määratud signeerimisressursi uuendamine (kõikides lõppkasutaja arvutites) peab asutuses olema IT-juhi või tema määratud isiku vastutusalas.

Selle eest vastutav isik peab tagama, et vastav ressurss saaks uuendatud aegsasti, ilma lõppkasutajale komplikatsioone tekitamata. Soovitavalt tuleb ressurssi uuendada hiljemalt siis, kui juurdepääsutõendite varu on prognoositavalt alles kaheks nädalaks. Ressursivaru ning võimaliku uuendamisaja prognoosimiseks on vajalik juurdepääsutõendiga määratud ressursside seire vähemalt kord kuus. Ka see peab olema IT-juhi või tema määratud isiku vastutusalas.

Kontrollküsimused:

- Kas asutuses on esinenud probleeme, mille on tekitanud ootamatult lõppenud signeerimisressurss?
- Kas ja kuidas kasutatakse asutuse sees juurdepääsutõendiga määratud signeerimisressursi seire käigus saadud andmeid?

M 4.E5 Nõuded ID-kaardi/PKI lahendusi kasutavale turvalisele autentimisele

Algatamise eest vastutavad: turvajuht

Rakendamise eest vastutavad: IT juht või tema määratud isik

ID-kaardi, digi-ID, mobiil-ID ja/või analoogilise seadme põhisel turvalisel autentimisel veebikeskkondades on mõned kitsaskohad, mis on seotud turvalise sessiooni haldamise eripäradega.

Seetõttu tuleb niisugustes süsteemides täita mõningaid erinõudeid:

- ID-kaardi või digi-ID põhisel turvalisel autentimisel tuleb turvaline sessioon lõpetada kaardi eemaldamisel arvutist.
- Turvalise sessiooni ajal peab vastaval veebilehel olema nähtava koha peal nupp “Välju” või “Logi välja”, mille vajutamisel tuleb turvaline sessioon lõpetada.
- Mõistlik oleks turvaline sessioon lõpetada ka veebibrauseri lehe (sh vahelehe) sulgemisel, kuid kõikide brauseritüüpidega see alati ei õnnestu. Vastavaid omadusi tuleb arendustööde ajal testida. Kui vahelehe sulgemisel turvalise sessiooni lõpetamine alati ei õnnestu, tuleb kohe sisselogimise järel, turvalise sessiooni alguses kuvada kasutajale selge teade, et sessiooni saab sulgeda “Välju”-nupule (või analoogsele) vajutamisega või veebibrauseri (brauseri kõikide lehtede) sulgemisega.
- Turvalise sessiooni sulgemise järel ei tohi arvuti ega brauseri vahemälusse jääda sessiooni sisu kajastavat jäätkeavet – see tuleb turvaliselt kustutada (vt M 2.167 Andmete kustutamiseks või hävitamiseks sobivate lahenduste valik). Nimetatud omadusi tuleb testimisel kontrollida (vt M 4.65 Uue riist- ja tarkvara testimine ja M 5.150 Penetratsioonitestide läbiviimine). Testi tulemusi kontrollib, hindab ja kinnitab turvajuht, kes otsustab ka, kas eelnõutud turvaomadused on täidetud. Lisaks tuleb asutuse sees mõelda’läbi tegevuskava olukordadeks, kus sertifikaatide kontrollimise (OCSP) teenused kättesaadavad ei ole.

Võimalik on sel juhul kaks varianti:

- autentimine infosüsteemi ei toimu enne vastavate teenuste taastumist
- autentimisel sertifikaadi kehtivust nimetatud juhtumitel kui eriolukordades ei kontrollita

Valitav lahendus korral tuleb läbi teha vastava valdkonna üldine riskianalüüs, millest nähtub ühe või teise variandi valik.

Kontrollküsimus:

- Kas ja millisel määral on süsteemide arendajad teadlikud eeltoodud nõuetest ning turvalise sessiooni erinevatest lõpetamise võimalustest praktikas?

M 4.E6 Keeld anda digiallkirja autentimisvõtmepaari ja PIN1-koodi kasutades

Algatamise eest vastutavad: turvajuht

Rakendamise eest vastutavad: IT juht või signeerimistesrkvara koostaja eest vastutaja

Lubamatu on kasutada signeerimistarkvara, mis kasutavad allkirja andmiseks mitte signeerimisvõtmepaarti ja PIN2-koodi, vaid autentimisvõtmepaari (autoriseerimisvõtmepaari) ning PIN1-koodi. DigiDOCi varasemad versioonid on seda lubanud teha ning kahjuks on selliseid tarkvarasid ka vääralt kasutusele võetud. Sellised digiallkirjad on uute standardite kohaselt kehtetud (ei verifitseeru), samuti kuhjuvad autentimisvõtmepaariga digiallkirja andmisel ülemäärased riskid. Kasutatava või kasutusele võetava digiallkirjastamistarkavara korral tuleb veenduda, et need kasutaksid allkirjade andmisel ikkagi signeerimisvõtmepaari ja PIN2-koodi.

M5: Side

Meetmete nimekiri

M 5.1 Tarbetute liinide kõrvaldamine või lühistamine ja maandamine

Algatamise eest vastutavad: tehnikajuht

Rakendamise eest vastutavad: administraator, tehnikaosakond

Tarbetud liinid on sellised, mis pole hoones kas kasutusala muutumise või moderniseerimise tõttu enam vajalikud. Tarbetud liinid tuleb täielikult eemaldada, et piirata hoone tulekoormust vajaliku miinimumini ja täita olemasolevaid trasse ainult vajalikes piirides. Liinide eemaldamisel tuleb jälgida, et tuletõkked suletaks pärast kaablite eemaldamist taas nõuetekohaselt. Liinide tarbetuse üle tohib otsustada alles pärast hoolikat kontrolli, mida teostab vastutava organisatsiooni allüksus. Vastav otsus tuleb dokumenteerida.

Kui juhtmestiku infrastruktuuri muudatusi tehakse tööprotsessidega paralleelselt, tuleb rakendada organisatsioonilisi meetmeid, et tööprotsesside segamine oleks minimaalne. Vajadusel tuleb selleks planeerida tööde tegemist nädalalõppudel ja öistel aegadel. Kui olemasolevates trassides ei ole piisavalt ruumi vanade ja uute kaablite mahutamiseks, tuleb kaablite jaoks paigaldada uued trassid, et ümberlülitusele kuluv aeg veel töötavalt vanalt infrastruktuurilt uuele infrastruktuurile üleminekul oleks võimalikult lühike.

Trasse ja kaableid, mida on mõistlik olemasoleva tehnika jaoks reservina edasi hoida, tuleb säilitada töökõlblikus seisundis. Tarbetud jaotused ja teed jaoturites tuleb eemaldada ja dokumentatsioonist kustutada. Ka ebavajalikud kaablid tuleks võimalusel eemaldada. Kui see on võimatu, näiteks kuna kaablid on paigaldatud krohvi alla, tuleb need lühistamisega desaktiveerida ja kaitsta. Kasutust kirjeldavas dokumentatsioonis tuleb kõik muudatused kontrollitavalt dokumenteerida. Mõistlike ajavahemike tagant ja igal korral pärast kaablitöid on soovitav lasta muudatused spetsialistil üle kontrollida. Vastavad kontrollid tuleb protokollida.

Kontrollküsimus:

- Kes otsustab kaablite terviklikkuse ja reservide suuruse üle?

M 5.2 Võrgu sobiv topoloogia

Algatamise eest vastutavad: IT-juht
Rakendamise eest vastutavad: planeerija, tehnika juht

Infotehnoloogias eristatakse füüsilist ja loogilist võrgutopoloogiat. Võrgu füüsiline ja loogiline topoloogia ei pruugi olla identsed. Loogilise võrgutopoloogia puhul on tegu andmevoogude jaotusega. Aktiivsete võrgukomponentide seadistamisega saab seda kujundada peaaegu et täiesti oma äranägemise järgi. Virtuaalsete kohtvõrkude (VLAN) abil saab võrgus kujundada täiendavaid loogilisi struktuure. Järgnevalt käsitletakse põhjalikumalt füüsilist võrgutopoloogiat, st kaablite paigaldust ja jaoturite asendit hoones. Füüsiline topoloogia lähtub peaaegu alati ruumidest, kuhu võrk üles seatakse.

Olulised on seejuures:

- võrgus osalejate asukohad,
- trasside ja kaablite olemasolev ruum (vt M 1.21 Liinide õige dimensioneerimine),
- vajalikud kaablitüübid (vt M 1.20 Kaablite valimine füüsiliste/mehaaniliste omaduste järgi),
- nõuded kaablite kaitsele (vt M 1.22z Liinide ja jaotuskilpide füüsiline kaitse).

Tavaliselt eristatakse võrgutopoloogia kahte põhivormi, täht ja siin. Täiendusena saab tähest tuletada puukujulise struktuuri ja siinist ringikujulise struktuuri. Hoonete IT-juhtmestiku esmakordse paigaldamise ja täiendamise puhul omavad praktilist tähendust tähe- ja puukujuline struktuur. Järgnevalt on loetletud võimalike topoloogiate eelised ja puudused. Muid võimalikke topoloogiad, mida siinkohal ei mainita, võib pidada vaadeldud struktuuride erijuhtudeks.

Täht
Tähe puhul on kõik võrgus osalejad ühendatud vastavaotstarbelise kaabli abil keskse sõlmega. Esmajoones just „Collapsed Backbone“- arhitektuuri puhul, milles (loogiline) keskne kommutaator ühendab kõiki servereid ja lõppseadmeid, paigaldatakse kaabliühendused hoones tähekujuliselt.

Antud topoloogia pakub järgnevaid eeliseid:

- Üksikute kaablite kahjustumine mõjutab ainult seda süsteemi, mis on kahjustunud kaabliga ühendatud.
- Võrgus osalejate jaotumise muutmist kesksõlme ühenduspunkti suhtes ning üksikute osalejate lahutamist saab teha tsentraalselt.
- Tähekujulise juhtmestikuga saab moodustada kõiki võimalikke loogilisi topoloogiaid.

Täht-topoloogial on järgnevad puudused:

- Kesksõlme avarii korral langevad välja kõik sellega ühendatud IT-süsteemid.
- Kuna iga osaleja on eraldi keskse sõlmega ühendatud, on kaablitööd väga mahukad.
- Individuaalsete liinide arvu suurenemisega kasvab signaalide kattumise võimalus.
- Tähekujulise kaabliühenduse puhul võib sõltuvalt kasutatud kaablitüübist ja rakendatud protokollist esineda ulatuvuse probleeme (vt M 5.3 Sidetehniliselt sobivad kaablitüübid). Ulatuvuse pikendamiseks võib kasutada võimendeid (Repeater). Kasutatud protokoll määrab ära võimalike võimendite arvu ühenduse kohta, samuti paralleelkasutamise kohta ühes kaablis. Sellega seotud täiendavate investeerimis- ja töökuludega tuleb arvestada majanduslikkuse kalkulatsioone tehes ning omavahel võrrelda alternatiivseid võimalusi.

Ulatuvuse probleemide korral on alternatiivseks lahenduseks kaabliühenduste realiseerimine puukujulises struktuuris.

Puu
Puustruktuur tekib mitme tähekujulise struktuuri ühendamisel keskse sõlmega. Detsentraalse võrgusõlme külge tähekujulise struktuuri abil ühendatud võrgus osalejad koondatakse kasutajarühmadesse. Detsentraalsed võrgusõlmed on omakorda ühe või mitme vastavaotstarbelise kaabliga koondatud keskse võrgusõlme juurde.

Puu-topoloogia pakub järgnevaid eeliseid:

- Süsteemide ühendamisel detsentraalse võrgusõlmega kehivad samad eelised nagu tähekujulise ühenduse puhul.
- Uute osalejate jaoks tuleb uued kaabliühendused luua ainult detsentraalse võrgusõlme juures.
- Detsentraalsete võrgusõlmede vastava teostuse juures on selliste sõlmede osalejatevaheline andmevahetus võimalik ka teiste sõlmede avarii puhul.
- Ühendades detsentraalsed sõlmed omavahel kaabli abil, vähenevad kaablitööd.
- Sõlmedevahelise suure kauguse ületamiseks piisab võimendist ühel kaablil.
- Sõlmede ühendamiseks on mõistlik kasutada kõrge kvaliteediga (tihti kalleid) kaableid, millega saab ka suuri vahemaid ületada ilma lisavõimendita. Soodsama hinnaga kaablite puhul tuleb kasutada võimendeid, mis mõjuvad negatiivselt töökindlusele ning arvestades sellega seotud investeerimis- ja töökulusid tähendab kallite kaablite kasutamine tihti ka kulude kokkuhoidu.

Puu-topoloogial on järgnevad puudused:

- Kui rike esineb mõnda teise detsentraalsesse võrgusõlme viivas üleminekus, katkeb töö kõikide sellega ühendatud osalejate vahel.

- Detsentraalsete võrgusõlmede jaoks vajalik dokumentatsioon ja haldus võivad võrgu töö tagamiseks vajaminevaid üldkulutusi suurendada.

Puu-topoloogia tüüpiline kasutusjuht on hoone kõikide korrusejaoturite (tähttopoloogia tertsiaarjuhtmestiku) ühendamine hoone juhtmestiku jaoturiga (sekundaarjuhtmestikuga).

Kui ressursid peavad olema varuga, võib korrusejaoturid ühendada ka mitme erineva hoonejaoturi külge.

Silmus-võrgutopoloogia täht- ja puustruktuuris
Tsentraalsete võrgusõlmede ja vastavate nõuete korral ka detsentraalsete võrgusõlmede täiendavat ühendamist nimetatakse silmusvõrgu loomiseks. Seeläbi luuakse liiasühendused, mida kasutatakse töökindluse ja kättesaadavuse suurendamiseks.

Siin
Siini korral ühendatakse kõik võrgus osalejad ühise kaabli külge. Tavaliselt tehakse seda keskse kaabli abil, mis ühendatakse harujuhtmete abil üksikute osalejate külge. Uuemad kaablitüübid ja kaabli spetsifikatsioonid ei toeta enam siinikujulist juhtmestikku. See topoloogia ei ole IT-juhtmestiku esmapaigaldamise või moderniseerimise puhul enam oluline.

Ring
Ring on topograafilisest vaatepunktist lähtudes siin, mille mõlemad otsad on omavahel ühendatud. Ringi erivormiks on topeltversioon ehk topeltrõngas, mida kasutatakse näiteks FDDI puhul. Uuemad kaablitüübid ja kaablispetsifikatsioonid ei toeta enam ringikujulist juhtmestikku. See topoloogia ei ole IT-juhtmestiku esmapaigaldamise või moderniseerimise puhul enam oluline.

Kaablitüübid ja maksimumpikkus
Väiksema hoone varustamisel tuleks kaaluda tsentraalse sõlme tähekujulist juhtmestikku. Eelduseks on võimalus paigaldada IT-juhtmestikku selliselt, et iga lõppseadme ühendus jääb vaskkaablite kasutamisel maksimaalselt 90 meetri kaugusele (vastavalt normile EN 50173 kasutusest sõltumatute sidekaablite süsteemide kohta). Selle maksimumpikkuse ületamisel on juhtivaks suuruseks normikohaselt nõutud elektrilistest edastusparameetritest kinnipidamine. Maksimaalselt paigaldatavate pikkuste ületamise vastu saab abi vastavast tootevalikust, mis annab mõningaid varusid. Töökindlust suurendab kõikide lõppseadmete võimalikult eraldi paigaldamine. Kui lõppseadmete ühendusi ei saa kauguse või tugeva elektrihäire tõttu vedada vaskkaablitega, tuleb kasutada valguskaableid. Sõltuvalt edastusprotokollist ja kaabli kvaliteedist saab Multimode -valguskaablite abil katta kuni umbes 2 km pikkuseid vahemaid. Kehtib reegel — mida suurem on edastatava signaali ribalaius, seda lühem on realiseeritav pikkus. Oluliselt suuremaid kauguseid saab vastava vajaduse korral katta Singlemode -valguskaablite kasutamisega.

Suuremate hoonete juhtmestik
Suuremate hoonete kaabeldamisel on soovitatav kasutada puukujulist struktuuri. Kesksest jaotuspunktist (hoonejaoturist) ühendatakse tähekujulise struktuuri alusel omavahel kokku kas korrused või hoone erinevad osad. Korruste tehnikaruumidest lõppseadmete juurde viivad ühendused ühendatakse omakorda tähekujulise struktuuri alusel. Töökindluse suurendamiseks on soovitav rakendada ühekordset liiasust, st süsteemi kaasatakse üks täiendav hoonejaotur, mis ühendatakse samuti kõikide korruste või hooneosadega. Tuleb jälgida, et juhtmestik juhitaks korrustele või hoone eri osadesse eraldi trasside abil. Lisaks tuleks püüelda silmusühenduse kasutamise poole hoonejaoturis, et välisühendusi, näiteks Carrier-kaableid oleks lihtne mõlema hoonejaoturiga ühendada.

Kontrollküsimused:

- Kas planeeritud võrgutopoloogia sobib olemasolevate ruumidega?
- Kas on tagatud, et kaablite maksimumpikkuseid ei ületata?
- Kas korruste või hoone osade ühendamiseks on ette nähtud liiasused?

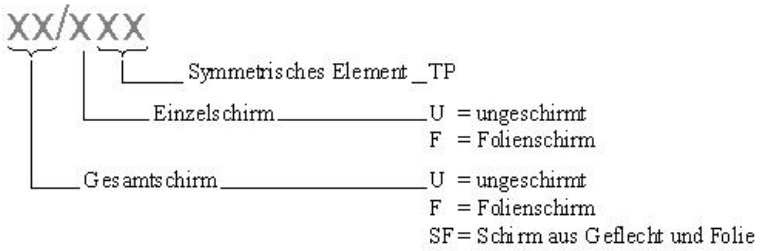
M 5.3 Sidetehniliselt sobivad kaablitüübid

Algatamise eest vastutavad: IT-juht
Rakendamise eest vastutavad: planeerija, tehnikajuht

Sidetehnilisest vaatepunktist määrab kaablite valiku nõutud edastusvõimsus (nimetatakse sageli ka ribalaiuseks, mis pole just päris korrektne nimetus) ja edastusseadmete vaheline kaugus. Lisaks tuleb arvestada ka hoone kujuga, milles tuleb hakata kaableid paigaldama ja kasutama, st trasside ja ümbritsevate tingimustega. Kuna ka need faktorid mõjutavad juhtmestiku ülesehitust, tuleb nendega kaablite valimisel arvestada. Järgnevalt kirjeldatakse eeliseid ja puuduseid IT-turbe seisukohalt. Tänapäeval loodavad edastussüsteemid kasutavad kaablite abil toimiva kommunikatsiooni jaoks elektrilisi või optilisi liideseid. Vastavalt peavad ka edastamisvahendina kasutatavad kaablid sisaldama metalljuhte elektrilise ülekande jaoks või plastikut või klaasi (valguskaabel) optilise edastamise jaoks.

Järgnevalt vaadeldakse lähemalt vask- ja valguskaableid:

- Keerdpaar kaabel (Twisted-Pair cable) - IT-vaskkaablite jaoks kasutatakse sümmeetrilist kaablite ehitust. Selle kaabli ehituse puhul punutakse kaks juhtmesoont omavahel paari ja neli sellist paari omavahel kaabliks (Twisted-Pair-kaabel - TP). Juhtmesoonte läbimõõt, isoleermaterjalid ja värvused, põimimise liik ja soonepaaride varjestus on faktorid, mis eristavad kaableid ribalaiuse ja rikkekindluse lõikes. Kaablitüüpide ühese märgistamise jaoks soovitab ISO/IEC 11801 „Infotehnoloogia – kasutusest sõltumatu asukohajuhtmestik“ 2. väljaanne järgnevat tüübitähiste ühtlustamist, mis määrab selgelt konstruktsiooni elemendid, alustades lugemisega väljastpoolt sissepoole:



Joonis 1: Vaskkaabli tüübi tähistamise süstemaatika

Joonis: Symmetrisches Element_TP – sümmeetriline element_TP (twisted pair), Einzelschirm – üksikvarjestus, Gesamtschirm – üldvarjestus, U = ungeschirmt – varjestamata, F = Folienschirm – kilevarjestus, SF = Schirm aus Geflecht und Folie – punutud ja kilega varjetus

Näiteks:

- varjestamata U/UTP,
- varjestamata, üldvarjestusega kõikide juhtmepaaride jaoks (F/UTP või SF/UTP),
- varjestatud, mille puhul on varjestatud ainult üksikud soonepaarid (U/FTP) – varem nimetati ka paarideks metallkiles (PiMf) - ja
- eelmainitud ehitus koos täiendava üldvarjestusega (F/FTP, S/FTP ja SF/FTP).

Kaablite ja ühenduskomponentide edastamisomadused on määratud normide alusel eri kategooriatesse ja klassidesse. Kategooriad kirjeldavad juhtmestiku infrastruktuuri üksikute detailide suhtes kehtivaid nõudeid ja piirväärtusi, klassid reguleerivad sama asja paigaldatud terviksüsteemi jaoks. Üksikute komponentide edastamisomadused on hetkel jaotatud kategooriatesse 1 kuni 7. Siinjuures kehtib reegel, et mida kõrgem on kategooria, seda suurem on ka edastuse võimalik ribalaius. Usaldusväärset kõrget edastuskvaliteeti on võimalik saavutada ainult seeläbi, kui valitakse välja omavahel kokkusobivad kaablid ja ühenduskomponendid (pesad ja pistikud) ja lastakse need professionaalselt paigaldada. Seadmed „ei tuvasta“ paigaldatud pikkust vaid reageerivad elektrisignaalidele. Seega on kaablite andmeedastuse olulisemaks faktoriks kaablite elektrilised piirväärtused.

ISO/IEC 11801 normi kohaselt on vaskkaablite puhul maksimumpikkuseks 90 m (koos keerdpaar- ja ühenduskaablitega 100 m). Nimetatud maksimumpikkust võib siiski ületada, kui peetakse kinni nõutud elektrilistest edastamisparameetritest.

TP-kaabel on juhtmestikunormidest lähtuvalt standardiks korruse nn Access-ala juhtmestiku jaoks. Antud kaablitüübil on järgmised eelised:

- TP-kaablid, eriti nende kokkuühendamine, on väikese lairibavajaduse korral valguskaabliga võrreldes suhteliselt odav.
- TP-kaablite vedamine ja ühendamine on suhteliselt lihtne.
- TP-kaableid või pidada universaaljuhtmestikuks, kuna teisi teenuseid (nt telefone) saab kasutada ilma suurema tehnilise vaevata.
- Paigaldatud kaableid on mõõtetehniliselt lihtne kontrollida.
- TP-kaablid võimaldavad varustada vooluga seadmeid, mille toite spetsifikatsiooniks on „Power over Ethernet“ (PoE).

Vastukaaluks on neil järgnevad puudused:

- Andmeedastuse käigus kaableid pidi liikuvad vahelduvvoolud ja kaablite põimitud juhtmetes alati esineda võivad väikesed asümmeetriad tekitavad elektromagnetilisi väljasid, mida saab ümbritsevas keskkonnas tuvastada (pealtkuulamise oht) ja mis võivad süsteeme segada. Kuid ka ümbritseva keskkonna elektromagnetilised väljad võivad segada kaablite kaudu edastamist.
- Varjestuse kasutamisega juhtmestiku ülesehituses saab neid efekte vähendada (võrdle U/UTP kuni SF/FTP). Arvestada tuleb erinevate kaablite, liinide ja süsteemide miinimumkaugustega ja varjestuse ning maanduse andmetega.

- Eelmainitud efektid tekivad ka kaabli sees. Üksikute paaride läbikoste eest pakuvad kõige vähem kaitset varjestamata paigalduskaablid (U/UTP). Siin mõjub ainult üksikute juhtmete põimimine.

Valguskaabel

Signaalide edastamiseks läbi valguskaablite kasutatakse valgust selle nähtavas kuni tugevalt infrapunases vahemikus. Niisuguse valguse loomiseks kasutatakse dioode või lasereid. Need muudavad elektrisignaali erineva suuna / erineva tugevusega valgussignaalideks. Valguskaabel, mida nimetatakse ka fiiberoptiliseks kaabliks, koosneb edastamiseks kasutatavast südamikust ja ümbrisest. Materjalid erinevad nn murdumisnäitaja poolest. Juhtmestikustandardid liigitavad Multimode -valguskaablid kategooriatesse OM-1, OM-2 ja OM-3. Need spetsifikatsioonid kehtivad valguskaablitele, mille murdumisnäitaja gradientprofiili ja südamiku/ümbrise nimiläbimõõt on 50/125 või 62,5/125 mikromeetrit. Singlemode -valguskaablitele kehtib kategooria OS-1. Singlemode -valguskaabli südamiku/ümbrise nimiläbimõõt on 9/125 mikromeetrit. Kui Multimode -valguskaabli kiududesse suubuvad ühe signaali mitu valgusmoodi, suubub Singlemode -valguskaablitesse väiksema südamiku läbimõõdu tõttu ainult üks valgusmood. Seetõttu erinevad kaablitüübid võimalike ribalaiuste ja maksimaalsete paigalduspikkuste osas, mida on võimalik saavutada ilma lisavõimenditeta. Valguskaablite eri tüüpe ei saa süsteemide ühendamisel mõnel juhul omavahel kokku ühendada.

Valguskaableid kasutatakse muuhulgas järgnevates valdkondades:

- suurte kauguste ületamisel laivõrkudes (Wide Area Network - WAN) ,
- linnavõrkudes (Metropolitan Area Network - MAN) ,
- ettevõttesisestes võrkudes (Local Area Network - LAN) hoonete- ja korrustevahelise ühenduse loomiseks,
- kõrge elektromagnetilise koormusega kohtades ning
- salvestusvõrkudes (Storage Area Network - SAN) arvutuskeskuste süsteemide ühendamiseks suurte andmeedastuskiiruste saavutamiseks.

Ühenduste kvaliteedi jaoks on määrava tähtsusega ka valguskaabli infrastruktuuri pistikühenduste valik.

Valguskaablite kasutamisel on järgnevad eelised:

- Valguskaablid võimaldavad vaskkaablitega võrreldes saavutada suuri ribalaiuseid ja ületada suuri kaugusi.
- Valguskaableid ei mõjuta elektromagnetilised väljad.
- Erinevalt elektrilistest juhtidest ei teki mingeid läbikoste efekte.
- Valguskaablid pakuvad potentsiaalse energia vaba ühendust juhtmestiku otspunktide vahel.
- Pealtkuulamine on võimalik ainult keeruka tehnoloogia abil.
- Suure kiuarvuga kaableid saab samaväärsete vaskkaablitega võrreldes ehitada kompaktsemalt, samuti on valguskaabli kaal oluliselt väiksem.

- Valguskaablite tulekoormus on vaskkaablitega võrreldes väiksem. Selle põhjuseks on väiksem materjalikogus, kaablite valmistamisel kasutatud materjalid ja suur võimalike kiudude arv, ilma et kaabli suurus oluliselt kasvaks.

Valguskaablite kasutamisega kaasnevad siiski ka järgnevad puudused:

- Valguskaablite paigaldamishind on esmajoones just vajalike ühendustööde tõttu suurem kui vaskkaablite puhul.
- Valguskaablite tööks vajalikud ühendamiskomponendid, eriti just Singlemode-valguskaablite jaoks, on kallimad kui sama otstarbega vaskkaablite ühenduskomponendid.

TP-kaabli kaudu toimiv LAN-ühendus on levinud töökohaarvutite poolt enamasti paremini toetatud kui valguskaabli kaudu. Töökoha kliendid ühendatakse LANiga hetkel tavaliselt vaskkaablitega.

Järgnevast tabelist leiate kaablite pikkuste piirangud seoses teatud enam levinud protokollidega:

Võrgu juurdepääsuprotokoll		Kaablitüüp	Maks pikkus
Ethernet	10Base-T	TP	100 m
	10Base-FL Monomode	Multimode valgusk.	2 000 m
	10Base-FL Singlemode	Singelmode valgusk.	25 000 m
Fast Ethernet	100Base-TX	TP Cat 5	100 m
	100Base-FX	Multimode valgusk.	400 m
Gigabit Ethernet	1000Base-T	TP Cat 5e	100 m
	1000Base-SX	Multimode valgusk.	550 m
	1000Base-LX	Multimode valgusk.	550 m
	1000Base-LX	Singelmode valgusk.	10 000 m

Võrgu juurdepääsuprotokoll		Kaablitüüp	Maks pikkus
10 Gigabit Ethernet	10GBase-T	TP Cat 6a	100 m

10GBase-LX4	Multimode valgusk.	300 m
10GBase-LW4	Singelmode valgusk.	10 000 m
10GBase-SR	Multimode valgusk.	300 m
10GBase-LR	Singelmode valgusk.	10 000 m
10GBase-ER	Singelmode valgusk.	40 000 m
10GBase-LW	Singelmode valgusk.	10 000 m

Tabel: levinud juhtmestiku tüüpide pikkuste piirangud

Pöörake tähelepanu sellele, et siin on nimetatud vastavad maksimumpikkused.
Maksimumpikkus koosneb sageli tegelikust paigalduskaablist ja ühenduskaablitest (keerdpaarkaablitest). 1000Base-T jaoks ei tohiks näiteks paigalduskaabli pikkus ületada 90 m, et jätta piisavalt varu ka keerdpaarkaabli jaoks.

Kokkuvõte
WANis ja MANis on Singlemode -kiududega valguskaablid standardiks. LAN-juhtmestiku puhul on fiiberoptika kasutamine hoonete vahel ja kaugete korrusejaoturite vahel 10 gigabitise Ethernet i pikkuse piirangute pärast tungivalt soovitatav. Valguskaablite kasutamist kuni töökohani ja sellest tulenevat vaskjuhtmestiku kõrvalejätmist terve korruse lõikes saab vaadelda ainult üldistavas võtmes.

Valguskaablite kasutamise poolt räägivad:

- väiksem tulekoormus,
- suurem kindlus pealtkuulamise vastu,
- EMC-neutraalsus,
- võimalik kokkuhoid trasside ehitamisel,
- kasutatava pinna kokkuhoid tänu vajalike jaoturruumide väiksemale arvule ja sellest tulenev kokkuhoid jaoturruumide väiksema elektrijuhtmestiku pealt,
- lihtsam UPS ja maandus.

Valguskaablite kasutamise vastu räägivad:

- suuremad kulutused lõppseadmetele ja võrgukomponentide liidesekaartidele,
- enamasti jätkuvalt püsiv vajadus vaskkaabli kasutamiseks telefonijuhtmestikus,

- võimalikud piirangud Power-over-Ethernet IP-telefoneerimise rakendamiseks või ka juurdepääsupunktide ühendamisel WLAN-is.

Uuspaigalduste ja moderniseerimise puhul on soovituslik planeerimisspetsialistiga nõu pidada ning kõik tehnilised, ohutustehnilised ja majanduslikud faktorid välja arvutada ja läbi analüüsida (vt M 5.2 Võrgu sobiv topoloogia).

Kontrollküsimus:

- Kas kaablitüüpide valik põhineb hoolikal analüüsil, mille käigus arvestatakse niihästi hoone ehituslike omadustega kui ka tehniliste ja majanduslike nõuetega?

M 5.4 Kaabelduse dokumenteerimine ja märgistus

Algatamise eest vastutavad: IT juht, tehnikajuht

Rakendamise eest vastutavad: tehnikaosakond, administraator

Juhtmestiku hooldamise, veaotsingu, töökorra tagamise ja eduka kontrolli jaoks läheb tarvis põhjalikku dokumentatsiooni ja kõikide komponentide selget tähistamist.

Auditeerimistulemuste kvaliteet sõltub dokumentatsiooni täielikkusest, värskusest ja loetavusest. Igal juhul tuleb määrata juhtmestiku dokumentatsiooni eest vastutav isik. Kuna võrgu võimaliku suurenemise tõttu ei ole võimalik kogu infot ühe skeemi peale kanda, on mõistlik info jaotada. Tegelik asendiinfo tuleb alati mõõtkavas plaanidele kanda. Muu info võib olla ka tabelite või skeemide kujul. Seejuures on oluline, et kõik andmed oleks üksteise suhtes selgelt liigitatud.

Seega peab dokumentatsioon koosnema kirjeldavast osast, nimekirjadest ja skeemidest. Kirjeldavad dokumendid, näiteks dokumenteerimise nõuded peavad sisaldama infot dokumentatsiooni koostamise ja andmeid info jaotumise ja tähistuse kohta. Selles tuleks näiteks üldistatud kujul kirjeldada, millised nimekirjad ja plaanid tuleb koostada ja kuidas neid hoida, et kõik vastaks auditeerimisnõuetele.

Nimekirja- ja komponendiplaanidesse tuleb kaasata kõik võrku puudutavad asjaolud. Nimekirjad peavad sisaldama muuhulgas järgnevat infot:

- tarnete ja komponentide info,
- täpsed kaablitüübid (valguskaablite puhul ka kiudude kvaliteet),
- kasutust kirjeldavad kaablitähised,
- keskuste ja jaoturite asukohad koos täpsete nimetustega ja juurdepääsu puudutavate regulatsioonidega ning ruumide ja hoonete kontaktisikutega,
- kõikide jaotuskohtade ja jaotuste asendiplaanid,
- kõikide kaablite kasutusala ja külge ühendatud võrgus osalejate loetelu,
- ühenduspunktide tehnilised andmed,
- ohupunktid,
- olemasolevad ja kontrollimist vajavad kaitsemeetmed.

Komponendiplaanid koosnevad tavaliselt järgnevast:

- asukohtade ülevaated ja mõõtkavas asendiplaanid koos trasside ja primaarjuhtmestiku täpse asukohaga,
- skeemidena hoone eri osad ja mõõtkavas korruste skeemid koos jaoturiruumide, trasside ja kaablite ning ruumide IT-ühenduste (nt kaablikanalite ja/või põrandaavade) asukohaga,
- tehnikaruumide plaanid ruumi paigutusjoonisega, vahepõranda joonisega ja kappide asendiga, voolujaotur ja potentsiaaliühtlustamise liist ning kui olemas, ka kliimaseade,
- lülituskappide plaanid asendikirjeldusega näitamaks paigaldatud passiivseid ja aktiivseid komponente koos pistikupesa liistudega,

- võrgu füüsilised ja loogilised ühendusskeemid.

Vastava dokumentatsiooni alusel peab saama lihtsalt ja kiirelt täpse ülevaate olemasolevast juhtmestikku. Dokumentatsiooni aktuaalsena hoidmiseks tuleb tagada, et kõik võrguga seotud tööd oleks õigeaegselt ja täielikult dokumentatsiooni eest vastutavale töötajale teatavaks tehtud. Lahenduseks võib olla näiteks see, et materjali väljastus, väljastpoolt tellitavate teenuste ning turvatud ressursside kasutusse andmine peab toimuma koostöös dokumentatsiooni eest vastutava töötajaga. Kuna vastav dokumentatsioon sisaldab konfidentsiaalset infot, tuleb seda hoida turvaliselt ja selle juurdepääsu kontrollida. Lisaks tuleb kaablid ise tähistada, et komponendiplaanide infot ühildada kaablitega. Kaablid tuleb märgistada mõlemas otsas. Vajadusel võib kaableid märgistada ka korduvalt eri kohtadest, et kaabli asukohta oleks võimalik trassis selgemalt tuvastada. Kasutage märgistusvälju või teipe, millele saab käsitsi või masina abil kirjutada nii, et need püsiksid pikka aega loetavad. Kilemarkeri kasutamine on sageli ebapiisav. Kuna kaableid vahetatakse aeg-ajalt välja, tuleks märgistamist vastavalt korrata.

Turul saadaolev tarkvara pakub dokumentatsiooni jaoks põhjalikku abi. Funktsioonid sisaldavad võimalusi dokumenteeritud komponentidele eraldi nimede andmiseks, jaotuskohtade ja kaabliteede, samuti külge ühendatud tehnoloogia vastavuskontrolliks kuni rakendatavate protsesside toetamiseni välja, pakkudes vajaminevat dokumendihaldust. Dokumendihaldus sisaldab muuhulgas kasutajate haldamist, pääsuõiguseid, muudetud dokumentide kontrolli ja kasutusse lubamist.

Mõistlik on dokumentatsiooniga alustada juba tarkvarameetmete planeerimisel ja pärast planeeritud seisundi realiseerimist see kasutusse üle võtta. Sel moel on lihtsam kasutajaid dokumentatsioonis eesseisvate muudatuste osas informeerida ja tagada dokumentatsiooni värskus.

Kontrollküsimused:

- Kes on vastutav juhtmestiku dokumentatsiooni eest?
- Kas dokumentatsiooni uuendatakse piisavalt kiiresti?
- Kuidas kaitstakse auditeerimise dokumentatsiooni volitusteta juurdepääsude eest?

M 5.5 Minimaalselt ohtlikud kaablitrassid

Algatamise eest vastutavad: planeerija, IT-juht, tehnikajuht

Rakendamise eest vastutavad: tehnikaosakond

Kaablitrasside planeerimisel tuleb jälgida, et nähtavatest ohuallikatest saaks mööda mindud. Üldjuhtudel tuleks trassid paigaldada ainult sellistesse aladesse, mis on eranditult asutuse ruumide piires ligipääsetavad. Trasside ülevaatlik paigaldus kergendab nende kontrollimist. Trassid ja üksikud kaablid tuleks paigaldada alati selliselt, et inimesed, sõidukid ja masinad ei saaks neid otseselt kahjustada.

Käimis- või sõiduala

Seadmetele tuleks valida sellised asukohad, et nende külge ühendatud kaablid ei jääks käimis- või sõidualasse. Kui seda ei saa vältida, tuleb kaableid kaitsta eeldatavate koormuste eest sobivate kanalisüsteemidega.

Kaablite tõmbepinge vähendamine

Seadmete ühendusliinide puhul tuleb jälgida, et pistikutes olevad kaablid ei oleks liiga suure tõmbepinge all. Mõnikord võib olla kasulik loobuda pistikute ettenähtud kruvikinnitustest. Liiga suure tõmbepinge korral tõmmatakse siis lahti ainult pistikud, aga mitte pistiku ja kaabli või pistiku ja seadme vahelised jootekohad. Eriti problemaatilised on kaablitrasside ohutuse tagamisel majaalused garaažid. Turvalülituste ja sissesõidukohtade pika lahtiolekuaegade tõttu ei saa võõraste isikute juurdepääsu kunagi täielikult välistada. Kuna garaažide laed on tavaliselt madalad, on lihtne seal asuvatele kaablitrassidele ligi pääseda. Sõidualas asuvad trassid vähendavad sõidukite lubatud kõrgust. Liiga kõrgetest sõidukitest põhjustatud trasside ja kaablite kahjustusi ei saa täielikult välistada.

Kolmandate isikute poolt kasutatavaid alasid läbivad kaablid

Hoonetes, mida kasutatakse koos kolmandate isikutega, tuleb jälgida, et põrandas, laes või seintes jooksvad kaablid ei läbiks võõraste poolt kasutatavaid alasid. Kõik kanalisüsteemid tuleb võõrkasutuses olevate alade suhtes mehaaniliselt turvaliselt sulgeda. Parem oleks, kui need lõppeksid oma alade piires. Kaablite vedamist läbi suure tuleohtlikkusega alade tuleks võimalusel vältida. Kui see ei ole võimalik ja kui kõikide trassil asuvate kaablite funktsioone on tarvis säilitada, tuleb vastav trassiala varustada tuletõkkega. Kui funktsiooni säilitamine on tarvilik ainult üksikute kaablite puhul, tuleks selleks valida sobilik kaabel ja sinna juurde kuuluv kinnitus. Funktsiooni säilitamiseks mõeldud kaabel üksinda ei suuda kunagi nõutud funktsiooni täita. Kaablisüsteemi tuleb vaadelda tervikuna ning selle juurde kuuluvad ka kinnitused nagu trassid, võrud või torud. Sama oluline on, et kaablisüsteem ei häviks selle kohal asuvate funktsiooni mitteomavate detailide tõttu, kui need tulekahju korral alla kukuvad. Tootmisettevõtetes tuleb arvestada suurte induktiivsete koormustega ja sellest tekkivate segavate väljadega. Ka sellega tuleb trasside ja kaablite paigaldamisel arvestada. Kaablite kaitsmisel kehtib sama mis tuletõkke puhul. Maapealsete trasside puhul tuleb trassi kohale umbes 10 cm kõrgusele paigaldada hoiatuslint. Üksikute kaablite puhul (ilma kaablitoruta) on mõistlik paigaldada kaablikatted. Liinid peavad olema paigaldatud selliselt, et torm ei saaks neid liigutada. Näiteks peavad vabalt katusel asetsevad liinid olema vähemalt iga 5 m tagant sobivalt kinnitatud. Seejuures tuleks arvestada, et tormi korral mõjuvad kaablile või kaabliharudele tugevad jõud. Lisaks peavad liinid olema kaitstud mehaaniliste kahjustuste eest, kuna esemed võivad neile peale kukkuda. Katusel asetsevad liinid või lamellseintega kaetud alades asuvad liinid tuleks seega alati paigaldada kaitsetorude sisse.

Täiendavad kontrollküsimused:

- Kas kõik trassid ja kaablid on paigaldatud selliselt, et need on otseste kahjustuste eest kaitstud?
- Kas kontrollimatuid alasid läbivad kaablid on võõraste juurdepääsu eest kaitstud?
- Kas hoone välispindadele paigaldatud kaablid on piisavalt tormi mõjude eest kaitstud?

M 5.7 Võrguhaldus

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: IT-juht

Võrke võib hallata tsentraliseeritult või lokaalselt üksikutes võrgusõlmedes. Valik sõltub lisaks tehnilistele võimalustele ka sellest, kes tegeleb võrgusõlme administreerimisega. Kõikidel juhtudel, ükskõik millise ettevõtte või ametiasutusega tegu, on tarvis, et võrgus aset leidvaid tegevusi koordineeritaks tsentraalselt, et vältida ebavajalikke kattumisi. Tsentraalselt tuleks juhtida järgmisi aspekte:

- kaablite valik ja paigaldus,
- kasutatavate IT-süsteemide ja rakenduste valik, et tagada koostalitlusvõime,
- võrguaadresside ja kasutaja-ID-de tsentraliseeritud väljastamine,
- võrgukomponentide töökorraldus, nt jaotumine osakondade lõikes.

Võrgusõlmesid ja nende külge ühendatud IT-süsteeme võib hallata ka lokaalselt. Siinkohal tuleb hoolitseda kindlasti ka selle eest, et süsteemiülemad tunneksid täpselt oma tööülesandeid ja teaksid kompetentsi piire (vt M 2.26 Süsteemiülema ja ta asetäitja määramine).

M 5.8 Võrgu regulaarne turvakontroll

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: administraator

Võrguadministraator peab regulaarselt, kuid vähemalt kord kuus, kontrollima võrgu turvalisust. Peaaegu kõikide operatsioonisüsteemide jaoks on saadaval kontrollifunktsioonidega programmid ning osad neist võivad kuuluda isegi kas operatsioonisüsteemi tarnekomplekti või distrosse. Turvakontrolli raames tuleb kontrollida nt järgnevaid punkte:

- Kas leidub ilma paroolita kasutajaid?
- Kas leidub kasutajaid, kes pole võrku enam ammu kasutanud?
- Kas leidub kasutajaid, kelle parool ei vasta nõutud tingimustele?
- Millistel kasutajatel on samad õigused kui administraatoril?
- Kas süsteemiprogrammid ja süsteemi konfiguratsioon on muutmata ja terviklik?
- Kas süsteemiprogrammide ja süsteemikonfiguratsiooni, rakendusprogrammide ja –andmete ja kasutajate kataloogide ja andmete volitused vastavad turvapoliitika nõuetele?
- Millised on eri süsteemides töötavad võrguteenused? Kas need on konfigureeritud vastavalt turvapoliitika nõuetele?

Regulaarse turvakontrolli puhul võib lokaalse alamvõrguga integreerida ka penetratsioonitestid. Penetratsioonitesti „astet” võib seejuures muuta (nt kord nädalas lihtne automaatkontroll, kord kuus põhjalikum kontroll osalt manuaalse teostusega, kord aastas põhjalik, kogu võrku hõlmav test).

Turvakontrolli tehes peab võrguadministraator oma sammud dokumenteerima selliselt, et neist saaks ka hiljem aru (nt kui tekib kahtlus, et süsteem võib olla kahjustatud). Samuti tuleb dokumenteerida turvakontrolli sündmused. Peale selle tuleb välja selgitada kõrvalekalded „nõutud olukorrast”.

Kontrollküsimused:

- Kas teostatakse regulaarseid võrgu turvakontrolle (vähemalt üks kord kuus)?
- Kas turvakontrolli korral võetakse arvesse kõiki olulisi punkte?
- Kas turvakontrolli teostamine ja tulemused dokumenteeritakse?
- Kas selgitatakse välja kõrvalekalded nõutud olukorrast ja võetakse täiendavad meetmed?

M 5.9 Serveri logi

Algatamise eest vastutavad: IT-juht, infoturbespetsialist
Rakendamise eest vastutavad: administraator

Võrgus oleva serveri võimalikud logimisfunktsioonid tuleb mõistlikus ulatuses sisse lülitada. Võrgu administraator peab regulaarsete ajavahemike tagant kontrollima võrgus oleva serveri logifaile. Kõik turvalisuse seisukohast olulised sündmused tuleb logida. Eriti olulised on siinkohal järgnevad sündmused:

- kasutajatunnusega seonduva parooli korduv vale sisestamine kuni kasutajatunnuse blokeerimiseni vigaste sisestuste piirväärtuse saavutamise tõttu,
- volitamata juurdepääsukatsed,
- elektrikatkestus,
- andmed võrgu koormuse ja ülekoormuse kohta.

Täiendavate andmete logimine sõltub muu hulgas vastavate IT-süsteemide kaitsevajadustest. Mida kõrgem on kaitsevajadus, seda rohkem andmeid tuleks logida. Kuna logiandmed võivad ajapikku muutuda vägagi mahukaks, tuleks nende analüüsimise intervall hoida võimalikult lühike, et tagada võimalikult mõistlik tööde maht analüüsimisel. Mõistliku analüüsimise võimaldamiseks peaksid igas logisissekandes kajastuma kasutajatunnus või protsessi number, lõppseadme märgistus, kuupäev ja kellaaeg. Tuleb kontrollida, millised on logifailidele kehtivad seadusest või lepingust tulenevad kohustuslikud säilitusajad. Sündmuste tagamaade väljaselgitamiseks võib olla andmetele kehtestatud minimaalne säilitusaeg, andmekaitsenõuetest tulenevalt võib aga kohaldada ka andmete kustutamiskohustust (vt M 2.110 Andmeprivaatsuse suunised logimisprotseduurides).

Täiendavad kontrollküsimused:

- Kas võrgus oleva serveri logimisfunktsioonid on sisse lülitatud?
- Kas võrguadministraatorid analüüsivad logifaile regulaarselt?
- Kas analüüside tulemused dokumenteeritakse?
- Kas logifailide puhul järgitakse seadustest või lepingutest tulenevaid säilitamiskohustusi?

M 5.10 Piiratud õiguste andmine

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: administraator

Juurdepääsuõigused failidele, mida hoitakse võrgus asuva serveri kõvakettal, tuleb väljastada piirangutega. Igal kasutajal peab olema juurdepääsuõigus vaid nendele failidele, mida tal läheb reaalselt oma tööülesannete täitmiseks tarvis. Juurdepääsuõigus ise tuleb piirata minimaalsele juurdepääsuliigile (vt M 2.5 Vastutuse ja ülesannete jaotamine , M 2.7 Süsteemi ja võrgu pääsuõiguste andmine ja M 2.8 IT-rakendustele ja andmetele pääsuõiguste andmine). See tähendab nt seda, et programmifailidele tuleb kirjutusõigusega juurdepääsuvolitusi väljastada vaid väga harvadel juhtudel. Enamikel juhtudel on võimalik volituste pärimise teel juurde pääseda ka alamkataloogidele, juhul kui juurdepääsuõigus kehtis hierarhias kõrgemal asetsevale kataloogile. Sellest tuleneb põhimõte, et hierarhias kõige kõrgemal asetseva tasandi (Volume -tasandi) pääsuõigusi tohib väljastada vaid suurte piirangutega. Pärast uute tarkvaratoodete installeerimist tuleb väljastatud volitused alati kindlasti üle kontrollida.

Eriti hoolikas tuleb volituste piirangutega olla disketilugejaga varustatud arvutite puhul. Juhul kui võrgus asuva serveri salvestimaht on väike, saab võrgus olevas serveris kehtestada igale kasutajale maksimaalse salvestimahu.

Täiendav kontrollküsimus:

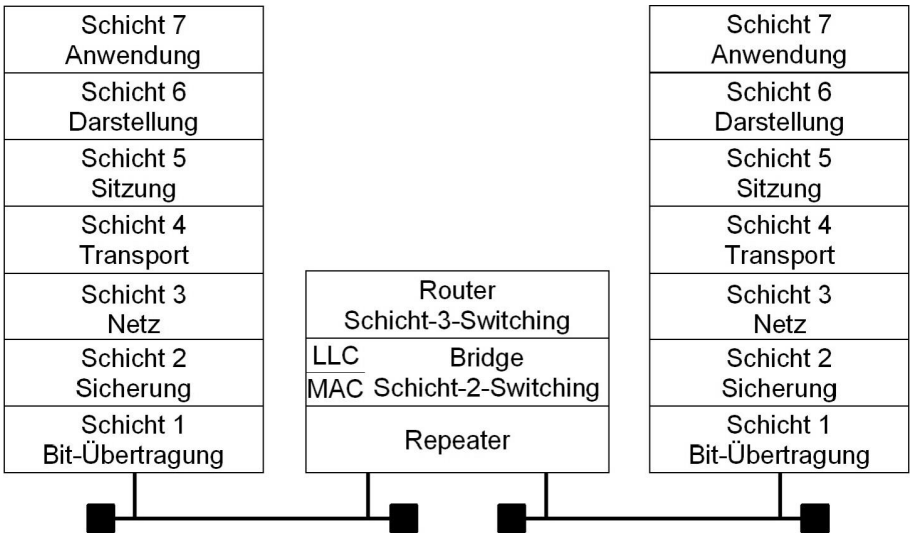
- Kas volituste väljastamise struktuuri kajastava dokumentatsiooni põhjal on võimalik tuvastada, kas väljastatud on vaid hädavajalikud õigused?

M 5.13 Võrgu ühendusaparatuuri õige kasutamine

Algatamise eest vastutavad: IT-juht, infoturbeosakond
Rakendamise eest vastutavad: IT-juht, administraator

Võrguühendusseadmeid nagu marsruutereid, sildu ja turvalüüse ei kasutata mitte ainult võrkude ühendamiseks, vaid ka võrkude füüsiliseks või loogiliseks segmenteerimiseks. Suurte võrkude alamvõrkudeks jaotamisega saab muuhulgas parandada nt käideldavust, kuna võimalikud vead esinevad sel juhul ainult võrgu teatud piiratud alas ning neid saab nõnda palju kiiremini tuvastada.

Võrgupunktide arvukuse kasvades võivad aga reaktsiooniajad muutuda vastuvõetamatult pikaks, mis muudab alamvõrkude loomise koormuse jaotamise eesmärgil möödapääsmatuks. Võrkude alamjaotuste loomise veel üheks põhjuseks võib olla ka vajadus konfidentsiaalsete andmete kaitsmise järele, kui tahetakse, et need ei oleks tervikvõrgus ligipääsetavad. Kaitseks väljastpoolt alguse saavate rünnete vastu võib olla mõttekas lubada andmepakettide edastust vaid suunal, mis kulgeb turvalisest võrgust ebaturvalisse võrku, kuid konfidentsiaalsete andmete kaitsmiseks seevastu võib olla mõttekas keelata andmepakettide edastuse turvalisest võrgust ebaturvalisse võrku. OSI mudeli järgi võib võrgu jaotamine segmentideks või ühenduspunktideks aset leida mitmes erinevas kihis. OSI mudeli füüsilises kihis (kihis nr 1) on võrguühenduse komponentideks nt järgurid, turvakihis (kihis nr 2) nt sillad, edastuskihis (kihis nr 3) nt marsruuterid ning rakenduskihis (kihis nr 7) reeglina turvalüüsid. OSI mudeli paremaks mõistmiseks oleme koostanud järgmise joonise.



Joonis: ISO / OSI etalonmudel

Schicht 7 Anwendung – kiht nr 7, rakenduskiht; Schicht 6 Darstellung – kiht nr

6, kuva; Schicht 5 Sitzung – kiht nr 5, sessioon; Schicht 4 Transport – kiht nr 4, transport; Schicht 3 Netz – kiht nr 3, võrk; Schicht 2 Sicheruung – kiht nr 2, varundamine; Schicht 1 Bit-Übertragung – kiht nr 1, bitiedastus; Router Schicht-3-Switching – marsruuter, kihi nr 3 kommuteerimine; Bridge Schicht- 2-Switching – sild, kihi nr 2 kommuteerimine; Repeater –järgur

Ühenduse loomine võrguga, mis asub OSI mudeli kõrgemas kihis (alates kihist nr 3), võimaldab näiteks korraldada andmevoogude liikumist, nii et see vastaks turvanõuetele, ning lubab omavahel kontrollitud viisil ühendada kaitstavaid ja ebaturvalisi võrke. Teisalt aga võib olla vajalik võrkude lahutamine, nt juhul, kui neid on tarvis kaitsta teistest võrkudest tulevate juurdepääsude eest või kui on tarvis tõsta võrkude käideldavust avariisituatsioonides, st kui on tarvis vähendada võrgu koormust võrgu eri segmentides. Manipulatsioonide tõkestamiseks tuleb kõik võrguühendusseadmed üles seada nõnda, et neile saaksid füüsiliselt ligi pääseda ainult selleks volitatud isikud.

Repeater
Järgurid (repeaters) töötavad OSI mudeli kihis nr 1 ja nende näol on tegemist tavaliste signaalivõimenditega. Nende rakendamine võimaldab pikendada olemasoleva võrgusegmendi maksimaalselt kaablipikkust, st aitab ühendada suuremat arvu võrgusegmente. Näiteks Etherneti puhul, mille jaoks on kasutusele võetud koaksiaalkaabel, saab nende abil pikendada maksimaalset kaablipikkust üle 185 m või üle 500 m (Thin - ja Thick-Ethernetcable). Arvestada tuleb siiski järguritele kehtivate konfiguratsioonireeglitega, mis seavad piirangud nende arvule ja paigutusele. Keerupaarijuhtmestiku korral (twisted pair cable) rakendatakse järgureid tihti tsentraalsete või detsentraalsete võrgusõlmedena, eesmärgiga ühendada omavahel üksikuid võrgus osalejaid. Kuna selleks otstarbeks tuleb ühes seadmes omavahel ühendada mitu järgurit, nimetatakse neid seadmeid ka mitmikportjärguriteks (Multiport-Repeater). Multiport-Repeater' eid nimetatakse sageli kas jaoturiteks (hub) või minijaoturiteks (mini-hub). Kuna nende kasutamine võimaldab lahutamist kihis nr 1, piiratakse elektrilised vead ühele segmendile. Sama ei kehti siiski kõrgemates kihtides esinevate vigade suhtes (nt liig sagedased kokkupõrked või Broadcast -tormid). Mõningad tootjad pakuvad juba ka selliseid Multiport-Repeater' eid, mis suudavad kihi nr 2 infot analüüsida (aga mis ei täida siiski veel silla funktsiooni) ning lubavad seetõttu rakendada näiteks juurdepääsupiiranguid. Selliste seadmetega on võimalik näiteks tagada, et võrgule pääsevad ligi ainult teatud kindlad võrgus osalejad.

Bridge
ISO-OSI-referentsmudeli kihis nr 2 asuvate võrkude ühendamiseks rakendatakse sildasid (bridge). Sild ühendab omavahel kahte võrku, mis kasutavad reeglina ühesugust Logical Link Control (LLC) protokolli, kuid erinevaid Medium Access Control (MAC) protokolle. Bridge suudab omavahel ühendada nt Etherneti ja Token-Ring -võrku. Niisugust silda nimetatakse sellisel juhul kas Translation-Bridge või T-Bridge.

Sellega kaasnevad kolm märkimisväärset eelist:

- Sild lahutab Collision -domeenid, st CSMA/CD baasil võrkudes tekkivad jõudlust alandavad kollisioonid ei jõua edasi teistesse segmentidesse.
- Sild suunab teise segmenti edasi ainult sellised andmepaketid, millel on olemas vastav, teise segmendi sihtkoha aadress. Niimoodi ei välju andmevahetus olukorrale vastavast minimaalsest segmendist, millel tagajärjel tõuseb pealtkuulamiskindlus.
- Igas segmendis kasvab andmete läbilaskevõime, kuna andmeid on võimalik edastada silla mõlemas otsas üksteisest sõltumatult, mis toob kaasa koormuse jaotumise.

Switch (Ethernet, Token-Ring, ATM)

Kommutaator (switch)kujutab endast silla varianti, mis ühendab omavahel mitut loogilist LAN-segmenti (Multiport-Bridge) ja töötab seega OSI-mudeli kihis nr 2. Mõningatel uutel toodetel on täiendusena olemas ka OSI mudeli kolmanda kihi switching -funktsioonid, mis lubavad segmenteerida ka kihti nr 3. Ethernet-Switch koosneb mitmest sillast, mis on sisemiselt omavahel sobival moel kokku ühendatud (nt niinimetatud Switching-Matrixi abil). Ethernet-Switch' il on kasutada bridge 'i eelised, hõlmates mitmeid ühendusi (hetkel on tavapärane 8–32 ühendust ühe switch 'i kohta), st iga võrgus osaleja või segment, mis on ühendatud switch 'i külge, moodustab omaette Collision -domeeni ning ühenduse loomine põhineb reaalsetel vajadustel. Seetõttu on võimalik, et iga külgeühendatud segment saab olla sideühenduses kõikide teistega, sõltumata sellest, milline on teiste segmentide liiklus ja koormus, eeldusel et vastav segment ei ole juba kuidagi teistmoodi hõivatud. Kommutaatorite peamine sihtotstarve on koormuse jaotamine ja tsentraalne ühenduselement mitmete osasegmentide tarbeks. Kommutaatorite kaskaadilaadse struktuuri tõttu, st tänu võimalusele, mis lubab tsentraalselt toimiva switch 'i külge ühendada järgmisi switch 'e, on võimalik, eeldusel et koostatakse optimaalne loogiline võrgustruktuur, luua vägagi kõrge jõudlusega võrke.

Ethernet-Switch 'id, msi töötavad IEEE-normi kohaselt sildade tarbeks, kasutavad Store-and-Forward -tehnoloogiat. Selle tehnoloogia puhul loetakse esmalt allikapordi kogu Etherneti pakett sisse ning kontrollitakse selle korrektsust. Sihtkoha segmenti edastatakse vaid sellised paketid, mis on korrektsed ja täies mahus vastu võetud. Niisuguste switch 'ide viivitusajad on suhteliselt pikad, kuid seevastu suudavad need ka garanteerida, et vigaseid pakette ei edastada teistesse segmentidesse. Vastavaid Store-and-Forward - Switch 'e on soovitatav kasutada siis, kui esmatähtsad on maksimaalne käideldavus ja terviklus, mitte aga ribalaius. Sellele vastukaaluks on arendatud ka alternatiivseid tehnoloogiaid, mis suurendavad Ethernet-Switch 'i läbilaskevõimet, st lühendavad andmepaketi töötlemisest tulenevat viivitust. Selleks kasutatakse nt On-the-Fly -tehnoloogiat (tuntud veel ka Cut-Through nime all), mis ei loe kontrolli eesmärgil sisse enam tervet paketti, vaid analüüsib ainult paketi sihtaadressi ja saadab seejärel kogu paketi kohe vastavale aadressile. Sellega on On-the-Fly - Switch 'id maksimaalselt faktor 20 võrra kiiremad kui Store-and-Forward-Switch 'id. Puudusena tuleb aga välja tuua asjaolu, et kiirusele vaatamata saadavad nad teise segmenti edasi ka vigased paketid, mille tulemusel võib kannatada saada teatud pakettide ribalaius ja seetõttu ka nende segmentide käideldavus. On-the-fly-Switch 'e tuleks kasutada võrku-

des, kus vigaste pakettide esinemise tõenäosus on väiksem ning kus peamiseks eesmärgiks on andmete maksimaalne läbilaskevõime. Enamik tootjaid pakub tänapäeval selliseid kommutaatoreid, mis suudavad opereerida mõlema tehnoloogiaga ning mida saab ka vastavalt konfigureerida. Leidub ka tooteid, millel on olemas juba ka OSI mudeli kihi nr 3 kommuteerimisfunktsioon. Selliste lahenduste puhul ei eraldata võrgus osalejaid mitte enam nende MAC-aadressi põhjal (Layer-2-Switching), vaid kihis nr 3 esinevate aadresside põhjal (TCP/IP-protokollistikus on selleks IPaadress). Layer-3-Switching võib endaga kaasa tuua jõudluse kasvu, kuid sellisel juhul peab kommutaator, sarnaselt marsruuteriga, suutma töötada kihis nr 3 rakendatavate protokollidega.

ATM-ide või Token-Ring 'ide kommutaatorid on oma funktsiooni poolest väga sarnased Ethernet-Switch' iga, st ka nende protokollide kommutaator võimaldab seda, et kaks võrgus osalejat või kaks võrguvaldkonda saavad omavahel suhelda teistest sõltumatult. ATM-võrkude puhul on nende aluseks oleva kontseptsiooni tõttu switch 'i kasutamine koguni möödapääsmatu. Valides kommutaatoreid, millega soovitakse luua Collapsed Backbone 'i, tuleb arvestada saadaoleva porditihedusega. Collapsed Backbone tüüpi magistraali loomisel tuleks vältida mitme kommutaatori kasutamist, millel puudub ühine (kõrge kiirusega) põhiplaat (vt M 5.2 Võrgu sobiv topoloogia).

Router

Marsruuterid (router) ühendavad või liidavad võrke OSI mudeli kihis nr 3. Sel põhjusel ei tööta marsruuterid enam protokollide vaatevinklist sugugi läbipaistvalt (nagu seda teevad nt järgurid või sillad), vaid peavad suutma rakendatavaid protokolle edastuskihi sees ka töödelda. Marsruuterite käitamise tagajärjel langeb märgatavalt kahe alamvõrgu vaheline andmeliikluse kiirus, kuna marsruuter peab analüüsima kõiki kihis nr 3 liikuvaid andmepakette. Tänu sellele, et marsruuterid suudavad töödelda ja käitada protokolle, kasutatakse neid peamiselt LAN-LANühendusteks ning LAN-i ühendamiseks WAN-i külge. Marsruuter suudab nt kahte LAN-i omavahel ühendada läbi ISDN-ühenduse. Selleks kapseldatakse LANprotokoll muutmata kujul WAN-protokolli sisse (encapsulation) ja edastatakse.

Samas valdkonnas võib kasutada veel ka X.25-protokolli. Suurtes võrkudes, mille alamvõrgud on omavahel ühendatud marsruuteritega, on marsruuteri peamiseks ülesandeks alamvõrkude vahelise teekonna valimine (Routing).

Antud valdkonnas on reeglina võimalik eristada kahte protseduuri:

- Staatilist marsruutimist, mille puhul antakse teekonna valik ette käsitsi.
- Dünaamilist marsruutimist, mille puhul määrab teekonna valiku marsruuter ning värskendab seda jooksvalt. Selleks on saadaval mitmed algoritmid ehk protokollid, mis võimaldavad ka marsruuterite omavahelist ühtlustamist. Tuntumad protokollid on RIP (Routing Information Protocol), OSPF (Open Shortest Path First) ja IGRP (Interior Gateway Routing Protocol). Sobiva mars-

ruutimisprotokolli valimisel tuleb arvestada ka meetmega M 4.82 Võrgu aktiivkomponentide turvaline konfigureerimine . Täiendava meetmena kasutusele võetavad filtrid võimaldavad sisse seada juurdepääsu kontrolli, st kehtestada normid, millised süsteemid tohivad milliste protokollide toel läbi marsruuteri millises suunas omavahel andmesides olla ja millised mitte.

Kontsentraatorid ja jaoturid

Jaoturi (hub) all peetakse silmas komponenti, mille külge ühendatakse üks või mitu aktiivset võrguühenduskomponenti ning mis võimaldab neil komponentidel omavahel suhelda sisemise põhiplaadi (backplane) vahendusel (vt M 5.2 Võrgu sobiv topoloogia). Jaotureid, mis suudavad vajadusel enda külge liita mitu võrguühenduskomponenti, nimetatakse modulaarseteks jaoturiteks. Sama loogika põhjal nimetatakse jaotureid, mis koosnevad ainult ühest võrguühenduskomponendist ning mis ei võimalda rohkemaid komponente endaga liita, mittemodulaarseteks jaoturiteks. Juhtudel, kus on võimalik mitme jaoturi põhiplaadid omavahel ühendada, kannavad vastavad jaoturid nimetust stackable Hubs. Jaoturi või kontsentraatori kasutuselevõtmisel kulgeb juhtmete paigutus lõppseadmeteni vähemalt osaliselt tähekujulise skeemi alusel ning seetõttu nimetatakse neid jaotureid ja kontsentraatoreid ka tähtühendajateks (star coupler). Nagu juba järgurite puhul sai märgitud, on kontsentraatori või jaoturi kõige väiksemaks vormiks Multiport-Repeater. Modulaarsed jaoturid seevastu võimaldavad enda külge liita erinevaid ühenduselemente, mis suudavad omakorda töötada erinevates kihtides (nt järgureid, sildu ja marsruutereid). Selline võimalus võrgukomponendid ühte kohta kokku koondada loob eelise, mille korral on võrku kergem hallata, kuid samas tuleb ka arvestada, et ühe sellise tsentraalse jaoturi rivist väljalangemine puudutab tervet võrku. Sellisteks juhtudeks tuleb kasutusele võtta sobivad vastumeetmed, nt saab võrgukomponendid sisse seada liiasusega (vt M 6.53z Võrgukomponentide liiasus).

Gateway

Lüüs (gateway) ühendab kahte võrku OSI mudeli rakenduskihis (kihis nr 7). Seetõttu ei täida lüüs mitte ainult võrguprotokolli konverteerimise ülesannet, vaid suudab vajadusel tegeleda ka andmete transportimisega rakenduste tasandil, andmete võimaliku modifitseerimisega ning turvakaalutlustest lähtuva analüüsiga. Lüüside tüüpiliseks rakendusvaldkonnaks on TCP/IP-võrgu süsteemide andmeside SNA-hostiga. Sellistel juhtudel koosneb lüüs riistvara ja tarkvara kombinatsioonist. Samas leidub ka lüüse, mis on lahendatud ainult tarkvara baasil. Nendeks on nt Mail-Gateway' d, mis suudavad mõista ja konverteerida erinevaid meiliformaate.

M 5.14 Sisemiste kaugpöörduste turve

Algatamise eest vastutavad: keskjaama spetsialist, infoturbeosakond

Rakendamise eest vastutavad: administraator

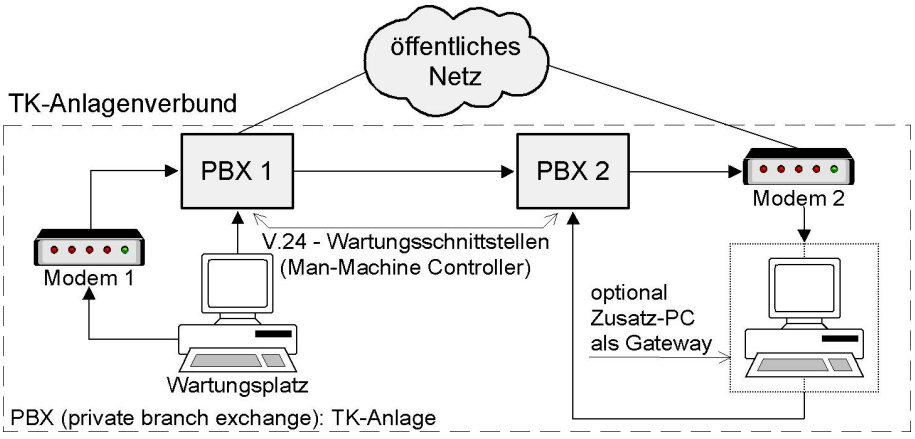
Kaugpöördust kasutatakse keskjaama korral kaughoolduse, kaughalduse ja võrguhalduse teostamiseks. Lisaks võib luua kaugpöördusligipääsu ka keskjaama kasutajatele (Dial-In funktsioon). Põhimõtteliselt võib eristada:

- kaugpöördust enda keskjaamasüsteemis (sisene juurdepääs) ja
- kaugpöördust teistest võrkudest (väline juurdepääs).

Sisemise kaugpöörduse korral vaadeldakse kaughoolduse turvet keskjaamasüsteemi siseselt. Süsteemi all vaadeldakse siinkohal mitmest eraldiseisvast süsteemist koosnevat terviksüsteemi, mis on eraldi võrguga omavahel ühenduses. Kui ühendus toimub avalike vahenduskeskuste kaudu, tuleb lisaks rakendada alajaotises M 5.15 Väliste kaugpöörduste turve kirjeldatud meetmeid. Avalike võrkude või virtuaalsete privaatvõrkude (VPN) kaudu suletud kasutajagruppide võrgustamisel tuleks rakendada sisemise kaugpöörduse meetmeid ja võimalusel * tähistatud punkte, mis käsitlevad välist kaugpöördust. Tähtsaim punkt sisemise kaugpöörduse turvamisel on välisvõrkudest tulevate sisenemiskatsete ärahoidmine ja võimalusel ka tuvastamine. Lisaks tuleks ligipääs enda võrgus piirata volitatud üksustele ja isikutele. Sõltuvalt ligipääsu viisist on olemas erinevaid meetodeid.

Sisemise kaugpöörduse turve modemi kaudu

Järgneval joonisel on kujutatud tavaline stsenaarium, mille korral toimub sisemine kaugpöördus kaughalduspordile modemi kaudu. Keskjaama PBX 1 hallatakse hoolduskeskusest otse V.24 hooldusliidese kaudu. Keskjaama PBX 2 hallatakse hoolduskeskusest otse modem 1 - PBX 1 - PBX 2 - modem 2 - V.24 haldusliidese kaudu.



Joonis: Kaughalduse loomine modemi kaudu (TK-Analgeverbund – keskjaamasüsteem; öffentliches Netz – avalik võrk; Wartungsplatz – hoolduskeskus; modem 1; PBX 1; V.24 Wartungsschnittstellen – V.24 hooldusliidesed; PBX 2; modem 2; optional Zusatz-PC als Gateway – valikuliselt lisa PC lüüsina; TK-Anlage – kodukeskjaam)

Sellisel juhul võib välisvõrgust loodavate ühenduste kaitseks kasutada järgmisi meetmeid:

- Modemil ei tohi olla väliste kõnede õigusi - Modemiühendusel, mille kaudu toimub ligipääs halduspordile, ei tohiks olla väljahelistamise õigusi! See nõue tuleks esimesena üle kontrollida. Sellega välditakse, et modemile on võimalik väljaspoolt otse helistada.
- Hoolduspordi (modemi) number peab olema salajane - Kuritahtliku ärakasutamise raskendamiseks ei tohiks hooldusaparaadi numbrit avaldada telefonikataloogis. Number peaks olema teada ainult inimestele, kes seda ilmtingimata vajavad.
- Püsiühenduste kasutamine (valikuline) - Kaugühenduste korral on enda püsiühenduse kasutamine, mis ei jookse üle vahenduskeskuse, üks kindlamaid meetodeid välise juurdepääsu takistamiseks kaugpöördusele. Kuna see meetod on küllaltki kallis, leiab see eeldatavasti kasutust ainult erandjuhtudel.

Kindlustamaks, et ainult volitatud üksused pääseksid sisevõrgus kaugpöördusele ligi, tuleb rakendada järgmisi meetmeid:

- Suletud kasutajagruppide moodustamine (Closed User Group - CUG) - Keskjaamas on võimalik luua ka ülesüsteemilisi CUG-sid. Need suletud kasutajagrupid moodustavad nagu võrgu võrgus. Kõik vajalikud kaugpöördused tuleks koos vastavate volitatud üksustega koondada sellistesse CUG-desse.
- Automaatne tagasihelistus (Callback) - Tuleks kasutada modemi tagasihelistusfunktsiooni (vt M 5.30 Olemasoleva tagasihelistusfunktsiooni aktiveerimine). Kasutades PC Gatewayd, tuleks tagasihelistus käivitada sealt.
- Kaugpordi õiguste piiramine (valikuline) - Kui kodukeskjaam toetab erinevate portide õigushaldust, saab seda kasutada, et keelata turbekriitilised tegevused kaugpöörduse kaudu ja lubada nende teostamine ainult koha peal. Paljud keskjaamad ei toeta kahjuks seda funktsiooni. Sellisel juhul saab lisatoodetega, näiteks protokollijaga, piirata pordi kaudu toimuvaid tehinguid.

Kindlustamaks, et ainult volitatud isikud pääseksid sisevõrgus kaugpöördusele ligi, tuleb rakendada järgmisi meetmeid:

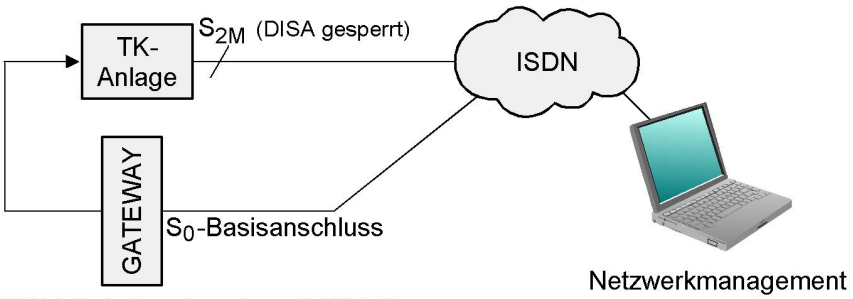
- identifitseerimine ja autentimine,
- kasutage autentimiseks challenge-response meetodit (valikuline).

Sisemise kaugpöörduse turve ISDN-võrgu kaudu

Praktilisusest lähtudes on mõttekas varustada võrguhaldusülesannetega arvutid ISDN-kaartidega. Moodustada tuleb suletud kasutajagrupp. Selleks võib kasutada helistava osaleja numbrit (Callin Line Identification and Presentation - CLIP). Lõppseade saaks seda ise realiseerida, kasutades selleks võrgu poolt võimaldatava helistava seadme numbrit (CLIP).

Otseste süsteemiligipääsude turve (Direct Inward System Access - DISA)

Otsesed süsteemiligipääsud tuleks võimalusel sulgeda. Kui see ei ole võimalik, tuleks õigused seadistada nii, et otsene süsteemiligipääs saaks toimuda ainult ühe püsiühenduse kaudu. Sellisel juhul on võimalik DISA-ühendus viia üle Gatewayle . Näite selle kohta leiate järgnevalt jooniselt:



Joonis: Otsese süsteemiligipääsu turve (Netzwerkmanagement – võrguhaldus; ISDN; S0-Basisanschluss – S0 baasühendus; Gateway; TK-Anlage – kodukeskjaam; S2M (DISA gesperrt) – S2M (DISA suletud))

Võrguhalduskeskuse loomine ja piiramine

Keskse võrguhalduskeskuse eeliseks on mugav süsteemihaldus, igapäevaste haldustööde tegemiseks ei ole enam vajalik füüsiline ligipääs keskjaamale. Keskse võrguhalduskeskuse loomisel tuleb see paigutada turvatud alasse. Ligipääs keskusele tuleb reguleerida organisatoorsete meetmetega. Vastavad nõuded leiate moodulist B 2.4 Serveriruum . Haldusarvutid, millel töid teostatakse, tuleks samuti kindlustada sobivate meetmetega. Näiteid leiate moodulitest B 3.204 Klient Unixi all .

Hoolduse logi

Hetkel kasutatav süsteemikonfiguratsioon ehk laialijagatud numbrid ja õigused, aktiveeritud ja deaktiveeritud jõudlusnäitajad, seadistatud grupp jne peavad olema mõistetavad. Selleks on vajalik tehtud muudatuste protokollimine. Sobiv meetod selleks on sundlogimine PC Gateway abiga.

Täiendavad kontrollküsimused:

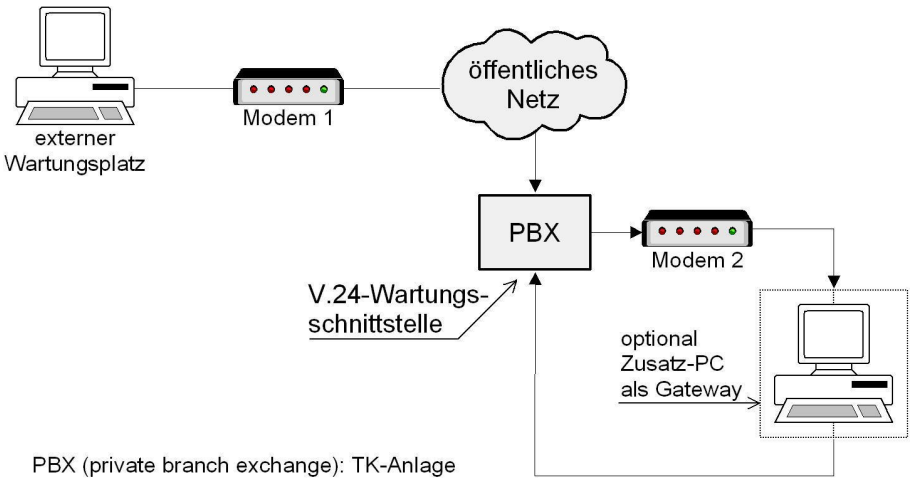
- Kas väline kaughaldus on keelustatud?
- Kas kaugpöördusel puudub teenuseklass?
- Kes ja kus saab kaugpöördust valida?
- Kellel on ligipääs kaughoolduskeskusele?
- Kas kaughoolduskeskus asub turvatud alas?
- Kas kõik kaughooldused ja sisestused protokollitakse?

M 5.15 Väliste kaugpöörduste turve

Algatamise eest vastutavad: keskjaama spetsialist, infoturbeosakond

Rakendamise eest vastutavad: administraator

Välise kaugpöördusena vaadeldakse siinkohal igat juurdepääsu keskjaama hoolduspääsu kaudu. See võib olla vajalik seetõttu, et kõik süsteemi osad ei ole omavahel seotud või mitte ainult seotud (vt märkus) püsiühenduse kaudu, või probleemi korral ei ole võimalik tootja kiire abita toime tulla. Sellisel juhul peavad halduspordil (modemil) olema lubatud kõik teenused. Järgneval joonisel on kujutatud tavaline stsenaarium, mille korral toimub kaugpöördus kaughalduspordile modemi kaudu. Keskjaama hallatakse välisest hoolduskeskusest modem 1 - avalik võrk - PBX - modem 2 - V.24 hooldusliidese kaudu.



Joonis: Välise kaughalduse loomine modemi kaudu (externer Wartungspatz – väline hoolduskeskus; modem 1; öffentliches Netz – avalik võrk; PBX; V.24 Wartungsschnittstelle – V.24 hooldusliides; modem 2; optional Zusatz-PC als Gateway – valikuliselt lisa PC lüüsina; TK-Anlage – kodukeskjaam)

Turvalisusest lähtuvalt on mõttekas välisest kaughooldusest loobuda. Kui see ei ole võimalik, tuleb lisaks sisemise kaugpöörduse meetmetele kasutusele võtta ka täiendavad turvameetmed. Mõned süsteemid võimaldavad juhtida ainult põhilise andmemahu üle püsiühenduse ning andmeside tipp (*peak*) marsruuditakse automaatselt üle avaliku võrgu. Sellest tegevusest ei teatata kasutajale.

PC Gateway

Halduspordi ja modemi vahele tuleks asetada PC *Gateway*. See peab täitma järgmisi turbefunktsioone:

- kasutaja identifitseerimine ja autentimine,
- ühenduse katkestamine turbekriitilistes olukordades,
- automaatne tagasihelistus (*Callback*) ja
- kõikide tegevuste protokollimine.

Peale selle võib paigaldada ka lisafunktsioone:

- ajapiiri määramine vigaste ligipääsukatsete korral,
- kaughoolduse sulgemine normaalkäituses ja selle lubamine kindlalt määratud ajavahemikuks; probleemi korral on mõttekas võimaldada juurdepääs kas tootjale või mõnele teisele hooldusettevõttele,
- hooldusperso nali õiguste piiramine; astmelise õigushalduse teostamiseks saab hooldusarvutile installida lisatarkvara, mis võimaldab piirata kasutaja võimalusi,
- sundväljalogimine ühenduse katkemise korral; kui ühendus kaughoolduskeskuse ja PC *Gateway* vahel mingil põhjusel katkeb, tuleb ligipääs süsteemile lõpetada sundväljalogimisega.

Kaughooldusligipääsu füüsiline väljalülitamine

Kui tavaolukorras ei vajata kaughooldust ja seda võimalust soovitakse kasutada ainult otsese vajaduse korral, tuleks ligipääs füüsiliselt välja lülitada. Vajadusel saab selle pärast tootja või hooldusfirmaga läbirääkimist lühiajaliselt aktiveerida.

Suletud kasutajarühmad (*Closed User Group* - CUG)

Avalikes ISDN ja X.25 võrkudes võimaldatakse CUG-de loomist. Sellisel viisil võimaldab võrgupakkuja kasutajatel luua virtuaalse „võrgu võrgus". CUG-d saab tellida teatud tasu eest võrgupakkujalt. Alternatiivina võib suletud kasutajagrupid ISDN-teenuste CLIP (*Calling Line Identification and Presentation*) ja COLP (*Connect Line Idendification and Presentation*) abil ise realiseerida. Seda saab teostada kas enda keskjaama vastava konfiguratsiooniga või PC *Gateway* vastava seadistusega. Seda meedet tuleks kasutada ka sisese kaughoolduse korral privaatse sisevõrgu kaudu (VPN).

Otseste sissehelistamisvõimaluste (*Dial In*) vältimine ja kontrollimine

Otsene sissevalimisvõimalus, näiteks teistest võrkudest DTMF (*dual-tone multifrequency*) järelvalimise kaudu, keskjaama tuleks võimalusel keelata. Selliseid meetodeid kasutatakse tihti ligipääsuks serveriteenustele. Kui keelustamine on ettevõttesisestel põhjustel vältimatu, on soovitatav aktiveerida kõik turvamehhanismid ja teostada regulaarselt kontroll võimaliku ärakasutamise suhtes.

Täiendavad kontrollküsimused:

- Kas kaughooldus on tavaolukorras füüsiliselt välja lülitatud?
- Kust kohast on kaughoolduse läbiviimine võimalik?
- Kas Callback on realiseeritud?
- Kas PC Gateway on realiseeritud?
- Kas kaughoolduse sisestused on mõistetavad?
- Kas kaughoolduse kaudu on võimalik juurdepääs logifailidele?
- Kas logiprinterit on kaughoolduse kaudu võimalik välja lülitada?
- Kas edutud sisselogimiskatsed protokollitakse?
- Kas pärast selliseid katseid katkestatakse ühendus?
- Kas ühenduse katkemisele järgneb sundväljalogimine?

M 5.16 Võrguteenuste inventuur

Algatamise eest vastutavad: infoturbeosakond, administraator

Rakendamise eest vastutavad: administraator

Enne seda, kui Unixi keskkonnas alustatakse erinevate võrguteenuste ja võrguprotsesside kontrollimist, tuleks koostada ülevaade, milliseid teenuseid on tarvis pakkuda ja millised teenused on ehk juba installeeritud. Viimase puhul on abiks käsk ps ja täiendavad valikud, millega saab koostada loetelu kõikidest võrguprotsessidest. Seejärel tuleks asuda välja selgitama, millist ülesannet iga loetletud protsess täidab, ning koostada ülevaade sellest, millistes kohtades ja milliste funktsioonidega see protsess käivitatakse. Sagedasti toimub see failides /etc/rc, /etc/rc.net, /etc/rc.local , mida loetakse süsteemi buutimise käigus.

Eriti olulisel kohal on inetd -deemon, kuna see suudab käivitada kõiki programme, mis sisalduvad failis /etc/inetd.conf . Kontrollida tuleb ka konfiguratsioonifaile /etc/services, /etc/protocols, /etc/hosts, /etc/gated.conf ja teisi faile.

M 5.17 NFSi turvamehhanismid

Algatamise eest vastutavad: infoturbeosakond, administraator
Rakendamise eest vastutavad: administraator

NFS (Network File System) võimaldab serveril asuvate failide ühiskasutamist kõigi arvutite (klientide) poolt, mis paiknevad samas võrgus ja on saanud serverilt selleks vastavad õigused. Igat serverit on võimalik käitada kliendina ja vastupidi, mistõttu tuleb kindlustada, et iga arvuti töötaks ainult selle jaoks ette nähtud funktsioonidega.

Näiteks ei ole mõtet Mount- deemonit mountd või NFS-deemonit nfsd käivitada NFS-kliendil:

- NFS-serveril peab üks fail (näiteks /etc/exports või /etc/dfs/dfstab) sisaldama igat failisüsteemi või kataloogi, millele peab teistel arvutitel olema juurdepääs ning neile kehtivad alltoodud nõuded.
- Eksportida tuleks ainult ilmtingimata vajalikud failid.
- Võtmesõnadega root ja access on võimalik täpsustada arvutid, millele on lubatud failisüsteemide eksport. Kui kindlate arvutite andmed puuduvad, on failisüsteem avatud kõikidele arvutitele - seda ei tohi aga mingil juhul juhtuda!
- Failisüsteemidel, mida peab olema võimalik ainult lugeda (siia kuuluvad kõik täitmisfailid), tuleks kasutada suvandit ro (read only).
- Tavaliselt muudetakse süsteemiadministraatori kasutajanumber (UID 0) NFS päringute korral kasutaja nobody numbriks (UID 2 või 65534), et UID 0-iga NFS-is failidele ligi ei pääsetaks. See ei kehti failidele, mis kuuluvad teistele privilegeeritud kasutajatele, nagu näiteks bin või daemon , ning seda tuleb arvestada ka haldustööde jaotamisel (vt M 2.32z Piiratud kasutajakeskkonna loomine), see tähendab, et failisüsteeme, mis sisaldavad neid faile, ei tohi eksportida. Kuna iga võrgus olev arvuti võib võtta mis tahes IP ja näiteks iga PC kasutajal on DOS-i all root- õigused, ei tohiks root i muutumist nobody ks deaktiveerida, ning tuleks kindlustada, et failis /etc/passwd oleks sissekanne nobody:*:-2:-2:anonymous user:: ja see ka toimiks. Sellega seoses tuleb arvestada, et iga kasutaja, kellel on võrguarvutil root- õigused (näiteks PC kasutajana) saab NFS-i kaudu endale võtta iga grupitunnuse, mida ta tahab, mis tähendab, et ühelgi eksporditud kataloogil ega failil ei tohi olla grupikirjutusõigusi ja lugemis- ning teostusõigus võib olla määratud ainult juhul, kui see on vältimatu. Peale selle tuleb meeles pidada, et kaitset ei vaja mitte ainult üksikud failid, vaid ka kataloogipuus nende peal asuvad kataloogid!
- Anonüümsete päringute keelamiseks tuleks kasutada suvandit anon=-1.anon=0 (root) ei tohiks kunagi kasutada, kuna seeläbi saavad kõik kasutajad endale root- õigustega faililigipääsu.
- Failidesse, nagu /etc/fstab või /etc/vfstab, on kantud kõik failisüsteemid, mida saab käskudega mount-a või mountall kättesaadavaks teha. Teatud juhtudel võib see toimuda ka alglaadimise (boot) ajal ilma päringuta. Seepärast tuleb selle faili õigsust aegsasti kontrollida.

- /etc/exports ja /etc/fstab (või sarnased failid teistes süsteemides) on süsteemifailid, millele on ligipääs lubatud ainult süsteemiadministraatoril.
- Eksporditavad failid tuleks paigutada eraldi plaadile või partitsiooni, et vältida näiteks süsteemiplaadi volitamata täiskirjutamist mõne teise arvuti kasutaja poolt.
- Vältimaks suid- programmide käitamist kliendil, tuleb eksporditud failide mountimisel kasutada suvandit nosuid.
- Kindlustamaks, et pakette aktsepteeritakse ainult priviligeeritud portide 0 - 1023 poolt, tuleb võimalusel NFS-deemon konfigureerida nii, et pordinumbri kontroll viidaks läbi automaatselt.
- Failide märgistamiseks kliendi ja serveri vahel kasutatakse nn file handlesit, mis on kergesti äraarvatavad. Neid tuleks seepärast programmiga fsirand muuta juhuslikuks (randomize).
- SECURE-NFS olemasolu korral tuleks seda kasutada, et andmeid krüpteeritult edastada. Sealjuures on olulised järgmised sammud:
- Võtmete loomine kõigile NFS-kasutajatele
- kasutaja nobody jaoks public key kustutamine,
- NIS master serveril ei tohi joosta rpc.ypupdated,
- public key map i edastamine kõigile arvutitele enne SECURE-NFS käivitamist,
- private key loomiseks sisse- ja väljalogimisel kasutage keylogin ja keylogout.
- igal kliendil peab jooksma keyserv- deemon,
- mountimisel tuleb kasutada suvandit secure,
- Kõikide arvutite kellad tuleb sünkroniseerida, kuna edastatud paketid on varustatud ajamarkidega, et vältida teadete taastamist.

M 5.18 NISi turvamehhanismid

Algatamise eest vastutavad: infoturvaosakond, administraator

Rakendamise eest vastutavad: administraator

NISi (Network Information Service) ei ole võimalik käitada ilma keeruliste turvaprobleemideta, seetõttu tuleks seda kasutada ainult turvalises keskkonnas. NIS-serverile kehtivad järgmised nõuded:

- Paroolifailis /etc/passwd ei tohi olla sissekannet +::0:0::: , kuna vastasel juhul on olemas nimi “+”, mis on ilma paroolita. Kui sissekanne on vajalik, tuleb parool asendada “*”-ga (kontrollige, kas ligipääs on suletud!). Samas jääb püsima oht, et esimese vahe tahtmatul kustutamisel (“+”) on võimalik luua ilma parooli ja kasutajanimeta privilegeeritud ligipääs.
- Sama kehtib grupifailile /etc/group ja teistele olulistele failidele, mis peavad olema NISi kaudu kogu võrgus ligipääsetavad, näiteks /etc/hosts, /etc/group või /etc/bootparams .
- Serveri protsess ypserv peaks vastama ainult eelnevalt määratud arvutite päringutele.

NIS-kliendile kehtib:

- Sissekanne +:*:0:0::: paroolifailis /etc/passwd tuleks dokumenteerida (vt M 2.31 Volitatud kasutajate ja õiguste profiilide dokumenteerimine) ning paroolivälјas peab igal juhul olema sissekanne, et NISi mittekasutamisel (tahtlikul või tahtmatul) ei loodaks kogemata kasutajanimega “+” ilma paroolita ligipääsu.
- Sama kehtib grupifailile /etc/group ja kõigile teistele olulistele failidele, mis peavad olema NISi kaudu ligipääsetavad.
- Kliendiprotsess ypbind peaks aktsepteerima ainult andmeid, mis tulevad privilegeeritud pordilt, kuna vastasel juhul võib ta saada andmeid (ka paroole!) igalt suvaliselt protsessilt, mis näitab ennast serverina.
- Vältimaks, et NIS-administraatoril on kõigil NIS-klientidel root- õigused, tuleks igal NIS-kliendil seadistada UID 0-iga lokaalne kasutaja.
- Tuleb jälgida, et NIS otsiks sobivaid sissekandeid alguses lokaalsetest failidest, näiteks sissekanded

root::0:0:::
+:*:0:0:::
failis /etc/passwd viivad selleni, et ei kasutata root- parooli NIS- Map ist, vaid esimest ilma paroolita sissekannet.

M 5.19 Sendmaili turvamehhanismid

Algatamise eest vastutavad: administraator

Rakendamise eest vastutavad: administraator

Kuna meilide edastamine on enim kasutatav rakendusvõrgus, on nendega seotud protsessid erilise tähtsusega ja üks sagedasemaid rünnakukohti süsteemis. Lisaks on neil protsessidel sageli suid-Bit ja need kuuluvad privilegeeritud kasutajale (näiteks root või bin). Näiteks oli viga sendmailis üks viisidest, kuidas interneti uss edasi kandus:

- Sendmail i käivitamisel on võimalik määrata palju suvandeid, mis root arvutil jooksutades tekitada turbeprobleeme. Kui sendmail i saavad käivitada suvalised kasutajad, tuleks kontrollida, kas see käivitumisel ühega nendest suvanditest suid-Bit i ignoreerib ja kasutaja UID-ga jookseb. Turbeprobleemide vältimiseks peaks administraator kindlustama, et privilegeerimata kasutajad saaksid suid-root-Bit i korral sendmail i käivitada ainult järgmiste suvanditega. 7, b, C, d, e, E, i, j, L, m, o, p, r, s ja v.
- Varem leitud turvaaukude tõttu tuleb alati kasutada sendmail i uusimat versiooni. Ajakohaste versioonide kohta leiate informatsiooni meetmest M 2.35 „Teabe hankimine turvaaukude kohta“ kirjeldatud kohtades, nagu BSI, CERT, DFN-CERT.
- Sendmail i ei tohi käitada silumisrežiimis (Debug Mode), vastasel juhul on võimalik omistada root õigused. Seda saab katsetada, kui sisestada käsu

telnet localhost 25,

kusjuures localhost võib olla kontrollitava arvuti nimi ja 25 võib olla pordi number, millega sendmail ile päring saadetakse. Arvuti või sendmail annab siis teate

Trying 123.45.67.8. . .

Connected to xxx.yy.de.

Escape character is ‘^]’.

220 xxx Sendmail 4.1/SMI-4.1 ready at Wed, 13 Apr 94 10:04:43 +0200

Kui te nüüd käsu debug showq või väga vanade versioonide korral wizard sisse trükite, peaks see protsessi

500 Command unrecognized

keelama. Pärast seda võite käsuga quit ühenduse jälle lõpetada.

- Kuna käsud vrfy ja expn näitavad meilinime juurde kuuluvat sisselogimise nime, ei tohi need olla kättesaadavad, vastasel juhul võib proovimise kaudu välja uurida ka sinna juurde kuuluva parooli. Sendmail versiooni 8 korral saab need käsud suvandiga p (privacy) välja lülitada. Nende käskude olemasolu saab kontrollida eelnevas punktis kirjeldatu abil, näiteks trükkides sisse käsu vrfy useralias.
- Konfiguratsioonifail sendmail.cf peaks kuuluma root ’ile ja olema ainult root ’ile loetav ja kirjutatav. Sama kehtib ka kataloogipuus ülevalpool asuvatele

kataloogidele, kuna vastasel korral on nende kataloogide ümbernimetamisel võimalik luua uus sendmail.cf fail.

- Täitmisprogrammide või failide kehtivate aadresside teatamine vastuvõtjale või saatjale tuleb sendmail.cf konfiguratsiooniga takistada või piirata vastavate meetmetega ainult ohututele programmidele ja failidele.
- F-käsklust (näiteks FX/path [^#]), mille abil on võimalik määratleda klasse, tuleks konfiguratsioonifailis (sendmail.cf) kasutada ainult failide lugemiseks, mis on niigi kogu süsteemis loetavad, sest vastasel juhul võib tekkida olukord, kus kaitstud failides sisalduv konfidentsiaalne informatsioon on vabalt kättesaadav. F-käskluse (näiteks FX|/tmp/prg) programmivormi ei tohiks kasutada!
- Väljastusagendi (Delivery Agent) määramisel (näiteks Mlocal) tohib kasutada ainult absoluutseid radu (näiteks P=/bin/mail). Peale selle tuleks Flag S (suid) määrata ainult siis, kui sellega lahendatakse võimalikud turbeprobleemid.
- Iga fail, millesse sendmail saab kirjutada, näiteks sendmail.st statistika jaoks, peaks olema ainult root i poolt kirjutatav ja paiknema ainult root ile kuuluvas kataloogis. Sama kehtib sendmail i poolt analüüsitavatele failidele meililistides, näiteks :include: .
- Privilegeeritud kasutajad, nagu bin ja root ei tohiks omada .forward faile. Kui kasutaja või grupi kirjutusõigused on selle faili jaoks valesti määratud või kui mõnel kasutajal õnnestub priviligeeritud gruppi sisse murda, võib ta endale moodustada priviligeeritud kasutajatunnustega kesta (Shell).

Tavakasutajatele peaks .forward fail olema kirjutatav ainult omanikule ja fail peaks paiknema omanikule kuuluvas kataloogis. Kui mõni kodukataloog peab olema terves süsteemis kirjutatav, näiteks uucp , siis järgneva meetodi abil saab takistada kahjuliku .forward faili loomist: Tuleb luua kataloog, mille nimi on .forward, mille õigused on 000 ja kelle omanikuks on root ja sellesse kataloogi tuleb luua fail, mille õigused on samuti 000 ja omanikuks root. See tagab, et mitte keegi peale root i ei saa seda faili muuta ega kustutada. uucp kodukataloog peaks samuti kuuluma root ile ning olema märgitud Sticky-Bit iga (t). Sarnane teostus on soovitatav ka teistele konfiguratsioonifailidele (näiteks .login, .cshrc) kogu süsteemis kirjutatavates kataloogides.

- Igast aliase failist tuleks eemaldada täitmisprogramm, eelkõige uudecode. Lisaks peaks alias fail ja sinna juurde kuuluv andmebaas kuuluma root ile ja samuti ka ainult root i poolt kirjutatav olema.
- Tuleb arvestada, et iga saadud meil võib olla võltsitud. See võib juhtuda nii Mail Queue s või port 25-le sisselogimisel. Esimest saab vältida, kui Mail Queue kataloog omab õigusi 0700 ja kuulub root ile. Queue fail peaks omama õigust 0600. Meili muutumist transpordi ajal ei saa vältida ja kasutajatele tuleb selgitada, et kui nad näiteks saavad root ilt meili, kus palutakse neil muuta oma parool, siis võib tegemist olla võltsinguga.

M 5.20 rlogin, rsh ja rcp turbemehhanismid

Algatamise eest vastutavad: infoturbeosakond, administraator

Rakendamise eest vastutavad: administraator

Programmiga rlogin ja sinna juurde kuuluva deemoniga rlogind on võimalik ennast võrguühenduse kaudu teise arvutisse sisse logida. Siinjuures küsitakse ainult parooli, kuna kasutajanimi edastatakse automaatselt. Käsklusega rsh või rcp ja deemoniga rshd on võimalik teisel arvutil lasta antud käsklus täita. Mõlemale käsklusele on võimalik määrata Trusted Hosts , kasutajaspetsiifiliselt failis $HOME/.rhosts või üle kogu süsteemi failis /etc/hosts.equiv. Iga arvutit, mis on nendesse failidesse sisse kantud, vaadeldakse usaldusväärse arvutina, nii et sisselogimine (rlogin) või käskluste täitmine (rsh) on võimalik ilma paroolita.

Kuna eelkõige personaalarvuti (PC) kaudu on võimalik võltsida ükskõik millist arvuti nime, tuleb kindlustada, et faile $HOME/.rhosts ja /etc/hosts.equiv ei oleks olemas või need oleksid tühjad ja kasutajatel puuduks neile ligipääs. Selleks tuleks regulaarselt kontrollida kasutajate kodukatalooge või takistada deemonite rlogind ja rshd käivitamine (vt faili /etc/inetd.conf ja M 5.16 Võrguteenuste inventuur). Kui faili /etc/hosts.equiv kasutamine on vältimatu, tuleb kindlustada, et failis ei oleks ühtegi '+' sissekannet, kuna seeläbi muutuksid kõik arvutid usaldusväärseteks.

„r-teenuste ” asemel võib kasutada *Secure Shell*i (*ssh*), mis kasutab konfidentsiaalsuse ja tervikluse turvaliseks autentimiseks ja säilitamiseks ulatuslikke funktsioone (vt M 5.64 Secure Shell (SSH)) . Selleks et vältida turbemeetmetest möödumist, tuleks *ssh* kasutamisel „r-teenused” vastavalt võimalusele välja lülitada. See eeldab aga, et kõigil kommunikatsioonipartneritel on sobiv *ssh*.

M 5.21 telneti, ftp, tftp, rexeci turvaline kasutamine

Algatamise eest vastutavad: infoturbeosakond, administraator

Rakendamise eest vastutavad: administraator

Käsklus telnet hostname võimaldab pärast kasutajanime ja parooli sisestamist ennast hostname- arvutil sisse logida. ftp võimaldab kopeerida suuremaid andmehulkasid ning rexec lubab ilma eelneva registreerimiseta mõnel teisel arvutil käsklusi teostada. Kõigi kolme programmi puhul edastatakse sisestatud kasutajanimi ja parool võrgu kaudu krüpteerimata, sellest lähtuvalt tohib kasutada ainult turvalisi võrke (vt G 5.7 Liinide pealtkuulamine). Kõik telnet i, ftp ja rexec i kasutamised tuleb protokollida. Eelkõige tuleb jälgida, kas esineb väliste IT-süsteemide ühenduskatseid. Deemoni ftpd kasutamisel tuleb jälgida, et sarnaselt sendmailile (vt M 5.19 Sendmaili turvamehhanismid) leitakse ikka ja jälle uusi suuri turvaauke, mis muuhulgas võimaldavad ilma paroolita saada administraatori õigusi. Ei tohiks kasutada kirjeldatutest vanemaid ftp versioone. Lisaks tuleks faili /etc/ftpusers kanda kõik kasutajad, kellele ei ole ftp ligipääs lubatud. Siia kuuluvad näiteks root, uucp ja bin . Uute kasutajate loomisel tuleb jälgida, et kui nad ei tohi vastavalt oma õigusastmele omada ftp ligipääsu, siis tuleb nad kanda /etc/ftpusers kausta (vt M 2.30 Kasutajate ja kasutajarühmade määramise protseduurid).

.netrc failiga lubatakse automaatne FTP ligipääs kaugematele IT-süsteemidele. Selle võimaldamiseks sisaldavad .netrec failid vajalikke paroole. Tuleb kindlustada, et kasutajate kataloogides ei oleks .netrc faile või need failid oleksid tühjad ja kasutaja ei omaks neile ligipääsu.

Deemonite tftpd, rexd ja rexecd kasutamine tuleb takistada, või vähemasti kindlustada, et tftp kasutamisel oleks Login-kataloogi kasutajatel failidele ainult piiratud ligipääs (vt M 2.32 Piiratud kasutajakeskkonna loomine). Seda saab kontrollida, trükkides sisse:

tftp hostname

tftp>get /etc/passwd /tmp/txt

Kui tftp deemon ei anna veateadet, tuleb selle kasutamine takistada. Kui aktiivsete võrguosade või X-terminali käivitamiseks on tftp ikkagi vajalik, tuleb see kindlasti dokumenteerida ja põhjendada. tftp kasutamisel tuleb jälgida, et tftp deemon käivitataks suvandiga -s kataloog. Seejuures tuleb kataloogi puhul kasutusele võtta ainult deemonile nähtav kataloog. telnet i ja rexec i asemel võib kasutada Secure Shell i (ssh), mis kasutab konfidentsiaalsuse ja tervikluse turvaliseks autentimiseks ja säilitamiseks ulatuslikke funktsioone (vt M 5.64 Secure Shell (SSH)). Tunneldamisega (tunneling) on ftp' d võimalik käitada ka turvalise krüpteeringuga. Selleks et vältida turbemeetmetest möödumist, tuleks ssh kasutamisel need teenused vastavalt võimalusele välja lülitada. See eeldab aga, et kõigil kommunikatsioonipartneritel on sobiv ssh.

Täiendavad kontrollküsimused:

- Kas faili /etc/ftpusers uuendatakse regulaarselt?
- Kas ligipääsukatsed telnet ile , ftp le ja rexec ile protokollitakse?
- Kas kindlustamiseks kasutatakse ssh 'd?
- Kas tftp on deaktiveeritud?

M 5.22 Saate- ja vastuvõtupoole ühilduvuse kontroll

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: vastutav spetsialist

Sõltuvalt saate- ja vastuvõtusüsteemi ühilduvusastmest saab informatsiooni edastamist andmekandjate vahelise kommunikatsiooni abil pidada rohkemal või vähemal määral usaldusväärseks. Seejuures tuleb sõltuvalt vahetatavate andmete keerukusest seada ühilduvusele erinevad nõuded. Ühilduvusprobleemide ennetavaks tuvastamiseks ja vastuabinõude rakendamiseks tuleb enne regulaarse andmekandjate andmevahetuse sisseseadmist kontrollida, kas järgnevad omadused sobivad omavahel kokku:

- Füüsilised komponendid: loomulikult on vajalik, et saate- ja vastuvõtusüsteemi füüsilised komponendid ühilduksid. Seejuures ei piisa mehaanilisest vastavusest, sest muude parameetrite sobimatus, näiteks lintide töökiirus, võib põhjustada probleeme.
- Kodeering (nt ASCII või EBCDIC): kui saate- ja vastuvõtusüsteemis kasutatav kodeering kattub, saab juhuslikult andmekandjale jaotatud üksikuid sektoreid või plokke füüsiliselt lugeda. Kui kasutatud kodeering ei ühti, tõlgendatakse edastatud andmeid valesti.
- Andmekandja operatsiooni-/failisüsteemi formaat: kui mõlemal süsteemil on lisaks sellele ka samasugune operatsiooni- ja failisüsteem või kui vastuvõttev operatsioonisüsteem suudab lugeda ka teiste operatsioonisüsteemide formaate (mitte kõik Unixi operatsioonisüsteemid ei suuda NTFS-andmekandjaid lugeda), saab taastada kõik andmed sellisel kujul, nagu need olid saatja juures. Sellest piisab informatsiooni jaoks, mida ei ole täiendavalt formaaditud nagu näiteks suurem osa rakendusprogrammidest (nt tekstitöötlusprogrammidest) seda teeb.
- Rakendustarkvara: kui edastatavate andmete loomiseks kasutati rakendusprogramme, tuleb jälgida nende programmide versioonide ühilduvust , kuna failide formaadid võivad erineda. Versioonide ühilduvus pole vajalik, kui programmi versioonid ühilduvad vanemate/uuemate versioonidega.
- IT-turvatarkvara ja IT-turvaparameetrid: kui täiendavalt rakendatakse ka IT-turvatooteid või teatud rakendusprogrammide turvamehhanisme (vt M 4.30 Rakendusprogrammide turvavahendite kasutamine), tuleb tagada nende toodete ühilduvus. Saatjad ja vastuvõtjad peavad kasutatavate võtmete või paroolide osas sobival teel kokku leppima.

Ühilduvusprobleemide esinemisel tuleb tarvitusele võtta meetmed/tooted, mis võimaldavad andmeid vastavalt konverteerida, või siis tuleb saate- ja vastuvõtusüsteeme vastavalt täiendada.

Täiendavad kontrollküsimused:

- Kas saate- ja vastuvõtupoolel rakendatakse ühilduvaid IT-tooteid (riist- ja tarkvara)?
- Kas saatja ja vastuvõtja rakendusprogrammide versioonid ühilduvad?
- Kas vastuvõtjale on vastavad koodid/paroolid info lugemise võimaldamiseks teada?

M 5.23 Andmekandjate sobivate edastusviiside valimine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: kasutajad

Lisaks meetmes M 2.3 Andmekandjate haldus kirjeldatud rakendusjuhistele peaks andmekandjate saatmisviis lähtuma ohupotentsiaalist. Kättesaadavusnõudeid arvestades tuleks valida selline saatmisviis, mis tagab õigeaegse kohaletoimetamise. Mida rohkem isikuid on edastamisega seotud ja mida pikemat aega on andmekandja ilma järelvalveta, seda vähem saab tagada selle konfidentsiaalsust ja terviklikkust. Sellest lähtudes tuleb valida sobivad saatmisviisid. Valida saab näiteks järgnevate saatmisviiside vahel:

- postisaadetised (erinevate saatmispakkumistega, mis sisaldavad erinevaid garantiisid transpordi kiiruste ja turvalisuse osas),
- kullerteenused,
- isiklik kohaletoimetamine ja
- isiklik üleandmine.

Ametiasutusel või ettevõttel oleks soovitav pidada nimekirja, milles on loetletud andmekandjaid ja nende turbevajadusi silmas pidades soovitavad saatmisviisid. See aitab kaastöötajatel valida mitte ainult parima hinna/kvaliteedi suhtega teenust, vaid ka optimaalselt arvestada turvalisusega. Vastav nimekiri peaks hõlmama vähemalt järgnevaid aspekte:

- saatmisviisi/kulleri keskmine transpordiaeg
- saatmisviisi/kulleri usaldusväärsus
- kulud.

Täiendavad kontrollküsimused:

- Kas andmekandja saatmisviisi valimisel lähtutakse turvalisusest?
- Kas on võimalik kasutada usaldusväärseid transpordiettevõtteid või kullereid?

M 5.24z Sobiva faksiblanketi kasutamine

Algatamise eest vastutavad: siseteenuste juht

Rakendamise eest vastutavad: faksi eest vastutav, kasutaja

Korrektse ja mõistetava faksiside tagamiseks on soovitatav kasutada standardiseeritud faksiblanketti. Nii on võimalik kontrollida, kas faks saadi täielikult kätte. Faksiblankett peaks sisaldama:

- faksiaparaadi numbrit,
- saatja nime (telefoninumbri ja aadressiga),
- kontaktisiku telefoninumbrit sideprobleemide korral kasutamiseks,
- saaja nime (faksiaparaadi numbri ja vajadusel aadressiga),
- lehekülgede arvu, kaasa arvatud faksiplank,
- vajadusel olulisusmärget (erinevad astmed) ja
- saatja allkirja

Samuti on sobilik palve valesti saadetud faksid edasi saata või saatjat teavitada.
Täiendavad kontrollküsimused:

- Kas faksiblankett sisaldab kõiki vajalikke osi?
- Kas faksiblanketti kasutatakse pidevalt?

M 5.25 Saate- ja vastuvõtulogide kasutamine

Algatamise eest vastutavad: infoturbeosakond

Rakendamise eest vastutavad: infoturbeosakond, faksi eest vastutav, administratiivosakond

Faksiteenuste, näiteks saate- ja vastuvõtulogi kasutamisel tuleb teha vahet tavalistel faksiaparaatidel ja faksiserveritel.

Tavalise faksiaparaadi kasutamine

Faksiaparaadi poolt peetav automaatne ülekandelogi tuleb regulaarselt välja printida. Kindlaks tuleb määrata, kes väljaprintimise käsib, kus ja kui kaua ülekandelogi säilitatakse ja millisel viisil viiakse läbi pistelisi ebakorrapärasuste kontrolle. Siinjuures tuleb pidada kinni andmekaitseseadusest. Eelkõige tuleb takistada volitamata isikute ligipääs. Lisaks tuleks pidada faksipäevikut, kus on näha, kes, millal ja kellele faksi saatis. Samas võib pidada ka sissetulevate fakside raamatut. Lisaks on olemas veel üks kontrollivõimalus, kui faksiaparaat on ühendatud kaasaegse telekommunikatsioonisüsteemiga. Sellisel juhul on võimalik telekommunikatsioonisüsteemis analüüsida faksinumbrite andmekulu (vt M 2.40 Töötajate esinduse õigeaegne kaasamine).

Faksiserveri kasutamine:

Ka faksiserveritel on võimalik andmete liikumine protokollida. Neid protokolle tuleks regulaarselt analüüsida ja arhiveerida. Logide analüüsimiseks ja arhiveerimiseks tuleb määrata raamtingimused ja vastutavad isikud. Selle eest võib näiteks vastutada fakspostikeskus, logisid tohib analüüsida aga ainult töötajate esinduse liikme, revisjoni liikme või andmekaitseosakonna liikme juuresolekul. Siinkohal tuleb arvestada andmekaitseseaduse nõuetega ja eelkõige tuleb takistada volitamata isikute ligipääs. Faksiserverite kasutamisel ei ole faksipäeviku pidamine vajalik. Sellisel juhul peaks piisama saate- ja vastuvõtulogi täielikust arhiveerimisest. Osaliselt on saadetud fakside arveldusandmeid võimalik kasutada ka faksiserveris konkreetsete kulutuste arvutamiseks.

Täiendavad kontrollküsimused:

- Millised nõuded kehtivad saate- ja vastuvõtulogile?
- Kus arhiveeritakse logid ja kes omavad neile ligipääsu?

M 5.29 Sihtaadresside ja logide perioodiline kontroll

Algatamise eest vastutavad: infoturbeosakond

Rakendamise eest vastutavad: faksi kasutamise eest vastutav töötaja

Programmeeritavate kiirvalikuklahvide või sihtaadresside salvestamise puhul tuleb aeg-ajalt kontrollida, kas soovitud faksinumber vastab programmeeritud numbrile ja kas seda läheb veel tarvis. See väldib olukorda, kus volitamata isiku poolt sisestatud võõras faksinumber on pikemat aega õige numbri asemel kasutuses.Lisaks saab niimoodi varakult tuvastada vajalikes sihtnumbrites märkamata jäänud muudatusi.

Täiendav kontrollküsimus:

- Kas salvestatud numbreid kontrollitakse pisteliselt?

M 5.30z Olemasoleva tagasihelistusfunktsiooni aktiveerimine

Algatamise eest vastutavad: infoturbeosakond, administraator
Rakendamise eest vastutavad: kasutaja, administraator

Paljud modemid toetavad automaatse tagasihelistamise (Callback) võimalust. Kui see funktsioon on aktiveeritud, katkestab modem sissetuleva kõne korral liini ja helistab tagasi eelseadistatud numbrile. Sellega takistatakse modemi kuritarvitamist autoriseerimata helistaja poolt, kui ta ei ole kättesaadav eelseadistatud numbril. Tagasihelistusfunktsiooni tuleb kasutada sellisel juhul, kui kindlal kommunikatsioonipartneril peab olema võimalus ennast automaatselt sisse valida. Samas tuleb meeles pidada, et automaatse tagasihelistamisega võetakse enda kanda ka andmeedastuskulud. Vajaliku käskluse leiate kasutusjuhendist, tavaliselt kasutatakse käsklust AT%S. Enne tagasihelistusfunktsiooni aktiveerimist tuleb kindlaks määrata, millisele numbrile tagasi helistatakse.

Mõned modemid võimaldavad automaatse tagasihelistuse siduda paroolipäringuga. Modem, millele helistatakse, nõuab pärast ühenduse loomist helistavalt modemilt parooli sisestamist. Modem, millele helistatakse, kontrollib parooli kehtivust. Igal kehtival paroolil on number, millele tagasi helistatakse. Erinevatest kohtadest lokaalse modemiga ühenduse loomiseks saab lokaalses modemis luua tagasihelistusnumbrite loendi. Tuleb jälgida, et automaatne tagasihelistusfunktsioon oleks aktiveeritud ainult ühel pool, vastasel juhul tekib süsteemis surnud ring. Tagasihelistus peaks olema aktiveeritud passiivsel poolel, st tähendab poolel, millelt faile saadakse või kuhu faile paigutatakse. Tüüpiline näide on välisteenistuses olev töötaja, kes tahab luua ühendust oma organisatsioonis paikneva IT-süsteemiga. Siin peab tagasihelistus olema aktiveeritud organisatsioonisisesel modemil. Tagasihelistusfunktsiooni eelseadistatud numbreid tuleb ükshaaval kontrollida ja uuendada.

Tagasihelistuse võib peale modemi luua ka rakendus. Kui kasutatav rakendus võimaldab seda funktsiooni, peaks tagasihelistuse looma rakendus, mitte modem. Kui tagasihelistuse loob modem, saab ründaja proovida ennast just sellel momendil sisse valida, kui modem tahab tagasihelistust käivitada ja nii selle kinni püüda. Kui tagasihelistuse teostab rakendus, on ründajal tunduvalt raskem õiget momenti tabada.

Täiendavad kontrollküsimused:

- Kas on selge, kes katab tagasihelistamise režiimi korral kulud?
- Millal kontrolliti viimati eelseadistatud numbrit?

M 5.31 Modemi sobiv konfigureerimine

Algatamise eest vastutavad: infoturbeosakond, administraator

Rakendamise eest vastutavad: kasutaja, administraator

Enamik modemitest töötab Hayesi standardi järgi (AT standard). See on normeerimata, tootjast sõltuv standard. Suur osa modemite baaskäsustikest kattuvad. Suuremaid erinevusi esineb laiendatud käsustikes. Kasutatava modemi käsustikku tuleb kontrollida lähtuvalt sellest, kuidas järgnevalt kirjeldatud funktsioonid on üle võetud ja kas vigase konfiguratsiooni tõttu võivad tekkida turvaaugud. Valitud seadistused tuleks salvestada modemi säilmällu (non-volatile memory) (vt M 1.38 Modemi õige paigutus). Lisaks tuleks need ka paberil välja printida, et oleks neid võimalik kogu aeg hetkeseadistusega võrrelda. Järgnevalt tutvustatakse mõningaid turbeks olulisi konfiguratsioone:

Automaatne vastamine (Auto-Answer) - Registri S0 kaudu saab määrata, et sissetuleva kõne korral vastab modem pärast määratud arvu kutsumisi. Seadistusega S0=0 see funktsioon takistatakse ja kõnedele tuleb vastata käsitsi. Seadistus tuleks valida, kui ei soovita, et väljaspoolt oleks võimalik märkamatult ühendus luua. Üldjuhul tuleks kasutada tagasihelistamismehhanismi (vt M 5.30 Olemasoleva tagasihelistusfunktsiooni aktiveerimine).

Modemi kaugkonfiguratsioon

Mõned modemid on võimalik seadistada nii, et neid on võimalik kaugkonfigureerida mõne eemal asuva modemi kaudu. Tuleb jälgida, et see võimalus oleks välja lülitatud. Probleemide kohta kaughooldusel modemi kaudu vt M 5.33 Kaughoolduse turve .

(Tagasihelistamis-)Numbrite salvestamine paroolikaitsega

Telefoninumbrite või tagasihelistusnumbrite salvestamisel modemi säilmällu (non-volatile memory) on paljude modemimudelite juures võimalik neid andmeid parooliga kaitsta. Selle võimaluse olemasolul tuleks seda kasutada vastavalt meetmele M 2.11 Paroolide kasutamise reeglid ja valida sobivad paroolid. Mõnede modemite korral kuvatakse pärast kindla käsu sisestamist nimekiri numbrite ja sinna juurde kuuluvate paroolidega. Sellest lähtuvalt peaks modemile ligipääs olema ainult volitatud isikutel (vt M 1.38 Modemi õige paigutus).

Täiendavad kontrollküsimused:

- Kas modemi eest vastutav töötaja teab modemi kogu käsustikku?
- Kas modemi konfiguratsioon on dokumenteeritud?

M 5.32 Sidetarkvara turvaline kasutamine

Algatamise eest vastutavad: infoturbeosakond, administraator

Rakendamise eest vastutavad: kasutaja, administraator

Turvaline ligipääs arvutile modemi kaudu sõltub suuresti kasutatavast sidetarkvarast. Peaaegu iga sidetarkvara võimaldab salvestada suhtluspartnerite telefoninumbreid ja teisi andmeid. Need on isiklikud andmed, mida tuleb vastavalt kaitsta. Kuigi see võib tunduda mugavana, ei tohi teiste arvutite ja modemite ligipääsuparoole salvestada sidetarkvaras. Igaüks, kes pääseb ligi IT-süsteemile ja sidetarkvarale, võib võõra kasutajanimega ligi pääseda teistele süsteemidele (vt M 1.38 Modemi õige paigutus ja M 2.8 IT-rakendustele ja andmetele pääsuõiguste andmine).

Paljud sideprogrammid võimaldavad andmeid jooksutada tagaplaanil, näiteks Windowsi all. Seda tohiks kasutada ainult usaldusväärsete sidepartnerite puhul, kuna sidepartner võib andmeside katkestada ja kokkulepitust erinevad failid arvutile laadida või arvutist alla laadida. Võimalik on arvuti nakatamine viirustega või konfidentsiaalsete andmete kopeerimine. On olemas ülekandeprotokolle, mis võimaldavad täisdupleks (full duplex) ülekannet, see tähendab, et andmeside toimub samaaegselt mõlemas suunas. Selliseid ülekandeprotokolle tuleks kasutada ainult usaldusväärsete sidepartneritega, kuna see vastab tagaplaanil toimuvale andmesidele. Kui sidetarkvara toetab paroolide kasutamist või logifunktsiooni, siis tuleb see aktiveerida.

Täiendavad kontrollküsimused:

- Kas sidetarkvaras salvestatakse paroole?
- Kas kasutajale on teada ohud, mis kaasnevad tagaplaanil toimuva andmeedastusega?

M 5.33 Kaughoolduse turve

Algatamise eest vastutavad: infoturbespetsialist, IT-juht
Rakendamise eest vastutavad: IT-juht, administraator

IT-süsteemide kaughooldus kujutab endast erilist turberiski. Kaughoolduse puhul tuleb eristada, kas IT-süsteemile pääseb ligi ettevõttesisene või -väline hoolduspersonal. IT-halduses kasutatakse tihti kaughooldust, et administraatorid saaksid kasutajaid kiiresti aidata, ilma et nad peaksid isiklikult vastava IT-süsteemi juurde minema. Turvalisuse seisukohalt oleks mõistlik kaughooldusest loobuda. Kui see ei ole võimalik, tuleb võtta täiendavaid turvameetmeid.

Hooldatav IT-süsteem peab hõlmama järgmisi turbefunktsioone:

- Kaughoolduse ühendus tuleks alati käivitada lokaalse IT-süsteemi kaudu. Seda on võimalik teostada hallatava IT-süsteemi kõnega kaughoolduspunkti või kasutades automaatset tagasihelistusfunktsiooni (callback).
- IT-süsteemi kasutaja peab kaugligipääsu kinnitama, näiteks vastava kinnitusega süsteemis.
- Väline hoolduspersonal peab end enne hoolduse algust autentima. Kui paroolid edastatakse krüpteerimata, tuleks kasutada ühekordseid paroole (vt M 5.34z Ühekordsed paroolid).
- Kaughoolduse käigus teostatu tuleb hooldataval IT-süsteemil protokollida.

Lisaks võiks hooldatavale IT-süsteemile paigaldada veel lisafunktsioone:

- ajapiiri määramine vigaste ligipääsukatsete korral;
- kaughoolduse keelustamine tavakäituse ajal ning ligipääsu lubamine määratud ajavahemikuks;
- hoolduspersonali õiguste piiramine – hoolduspersonalil ei tohiks olla kõiki administratiivseid õigusi, tuleks rakendada astmelist õigushaldust, UNIX-süsteemide korral tuleb järgida meedet M 2.33z Unixi ülemarollide jagamine ja M 2.38 Administraatorirollide jagamine . Hoolduspersonalil peaks olema ligipääs ainult failidele ja kataloogidele, mis on seotud hetkehooldusega;
- hoolduspersonalile peaks IT-süsteemis olema loodud eraldi kasutajatunnus, mille all teostatakse võimaluse korral kõik hooldustööd;
- Kui kaughoolduse ühendus mingil põhjusel katkestatakse, tuleb ligipääs süsteemile lõpetada sunnitud väljalogimisega.

Kui välisest kaughooldust pole võimalik loobuda, tuleb lisaks ülaltoodud turvameetmetele järgida järgmisi punkte:

- Kaughoolduse korral väliste kommunikatsiooniühenduste kaudu tuleb ligipääsud ja ühendused turvata. Kaughoolduspersonal tuleb autentida, edastatavad andmed krüpteerida ja haldustööd protokollida. Näiteks võib kasutada virtuaalset privaatvõrku (VPN) või eksklusiivühendusi.
- Kohalikud IT-spetsialistid peaksid kaughooldust jälgima. Isegi kui kaughooldust kasutatakse põhjusel, et organisatsioonisiseselt puuduvad teadmised

või maht, ei tohi hoolduspersonali jätta järelevalveta (vt M 2.4 Hooldus- ja remonditööde reeglid). Ebaselguste korral peaks kohalik IT-spetsialist tegema kohe järelpärimise. Kaughooldust peab olema võimalik lokaalselt katkestada.
- Kui hoolduse ajal paigaldatakse IT-süsteemile andmeid või programme, peab see olema selgesti nähtav ja arusaadav, näiteks võib seda teha ainult eriliselt märgistatud kataloogides või kindlate kasutajatunnustega.

Meetme M 3.55 Konfidentsiaalsuslepingud kohaselt tuleb ka välise hoolduspersonaliga sõlmida leping andmete konfidentsiaalsuse kohta. Kindlaks tuleb määrata, et hoolduse raames väliselt salvestatud andmed tuleb pärast tööde lõpetamist kustutada. Samuti tuleb kindlaks määrata välise hoolduspersonali kohustused ja kompetentsid.

Kontrollküsimused:

- Kas on tagatud, et kaughooldus teostatakse ainult turvalises keskkonnas?
- Kas on kindlustatud, et kaughoolduse ligipääsud käivitatakse alati lokaalsest IT-süsteemist?
- Kas kaughoolduse läbiviimine on piisaval määral dokumenteeritud?

M 5.34z Ühekordsed paroolid

Algatamise eest vastutavad: infoturbespetsialist, administraator

Rakendamise eest vastutavad: administraator

Võrkudes, kus paroole edastatakse krüpteerimata kujul, on võimalik neid lihtsalt teada saada. Peale selle võivad teostus- või protokollivead operatsioonisüsteemides ja rakendustarkvaras viia ka krüpteeritud paroolide kompromiteerimiseni. Seetõttu on soovitatav kasutada ühekordseid paroole, mis tuleb pärast kasutamist välja vahetada. Ühekordseid paroole saab luua nii tarkvara kui ka riistavara abiga. Ühekordsete paroolide kasutamisel peab kasutaja looma ühekordse parooli IT-süsteemis või volitustõendi abil või lugema selle sisse nimekirjast, mis on loodud välisel IT-süsteemil ja mida tuleb turvaliselt säilitada. Eemalolev IT-süsteem peab seejärel ühekordse parooli kinnitama.

Volitustõendid, mis genereerivad ühekordseid paroole, on väikesed riistvara komponendid. Need võivad olla kiipkaardid või taskuarvutisarnased seadmed. Esmalt peab kasutaja end volitustõendi suhtes autentima. Pärast kasutaja edukat autentimist autendib volitustõend end serveri suhtes automaatselt või näitab kasutajale ekraanil ühekordset parooli, mis tuleb sisestada klienti. Kuna üha rohkem konfidentsiaalset informatsiooni on kaitstud ainult paroolidega, on ühekordsetel paroolidel ja riistvaral põhinevatel autentimismeetoditel üha suurem tähtsus. Paljud riistvaral põhinevad süsteemid võimaldavad ainulogimisega (ingl single-sign-on, SSO) lahenduse loomist. SSO-ga saavutatakse olukord, kus kasutajad ei pea ennast iga IT-süsteemi või iga rakenduse juures uue parooliga autentima. Kasutajad logivad ennast IT-süsteemi või spetsiaalsesse portaali sisse ja saavad siis rakendusi ja IT-süsteeme kasutada ilma täiendava käsitsi autentimiseta. Riistvaral põhinevate ühekordsete paroolide tõttu muutuvad paljud meetmes M 2.11 Paroolide kasutamise reeglid kirjeldatud reeglid kasutajatele üleliigseks, kuna need täidetakse ühekordsete paroolidega.

Kontrollküsimus:

- Kas on kindlustatud, et võrgus ei kanta üle krüpteerimata taaskasutatavaid paroole?

M 5.35 UUCP turvamehhanismid

Algatamise eest vastutavad: infoturbeosakond, administraator
Rakendamise eest vastutavad: administraator

Unix süsteemides sisalduv ja samuti ka teistele operatsioonisüsteemidele saadav programmipakett UUCP (Unix-to-Unix Copy) võimaldab IT-süsteemide vahelist andmevahetust ja käskluste täitmist eemal asuvatel arvutitel. Eelduseks on ainult osalevate süsteemide ühilduvus uucico- programmidega. Vaatamata sellele, et UUCP tähtsus on ISDN-i ja TCP/IP võimaluste tõttu vähenenud, on see ikka veel laialdaselt levinud. UUCP-d kasutatakse meilide ja uudiste vahendamiseks arvutite vahel (uucp). UUCP võimaldab ka sisselogimise (cu) ja programmide käivitamise võõrastel arvutitel. On olemas erinevaid UUCP variante: 1983. a Peter Honeyman, David Nowitz ja Brian E. Redman'i poolt loodud rakenduse asemel (HoneyDanBer UUCP) kasutatakse sageli ka AT&T UNIX algset UUCP süsteemi versioon 7-t, mille teine versioon on hetkel aktuaalne (seda UUCP-d nimetatakse versioon 2 UUCP) või Tahoe-UUCP-d (tarnitakse BSD 4.3-ega). Kasutatavat UUCP varianti saab vaadata failide järgi, mis asuvad kaustas /usr/lib/uucp (mõningatel süsteemidel /etc/uucp). Versioon 2 UUCP korral leiate sealt faili L sys ja HoneyDanBer UUCP korral faili Systems. Versioon 2 UUCP-l on suured turvaaugud (viga uucico s, turbespetsiifiliste haldusfailide keerukuse tõttu võib esineda vigase konfiguratsiooni oht). Sellest tulenevalt tuleks kasutada HoneyDanBer UUCP-d.

UUCP kasutamisel tuleks arvestada järgmiste turbeküsimustega:

- UUCP haldus eeldab pidevat tegelemist konfiguratsioonivõimalustega ja sinna juurde kuuluvate failidega. Tuleb arvesse võtta, et erinevate Unixi versioonide UUCP pakettide vahel võib esineda erinevusi, isegi kui need põhinevad HoneyDanBer UUCP-l.
- UUCP failide, programmide ja kataloogide haldamisel kehtivad samad nõuded nagu süsteemifailide ja -kataloogide haldamisel (vt M 2.25 Süsteemi konfiguratsiooni dokumenteerimine , M 2.31 Volitatud kasutajate ja õiguste profiilide dokumenteerimine ja M 4.19 Unixi süsteemifailide ja -kataloogide atribuutide jaotuse piirangud).
- Enamikel süsteemidel on ainult üks kasutaja nimega uucp. Sellele kasutajale kuuluvad UUCP failid, programmid ja kaustad. See konto tuleb kindlasti kaitsta parooliga vastavalt meetmele M 2.11 Paroolide kasutamise reeglid .
- Kasutaja uucp kodukaustaks ei tohi olla avalik kaust /usr/spool/uucppublic vaid eraldi kaust, millele omab ligipääsu ainult kasutaja uucp.
- Igale IT-süsteemile, mis peab saama ennast UUCP kaudu lokaalsesse IT-süsteemi sisse logida, tuleb failis /etc/passwd sisestada kasutajatunnus ja parool. UID-na (User ID) ei tohi kasutada uucp oma, vaid igale IT-süsteemile tuleb valida oma UID.
- UUCP paroolid on salvestatud krüpteerimata vastavas UUCP eemal asuvate arvutite nõuete konfiguratsioonifailis ning edastatakse kommunikatsiooniprotsessi korral samuti krüpteerimata kujul. Sõltuvalt kasutusest ja keskkonnast (eelkõige laivõrkude kasutamise korral) tuleb kasutusele võtta vastavad turvameetmed, näiteks tuleks kasutada ühekordseid paroole. UUCP kasutamiseks tuleb luua erinevad konfiguratsioonifailid. Kõik seadistused tuleks

dokumenteerida ja erinevused järgnevalt kirjeldatud seadistustest põhjendada, et pärast oleks võimalik mõista, miks need muudatused olid vajalikud.

Järgmised failid sisaldavad konfidentsiaalseid andmeid, mistõttu tuleb neid hallata eriti hoolikalt. Need failid asuvad kaustas /usr/lib/uucp või /etc/uucp).

Sellele kaustale võib kirjutavat ligipääsu omada ainult kasutaja uusp:

- Systems: See fail sisaldab informatsiooni ühenduse loomiseks eemal asuvate IT-süsteemidega. Iga kasutatud IT-süsteemi tarvis saab määrata ajavahemiku, mille jooksul on lubatud UUCP andmevahetus. Need ajavahemikud peaksid olema võimalikult lühikesed. Lisaks sisaldab see fail IT-süsteemide telefoninumbreid ja sisselogimise jada, millega luuakse UUCP kaudu ühendus.

Kuna siia faili on kantud ka eemal asuvate IT-süsteemide paroolid, võib Systems faili lugemisõigus olla ainult uucp omanikul.

- Permissions: Selles failis määratakse eemal asuvate süsteemide ligipääsuõigused. Tarnimisel ei sisalda Permissions ühtegi IT-süsteemi, see tähendab, et UUCP kaudu puudub ligipääs. Igale arvutile, kes tohib sisse helistada ja ennast sisse logida, ning igale arvutile, kellele tohib helistada, tuleb selles failis teha seadistused ehk määrata vastavad ligipääsuõigused ja teised tingimused. IT-süsteemide, millele helistatakse lokaalselt IT-süsteemilt, ligipääsuõigused määratletakse MACHINE le järgnevates sissekannetes ja sissehelistavad IT-süsteemid määratletakse LOGNAME ile järgnevates sissekannetes. Selle konfiguratsioonivõimaluse kasutamisel saab turvalisust märgatavalt tõsta.

Käsklusega uucheck-v peaks failis Permissions määratud suvandeid regulaarselt kontrollima.

Suvandid peaksid olema järgmised:

- **REQUEST -** Selleks et keelata eemalolevatel süsteemidel lokaalsete failide lugemine, peaks selle suvandi puhul olema valitud NO (vaikeväärtus).
- **COMMANDS** - Lubada tohib ainult käsklusi, nagu rnews või rmail , mitte mingil juhul ei tohi olla sisse kantud ALL. Käsklused peaksid olema märgitud täispikkuses rajanimega (Pathname).
- **WRITE/READ** - Kui neid suvandeid ei kuvata, on kirjutav ja lugev ligipääs võimalik ainult kataloogile /usr/spool/uucppublic. Kui sellega määratakse kataloogid, millele ligipääs lubatakse, tuleb dokumenteerida, millisel viisil ja miks. Mingil juhul ei tohi olla siin sisse kantud root kataloog ja kataloog, milles paiknevad UUCP konfiguratsioonifailid.
- **NOWRITE/NOREAD** - Sellega määratakse WRITE/READ-iga kindlaks määratud suvandite erandid. Siia tuleks märkida konfidentsiaalse sisuga kataloogid. See välistab, et piirangute määramise unustamisel teiste IT-süsteemide ligipääsu konfidentsiaalsetele failidele, kui kataloogipuus ülal pool paiknevatel failidel on READ/WRITE õigused.

- **PUBDIR** - Sellega saab /usr/spool/uucppublic asemel määratleda mõne muu avaliku UUCP kataloogi. UUCP kommunikatsiooni korral mitme IT-süsteemiga tuleks iga IT-süsteemi jaoks luua eraldi UUCP kataloog.
- **CALLBACK** - Kui CALLBACK on aktiveeritud (YES), peab lokaalne IT-süsteem helistavale IT-süsteemile enne andmeside toimumist tagasi helistama. See on mõttekas ainult LOGNAME sissekannete korral. Kommunikatsioonipartnerid peaksid kokku leppima, kes neist aktiveerib CALLBACK funktsiooni.
- **MYNAME** - Kui MYNAME=name , siis identifitseerib lokaalne süsteem end UUCP ühenduse loomisel eemal oleva süsteemi suhtes mitte arvutinimega, vaid määratud nimega (name). Seda võimalust tuleks kasutada, et ennast identifitseerida nimega, mida kasutatakse ainult selle ühenduse korral ja mida seetõttu ei ole nii kerge välja uurida.
- **VALIDATE** - Kui VALIDATE=name, saavad LOGNAME all märgitud süsteeminimede kaudu ühenduse luua ainult name all märgitud IT-süsteemid. Selle suvandi all peab ilmtingimata esinema sissekanne, kuna vastasel juhul võib mõni eemal asuv IT-süsteem ennast MYNAME kaudu mõne muu arvutinimega esitleda.
- **SENDFILES** - Siin tuleks säilitada vaikeseadistus (SENDFILE=CALL), sest siis edastatakse lokaalses allikas paiknev ülesanne välisvõrku juhul, kui ühendus on loodud lokaalse võrgu poolt.
- **HoneyDanBer** UUCP fail /usr/lib/uucp/remote.unknown käitatakse, kui ühendust üritab luua IT-süsteem, mis ei ole faili Systems sisse kantud. See protokollib ning keelustab selle. Kui remote.unknown ei ole käitatav, teostab lokaalne IT-süsteem kõik väliste IT-süsteemide ühenduse loomise üleskutsed. Sellest lähtuvalt tuleb kindlustada, et remote.unknown oleks alati käitatav.

Remote.unknown on vastavalt Unixi süsteemile realiseeritud kas täidetava Shell Script ina või C-programmina. Kui remote.unknown on lokaalsel IT-süsteemil realiseeritud Shell Script ina, tuleks see turvalisusest lähtudes asendada programmiga.

Vastasel juhul esineb oht, et sissehelistav IT-süsteem sisestab süsteeminimena käskluse nagu „cat < /etc/passwd“, mis võidakse järgnevalt teostada.

- UUCP jaoks on mõningad Clean Up Schell Script id, mis teostatakse automaatselt deemoni crontab kaudu. Seda ei tohi käivitada root , nagu see paljudel süsteemidel tavaline on, vaid seda peab tegema kasutaja uucp.
- UUCP kasutamisel salvestatakse erinevad logiandmed automaatselt. HoneyDanBer UUCP korral paiknevad need /usr/spool. alamkataloogides. Siin salvestatakse edukad ja keelatud ühenduskatsed, saadetud ja vastuvõetud andmemahud, veateated ja andmesidestatistikad. Neid logiandmeid tuleb regulaarselt analüüsida (vt M 4.25 Logimine Unix-süsteemis).

Kontrollküsimused:

- Kas administraator on saanud UUCP kasutamise alase väljaõppe?

- Kas on olemas UUCP kasutusjuhendid?
- Millist UUCP varianti kasutatakse?
- Kas konfiguratsioonifailide seadistus on dokumenteeritud?
- Kas UUCP logifaile kontrollitakse regulaarselt?

M 5.39 Protokollide ja teenuste ohutu kasutamine

Algatamise eest vastutavad: IT-juht, infoturbespetsialist

Rakendamise eest vastutavad: infoturbespetsialist, administraator

Järgnev lühike internetis kasutatavate protokollide ja teenuste kirjeldus peaks näitama, millist informatsiooni nende protokollidega edastatakse ja kuidas tuleb turvalüüsi vastavalt sellele seadistada. Lisaks on lühidalt kirjeldatud raamtingimusi, mida tuleb erinevate protokollide ja teenuste kasutamisel täita.

ISO/OSI turbemudeli sügavamate kihtide alusprotokollid

IP

Internetiprotokoll (IP) on protokoll, millel põhinevad peaaegu kõik lokaalse võrgu protokollid. IP on ühenduseta protokoll IP-päis sisaldab muu hulgas kahte 32-bitilist aadressi (IP aadress) omavahel suhtlevate arvutite sihiks ja allikaks. Kuna IP-aadresse on võimalik kergesti võltsida (vt G 5.48 IP-aadressi võltsimine), võib neid autentimiseks kasutada ainult olukordades, kus on kindlustatud, et aadresse ei ole võimalik muuta. Näiteks ei tohi turvalüüs läbi lasta pakette, mis tulevad väljastpoolt, kuid omavad kaitstava võrgu saatja-aadressi.

APR

Aadressiteisenduse protokolli (*Address Resolution Protocol* - ARP) kasutatakse selleks, et leida 32-bitilisele IP-aadressile vastav 48-bitiline MAC-aadress (*Media Access Control* ka riistvara või *Ethernet* aadress). Iga arvuti peab teiste jaamade (*Station*) jaoks oma levipiirkonnas tabelit, milles on salvestatud IP- ja riistvara aadressi kuuluvus. Kui selles tabelis vastavat sissekannet ei leita, saadetakse välja IP-aadressiga ARP leviedastuspakett, millele otsitakse MAC-aadressi. Vastava IP-aadressiga arvuti saadab ARP vastuspaketiga tagasi oma MAC-aadressi. ARP vastuspaketid ei ole manipuleerimiskindlad (ARP-spuufing, vt G 5.112 ARP-protokolli tabelitega manipuleerimine).

ICMP

Interneti kontrollsõnumiprotokolli (*Internet Control Message Protocol* - ICMP, spetsifitseeritud RFC 792) ülesandeks on vea- ja diagnoosiinformatsiooni transportimine IP jaoks. Süsteemisiseselt töötleb ja käivitab selle IP, TCP või UDP. ICMP-protokoll teab erinevateks otstarveteks mitmeid erinevaid nn. uudistetüüpe. Vastavalt kasutusstsenaariumile tuleks kindlad ICMP uudistetüübid valikuliselt lubada või blokeerida. ICMP-protokolli käsitluseks turvalüüsis vaata M 5.120 ICMP-protokolli käsitlus turvalüüsis .

Marsruutimisprotokoll

Marsruutimisprotokolle nagu RIP (*Routing Information Protocol*) või OSPF (*Open Shortest Path First*) kasutatakse kahe võrgu kaudu seotud süsteemi vaheliste marsruudi muutuste edastamiseks seotud süsteemidele, võimaldades nii marsruutimistabelit dünaamiliselt muuta. Lihtne on luua valesid RIP pakette ja konfigureerida seeläbi soovimatuid marsruute. Seetõttu tuleks dünaamilist marsruutimist kasutada ainult kindlates olukordades. Turvalüüsis tuleks marsruudiprotokolle kasutada ainult vajalikus mahus. Võimaluse korral tuleks kasutada ainult turvalisi marsruutimisprotokolle. Lisainformatsiooni leiab punktist M 5.112 Marsruutimisprotokollide turvaaspektide arvestamine .

UDP

Kasutajadatagrammi protokoll (*User Datagram Protocol* - UDP) on transpordikihi ühenduseta protokoll. Ülekande õigsuse kontrolliks puuduvad turbemeetmed. Päis sisaldab (sarnaselt TCP-le) teiste hulgas kahte 16-bitilist pordinumbrit, mis on aga sõltumatud TCP poolt kasutatud pordinumbritest. Kuna neid on lihtne võlt-

sida, saab neid autentimiseks kasutada ainult kindlates olukordades. Protokollides ei ole määratletud erinevust ühenduse loomise ja andmeside vahel, mistõttu peab selle ülesande teostama osa turvalüüsist. Võimalik peab olema ühenduse oleku kontroll ning samuti peab olema võimalik liigitada kindel pakett kindlale ühendusele. See on saavutatav näiteks siis, kui UDP ühenduse loomisel on sihtport salvestatud ja ajutiselt vabaks antud, kui vastusepakette lastakse ainult selle pordi juurde ja pärast ühenduse lõpetamist või pärast *timeout* i port suletakse.

Rakenduse kihi protokollid

DNS

Domeeninimede teenust (*Domain Name Service* - DNS) kasutatakse arvutinimede teisaldamiseks IP-aadressideks ja vastupidi ning see võimaldab näha informatsiooni võrgus olevate arvutisüsteemide kohta. DNS-i on võimalik kasutada nii TCP kui ka UDP kaudu. Server kasutab mõlemal juhul kandjapordina porti 53. Enamasti kasutatakse kandjaprotokollina UDP-d. Ülekantud informatsioon ei ole krüpteeritud, nii et võltsitud andmete abil on võimalikud spuufingu rünnakud (vt G 5.78 DNS-i võltsimine). Seda tuleks eelkõige arvesse võtta internetist saabuvate DNS-vastuste korral. Üldiselt tuleb arvestada sellega, et kogu DNS-i poolt võimaldatavat informatsiooni on võimalik kuritarvitada. DNS-i integreerimine turvalüüsi on vajalik (vt M 2.77 Serverite integreerimine tulemüüri ja M 5.118 DNS-serveri integreerimine turvalüüsi koostisse).

SMTP

Lihtsat meiliedastusprotokolli (*Simple Mail Transfer Protocol* - SMTP) kasutatakse e-mailide edastamiseks. SMTP-server (nimetatud ka meiliserver või *Mail Transport Agent* - MTA) kasutab standardina porti 25. SMTP, mida defineeritakse RFC 82, koosneb vähestest käsklustest, mis on mõnedel juhtudel turbe seisukohast murettekitavad. Käskudega *VERFY* ja *EXPN* saab esitada näiteks päringuid kasutajatesisese informatsiooni kohta, mistõttu peaks nende käskude kasutamine olema lubatud ainult kaitstud võrgus. Ebausaldusväärsetele kasutajatele, eelkõige internetist tulevatele päringutele tuleb *VRFY* ja *EXPN* kas ALG-l (*Application Level Gateway*) või otse MTA-l (*Mail Transport Agent, Mail Server*) keelata. Ideaalis peaks turvalüüs olema võimeline krüpteerima usaldusväärsete kasutajate vahelist SMTP ühendust. Mõttekas on see ainult juhul, kui kasutatakse rangeid autentimismehhanisme.

HTTP

Hüperteksti edastusprotokolli (*HyperText Transport Protocol* - HTTP) kasutatakse andmete ülekandmiseks veebiklientide (enamasti veebibrauserite) ja veebiserverite vahel. HTTP ja mitmed laiendused on määratletud RFC-des, RFC 2616, milles on spetsifitseeritud HTTP aktuaalne variant 1.1, sisaldab mitmeid viiteid ja vanemaid dokumente. Standardina kasutab veebiserver TCP porti 80. HTTP on avatekstprotokoll, mis ei võimalda turvalist autentimist ega garanteeri edastatud andmete konfidentsiaalsuse ja tervikluse säilimist. Sellega tuleks arvestada HTTP-ga ülekandeid tehes. Lisainformatsiooni leiate M 4.100 Tulemüür ja aktiivsisu ja M 4.222 Turvaprokside õige konfigureerimine .

HTTPS

HTTPS (HTTP üle SSL-i või HTTP üle TLS-i) on HTTP variant, mille korral saab autentimist ja andmete ülekandmist krüpteerimisega ja sertifikaatidega kaitsta. HTTPS spetsifitseeritakse RFC 2818. Enamasti kasutab HTTPS toega veebiserver TCP porti 443. HTTPS kasutamisel tuleb arvestada, et TLS toetab ka režiimi, kus ei toimu krüpteerimist. Vastavate turbenõuete korral tuleks HTTPS proksil keelata vastavate ühenduste loomine. Lisainformatsiooni leiate meetmetest M M

4.100 Tulemüür ja aktiivsisu , M 4.222 Turvaprokside õige konfigureerimine ja M 5.66 TLS-i/SSL-i kasutamine .

Turvakest (*Secure Shell*)/turvakoopia (*Secure Copy*)

Turvakesta (*Secure Shell* - SSH) protokoll lubab turvalise käsuriba ühenduse loomist eemaloleva arvutiga SSH protokoll võimaldab turvalist autentimist erinevate autentimismehhanismidega (teiste hulgas kasutajanime ja parooli kaudu, spetsiaalsete sertifikaatidega, keskselt hallatud PKI infrastruktuuri kaudu või *Kerberos* e kaudu). SSH sobib seega *Telnet* i asendajaks. Võimaluse korral tuleks *Telnet* asendada SSH-ga. Standardina kasutab SSH-server TCP porti 22. SSH protokollide hulka kuulub ka SCP protokoll (*Secure Copy Protocol*), mis kasutab andmete edastamisel SSH autentimis- ja krüpteerimismehhanisme. SCP on FTP turvaline alternatiiv. SSH-le esineb hulk juurutamisvõimalusi pea kõigile üldlevinud operatsioonisüsteemidele ja lisaks veel operatsioonisüsteemist sõltumatuid juurutamisvõimalusi, näiteks *Java* . Erinevad juurutamisvõimalused erinevad üksteisest osaliselt autentimismehhanismide arvu ja teiste detailide poolest. Enamik SSH kliente pakub lisaks võimalust olemasoleva SSH ühenduse kaudu teisi protokolle nö. tunneldada, et sel moel vältida näiteks avatekstprotokolli puudusi. Teisest küljest kaasneb sellise funktsiooniga ka risk, kuna seeläbi on võimalik andmeedastusi „peita". SSH kasutamisel tuleks seepärast hoolikalt kontrollida, milliste kommunikatsioonipartneritega ühendusi lubatakse. Vajadusel tuleks kasutada turbeproksi, mis katkestab turvalüüsis krüpteeritud ühenduse. SSH-protokolli algsel versioonil (ssh1) oli viga, mis lubas *Man-in-the-Middle* tüüpi rünnakutes osalemist. Sellel põhjusel loodi protokolli uus versioon (ssh2), milles see viga parandati. *Ssh1* -i ei tohiks, vähemasti avalikes võrkudes, enam kasutada. Kui SSH jaoks paigutatakse turvalüüsi turbeproksi, siis peaks antud proks võimaldama *ssh2* ühenduste loomist ega tohiks lubada *ssh1* ühendusi.

Telnet

Telnet spetsifitseeritakse RFC 854. Sarnaselt SSH-le lubab *Telnet* terminalistungite loomist eemal olevate arvutitega. *Telnet* on avatekstprotokoll, mis ei võimalda ühtegi moodust autentimisinformatsiooni ja andmeedastuse või käskluste turbeks. *Telnet* -server kasutab tavaliselt TCP porti 23. Kuna *Telnet* lubab käsurea täieliku ligipääsu arvutile, kuid ei paku seejuures turvamehhanisme, tuleks *Telnet* võimaluse korral alati asendada SSH-ga. Alternatiivina võib *Telnet* ühendusi kasutada SSH kaudu. Kui mõjuvatel põhjustel ei ole *Telnet* i asendamine SSH-ga või tunneldamine võimalik, võib sisevõrgus jätkuvalt kasutada *Telnet* i. Seejuures tuleks lubatud kommunikatsioonisidemed vastavate paketi filtreerimise reeglitega minimeerida. Süsteemi haldamiseks tohiks *Telnet* it kasutada ainult spetsiaalselt eraldatud haldusvõrgus. Ründajal, kes omab ligipääsu võrguosadele, mille kaudu vastav ühendus käib, võib *Telnet*- ühenduse üle võtta (vt G 5.89 Võrguühenduse ülevõtt). *Telnet*i ei tohiks avalikes võrkudes kasutada ka siis, kui kasutuses olev *Telnet*- server on laiendatud autentimismehhanismidega, nagu näiteks ühekordsed paroolid.

FTP

Failiedastusprotokoll (*File Transfer Protocol* - FTP) spetsifitseeritakse RFC 959. See võimaldab FTP failide edastamist kaugel asuvate arvutite vahel. Nagu *Telnet*, ei võimalda ka FTP avatekstprotokoll ülekantava autentimisinformatsiooni ja andmete krüpteerimist. FTP kasutamisel luuakse kaks ühendust, kus TCP port 21 edastab käsklused ja TCP port 20 andmed. *Telnet* määratleb teatud arvu standardkäske, mille abil on võimalik juhtida andmeside viisi ja vormi ning mis võimaldavad FTP kliendil liikuda FTP-serveri kataloogipuus. Turvalüüsile on need

standardkäsud olulised, sest ainult need edastatakse. FTP käskühendus luuakse kliendi poolt serveri pordiga 21. Andmeedastuseks on FTP-s kaks käitusrežiimi, *Active* ja *Passive Mode. Active Mode* korral loob FTP-server ühenduse kliendiga, *Passive Mode* korral loob ühenduse klient. *Active Mode* kujutab endast turvariski, kuna ründaja võib näidata ennast serverina ja saada seeläbi võimaluse luua ühendus sisevõrguga. FTP kasutamisel tuleks seda teha alati *Passive Mode* 'i kasutades, mille korral toimub käskluste edastamine ja andmeside kaitstud sisevõrgust välisvõrku. Kõik käsud, mis faile või katalooge loevad või nendega manipuleerivad (*CWD, CDUP, RETR, STOR, DELE, LIST, NLIST*), peavad olema seotud vastava õigushaldusega. Ebausaldusväärsete kasutajatele antakse ligipääs vaid kindlatele failidele või keelatakse ligipääs täielikult. See eeldab tugevat autentimismehhanismi. Ka käsk *SYST,* millega klient saadab päringu serveri operatsioonisüsteemi versiooni kohta, peaks olema seotud vastava õigushaldusega ja ebausaldusväärsetele kasutajatele suletud. Hiljem peab olema võimalik failide, kataloogiinformatsiooni ja paroolide edastamist krüpteerida.

FTP-d ei tohiks kasutada konfidentsiaalsete failide edastamiseks avalike võrkude kaudu. Kui konfidentsiaalseid faile edastatakse välise FTP ühenduse kaudu, tuleb neid kaitsta teiste vahenditega, näiteks krüpteerimise kaudu. Võimalusel tuleks FTP asendada mõne turvalise protokolliga, näiteks SCP-ga. FTP-d kasutatakse tihti andmete kuvamiseks avalikelt serveritelt. See ei ole kriitiline, kui selleks ei kasutata autentimisinformatsiooni, mida kasutatakse ka teistel süsteemidel (näiteks *anonymous FTP*) ja kui ei esitata nõudeid laaditud failide terviklusele ja autentsusele (näiteks informatsiooni laadimine). Kui andmete terviklus ja autentsus on oluline (näiteks programmide allalaadimine, paigad või tähtsad dokumendid), tuleks tootjatel kasutusele võtta digitaalallkirjad, mille abil saab andmete õigsust kontrollida.

POP3 ja IMAP

Protokolle POP3 (*Post Office Protocol* versioon 3, spetsifitseeritud RFC 1939) ja IMAP (*Internet Message Access Protocol,* spetsifitseeritud RFC 3501) kasutatakse meiliklientide poolt selleks, et meile meiliserverilt alla laadida (POP3) või hallata (IMAP). Protokollide standardpordid on port 110/TCP (POP3) ja 143/TCP (IMAP). Mõlemad protokollid on avatekstprotokollid ega sobi seega avalikes võrkudes kasutamiseks. Mõlema protokolli puhul on olemas variandid, mille korral kaitstakse ühendust krüpteeringuga (SSL, TLS). POP3 (standardport 995/TCP) ja IMAP (standardport 993/TCP). Juhul kui meile hallatakse sisevõrgus, tuleks ikkagi kasutada POP3-e ja IMAP-i turvalist varianti. Kui meile tahetakse laadida väliselt POP3- või IMAP- serverilt (näiteks meiliteenuse pakkujalt), tuleks kasutada protokollide turvalisi versioone, vajadusel krüpteeritud ühenduse katkestamisega vastaval turvaproksil.

Veel teenuseid

Jaotatud failisüsteemid

Jaotatud failisüsteemid, mille korral ei salvestata andmeid lokaalselt arvutil, vaid failiserveril, ja millele pääsetakse ligi võrgu kaudu, on juba ammu olemas ning IT-maailm ei oleks ilma nendeta enam mõeldav. Kõige levinum näide on ketta jagamine Microsoft Windowsi all, mis põhineb SMB / CIFS protokollil (*Server Message Block/ Common Internet File System*). Koos Sambaga on seda protokolli võimalik juurutada paljudel Unix-versioonidel. Unixi maailmas realiseeritakse jaotatud failisüsteeme juba ammu võrgu-failisüsteemi kaudu (*Network File System* - NFS). NFS-i saab kasutada ka Windowsi all. Peale selle on olemas veel hulk teisi jaotatud failisüsteeme, nagu näiteks AFS (*Andrew File System*). Jaotatud failisüs-

teeme ei tohiks kasutada väljaspool turvalist võrku, kuna nendega kaasneb hulk probleeme (autentimise turvalisus, edastatud andmete turvalisus), mis muudavad kasutamise välises võrgus keeruliseks. Kui erandjuhtudel on ligipääs jaotatud failisüsteemile ikkagi vajalik, tuleks seda turvata VPN-iga.

Kaugarvuti protokoll (*Remote Desktop Protocol*) (Windows Terminal Server, X-Windows jne)

Nii Microsoft Windows kui ka X Windows süsteemid, millega Unixi all realiseeritakse graafilisi pindu, võimaldavad kuvada üksikuid aknaid või kogu töölauda eemalolevas arvutis. Kaugarvuti protokolli, mis ei paku kaitset või pakub vaid nõrka kaitset, võib sisevõrgus kasutada ainult erandjuhtudel ja turvalüüsist kaugemal välisvõrgus ei tohiks kaugarvuti protokolli põhimõtteliselt kasutada. Kui seda tuleb erandjuhtudel ikkagi teha, tuleb kasutusele võtta lisameetmed, näiteks kasutada VPN-i (virtuaalne privaatvõrk), mis võimaldab kasutada vastava turvalist ühendust.

Voogedastusprotokoll

Multimeedia andmete (voogaudio ja voogvideo) edastamiseks on olemas hulk protokolle, mis erinevad üksteisest ribalaiuse (*bandwidth*) ja kasutatavate portide poolest. Kuna neid protokolle on halb paketi filtreerimise reeglitega kindlustada, on enamik neist turvalüüsi jaoks problemaatilised. Kahtluse korral tuleks voogedastusrakendustest loobuda või kindlaid pakkumisi saab eraldatud internetiarvutite kaudu esitada(vt B 3.208 Interneti-PC).

IP-kõne (VoIP)

Verbaalseks suhtlemiseks IP-võrkude kaudu on mitmeid võimalusi (*Voice over IP,* VoIP). VoIP-lahenduste puhul on enamasti vajalikud mitu erinevat protokolli, näiteks erinevad protokollid signaliseerimiseks ja kõneandmete edastamiseks. VoIP lahendused (näiteks sellised, mis vastavad H. 323 standardile) on turvalüüsidele tihtipeale probleemsed, kuna erinevad pordid toimivad lõppseadmete vahel osaliselt dünaamiliselt ja seetõttu ei ole võimalik seda lihtsustatult pakettfiltri kaudu turvata. Kui soovitakse kasutada VoIP teenust, mille korral üks sidepartneritest paikneb väljaspool enda (turvalist) võrku, on vajalik turvameetmete ülevaatus, et vältida VoIP lahenduse nõuete tõttu turvalüüsi seadistuse leevendada ja sellega kaasnevat ohtu võrgule.

NTP

RFC 1305 spetsifitseeritud võrguaja protokolli (*Network Time Protocol* - NTP) kasutatakse ajaserverilt täpse aja saamiseks. Kui sisevõrgus kasutatakse serverite ja turvalüüsi komponentide aja sünkroniseerimiseks NTP-d, siis tuleks võimalusel kasutada eraldi ajaserverit sisevõrgus või turvalüüsis. Mõningatel juhtudel võib kasutada ka NTP-proksi, mis saab oma andmed ühelt keskselt ajaserverilt ja toimib sisevõrgus olevatele arvutitele ajaserverina (vt M 4.227 Lokaalse NTP -serveri kasutamine aja sünkroniseerimiseks).

NNTP

RFC 977 spetsifitseeritud *Network News Tranfer Protocol* (NNTP) on kasutuses uudiseartiklite ülekandmisel. Uudisteserver kasutab tavaliselt TCP porti 119. Nagu kõik teised „varajased" internetiprotokollid, on ka NNTP avatekstprotokoll. Sisese uudisteserveri käitamisel või sisevõrgust välistele uudisteserveritele ligipääsemisel, peab turvalüüs olema võimeline takistama teatud uudistegruppide transporti või lubama neid ainult teatud arvutitele. Tuleb kindlustada, et enda loodud uudiste saatmisel ei satuks välisvõrku informatsiooni kaitstava võrgu kohta (näiteks arvutite nimed).

r-teenused

Nn „r-teenused” nagu *rlogin, rsh, rcp* ja teised põhinevad UDP-l ja ei võimalda turvalist autentimist ega ühenduse kaitset. Neid teenuseid tuleks ka sisevõrgus kasutada ainult erandjuhtudel. Neid tohib kasutada ainult kaitstud võrgu piires. Turvalüüs peaks vastavad paketid blokeerima. Enamikel kasutusjuhtumitel on SSH täisväärtuslik asendus „r-teenustele”.

Juhised nn. “priviligeeritud portide” kohta

TCP/IP kommunikatsiooni korral loob klient suvaliselt pordilt pordinumbriga > 1023 ühenduse serveriga, mille pordinumber on < 1024 (*well known port*). Porte numbriga < 1024 nimetatakse priviligeeritud portideks, sest näiteks Unixi all tohib neid kasutada ainult *root*- õigustega protsessideks. Piirang, mille korral tohib porti < 1024 kasutada ainult root- õigustega, on ainult teatud tava, millest on võimalik mööda minna ja mis ei mängi mingit rolli, kui ründaja on arvuti võtnud oma kontrolli alla. Seetõttu ei tohi turvakontseptsioonis eeldada, et kõik IT-süsteemid kaitsevad oma privilegeeritud porte sellisel moel. Isegi kui FTP-ga saadakse juurdepääs portidele 20 ja 21, ei tohi seda vaadelda kui turvalist ühendust.

Täiendav kontrollküsimus:

- Milliseid protokolle kasutatakse turvalüüsi kaudu?

M 5.44z Ühesuunaline ühenduse loomine

Algatamise eest vastutavad: infoturbeosakond

Rakendamise eest vastutavad: administraator

Reeglina on ühel modemil võimalik kasutada vaid ühte telefoniühendust. Selle telefoniühenduse kaudu algatab modem väljuvad kõned ja võtab vastu sissetulevad kõned.Selleks, et ükski ründaja ei saaks ühendatud IT-süsteemile märkamatult ligi pääseda, tuleks kasutada vähemalt tagasihelistusmehhanismi (Callback) (vt M 5.30 Olemasoleva tagasihelistusfunktsiooni aktiveerimine). Aktiveeritud tagasihelistamisest hoolimata võib siiski esineda probleem, et sisenev kõne ei katke enne, kui helistaja kõne lõpetab. Avalik ühenduspunkt sulgeb sellise ühenduse alles teatud aja möödudes.See probleem esineb esmajoones siis, kui pole ühtki kodukeskjaama, mis ühenduse täiendavalt katkestaks. Seeläbi suudab ründaja käivitada tagasihelistamise, kuid samal ajal ka liini hõivatuna hoida, mis tähendab, et modem teeb küll õigesti ja valib tagasihelistamiseks õige salvestatud numbri, kuid ühendus ründajaga ei katke.

Selle takistamiseks tuleb kontrollida, kas sisenev ühendus katkestatakse ka siis, kui helistaja ise kõnet ei lõpeta. Kui seda ei tehta ja lisaks pole ka võimalik tagada, et hooldaja kõiki modemiühendusi jälgib, tuleks kaaluda võimalust kasutada eraldi telefoniühendusi ühesuunalise ühenduse jaoks, st kasutada ühte eraldi ühendust väljuvate ja ühte eraldi ühendust sisenevate ühenduste jaoks. Selleks vajab iga ühendus eraldi modemit ja rakenduse kaudu tagasihelistamise sundimist. Arvestage, et väljuvate ühenduste modem ei võta kõnesid vastu automaatselt (S0=0 , st automaatvastamine puudub). Selleks, et sisenevate ühenduste modem ei saaks luua väljuvaid ühendusi, tuleb vastava modemi väljuvad ühendusvõimalused kas sisemises kodukeskjaamas blokeerida või paluda vastavat blokeeringut sideoperaatorilt.

M 5.45 Veebibrauserite turvaline kasutamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator, kasutaja

Brauserid on veebilehtede kuvamise programmid. Brausereid ei kasutata mitte ainult tööarvutites, vaid ka mobiilsetes seadmetes, nt PDA-des ja mobiiltelefonides. Erinevate meediavormingute kuvamine ja taasesitamine ei sõltu brauseritel operatsioonisüsteemist, kuid osaliselt läheb selleks tarvis pluginaid ja lisasid (addons). Pluginad ja lisad võivad väärkasutuse, ebapiisava konfiguratsiooni või programmeerimisvigade tõttu põhjustada turbeprobleeme. Lokaalseid andmeid ohustavad näiteks programmid, mis laaditakse internetist alla ja installitakse lõppseadmesse kasutajalt luba küsimata (nt ActiveX-i programmid, Java). Ka dokumendid, pildid või animatsioonid võivad sisaldada kahju tekitavaid käske, mis käivitatakse automaatselt nende failide avamisel. Suur hulk funktsioone toovad endaga kaasa keerukad konfiguratsioonivõimalused ja võimalikud turbeprobleemid. Kirjeldatud probleemide vältimiseks tuleks võtta järgmised meetmed.

Baasfunktsioonid

Enamiku brauserite vaikeseadistus on tihti ebaturvaline. Seetõttu tuleks esmalt viia brauseri turbeseadistused vastavusse institutsiooni nõuetega.

Väliste failide käivitamine

Väliste failide ja/või programmide käivitamisel võib esineda suur hulk turbeprobleeme, nt kahjurvara käivitus. Kasutajad ei saa interneti kasutamisel kunagi kindlad olla, et allalaaditud failid ja programmid pärinevad usaldusväärsetest allikatest. Kasutajatel on raske hinnata, kas internetis olevad andmed on usaldusväärsed ning ega neid manipuleeritud ei ole. Kuna allalaaditavad failid võivad sisaldada kahjurvara, tuleb brauseri konfigureerimisel jälgida, et failide allalaadimisel ei käivitataks automaatselt sinna juurde kuuluvaid rakendusi (vt M 4.3 Viirusetõrjeprogrammide kasutamine). Failid tuleks esmalt salvestada ja seejärel neid kahjurvara suhtes kontrollida ning alles siis käivitada. Alternatiivse variandina võib kasutada vaatajaid (viewer), mis näiteks Office'i dokumentide makrosid ei käivita. Kasutajate tähelepanu tuleb juhtida sellele, et failide allalaadimisel vastutavad nad kõikide vajalike ettevaatusabinõude eest ise. Vaatamata kõigile ettevaatusabinõudele jääb institutsioonis alles ikkagi mõningane jääkrisk.

Pluginad ja lisaprogrammid

Leidub mõningaid failivorminguid, mida brauserid ei ole võimelised otse töötlema. Selliste failivormingute käivitamiseks tuleb kasutada lisaprogramme, mida pakuvad sageli kolmandad tootjad, ning brauseriga integreeritakse need pluginate või lisade näol. Faili ei kuvata sel juhul enam eraldi aknas, vaid otse brauseris. Levinud pluginad ja lisad on nt Flash Player ja Java. Lisaprogrammid, nt vaataja (viewer), on iseseisvad programmid, mis töötlevad kindlaid failivorminguid. Sellise lisaprogrammi käivitumist juhitakse brauseri konfiguratsioonifailidega, kus on ühendatud failitüüp ja programm. Programmide installimisel tuleb järgida institutsiooni turbereegleid. Installida tohib ainult katsetatud ja kasutusse lubatud programme. Enne installimist töökeskkonda tuleks programmide veatust kontrollida eraldiseisvates arvutites. Tarkvara installimise õigus peaks olema ainult administraatoritel (vt M 4.65 Uue riist- ja tarkvara testimine ja M 4.177 Tarkvarapakettide tervikluse ja autentsuse tagamine). Kuna iga lisatud programm kujutab

endast turberiski, tuleks installida ainult ilmtingimata vajalikud pluginad, lisad ja lisaprogrammid.

Aktiivsisu

Enamik interneti kasutamise turbeprobleeme on seotud aktiivsisuga, nt JavaScripti, ActiveX-i, Flashi või Javaga, samuti teiste pluginate ja lisadega. Aktiivsisusid käivitatakse brauseri kaudu klientsüsteemis, mitte serveris. Nõnda võivad klientsüsteemis tekkida turbeprobleemid. Sisevõrgu kaitseks internetist pärineva aktiivsisu eest tuleks võimaluse korral loobuda aktiivsisu käivitamisest (vt M 5.69 Aktiivsisu tõrje).

Krüpteerimine

Edastusprotokoll HTTP (Hypertext Transfer Protocol) edastab kõik andmed avatekstina. Seetõttu ei ole tagatud edastatava info konfidentsiaalsus. Isegi kui veebilehed on kaitstud parooliga, ei tähenda see automaatselt, et autentimisandmed edastatakse krüpteeritult. Kui veebilehele tuleb sisestada konfidentsiaalne info (nt krediitkaardinumber või pangainfo või ka lihtsalt isikuandmed), tuleks kasutada HTTPS-iga krüpteeritud ühendust (vt M 5.66z SSL-i/TLS-i kasutamine kliendis).

Olemasolevate turbefunktsioonide kasutamine

Alati tuleks kasutada brauseri olemasolevaid turbefunktsioone (eelkõige küsimuse esitamist enne programmide käivitamist). Brauserite ründamise ja ärakasutamise võimaluste vähendamiseks tuleks aktiveerida ainult sellised funktsioonid, mis on ülesannete täitmiseks hädavajalikud. Süsteemiadministraator ei saa pidevalt kontrollida kõikide meetmete võtmist, nt kindlate suvandite aktiveerimist, mistõttu on osa ülaltoodud meetmetest kasutajate vastutada. Võimaluse korral peaks haldusosakond võtma meetmeid, mis raskendavad kasutajatel teatud seadistuste muutmist või keelavad selle täielikult. Näiteks võib mõningate programmide konfiguratsioonifaili kaitsta kirjutuskaitsega. Süsteemi haldajad peavad turvalise eelseadistusega hoolitsema selle eest, et võimalikult hea turve oleks tagatud ka kasutajate sekkumiseta.

Turvaaukude kohta info hankimine

Kuna sageli teatatakse uutest turvaaukudest brauserites, tuleb regulaarselt hankida infot nii turvaaukude kui ka nende kõrvaldamise kohta. Esmatähtis ei ole iga toote kõige uuema versiooni hankimine, sest uute programmiosadega võivad kaasneda omakorda uued turvaaugud. Kõikidel juhtudel tuleks paikade installimisega tagada teadaolevate turvaaukude kõrvaldamine (vt M 2.273 Turvalisust mõjutavate paikade ja värskenduste kiire paigaldamine). Seejuures ei tohi unustada, et paikasid ilmub ka pluginatele ja lisadele. Need tuleb samuti kohe installida. Kui brauseriga kasutatakse ettevõtte tähtsaid rakendusi või kui käideldavuse turbevajadus on tavalisest suurem, tuleks turvapaikasid enne paigaldamist katsesüsteemis katsetada. Seejuures tuleks kontrollida, kas ei esine mingisuguseid kõrvalmõjusid, mis võiksid häirida turvalist ja tõrkevaba käitust.

Kontrollküsimused:

- kas brauseri turbeseaded viiakse kooskõlla institutsiooni vajadustega?
- kas väliste veebilehtede käivitamisel võetakse kasutusele ettevaatusabinõud?

M 5.46 Autonoomsüsteemide installeerimine interneti kasutamiseks

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: administraator

Vähendamaks Internetist lähtuvate rünnete ohtu kohtvõrgu lokaalsetele andmetele või arvutitele, oleks mõistlik kasutada arvuteid, mis on ühendatud ainult internetiga, st mille puudub ühendus kohtvõrguga. Erinevad operatsioonisüsteemid pakuvad selleks erinevaid võimalusi, millega kaasnevad ka erinevad ohud arvutis hoitavate andmete konfidentsiaalsusele ja terviklusele.

Täpsemat infot selle kohta, kuidas rakendada turvaliselt interneti kasutamise otstarbel autonoomsüsteeme, leiate moodulist B 3.208 Interneti-PC .

M 5.47z Kinnise kasutajagrupi konfigureerimine

Algatamise eest vastutavad: infoturbeosakond, kodukeskjaama eest vastutav töötaja,

Rakendamise eest vastutavad: administraator

Integrated Services Digital Network (ISDN) võimaldab luua kinnist kasutajagruppi, tuntud ka kui CUG (Closed User Group). Sellise grupi puhul on võimalik, et ühe CUG kõik liikmed saavad avaliku ISDN-i kaudu omavahel suhelda, kuid CUG liikmetele suunatud välised ühendamissoovid lükatakse samamoodi tagasi kui CUG liikmete soovid ühendada ennast avaliku ISDN-i liikmetega.

Tööpõhimõte

Kõik suhtluspartnerid on võrguoperaatori kinnises kasutajagrupis liikmed. Kommunikatsioonivolituste kontroll leiab aset CUG-ga selgesti seotud lukustuskoodi (Interlock Code) põhjal ja kontrolli teostab kommunikatsioonipartneri vastav digitaalne keskus.Alguses edastab helistav kommunikatsioonipartner talle määratud digitaalsele keskusele ühendustaotluse.Digitaalne keskus lisab ühendustaotlusele helistava kommunikatsioonipartneri ISDN-i numbri ja vastava kinnise kasutajagrupi lukustuskoodi.Selle sidepartneri, kellele helistatakse, digitaalne keskus tuvastab lukustuskoodi abil, kas ühendustaotlusele võib anda positiivse vastuse.Eduka identifitseerimise korral edastatakse ühendamissoov kommunikatsioonipartnerile, kellele soovitakse helistada. Kirjeldatud funktsiooni eeliseks on see, et keelatud juurdepääsukatsed blokeeritakse juba võrguoperaatori digitaalses keskuses ja need ei jõuagi kommunikatsioonipartneri võrguühenduselementideni. Probleemiks on see, et võrguoperaatorit tuleb iga CUG liikme võimalikest muudatustest alati teavitada, kuna ainult tema saab vajalikke volitusi muuta. Lisaks tähendab see ka seda, et võrguoperaatoril on täielik kontroll CUG liikmete üle ja CUG liikmed ei saa operaatori tehtud muudatusi kontrollida.Samuti tuleb juhtida tähelepanu sellele, et CUG sisseseadmine ja tööshoidmine võrguoperaatori poolt toob endaga kaasa nii ühekordse väljamineku kui ka püsikulu. Kinnise kasutajagrupi sisseseadmine avaliku võrguoperaatori poolt on mõistlik järgnevatel juhtudel:

- teiste meetodite kasutamiseks vajalik riist- ja tarkvara on soetamata,
- CUG liikmed vahetuvad harva ja
- võrguoperaator on piisavalt usaldusväärne.

Täiendavad kontrollküsimused:

- Kas sisseseatud CUG on piisavalt põhjalikult ja selgestimõistetavalt dokumenteeritud?Kas dokumentatsioon on aktuaalne?
- Kas regulaarselt kontrollitakse, kas reeglina tasuline CUG funktsioon on jätkuvalt vajalik?

M 5.51 Turvanõuded kaugtööarvuti ja organisatsiooni vahelisele sideühendusele

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator, kaugtöötaja

Kaugtöö raames edastatakse andmeid kaugtööarvuti ja organisatsiooni sidearvuti vahel ning vastav ülekanne toimub tavaliselt avalike sidevõrkude kaudu. Kuna ei organisatsioon ega kaugtöötaja ei saa eriti mõjutada seda, kas avalikus sidevõrgus säilib andmete konfidentsiaalsus, terviklus ja käideldavus, läheb tarvis lisameetmeid. Kaugtööarvuti ja organisatsiooni vaheline andmeedastus peab reeglina vastama järgnevatele turvanõuetele:

- Edastatavate andmete konfidentsiaalsuse tagamine. Piisavalt turvalise krüpteerimise abil tuleb tagada, et kaugtööarvuti ja organisatsiooni sidearvuti vahelise side pealtkuulamisel ei saaks teha järeldusi andmete sisu kohta. Lisaks sobivale krüpteerimismeetodile läheb tarvis ka kohandatud võtmehaldust koos regulaarse võtmevahetusega.
- Edastatavate andmete tervikluse tagamine. Kasutatavad edastusprotokollid peavad ära tundma andmete juhusliku muutmise ja probleemi kõrvaldama. Selleks, et tahtlikke manipulatsioone saaks tuvastada andmete edastamise käigus, tuleb andmed allkirjastada ja/või krüpteerida.
- Andmeedastuse käideldavuse tagamine. Kui viivitused kaugtöös pole eriti vastuvõetavad, tuleks andmeedastuseks valida liiasusega avalik sidevõrk, et üksikute ühenduste tõrge ei tooks endaga kaasa kõikide sidevõimaluse täielikku katkemist. Kaugtööarvuti võrguühenduse ja organisatsiooni liidese liiasus pole alati vajalik.
- Andmete autentsuse tagamine. Andmete edastamisel kaugtööarvuti ja organisatsiooni vahel peab olema võimalik usaldusväärselt kontrollida, kas side toimub õigete osalejate vahel, et välistada teesklust. See tähendab, et andmed, mille saatjaks on märgitud „Kaugtööarvuti“, pärinevad ka reaalselt nimetatud allikast. Samuti peab saama kindlatel alustel kontrollida, kas organisatsiooni andmed tõesti pärinevad organisatsioonist.
- Andmeedastuse kontrollitavuse tagamine . Selleks, et side oleks kontrollitav, saab kasutada logimisfunktsioone, mis lubavad hiljem kontrollida, milliseid andmeid ja kellele edastati.
- Andmete vastuvõtu tagamine. Kui andmete õige vastuvõtmine on kaugtöö jaoks oluline, saab kasutada kinnitusmehhanisme, millest on näha, kas vastuvõtja on andmed õigesti kätte saanud.

Selleks vajalike mehhanismide tugevus sõltub edastatavate andmete kaitsevajadusest.

Täiendavad kontrollküsimused:

- Kas kasutatavad sideprotokollid ja turvamehhanismid vastavad piisaval määral ülalmainitud nõudmistele?
- Kas on tagatud edastatavate andmete konfidentsiaalsus, terviklus ja autentsus ning sidepartnerite autentsus?

M 5.52 Sidearvutite turvanõuded

Algatamise eest vastutavad: IT-juht, infoturbespetsialist

Rakendamise eest vastutavad: administraator

Kaugtöö liigist ja selle käigus täidetavatest ülesannetest olenevalt on ka kaugtöötaja juurdepääs organisatsiooni andmetele erinev. Võimalik, et kaugtöötaja ja organisatsiooni vahel saadetakse ainult meile. Kuid on ka võimalik, et kaugtöötaja vajab juurdepääsu organisatsiooni serveritele.

Ükskõik millist juurdepääsu liiki parasjagu kasutatakse, peab organisatsiooni sidearvuti täitma üldjuhul siiski järgmisi turvanõudeid:

- Identifitseerimine ja autentimine: kõik sidearvuti kasutajad, seega administraatorid, organisatsiooni töötajad ja kaugtöötaja, peavad enne arvutisse ligipääsemist end tuvastama ja autentima. Juurdepääs tuleb korduva ebaõnnestumise korral sulgeda. Eelseadistatud paroolid tuleb muuta. Vajaduse korral peab sidearvuti suutma ka andmete edastamisel nõuda kaugtöötaja või kaugtöötaja arvuti uut autentimist, et tõrjuda liitunud ründajaid. Kasutajate tuvastamise ja autentimise raames peaks toimuma ka kaugtööarvuti täiendav tuvastamine (nt telefoninumbrite ja tagasihelistamisfunktsiooni abil). Tasub kaaluda võimalust kasutada kaugtöö juurdepääsuks ainult tugevaid autentimisvõimalusi. Selleks võib kasutada nt kiipkaarte, volitustõendeid või ka biomeetrilist tuvastamist.
- Rollijaotus: sidearvuti administraatorite ja kasutajate töörollid peavad olema lahutatud. Pääsuõiguste määramise võimalus tohib olla ainult administraatoritel.
- Õiguste haldamine ja kontroll: juurdepääs sidearvuti failidele tohib olla võimalik ainult sobivate õigustega. Lisaks peab olema reguleeritud juurdepääs organisatsiooni teistele ühendatud arvutitele ja neisse salvestatud failidele. Juurdepääsuvõimalusi tuleb piirata vajaliku miinimumini. Süsteemi avarii või muude kõrvalekallete puhul peab sidearvuti lülituma turvalisse seisundisse, mis võib olenevalt vajadusest tähendada seda, et juurdepääs tõkestatakse.
- Teenuste miinimum: sidearvuti pakutavad teenused peavad vastama minimaalsete vajaduste rahuldamise põhimõttele: kõik, mis pole selgelt lubatud, on keelatud. Teenused peavad olema piiratud sellise määrani, mis on vajalikud kaugtöötaja ülesannete täitmiseks.
- Logimine: andmete ülekandmine sidearvutist, sidearvutisse ja sidearvuti vahendusel tuleb logida koos kellaaja, kasutaja, aadressi ja teenusega. Administraatorid või auditeerijad peavad saama kasutada tööriistu, et logiandmeid analüüsida. Kõrvalekalletest teavitamine peab toimuma automaatselt.
- Automaatne arvutiviiruste kontroll: edastatud andmeid tuleb kontrollida automaatselt viiruste suhtes.
- Krüpteering: andmed, mida hoitakse sidearvutis kaugtöötajate jaoks, tuleb vastava kaitsevajaduse korral konfidentsiaalsuse tagamiseks (lähtuvalt organisatsiooniülesest infoturbe poliitikast) krüpteerida. Reeglina tuleb side kaugtööarvuti ja sidearvuti vahel krüpteerida.
- Kaugadministreerimise vältimine või kaitse: kui sidearvuti ei vaja kaugadministreerimist, tuleb kõik kaugadministreerimise funktsioonid sulgeda. Kuna aga enamasti on kaugadministreerimine siiski vajalik, peab see olema pii-

savalt kaitstud (nt VPN-tunneli või eraldiseisva ühenduse kaudu). Igasugune kaugadministreerimine tohib toimuda alles pärast eelnevat edukat tuvastamist ja autentimist. Tuleks kaaluda võimalust kaugadministreerimise ajal tehtut logida. Administreerimise pääsuandmeid ja konfiguratsiooniandmeid tohib edastada ainult krüpteeritult. Eelseadistatud paroolid ja krüptograafilised võtmed tuleb ära muuta.

Kontrollküsimused:

- Kas sidearvuti konfiguratsioon vastab turvanõuetele?
- Kas kõik sidearvuti kasutajad peavad enne arvutile juurdepääsemist end arvutis tuvastama ja autentima?
- Kas juurdepääsuvõimalused sidearvutile on piiratud vajaliku miinimumini?
- Kui sageli kontrollitakse, kas valitud seadistused ja volitused vastavad reaalsele vajadusele?

M 5.54 Meili ülekoormuse ja spämmi tõrje

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator, kasutaja

Soovimatuid meile, mida nimetatakse ka rämpspostiks ehk spämmiks, saadetakse massiliselt. Need häirivad saajaid ning segavad IT infrastruktuuri jooksvat kasutamist, alustades meile edastavatest süsteemidest kuni kasutajate klientideni välja. Soovimatute meilide hulka kuuluvad ahelkirjad, soovimatu reklaam, kerjuskirjad, rämpspost, andmepüüki tegevad meilid ning meilid, mille manuses on kahjurvara. Eriti ohtlikuks muutub olukord siis, kui avatakse meilides olevad manused, mis põhinevad HTML-il või mis juhivad meili saaja lingi kaudu manipuleeritud veebilehekülgedele edasi. Soovimatute meilide kuhjumine või sissetulevate meilide abil meilisüsteemi tahtlik ülekoormamine ei pruugi meilisüsteemi mitte ainul blokeerida, vaid võib meilide saajale ka küllaltki kalliks minna.

Kulutused tekivad andmeedastuskuludest, seda eriti siis, kui soovimatud meilid sisaldavad pilte või multimeediumfaile. Lisanduvad veel meilide filtreerimise kulud ja/või töötajate ajakulu, mis tuleneb vajadusest kogu rämpspost üle vaadata ja kustutada. Et ennast soovimatute meilide eest kaitsta, peaks iga kasutaja mõtlema, kellele oma meiliaadressi anda. Kasutajad peaksid eriti ettevaatlikud olema uudistegruppide või meililistide, võidumängude, küsitluste ja muude sarnaste kohtade puhul. Nendel juhtudel tuleks mõelda mitteametliku meiliaadressi kasutamise peale, et mitte anda võõrastesse kätesse oma isiklikku, „põhiaadressi". Samas tuleks ka jälgida, et sidepartnerite meiliaadresse ei edastataks kergekäeliselt. Eriti siis, kui meil saadetakse mitmele inimesele korraga, ei ole vaja teistel teada, kes veel selle kirja millisele aadressile sai.

Selle vältimiseks võib kasutada pimekoopia (Blind Carbon Copy, BCC) funktsiooni, mida toetavad peaaegu kõik meilikliendid. Samuti peaks kasutaja arvuti olema vaba igasugusest kahjurvarast – on olemas kahjurvara, mis hangib informatsiooni kohalikust aadressiraamatust ja paigutab seal olevad meiliaadressid rämpsposti saajate nimekirja. Kasutajad peaksid rämpsposti ignoreerima ja kustutama. Kuna sellel võivad olla negatiivsed tagajärjed, ei tohi meilidele lisatud linke ega manuseid mingi juhul avada. Kinnitus meili eduka edastamise kohta on samuti kinnitus selle kohta, et vastav meiliaadress sobib spämmi saatmiseks ja et vastav kasutaja rämpsposti ka loeb. Lisaks on olemas risk, et arvutid nakatuvad kahjurvaraga ning saavad nii osaks robotvõrgust. Kõiki töötajaid peaks sellest teavitama.

Ebasoovitavate e-mailide vastu võib võtta allpool kirjeldatud meetmeid:

- Rämpsposti vältimiseks või vähemalt vastuvõtjale tuvastamiseks on vaja, et soovimatud meilid tuntaks masinate abil või automaatselt ära ning eemaldataks või märgistataks. Selleks tuleb kasutada vastavat meilifiltreerimise süsteemi (vt M 5.109z Meiliskanneri kasutamine meiliserveril).
- Soovimatud meilid sisaldavad tihtipeale manuseid, mis põhjustavad teadmatuid kõrvalmõjusid, või failivorminguid, mis tuleb liigitada potentsiaalselt

ohtlikeks. Kõik sellega seotud isikud peaksid probleemist teadlikud olema ja võtma vastavaid ettevaatusabinõusid (vt M 4.199 Ohtlike failivormingute vältimine).

- Enamikke meilikliente on võimalik konfigureerida nii, et nad paigutaksid soovimatuks markeeritud meilid eraldi kausta. Vastava filtri saab üles seada nii kasutaja kui ka administraator. Kasutajaid tuleks sellest teavitada.
- Ka mõned meiliprogrammid sisaldavad soovimatute meilide tuvastusmehhanisme. Kasutajatel on võimalik neid käivitada ja sisenevat posti vastavalt liigitada.
- Iga asutus peaks kindlaks määrama, kas selle töötajad võivad uudistegruppidesse postitusi saata ning kui jah, siis millises vormis ja millistel teemadel. Kasutajate tähelepanu tuleb juhtida interneti heade tavade järgimisele ning sellele, et avalikkusele ebavajaliku teabe levitamine tuleb lõpetada.
- Teatud juhtudel on mõttekas kasutada keerulisemaid meiliaadresse (vt M 2.122z Meiliaadresside standard). Kui meiliaadressi avalikustamine on vajalik (meililistid, päringud), on üheks võimaluseks luua spetsiaalne meiliaadress, mida kasutataks just sellistel juhtudel. Sellele aadressile saadetud meile on hiljem võimalik filtreerida, ignoreerida või kustutada. Kui nendeks aadressideks ei taheta kasutada enda domeeni aadresse, võib kasutada ka tasuta meilikontode pakkujaid.
- Mingil juhul ei tohiks rämpsposti saatjaid karistada meilipommide või muude sarnaste meetoditega. Spämmile ei tohiks isegi vastata. Saatja andmed on neis kirjades sageli võltsitud ning teie vastus jõuab siis ainult süütute inimesteni või tuleb tagasi teatega, et meili ei olnud võimalik edastada. Igal juhul põhjustab vastamine jällegi suuremat võrgukasutust ja halvimal juhul kinnitate te reklaammeili saatjale oma meiliaadressi õigsust ja olemasolu.
- Kuigi rämpspostikirjades pakutakse tihti võimalust, et järgmiseid meile enam ei saadeta, ei tohiks siiski sellistele meilidele vastata. Vastasel juhul võtab saatja vastust kinnitusena, et sisestatud meiliaadress on olemas.
- Veel üks võimalus rämpsposti vastu võidelda on teatada sellest meiliteenuse pakkujale ja ka spämmisaatja meiliteenuse pakkujale, et need saaksid võtta vastavaid meetmeid. Siinkohal tuleb arvesse võtta, et mitte kõik meiliteenuse pakkujad ei pruugi sellele kaebusele kohe reageerida.

Kõik meetmed ei ole kõikides keskkondades otstarbekad, kuna nendega kaasneb suur hulk piiranguid. Ühest küljest on reklaammeilide vältimiseks mõttekas kasutada meiliaadressina midagi muud, mitte kasutajanimest tuletatud meiliaadressi.

Teisest küljest aga võivad keerukad meiliaadressid raskendada suhtlust väliste klientidega, kuna neid on raske meelde jätta. Meiliaadresside vorm peab igal juhul vastama asutuse reeglitele. Suure meilikoormuse võib endaga kaasa tuua meililistidega liitumine. Üldjuhul tuleks regulaarselt kontrollida, kas meililistides arutatud teemad on lugemist väärt. Vastasel juhul tuleks listiga liitumine tühistada. Kasutajaid tuleb teavitada, et pärast meililistiga liitumist tuleb seetõttu tekkivat meilikoormust pidevalt (võimalusel iga päev) kontrollida. Suuremates asutustes peaks huvitavate meililistidega liituma ainult üks töötaja (näiteks meiliadministraator), kes need siis kõigile kättesaadavaks teeb.

Rämpspostile peaks mõtlema ka veebilehtede kujundamisel. Spämmisaatjad üritavad oma aadressikogu laiendada sellega, et otsivad teatud programmidega veebilehtedelt sinna märgitud meiliaadresse (näiteks päringute esitamiseks). Kahjuks ei ole peaaegu ühtegi tõhusat võimalust, kuidas end nende automaatsete otsinguprogrammide vastu kaitsta. Seepärast tuleks hoolikalt mõelda, kas ja millised meiliaadressid veebileheküljel avalikustatakse. Selleks on võimalik luua spetsiaalsed meiliaadressid. Loomulikult saadetakse ka neile rämpsposti, aga sel moel on võimalik probleemi piirata. Saadud meilide ehtsateks kirjadeks ja rämpspostiks liigitamiseks tuleks varuda aega.

Kontrollküsimused:

- Kas kasutajaid on teavitatud rämpsposti probleemsusest ja sellest, kuidas soovimatute meilidega õigesti ümber käia?
- Kas kasutajad saavad meilide liigitamisel abi administraatoritelt või tehnilistelt süsteemidelt?
- Kas kasutajad saavad foorumites ja meililistides kasutamiseks luua mitteametlikke meiliaadresse?

M 5.56 Meiliserveri turvaline kasutamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator

Meiliserveri turvaline kasutamine eeldab, et kindlustatud on nii lokaalne kui ka avalikust võrgust tulev suhtlus. Meiliserver võtab teistelt meiliserveritelt kirju vastu ja saadab need ühendatud kasutajatele või meiliserveritele edasi. Lisaks edastab meiliserver lokaalsete kasutajate saadetud meile välistele meiliserveritele. Meiliserver peab kindlustama, et ühendatud kasutajate lokaalseid meile saadetaks edasi ainult asutuse piires ning et need ei satuks välisvõrku. Meiliserverid salvestavad meile kuni nende edasisaatmiseni. Samuti arhiveerivad paljud internetiteenuse pakkujad ja administraatorid sissetulevaid ja väljuvaid meile. Selleks, et volitamata isikud ei saaks meiliserveri kaudu sellel paiknevatele teadetele ligipääsu, tuleb meiliserverit volitamata ligipääsu eest kaitsta.

Selle jaoks tuleks server paigaldada turvatud kohta (serveriruumi või serverikappi). Meiliserveri korrapärase kasutamise tagamiseks tuleb määrata administraatorid ja nende asetäitjad ning neid koolitada, et nad oskaksid meiliserverit ja selle aluseks olevat operatsioonisüsteemi kasutada. Sisse tuleb seada Postmaster- ja Abuse-Account (vt M 2.456 Rühmatarkvarasüsteemide turvaline haldamine). Lokaalselt ühendatud meilipostkastidele võib ligipääs olla ainult kasutajatel endil. Aladele, kuhu meile ainult ajutiselt vahesalvestatakse (näiteks spooled file), on ligipääs keelatud ka lokaalsetele kasutajatele.

Regulaarselt tuleb kontrollida, kas ühendus meiliserveriga, eriti meiliteenuse pakkuja meiliserveriga, on veel stabiilne. Samuti tuleb regulaarselt kontrollida, kas meilide vahesalvestuseks kasutatavat kettaruumi on veel piisavalt, kuna ruumi lõppemisel ei ole teateid enam võimalik edastada. Meiliserveri toimingute logimise maht ja sisu tuleb kindlaks määrata. Logiandmeid tuleb regulaarselt analüüsida, eelkõige selleks, et kindlaks teha, kas meiliserverile on toimunud rünnakuid ja millised on olnud nende tagajärjed. Meiliserveri kasutatavusest ei tohiks sõltuda mitte ükski teine teenus, näiteks ei tohiks meiliserverit samal ajal failiserverina kasutada.

Meiliserverit peaks olema võimalik igal ajal mõneks viivuks välja lülitada, näiteks teenusetõkestamise rünnete (Denial-of-Service Attack) või manipulatsioonikahtluse korral (vt M 4.97z Ainult üks teenus serveri kohta).Kasutajakontode vastu suunatud rünnete raskendamiseks ei tohiks olla võimalik meiliserveril paiknevaid kasutajanimesid meiliaadressidest välja lugeda.

MX-sissekanded ja rämpsposti edastamine

Nendele meetmetele vaatamata saavad volitatud kasutajad ka edaspidi suvalistele aadressidele meile saata. Samuti on neil võimalik meile suvalistelt aad-

ressidelt vastu võtta. Sisenevate meilide ülalkirjeldatud filtreerimisega takistatakse väliseid kasutajaid, et nad ei saaks meiliserverit rämpsposti edasisaatmiseks kuritarvitada.Interneti domeeninimede süsteem (DNS) näeb ette, et nn MX-sissekandega märgistatakse üks kindel server Mailexchanger 'ina. Tavaliselt peaks siis erinevate domeenide vaheliste arvutite meile edasi juhitama vastava Mailexchanger 'i kaudu. Meilide erinevate domeenide vahel edastamist nimetatakse Relaying 'uks. Meiliserverit tuleks kaitsta, et seda ei kasutataks rämpsposti edastajana. Selleks tuleks meiliserver konfigureerida nii, et see võtaks vastu ainult enda organisatsioonile mõeldud meile ja saadaks edasi ainult organisatsiooni töötajate saadetud meile. Meiliserver peaks sisenevaid meile ainult siis vastu võtma, kui administraator on saatja IP-aadressi lubatud IP-de võrgus eraldi välja toonud või kui see toimib vastuvõtja aadressi jaoks ise Mailexchangerina. Kõigist teistest meilidest tuleks veateate abil loobuda. Juhul, kui nimekirjas ei ole kõiki erinevaid IP-võrke, millest meile vastu võetakse, tuleb meiliserveri administraatorit sellest teavitada. Ta saab need vastavad IP-võrgud tagantjärele sisse kanda.

Non Delivery Notifications

Ilmtingimata tuleb vältida seda, et Non Delivery Notificationseid loodaks vastuvõtjate valede aadresside korral. Pigem tuleb hoolitseda selle eest, et kirju, millega asutus ei tegele, ei võetaks isegi vastu. Seejuures tuleb ilmtingimata jälgida, et asutuse meile kontrolliv teenusepakkuja teaks samuti, milliseid meile vastu võtta tohib ja milliseid mitte. Nii ei peaks ta Non Delivery Notifications 'it looma, kui neid ei õnnestu kohale toimetada. Kui seda ei jälgita, võivad rämpsposti saatjad Non Delivery Notifications 'i saatmist ära kasutada, et kolmandatele isikutele vastava asutuse nimel rämpsposti edastada.Põhimõtteliselt on Non Delivery Notifications 'id RFC-ga vastavuses ja mõttekad – need teavitavad meilisüsteemi pidevate vigade korral meili saatjaid, et meili ei olnud võimalik kohale toimetada. Non Delivery Notifications' ite loomine peab piirduma veajuhtumitega ja selle teate esinemine tuleb üldjuhul minimeerida.

Non Delivery Notificationsitest tulenevate riskide vältimiseks võib olla soovitatav järgmine teguviis: Non Delivery Notifications on põhimõtteliselt lubatud. Asutuse meile edastavad süsteemid ja väliste teenusepakkujate meilisüsteemid (selle serverini, millele MX- Record viitab) ühtlustatakse omavahel nii, et Non Delivery Notification luuakse ainult vea korral. Muuhulgas ei tohi luua ühtegi Non Delivery Notifications 'it siis, kui saajat olemas ei ole, kui meilisüsteem hindab meili liiga suureks (kuigi eespool seisev meiliserver on selle juba vastu võtnud) või kui postkast on täis. Administraator peaks endale sisse seadma häire, mis teavitaks teda süsteemis Non Delivery Notifications 'i loomisest. Ta peaks seejärel kontrollima, miks see juhtus, ja vea kõrvaldama. Põhimõte: domeeni korral tuleb alates MX-Records 'i IP-aadressi kaudu vastuvõtmisest kuni kasutaja postkastini kindlustada, et meilid edastatakse ning et Non Delivery Notifications 'eid ei tekiks osalevate meiliedastajate vastuoluliste konfiguratsioonide tõttu.

Autoresponder

Non Delivery Notificationsite ohud viitavad meilikommunikatsiooni üldistele probleemidele. Meili saatjat saab vabalt valida ning seda aadressi on võimalik võltsida. Kui keegi saadab automaatselt vastavale süsteemile võltsitud aadressiga meili, saadab see vastuse omakorda saatja võltsitud aadressile. Ründaja

võib seda kasutada selleks, et ujutada kolmandad isikud asutuse nimel meilidega üle. Selle rünnakustsenaariumi jaoks sobivad peaaegu kõik automaatselt meilidele vastavad süsteemid. Seetõttu tuleb ka äraolekuteateid, meili kättesaamise kinnitusi ja edastusi kasutada suure ettevaatusega.

Tõrjeks tuleb kasutusele võtta järgmisi meetmeid:

- Rämpspostina märgistatud meilidele ei tohi automaatselt vastata ja neid ei tohi edasi saata.
- Vastuse saatja aadress peab olema asutuse sees kasutatav aadress. Kasutada ei tohi sissetulnud meili saatja aadressi.
- Ühe kindla sihtmärgi (sihtaadressi või sihtdomeeni) kontrollimatult suure hulga meilidega pommitamist tuleb vältida. Äraolekuassistentide puhul võib saatjale saata ainult ühekordse äraolekuteate.

Tulemüür / DMZ

Loomulikult peab meiliserverile internetist ligi pääsema. Seepärast tuleks serverit vastavate meetmetega ka võrgu tasandil kaitsta, näiteks võiks võrgu ette paigutatud tulemüürist lubada väliseid ühendusi ainult kindlate portidega. Veel parem oleks paigutada meiliserver demilitariseeritud tsooni (DMZ) ning piirata ka internetiühendus ainult vajalikele protokollidele ja teenustele.

Määrake logi ja teenused

Tuleb kindlaks määrata, millised protokollid ja teenused meiliserveril lubatud on. Näiteks on tavaline lubada mõlemapoolset SMTP-(TCP-port 25). Seevastu protokolle POP3 või IMAP (TCP port 110 või 143, olenevalt sellest, kuidas meile serverilt alla laaditakse) tuleks lubada ainult sisevõrgu ligipääsudeks. Nii POP3-e kui ka IMAP-i jaoks on olemas variandid, mille korral toimub registreerimine ja andmeedastus SSL-i kaudu. Kui kasutatav tarkvara neid võimalusi toetab, tuleks neid ka kasutada.

Soovimatute meilide tõrje

Kui asutusel endal meiliservereid pole ning teenusepakkuja meiliserverile pääsetakse ligi ühe või mitme meilikliendi kaudu, tuleks teenusepakkujaga läbi rääkida, millised on pakkuja regulatsioonid ning rakendatud turbemeetmed (vt M 2.123z Rühmatarkvara või meiliteenuse pakkuja valimine). Meilid on kõige levinum viis edastada rämpsposti ja kahjurvara, mille vältimiseks on mitmeid strateegiaid (vt M 2.156 Sobiva viirusetõrjestrateegia valimine). Kogemus on näidanud, et meile peaks kontrollima nii tulemüüril, meiliserveril kui ka klientarvutil (vt M 5.109z Meiliskanneri kasutamine meiliserveril). Kõiki kasutatavaid viirustõrjeprogramme tuleb regulaarselt uuendada.

Kontrollküsimused:

- Kas meiliserver on volitamata ligipääsu suhtes turvatud?
- Kas meiliserveri kasutamiseks on olemas vastavalt koolitatud personal?
- Kas meiliserveri tegevust logitakse ja analüüsitakse regulaarselt?

- Kas meiliserver on konfigureeritud nii, et seda ei saaks kuritarvitada rämpsposti edastamiseks?

M 5.57 Rühmatarkvara/meiliklientide turvaline konfiguratsioon

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator, kasutaja

Administraatoril tuleb k asutaja rühmatarkvaraprogramm konfigureerida nii, et kasutajat oleks võimalik lihtsalt kaitsta. Kasutajatele tuleb selgitada, et nad ei tohi konfiguratsiooni ise muuta. Rühmatarkvaraklientide konfigureerimisel tuleb silmas pidada järgmisi punkte:

Saatja aadressiks peab olema kasutaja ametlik meiliaadress. Nii ei satu sisemised meiliaadressid asutusest väljapoole.

- Võrgukoormuse madalana hoidmiseks ei tohi meiliklient liiga sageli meiliserverilt uusi sõnumeid kontrollida. Tavaliselt soovitatakse automaatset, iga 30 minuti tagant toimuvat kontrolli. Enamasti peaks sellest piisama. Kui kasutaja ootab pakilist sõnumit, seadistatakse meiliprogramm postkasti käsitsi kontrollima.
- Kui sõnumid tulevad meiliserverilt POP3-i (Post Office Protocol Version 3) kaudu , tuleb nad sealt ka kustutada , et samu sõnumeid ei esitataks mitu korda ja et meiliserverit ei koormataks üle. Kui sõnumid salvestatakse meiliserveril, mille poole pöördutakse IMAP-i (Internet Message Access Protocol) kaudu, tuleb serveripoolsele postkastile määrata mahupiirang. Kasutajad peavad sel juhul serverilt regulaarselt meile kustutama või neid kohalikesse postkastidesse tõmbama. Postkasti mahu ülempiiri saavutamisest tuleb kasutajaid sobival viisil (näiteks meilitsi) teavitada. Sõnum võiks kõlada umbes nii: „Teie postkast on ületanud ühe või mitu administraatori seatud mahupiirangut. Postkasti suurus on xxx GB. Postkasti maksimaalne suurus: xxx GB. Teile teatatakse, kui postkasti maht ületab yyy MB. Uute sõnumite saatmine ja vastuvõtmine võib enne postkasti mahu vähendamist olla raskendatud. Ruumi vabastamiseks kustutage osa meile või tõstke need kohalikku arvutisse."

HTML-vormingus meilid

HTML-vormingus meilid võivad sisaldada aktiivsisu (näiteks Javascript, Flash, ActiveX või Java). Seepärast esineb just selles vormingus meilide puhul meiliklientide turvaaukudega koosmõjus sageli probleeme. Nende vältimiseks tuleb meiliprogrammid seadistada nii, et HTML-vormingus meilide aktiivsisu ei esitataks ilma päringuta. Lisaks tuleks võimalusel kasutada ainult selliseid meilikliente, mis muudavad HTML-vormingus meilid enne avamist tuvastatavaks. Kui meiliklient pakub võimalust kuvada HTML-vormingus meile mitte automaatvormingus, vaid esmaavamisel lihtsalt tekstina (HTML-alliktekst), tuleb seda võimalust kasutada. HTML-vormingus meilidest tuleneva võimaliku ohu tõttu peaks nende saatmist võimalusel vältima. Meilikliendi konfiguratsioonis tuleb uue meili standardvorminguks määrata „ainult tekst ". Kui selliseid vorminguelemente nagu kiri ja värv on tingimata vaja, tuleb kasutada RTF-vormingut.

Meilimanused

Meilimanused (Attachments) on arvutiviiruste, Trooja hobuste, usside ja muu kahjurvara lemmikliiklusvahend, mistõttu tuleb meiliprogrammid seadistada nii, et manuseid ei saaks kogemata käivitada, vaid programm hoiataks kasutajat või vähemalt küsiks enne, kas faili tohib avada. Operatsioonisüsteem või meiliklient tuleb lisaks seadistada nii, et faile näidatakse esmalt ainult vaaturis (Viewer) või muus kuvamisprogrammis, mis ei käivitaks failis sisalduda võivat programmikoodi (nt makrot või skripti).

Eelvaatefunktsioon

Mõned kliendiprogrammid pakuvad meilide puhul eelvaatefunktsiooni. Sealjuures näidatakse valitud meili sisu ilma, et kasutaja peaks seda eraldi avama. Nii tekib oht meilis sisalduvat kahjulikku sisu kogemata käivitada. Seetõttu tuleb eelvaatefunktsioon desaktiveerida.

Meilifiltrireeglite konfigureerimine

Soovimatud meilid, eelkõige rämpspost, segavad tööd. Üldiselt soovitatakse rämpspost filtreerida juba serveril. Sellee eliseks on, et kõik meilid filtreeritakse järjekindlalt ja administratiivne kulu ei kasva lõputult. Peale selle on võimalik meile ka kliendi juures filtreerida. Enamikku meiliklientidest saab konfigureerida nii, et nad paneksid soovimatuks märgitud meilid eraldi kataloogi. Vastavad filtreerimisreeglid saab kehtestada kasutaja või administraator, ent esmalt tuleb kasutajat sellest teavitada.

Meilide automaatedastus

Asutuste ja ettevõtete kasvava mobiilsuse tõttu on üha enam vaja oma meilidele suvalisest maailmapunktist ligi pääseda. Vastavaks mehhanismiks on meilide automaatedastus. Mõtlematult sisselülitatud edastuse puhul tekib aga andmete või konfidentsiaalsuse kaotsimineku oht. Andmekadu võib tekkida näiteks siis, kui kiri sisaldab ootamatult konfidentsiaalset sõnumit. Seetõttu soovitatakse meile mitte automaatselt edastada.

Kontrollküsimused:

- Kas administraatorid on rühmatarkvarakliendid turvaliselt eelkonfigureerinud?
- Kas kasutajad teavad, et nad ei tohi meilikonfiguratsiooni iseseisvalt muuta?
- Kas rühmatarkvarakliendid on nii seadistatud, et meilimanuste ja HTMLvormingus meilidega käidaks võimalikult turvaliselt ümber?

M 5.58 Andmebaasiliidese draiverite valik ja installeerimine

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: administraator

Andmebaasiliidese draiverid, nt ODBC- (Open Database Connectivity), IDAPI- (Integrated Database Application Programming Interface) või JDBC-draiver (Java Database Connectivity), installeerivad andmebaasirakenduste ja vastava andmebaasiprotokolli vahele täiendava tarkvarakihi. Andmebaasi juurde sobiva draiveri installeerimisel luuakse rakenduse ja andmebaasi vahele ühtne liides, mille kaudu toimub side andmebaasiga (andmebaasipäringute esitamine, andmete lugemine). Vastav ANSI-SQL-toega SQL-liides võimaldab koostada rakendusi, mille juures pole tarvis arvestada erinevate andmebaasitoodete eripäradega. Seepärast pole andmebaasitarkvara vahetamisel ideaaljuhul tarvis rakendust kohandada, piisab draiveri vahetamisest. Algselt firmade Microsoft, Sun, jne toodete jaoks väljatöötatud andmebaasiliidese draiverid on kujunenud standardiks ja on saadaval kõikidele levinud andmebaasitoodetele. Draiveri valimisel tuleb arvestada erinevate kriteeriumitega. Olulisemad neist on järgmised:

- Millised draiverid on olemas pöördumise sihiks oleva andmebaasiversiooni jaoks?
- Millised draiverid on olemas rakendusprogrammi käitava arvuti operatsioonisüsteemi versiooni jaoks?
- Kas tuleks kasutada andmebaasi tootja draivereid (tavaliselt on need tasuta) või teiste tootjate omi?
- Milline on liidese poolt võimaldatav SQL-keele ulatus?
- Millised on muud nõudmised, mida rakendatav arvutiarhitektuur ja tarkvara endaga kaasa toovad?

Nende kriteeriumite alusel ja vajadusel täiendavate nõuete põhjal, mis sõltuvad kasutusvaldkonnast, tuleb valida sobiv draiver. Hiljem tuleb seda valikut regulaarselt kontrollida. Selle põhjuseks võib lisaks regulaarsele süsteemikontrollile olla muuhulgas andmebaasitarkvara või operatsioonisüsteemi värskendamine või uus draiveriversioon. Andmebaasiliidese draiverite installeerimisel tuleb jälgida, et vigade või hooletuse tõttu ei tekiks andmebaasisüsteemi juurdepääsukontrolli mehhanismidesse turvaaukusid.

Rakenduse andmebaasiga ühendamiseks tuleb andmebaasiliidese draiveriga sisse seada nn andmeallikas, mis toetab sidet rakenduse ja andmebaasi vahel. See installeerimistöö on ainult administraatori ülesanne. Mõned rakendused installeerivad lisaks ka näidisandmebaaside andmeallikaid või andmebaasiliidese draivereid, mida teie organisatsioon ei pruugi üldse kasutada. Takistamaks soovimatut ning võimalik, et ka kontrollimatut juurdepääsu nende andmeallikate või draiverite kaudu, tuleb kõik ebavajalikud andmeallikad ja draiverid eemaldada.

Näide

Microsoft Accessi andmebaasides pole kasutajatunnuste kasutamine kohustuslik ja arendaja peab selle eraldi aktiveerima. Juurdepääsukontrolli aktiveerimisel hallatakse kasutajatunnuseid ja grupikuuluvusi eraldi Microsoft Accessi andmebaasi, nn töögruppide infofaili kaudu, mis salvestatakse eraldi failina (standardni-

meks alates Microsoft Access 97-st on: system.mdw , varem system.mda). Installeerides ODBC-draiverit, eesmärgiga luua juurdepääs Microsoft Accessi andmebaasile, ei toimu töögruppide infofaili integreerimine sugugi mitte automaatselt. Installeerimise ajal kasutatud standardsed seadistused ei arvesta töögruppide infofailiga, mis võib juba olemas olla. Kui ODBC-draiveri installeerimisel jäeti töörühmade infofail selgelt määratlemata, võib tekkida olukord, kus ODBC kaudu saab andmebaasile ligi pääseda, ilma et oleks tarvis end töögruppide infofaili alusel identifitseerida. See võib juurdepääsukontrolli kasutuks muuta. Sellise olukorra vältimiseks tuleb vastavas Accessi rakenduses määrata sellised õigused, et juurdepääs Microsoft Accessi andmebaasile on võimalik ainult määratletud töögruppide infofaili baasil.

Lisaks võib regulaarselt kontrollida, kas töögruppide infofail on integreeritud, kuna seda mehhanismi saab igal ajal tühistada, st manipuleerida.

Täiendavad kontrollküsimused:

- Kas andmebaasi jaoks on installeeritud andmebaasiliidese draiver?
- Kas draiveriversiooni valimisel on arvestatud andmebaasisüsteemile ja rakendusele kehtivate nõuetega?

M 5.59 DNS võltsimise tõrje

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: administraator

DNS-spuufingu oht tekib, kui autentimine viiakse läbi arvutinime abil. Hostil põhinev autentimine tähendab seda, et õigused antakse sõltuvalt arvutinimest või IP-aadressist ja tuleks ühega järgmistest konfiguratsioonidest (ka kombineeritult) raskendada:

- Hostinimede asemel tuleks kasutada IP-aadresse.
- Kui kasutatakse hostinimesid, tuleks eemaldada kõik lokaalsed nimed (sissekanded failis /etc/hosts).
- Kui kasutatakse hostinimesid ja neid ei ole võimalik lokaalselt eemaldada, tuleks nimed eemaldada otse nimeserverilt, mis on nende nimede jaoks nn. esmane või sekundaarne server, mis tähendab, et need nimed ei ole salvestatud ajutises vahemälus, vaid põhimälus.

Punkt 1 pakub suurimat ja punkt 3 madalaimat kaitset. Nimetatud konfiguratsioonide eesmärgiks on IP-aadressite ja arvutinimede ühendamine kindlas keskkonnas. Mitte mingil juhul ei tohiks lubada hostil põhinevat ligipääsu hostinime kaudu, kui nimede eemaldamist ei ole võimalik otseselt läbi viia (vahemälu on vahele lülitatud).

Täiendav kontrollküsimus:

- Kas ligipääsu juhtimine toimub arvutinimede kaudu? Kui jah: Millist meetodit kasutatakse DNS-spuufingu kaitseks?

M 5.60 Sobiva magistraalvõrgutehnika valimine

Algatamise eest vastutavad: IT-juht, infoturbeosakond
Rakendamise eest vastutavad: IT-juht, administraator

Magistraalvõrgu ala võrguprotokolli valimine on oluline faktor kohtvõrgu rakenduste käideldavuse kaitse tagamisel, kuna valitud protokoll mõjutab olulisel määral võrgu jõudlust ja kasutatavaid ribalaiuseid. Juhul kui aluseks olev kaabeldus on planeeritud, ilma et oleks valitud kindlaid teenuseid (nt kindlate toojate lahendusi) (vt G 2.45 Võrgu konseptuaalsed puudused), on magistraalvõrgutehnika vahetamine enamasti probleemivaba. Sellele vaatamata kaasneb vastava tegevusega üldjuhul märkimisväärne organisatoorne, tööjõu ja finantside kulu. Üldkehtivat soovitust kindla, IT-turvalisust arvestava magistraalvõrgutehnika valimiseks ei ole võimalik anda, kuna on palju erinevaid aspekte, mida tuleb silmas pidada. Järgnevalt on seega ära toodud olulisemate võrgu juurdepääsuprotokollide eelised ja puudused. Kokku eksisteerib neli allkirjeldatud põhitehnoloogiat: Ethernet, Token-Ring, FDDI ja ATM.

Ethernet

Etherneti tehnoloogiat on kirjeldatud Institute of Electrical and Electronics Engineers (IEEE) 802.3 standardis ja see põhineb CSMA/CD-juurdepääsuprotseduuridel (Carrier Sense Multiple Access/ Collision De-tection). Selle meetodi puhul on kõikidel lõppseadmetel ühesugune õigus sidekanali kasutamiseks, kuigi korraga saab seda kasutada ainult üks lõppseade. Niipea kui mõni lõppseade tahab andmeid edastada, kontrollib see esmalt, kas sidekanal on kasutamiseks vaba (Carrier Sense). Kui see on vaba, algab andmete edastamine. Juhul kui mitu lõppseadet teevad seda samaaegselt (Multiple Access), tekib kokkupõrge, mis tuvastatakse asjassepuutuvate lõppseadmete poolt (Collision Detection) ja seejärel toimub sidekanali uus kontroll, millele järgneb edastamise kordamine. CSMA/CD on stohhastiline meetod ja ei suuda seepärast tagada kindlat ribalaiust. Seepärast ei sobi see eriti hästi nt multimeediarakendustele, mis vajavad kindlat ribalaiust. Ethernetil põhinevates võrkudes on seega üldjuhul võimatu tagada teatud kindlat teenusekvaliteeti (Quality of Service - QoS). Gigabit-Etherneti puhul on olemas QoS-i analoog.

Ethernetist eksisteerib kolm erinevat varianti, mis erinevad toetatava andmeedastuskiiruse poolest ja kaablite infrastruktuurile ning aktiivsetele võrgukomponentidele esitatavate nõuete poolest:

- Standard-Ethernet - Standard-Ethernet on juba ammu kasutatav standard ja eelnevate variantide eelkäija. Seda iseloomustab andmeedastuskiirus 10 Mbit/s. Standard Ethernet eeldab Twisted-Pair kaablit (vähemalt CAT-3), millel on aktiivsed vahevaraüksused, nt jaoturid või kommutaatorid, siinikujulist BNC-kaabeldust, AUI-liidesega kaabeldust või valguskaablit. Puhtakujulist Standard Etherneti riistvara toetavad tänapäeval vaid vähesed teenusepakkujad. Uuemad seadmed võimaldavad samade soetamiskulude juures kõrgemat andmeedastust, kuid vanemate süsteemidega ühilduvuse tagamiseks võib andmeedastust piirata kiirusele 10 MBit/s. Puhtakujulise Standard Etherneti riistavara soetamise vajadus võib tavakasutuses tekkida vaid erandjuhtudel. Kui kõik asjassepuutuvad seadmed toetavad Ether-

neti uuemaid variante, tuleks kasutada mõnda kiiremat meetodit, nt Fast Ethernet-i.

- Fast Ethernet - Ühendatud arvutite suureneva arvu ja seega ka suureneva võrgukoormuse tõttu oli Standard-Etherneti edasiarendus hädavajalik, et reageerida kasvavatele vajadustele. Selle tagajärjel töötati välja Fast Ethernet, mille andmeedastuskiirus on 100 Mbit/s. Hetkel on see suurema osa kohtvõrkude jaoks piisav ja lisaeeliseks on võimalus eelnevalt juurutatud tehnoloogiat (CSMA/CD) edasi kasutada. Väikese hinna tõttu tuleks lõppseadmete ja juurdepääsukommutaatorite ühendamiseks kasutada vähemalt Fast Etherneti.
- Gigabit Ethernet - Kuna Fast Etherneti kasutuselevõtt oli väga edukas, tekkis nõudlus veelgi kiirema magistraalvõrgutehnika järele. Selle tulemusel loodi Gigabit Ethernet Alliance (GEA), millesse kuuluvad mitu nimekat tootjat, kes tahavad saavutada andmeedastuskiirust 1 Gbit/s. Langevate soetamishindade tõttu kasutatakse Gigabit Etherneti üha sagedamini lõppseadmete ja juurdepääsukommutaatorite ühendamiseks. Kui otsustada sidekanali valikul vaskkaabli kasuks, tuleks valida vähemalt CAT-5-tüüpi kaabel. Kuna seda kasutatakse sageli ka Fast Etherneti puhul, on võimalik olemasoleva kaabliinfrastruktuuri pealt ümber liikuda Gigabit Etherneti peale.
- 10 Gigabit Ethernet - Etherneti variantide järgmiseks generatsiooniks on 10 Gigabit Ethernet (10 Gbit/s). 10 Gigabit Ethernet võimaldab infot vahetada kaheksa erineva sidekanali kaudu. Lisaks vaskkaablile (vähemalt CAT-6, eelistatult CAT-7) saab kasutada seitset liiki valguskaableid. Kõrge hinna ja vähese leviku tõttu sobib 10 Gigabit Etherneti kasutada ainult magistraalvõrgu valdkonnas.

Token-Ring

Loaringi tehnoloogiat (Token-Ring) on kirjeldatud standardis IEEE 802.5 ja see põhineb loa kettedastuse (Token-Passing) meetodil. Selleks kasutatakse erilist ringlevat andmepaketti (Token), mis määrab, milline lõppseade tohib sidekanalit kasutada. Kui lõppseade saab loa, hõivab ta sidekanali ja edastab loa järgmisele lõppseadmele. See tagab, et sidekanal on hõivatud alati ainult ühe lõppseadme poolt. Selle deterministliku meetodi puhul ei saa erinevalt Ethernetist esineda olukorda, kus üksikud lõppseadmed peavad võrgu suure koormuse puhul ootama määramatult kaua andmete edastamise võimalust. Loaring võimaldab fikseeritut maksimaalset ooteaega. Loaringi võrk on teostatud tavaliselt füüsilise topeltringina, mille tõttu suureneb olulisel määral võrgu käideldavus, kuna ühe jaama tõrke või ühe ringi katkemise korral saab vigasest kohast teise ringi kasutamisega mööda pääseda. Loaringi andmeedastuskiirus võib olla 4 või 16 Mbit/s, mistõttu ei soovitata seda praegu enam suuremas osas kohtvõrkudes magistraalvõrgu tehnoloogiana kasutada. Kasutatav ribalaius on liiga väike. 1997. aasta septembris asutati mitme nimeka tootja poolt High Speed Token Ring Alliance (HSTR), eesmärgiga saavutada andmeedastuskiirus 100 Mbit/s ja hiljem 1 Gbit/s. Eesmärgiks seati IEEE 802.5 standardit täiendamine 1998. aasta keskpaigaks. Kuna neid variante alles arendatakse, ei saa praegusel hetkel nende kasutamist soovitada.

FDDI

FDDI (Fiber Distributed Data Interface) standard defineeriti aastal 1989 ANSI poolt ja see põhineb sarnaselt loaringile loa kettedastuse meetodil. Sarnasusele vaatamata kasutatakse siin täiendavalt Early-Token-Release tehnoloogiat, mille puhul saadetakse luba kohe pärast viimast andmepaketti edasi järgmisele lõpp-

seadmele. See vähendab loa tühikäiguaega ja võimaldab saavutada suuremat ribalaiust. FDDI kasutab andmete edastamiseks valguskaableid edastuskiirusega 100 Mbit/s. Tänu suurele läbilaskevõimele on see ideaalne magistraalvõrkudele. Lisaeeliseks on veataluvus tänu topeltringi topoloogiale ja valguskaablite kasutamisest tulenevale häirekindlusele elektromagnetiliste segajate suhtes. Erinevalt Ethernetist sobib FDDI ka kasutusajast sõltuvate multimeediarakenduste jaoks, kuna see suudab tagada maksimaalset viivitusaega. Kui kasutada andmete edastamiseks mõlemat ringi, on võimalik isegi andmeedastuskiirus 200 Mbit/s, kuid sel juhul jääb ära kõrgema veataluvuse eelis, kuna ühe ringi tõrke korral ei saa enam automaatselt kasutada teist ringi. Samas on FDDI-komponendid sarnase funktsiooniga Etherneti komponentidest kallimad, nii et FDDI kasutamisest tekkivaid eeliseid tuleb alati võrrelda sellega kaasnevate kuludega. FDDI-d saab kasutada ka vaskkaablitega, sellisel juhul nimetatakse seda CDDI-ks (Copper Distributed Data Interface).

ATM

ATM on asünkroonse edastusrežiimi lühend (Asynchronous Transfer Mode). See mõiste tähistab andmeedastusmeetodit, mis sobib väga hästi kasutamiseks magistraalvõrgu valdkonnas ja suudab seal pakkuda ka reaalajateenuseid. ATM-i puhul edastatakse igat liiki infot fikseeritud pikkusega pakettides, mida nimetatakse rakkudeks. Tegu võib olla suvaliste andmetega, nt heli- või videoandmetega. Pakettide ühesugune pikkus võimaldab ATM-kommutaatoritel rakkude töötlemise jätta peaaegu täielikult riistvarakomponentide hooleks, millega saavutatakse parem läbilase. Sellest tulenevalt saab ükskõik millise info edastamiseks välja arvutada viivituse, mis tähendab, et rakendustele saab anda garanteeritud ribalaiuse. Tänu sellele on ATM väga sobiv tehnoloogia multimeediarakendustele, kuna see võimaldab garanteerida arvutatavat reaalajakäitumist ja teenuse kvaliteeti (Quality of Service, QoS). See tähendab, et igale ühendatud seadmele saab määrata vajaliku ribalaiuse staatiliselt või dünaamiliselt. Edastamine ise toimub virtuaalühenduste põhimõtte alusel. Sides osalevate seadmete vahel ei kasutada fikseeritud kanaleid. Rakke transporditakse läbi võrgu alles nende loomise hetkel eelnevalt kindlaksmääratud teed mööda. Sellisel moel saavutatakse edastuskiiruseks tavaliselt 25 MBit/s, 155 MBit/s või 622 MBit/s. ATM-komponendid on väga kallid, seepärast tuleks investeerimiskindluse tagamiseks püüda neid integreerida kohtvõrgus juba olemasolevate teiste tehnoloogiate komponentidega. Tuleb arvestada, et ATM ei toeta leviedastust (broadcasts) ega MAC-aadresside rakendamist, mis on aga suurema osa protokollistike nagu TCP/IP või SPX/IPX puhul kasutamise eelduseks.

Selleks puhuks on olemas kolm lahendust:

- Classical IP-over-ATM (CIP) - Selleks, et kasutada IP-d ATM-i kaudu, loodi RFC 1577 (Classical IP-over-ATM), mis võimaldab TCP/IP-protokollistikuga varustatud lõppseadmetel transportimiseks ATM-i kasutada.
- LAN Emulation (LANE) - Siin emuleeritakse klientsüsteemide jaoks OSI-mudeli 2. kihis kõiki olulisi LAN-tehnoloogiaid, mille tagajärjel muutub ATM nende jaoks sarnaseks Etherneti või loaringi võrguga. Seeläbi muutub võimalikuks side tavalise LAN-i ja ATM-i vahel.
- Multiprotocol-over-ATM (MPOA) - MPOA on üldjoontes klassikalise ATM-i ja LANE-i edasiarendus. Erinevalt LANE-st töötab MPOA OSI-mudeli 3. kihis

ja kasutab LANE-i andmete edastamiseks 2. kihti. Kuna MPOA rakendab seega nii sildamist (2. kiht) kui ka marsruutimist (3. kiht), suudab see täielikult konfigureerida marsruuditud ATM-võrku. Samal ajal jäävad alles kõik ATM-tehnoloogia eelised, nt rakendustele garanteeritud ribalaiused.
- 40- ja 100-gigabitine Ethernet - Etherneti-variantide järgmine põlvkond on 40/100-gigabitine Ethernet. Osaliselt veel väga kõrgete hindade tõttu neid variante praegu eriti ei kasutata.

Magistraalvõrgu tehnoloogia valimiseks on üldkehtiva soovituse andmine, nagu juba mainitud, võimatu. Lisaks turvanõuetele on siin olulised ka tulevikuperspektiivi, ökonoomsuse, skaleeritavuse ja olemasolevate komponentide integreerimise kriteeriumid. Olenevalt valitud protokollist saab kasutada ainult teatud kaablitüüpe, millele kehtivad omakorda teatud kindlad pikkuse piirangud (vt ka M 5.2 Võrgu sobiv topoloogia).

Sobiva magistraalvõrgu tehnoloogia valimine peab toimuma kohtvõrgu magistraalvõrgu piirkonnale kehtestatud nõuete alusel, võttes arvesse kättesaadavust, ribalaiust ja jõudlust. Need nõuded peavad olema määratletud ja dokumenteeritud.

Kontrollküsimused:

- Kas kohtvõrgu magistraalvõrgu valdkonnale esitatavad nõudmised, mis puudutavad käideldavust, ribalaiust ja jõudlust, on sõnastatud ja dokumenteeritud?
- Kas valiku tegemisel võrreldi kõiki olulisi magistraalvõrgu tehnoloogiaid?
- Kas kohtvõrgu magistraalvõrgu piirkonnale esitatavad nõuded, mis puudutavad kättesaadavust, ribalaiust ja jõudlust, on sõnastatud ja dokumenteeritud?
- Kas sobiva magistraalvõrgu tehnoloogia valik toimus kehtestatud nõuete alusel?

M 5.61 Sobiv füüsiline segmenteerimine

Algatamise eest vastutavad: IT-juht, infoturbeosakond
Rakendamise eest vastutavad: administraator

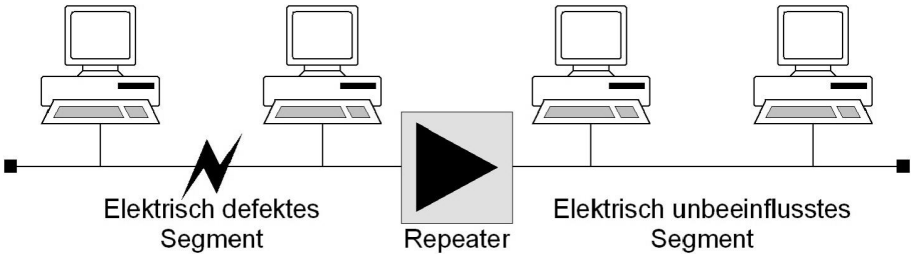
Füüsilise segmenteerimise all mõistetakse segmentide moodustamist aktiivsete ja passiivsete võrgukomponentide abil 1., 2. või 3. kihis. Sobiv füüsiline segmenteerimine võib suurendada käideldavust, terviklust ja konfidentsiaalsust. Selle saavutamiseks võib kasutada erinevaid võrgukomponente (vt M 5.13 Võrgu ühendusaparatuuri õige kasutamine).

Käideldavus

Käideldavuse valdkonna all käsitletakse võrgu jõudlust ja saadaolevat ribalaiust. Seda saab suurendada, kui võrk OSI-mudeli 1., 2. või 3. kihis lahutada. Esimese kihi lahutamisel suureneb üksikute segmentide käideldavus vähimal võimalikul määral, kuid selle eest saavutatakse segmentidevaheline maksimaalne läbilase.

Kolmanda kihi lahutamisel suureneb käideldavus maksimumini ja segmentidevaheline läbilase langeb miinimumini. Kasutades 1. kihi segmenteerimiseks järgurit, suureneb võrgu käideldavus seeläbi, et ühe segmendi elektrivead ei saa mõjutada teisi segmente.

Näide: võrgus, mis koosneb kahest omavahel järguriga ühendatud Thin-Ethernet- segmendist, ei mõjuta ühes segmendis ära jäänud lõpetamine teise segmendi tööd.



Joonis: segmentide elektriline lahutamine järguri abil, eesmärgiga suurendada käideldavust
Elektrisch defektes Segment – elektririkkega segment, Repeater – järgur; Elektrisch unbeeinflusstes Segment – elektriliselt korras segment

Sildade ja kommutaatorite puhul kehtib esmalt sama põhimõte mis järgurite puhul, kuna need katavad 1. kihi. Sellele funktsioonile lisaks isoleeritakse 2. kihi vigased andmepaketid ja segmendis toimuvad kokkupõrked. Täiendavalt vähendatakse veel ka segmentide koormust, kuna andmepakette saab segmentide vahel sihipäraselt juhtida. Seejuures tuleb jälgida, et kasutatav sild või kommutaator oleks piisavalt suure jõudlusega (filtreerimis- ja edastamisjõudlusega), et segmentidevahelist andmeliiklust saaks töödelda ilma viivitusteta. Tavaliselt töötavad sillad/kommutaatorid OSI-mudeli 2. kihis. Need analüüsivad ühendusmaatriksi ülesehitamiseks osalevate süsteemide MAC-aadresse vastavates segmentides.

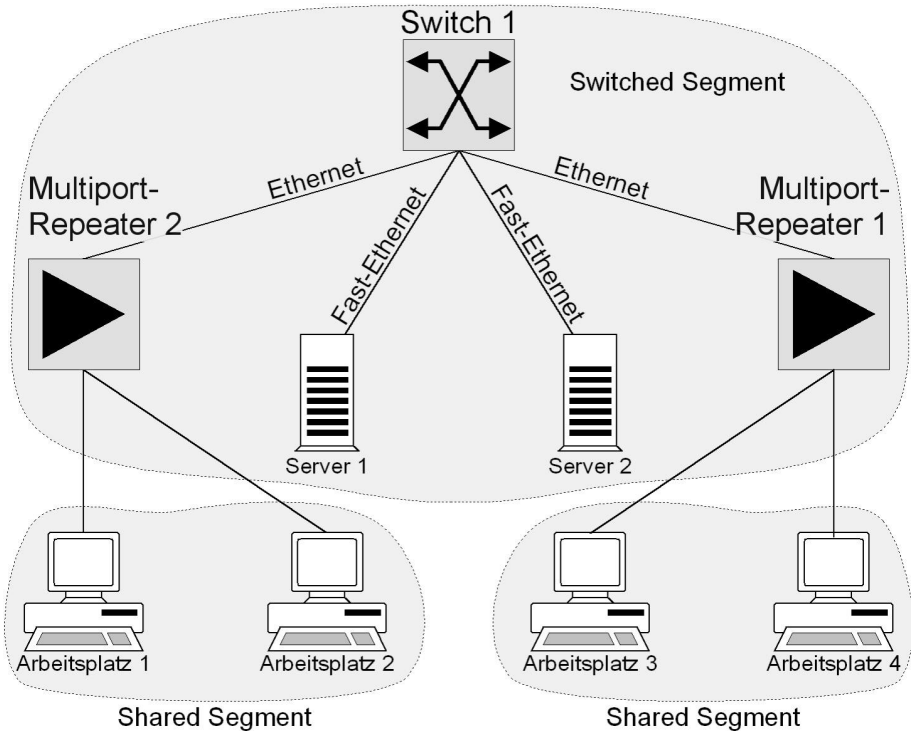
Mõningad tootjad pakuvad ka 3. kihis töötavaid kommutaatoreid, mis kasutavad ühendusmaatriksi ülesehitamiseks nt IP-aadressi. Vastav ülesehitamine toimub mõlemal juhul automaatselt, kuid mõne mudeli puhul on võimalik seda ka käsitsi mõjutada. Mõned tootjad pakuvad lisavõimalust, mis lubab ühendusmaatriksit luua käsitsi (tsentraalse vahendiga) portide tasandil, st tegeliku kaablitrassi tasandil (pordi või konfiguratsiooni Switching). Marsruuterid, mis töötavad 3. kihis, koondavad endasse järgurite ja sildade käideldavuse omadused ja täiendavad neid võimalusega analüüsida 3. kihi logisid. Seeläbi toimub koormuse jaotamine kõrgemal tasandil ja see võimaldab võrguliiklust peaaegu täielikult kontrolli all hoida. Eriti oluline on see, et juhul, kui segmendid on lahutatud marsruuteriga, ei suunata nende segmentide (osavõrkude) vahel edasi leviedastusi. Ühe segmendi leviedastuse torm ei saa seega mõjutada teist segmenti.

Lähtuvalt võrguliikluse analüüsi tulemustest (vt M 2.139 Olemasoleva võrgukeskkonna läbivaatus), tuleks vajadusel kasutada füüsilist segmenteerimist, et ribalaiust/jõudlust vajalikul määral suurendada.

Näide:

Ühe võrgu piires on olemas või kavandatud tsentraalsed serverid faili- ja trükiteenustele ning rakendustele. Kõrge jõudluse ja käideldavuse tagamiseks võib olla vajalik ühendada neid eraldi kommutaatoriga ja ühendad selle kommutaatori kaudu üksikute tööjaamadega (jagatud või kommuteeritud). Võimalusel peaks serveri ja kommutaatori vaheline ühendus olema vähemalt Fast Etherneti ühendus. Reeglina võib öelda, et parema jõudluse jaoks tuleks kommuteeritud võrku eelistada jagatud võrgule, kuna jagatud võrgus peavad kõik ühendatud osalejad jagama saadaolevat ribalaiust. Kommuteeritud võrgus seevastu saab iga kasutaja kasutada vähemalt kuni järgmise aktiivse võrgukomponendini täit ribalaiust. Seejuures tuleb siiski arvestada vajadusega struktureeritud juhtmestiku (tähekujulise) järele ning täielikult kommuteeritud võrgu suhteliselt suurte kuludega.

Alternatiiviks on lahendused, mis ühendavad üksikuid segmente magistraalvõrgu valdkonnas või suure võrgukoormuse valdkonnas (nt töögruppides) kommutaatori kaudu ning need segmendid on omakorda teostatud Shared-Media kohtvõrguna (vt joonis 2). Lisaks on alati võimalik üksikuid kõrge jõudlusvajadusega töökohasüsteeme otse kommutaatori külge ühendada. Siis, kui jagatud võrk või jagatud segment võib olla nii siini- kui ka tähekujuline, on käideldavuse ja investeeringute seisukohast mõistlik teostada see samuti struktuurjuhtmestikuna (tähekujulisena) (vt M 5.2 Võrgu sobiv topoloogia).



Joonis: kommuteeritud ja jagatud segmentidest koosneva võrgu näide. Serverite ühendamine toimub Fast Etherneti abil.

Switch – kommutaator; Switched Segment – kommuteeritud segment; Arbeitsplatz – töökoht; Shared Segment – jagatud segment

Konfidentsiaalsus

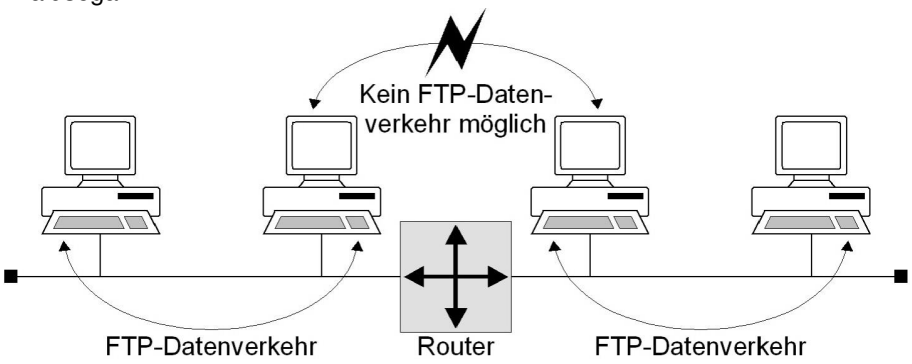
Konfidentsiaalsuse suurendamiseks sobivad kõik meetmed, mis takistavad andmete vahetamist kahe segmendi vahel. Sel põhjusel ei sobi kasutada ainult järgurit (repeater). Mõningad tootjad pakuvad mitmepordilisi järgureid, mida saab seadistada selliselt, et vastava järguri vahendusel saavad võrgus töötada ainult teatud osalejad. See võimaldab teatud määral välistada olukorda, kus volitusteta kasutajad ise võrguga liituvad. Sillad/kommutaatorid ja marsruuterid suurendavad konfidentsiaalsust seeläbi, et nad suudavad takistada ja kontrollida 2. ja 3. kihi andmeliiklust ning segmente eraldi pordi tasandil ühendada ja lahutada. Ka teatud tootjate sildade/kommutaatorite puhul on võimalik võrgus osalejate juurdepääsu piirata.

Marsruuterid pakuvad siinkirjeldatud komponentidest kõige ulatuslikumaid kontrollivõimalusi. Marsruuterid võimaldavad määrata juurdepääsu teistesse võrkudesse ja selleks juurdepääsuks kasutatavaid teid, lisaks saab nendega täpsustada, milline võrgus osaleja tohib teiste segmentide süsteemidega sidet pidada ja millisel alusel. Välistades marsruuteril teatud 3. tasandi protokollid, saab takistada olukorda, kus selle protokolli andmed võiksid sattuda teise segmenti. See toimub marsruuterites sobivate filtrireeglite defineerimisega, mis võidakse moodustada protokolli tasandil. Näites saab TCP/IP protokollistiku puhul kindlad TCP ja UDP pordid üleminekuks teise segmenti valikuliselt sulgeda või vabaks anda. Kõrgema-

tel kihtidel töötavaid komponente, nt rakendustasandi tulemüüre, siin ei käsitleta (vt M 2.75 Sobiva rakenduslüüsi valimine).

Näide:

Kui võrk eraldada marsruuteriga ja vastavate filtrireeglite konfigureerimisega, saab luua olukorra, kus segmentide vahel pole FTP- ja TFTP-andmeedastus (port 20 ja 21 või 69) enam võimalik ja seega pole ka enam midagi, mida keegi kõrvaline saaks pealt kuulata. Samuti ei edastata osavõrkude vahel leviedastuse andmeid. Lisaks peavad filtrid olema standardina konfigureeritud selliselt, et esmalt on side maksimaalselt piiratud ja alles seejärel avardatakse kasutusvõimalusi vastavalt vajadusele ja teenustele. Siin tuleks võib-olla arvestada IP-põhise filtreerimise võimalusega.



Joonis: näide osavõrkude lahutamisest 3. kihis marsruuteri abil
Kein FTP-Datenverkehr möglich – FTP-andmeside on võimatu; FTPDatenverkehr – FTP-andmeside; Router - marsruuter

Andmete ja võrgu terviklus

Kuni 3. kihini tagatakse andmete terviklus enamasti rakendatava võrgujuurdepääsuprotokolliga, sellal kui võrgu tervikluse tagamine, st tegeliku võrguolukorra kattuvus planeeritud ja ettenähtud füüsilise ja loogilise segmenteerimisega vajab lisameetmeid. Need meetmed peavad takistama volitamata ja valede sideühenduste loomist ning süsteemijuurdepääsusid, mis on terviklikus võrguseisundis keelatud.

Võrgu terviklus tagatakse seega suuremas osas järgnevalt:

- võrgukomponentide muudatusi (möödamanööverdamine, uute, volitamata komponentide installeerimine jne) kas takistatakse või vähemalt tuvastatakse (riistavarapõhine ohutus)
- võrgukomponentide konfiguratsiooni muudatusi (nt marsruutimisprotokollid, Port-Switching-Matrix või VLAN-i kuuluvuse määramine) suudetakse takistada või vähemalt tuvastada (tarkvarapõhine ohutus).

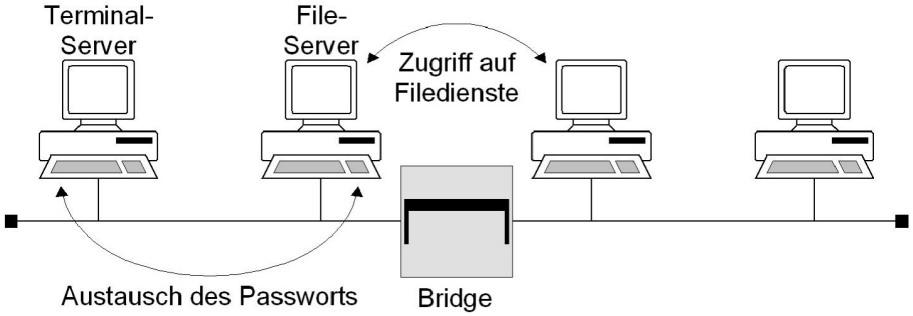
See eeldab võrgukomponentidele juurdepääsu piiramist piisava rangusega (nt kasutades infrastruktuuri meetmeid, mis puudutavad jaotusruumi, juhtmestikku jne) ja võrguhalduse sellist kavandamist, et võrgust võrgukomponentidele suunatud volitamata juurdepääsud oleksid takistatud. Kolmanda kihi andmete (nt raken-

dusandmete) tervikluse kaitse suurendamist ei saa tagada ainult võrgukomponentide abil, kuid andmetervikluse pihta suunatud rünnak muutub raskemaks. Selleks saab kasutada võrgukomponente, mis takistavad andmepakettide pealtkuulamist ja muutmist.

Nendeks võivad olla nt sillad/kommutaatorid ja marsruuterid, mis suudavad jaotada võrgu segmentideks või osavõrkudeks, millevahelist andmeliiklust saab kontrollida, piirata või konfigureerida. Eriti just end automaatselt konfigureerivate võrgukomponentide puhul, nt sildade ja kommutaatorite puhul, on loogilise kokkukuuluvuse vastavus füüsilise konfiguratsiooniga vägagi oluline. Ainult nii on võimalik tagada, et loogilise rühma andmepaketid jäävad ka tegelikult samasse füüsilisse segmenti. Sildade/kommutaatorite puhul, mis lubavad võimalike ühenduste konfigureerimist portide põhjal (Port-Switching), saab ühendusvõimalusi 1. kihis kontrollida ka käsitsi.

Näide:

Süsteemid, mis võimaldavad terminalide ühendamist võrguga (terminaliserverid) ja süsteemid, millele terminaliserverist peab ligi pääsema, tuleb silla abil ühe segmendina ülejäänud võrgust eraldada. Ainult nii saab vältida olukorda, kus terminaliserveri ja sihtsüsteemi vahel toimunud paroolivahetust kuulatakse pealt (ja muudetakse) mõnest muust segmendist.



Joonis: segmentide eraldamine silla abil tervikluse ja konfidentsiaalsuse suurendamiseks

Terminalserver – terminaliserver, Fileserver – failiserver; Zugriff auf Filedienste – juurdepääs failiteenustele; Austausch des Passwoerts – paroolide vahetamine, Bridge - sild

Lisaks tuleb sobiva dimensioneerimise ja võrgukomponentide valimisega tagada, et ülekoormusest või riketest tulenev andmepakettide kadu ja võltsimine oleksid välistatud.

Kontrollküsimused:

- Kas kohtvõrgu kavandamisel mõeldi füüsilisele segmenteerimisele?
- Kas käideldavust (eriti aga jõudlust), konfidentsiaalsust ja terviklust puudutavad nõuded on välja töötatud ja kas nendega on arvestatud?

M 5.62z Sobiv loogiline segmenteerimine

Algatamise eest vastutavad: infoturbeametnik, IT-juht

Rakendamise eest vastutavad: infoturbeametnik, IT-juht

Sobivate aktiivsete võrgukomponentidega on võimalik võrku vaatamata selle kindlale füüsilisele segmenteerimisele ka veel loogiliselt segmenteerida. Selleks pakuvad võimalust niinimetatud virtuaalsed LAN-id (VLAN-id). VLAN-idega saab rühmi võrgus ühendada nii, nagu need oleksid samas füüsilises segmendis. Seetõttu tekib eelkõige võimalus moodustada dünaamiliselt ja ajakohaselt uusi rühmi või neid ümber rühmitada, ilma et oleks vaja muuta füüsilist võrku.

Olemas on kaks liiki VLANe: staatilised ja dünaamilised VLAN-id. Staatiliste VLAN-ide (mida nimetatakse ka portidel põhinevateks VLAN-ideks) korral määratakse kommutaatori pordid kindlalt ühele VLAN-ile, olenemata ühendatud seadmest. Dünaamiliste VLAN-ide korral juhitakse VLAN-ide kuuluvust näiteks ühendatud seadme MAC-aadressi või IP-aadressi kaudu. Kuna neid sisusid on kerge manipuleerida, tuleks ka juba tavalise kaitsevajaduse puhul loobuda võimaluse korral dünaamiliste VLAN-ide kasutamisest. Seetõttu neid siin rohkem ei vaadelda.

Võrgu tõhusaks eraldamiseks VLAN-idega võib valida arhitektuuri, mis koosneb neljast tsoonist:

- sisevõrk,
- turvalüüsi tsoon (ALG-tsoon),
- internetiühendus ja
- haldustsoon (vt M 2.467 Terminaliserveri regulaarsete taaskäivitustsüklite plaanimine). Tsoonid peavad olema füüsiliselt eraldatud. Selle põhjal võib moodustada vastavad alamvõrgud (vt ka M 5.77z Alamvõrkude rajamine).

Igal juhul peavad kaitsevajadust silmas pidades olema täidetud järgmised põhilised alamvõrkude tingimused:

- VLAN-ide sees peaksid olema üksnes sama kaitsevajadusega tööprotsessid/töörühmad.
- Eraldatud alamvõrkude kaitsevajadus tohib olla üksnes kas „normaalne” või „kõrge”. Väga kõrge kaitsevajaduse korral ei tohi VLAN-e turvalisuse põhjustel kasutada.
- Kui eraldatavate alamvõrkude kaitsevajadus on sama, on VLAN-ide kasutamine põhimõtteliselt mõeldamatu. Erandi moodustab üksnes olukord, kus VLAN-ide omanikud on erinevad asutused. Sellisel juhul peaks eraldamine olema kas füüsiline või tuleks rakendada krüpteerimist, et kaitsta edastatavaid andmeid lubamatu juurdepääsu eest.
- Kui eraldatavate alamvõrkude kaitsevajadus on erinev, sõltub VLAN-ide kasutamine kasutusolukordadest (vt VLAN-ide kasutusolukorrad).

Lisaks eespool mainitud, kaitsevajadust puudutavatele põhilistele tingimustele tuleb tähelepanu pöörata ka järgmistele üldistele ja tehnilistele, võrguühenduselementidele esitatavatele nõuetele:

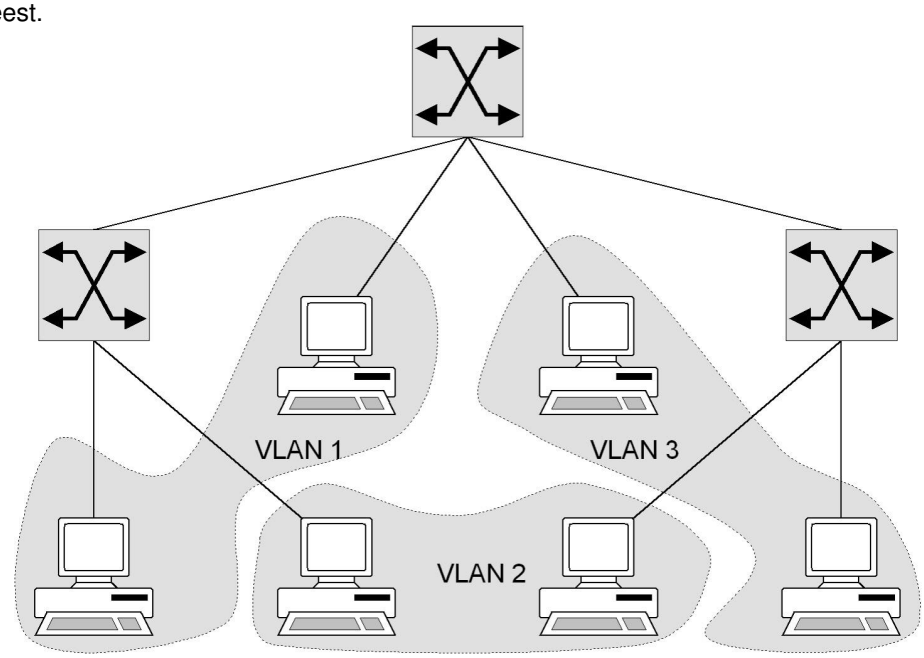
- mingil juhul ei tohi luua VLAN-i kaudu ühendust rakenduslüüsi (ühendus internetiga) ees oleva tsooni ja selle taga asuva sisevõrgu vahel.
- VLAN-id ei paku nimetamisväärset kaitset füüsilise edastustehnika (kaablid, pistikud, liidesed jne) pealtkuulamise vastu. Kui näiteks paroole edastatakse loetava tekstina, on neid võimalik pealt kuulata. Seetõttu tuleb rakendada täiendavaid turvameetmeid, nagu näiteks krüpteerimine.
- Kasutatavate aktiivsete võrgukomponentide põhiplaatidel ja üleslüliportidel peab olema piisav läbilaskevõime.
- Kasutatavad kommutaatorid tuleb konfigureerida turvaliselt (vt M 4.202 Marsruuterite ja kommutaatorite turvaline võrgu-aluskonfiguratsioon).

VLAN-ide kasutusstsenaariumid

Alljärgnevate stsenaariumide puhul lähtutakse võrguarhitektuurist, mis koosneb neljast tsoonist (vt ka M 2.476 Interneti turvalise ühendamise kontseptsioon).

1. stsenaarium: VLAN-ide kasutamine sisevõrgus

Sisevõrgus tohib VLAN-e kasutada, et eraldada üksteisest erineva kaitsevajadusega alamvõrke. Erand tehakse siiski juhul, kui kommutaatoril olevatel VLAN-idel on sama kaitsevajadus, need täidavad samu ülesandeid, aga kuuluvad erinevatele asutustele. Sellisel juhul peaks eraldamine olema kas füüsiline või tuleks rakendada krüpteerimist, et kaitsta edastatavaid andmeid lubamatu juurdepääsu eest.

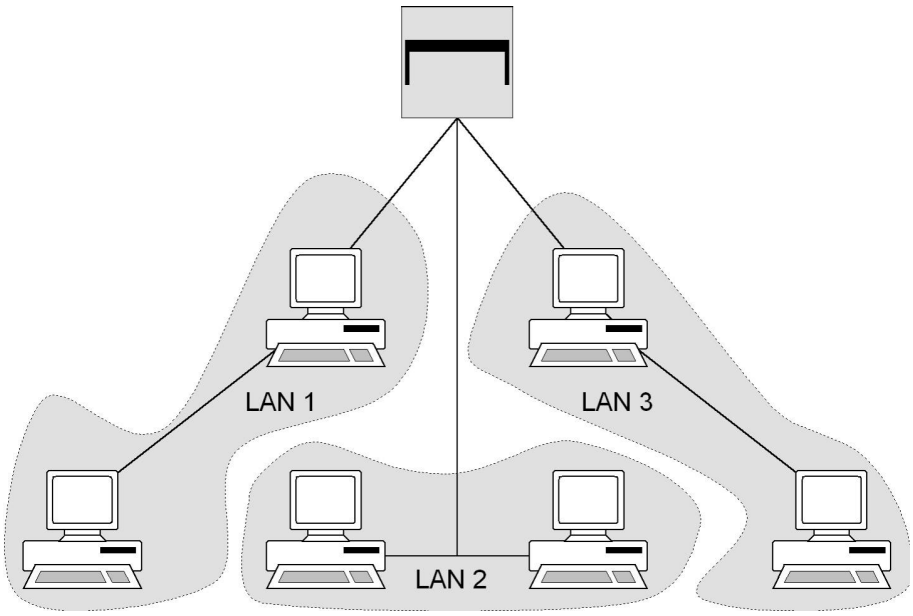


Joonis: VLAN-i moodustamine mitme kommutaatoriga

2. stsenaarium: VLAN-ide kasutamine ALG-tsoonis

Soovitatav on jaotada ALG-tsoon kaheks alamtsooniks (sisemine ja väline DMZ). Välises DMZ-is peaksid asuma IT-süsteemid, millel on avalik IP-aadress,

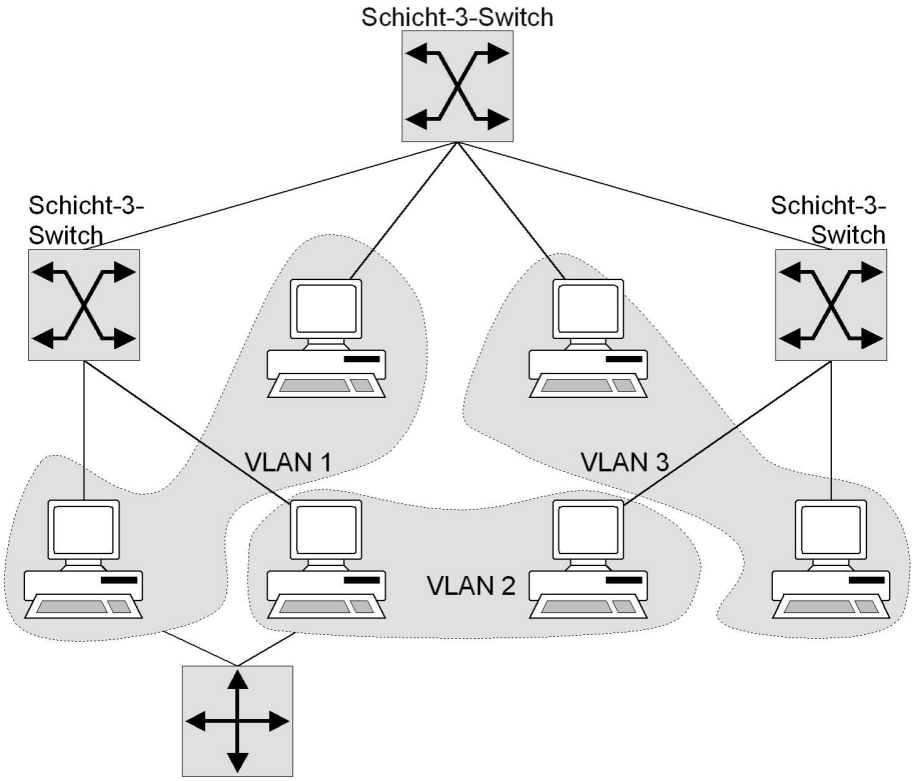
et need oleksid internetist kättesaadavad. Sisemises DMZ-is peaksid olema IT-süsteemid, millel on tavaliselt privaatsed IP-aadressid ja mis seega ei ole internetist põhimõtteliselt otse kättesaadavad. Vastavates DMZ-ides tohib eraldamiseks kasutada VLAN-e. Sisemist DMZ-i ei tohiks siiski välisest DMZ-ist VLAN-ide abil eraldada.



Joonis: VLAN-i moodustamine sillaga

3. stsenaarium: VLAN-ide kasutamine haldustsoonis

Füüsiliselt eraldatud haldusvõrke tohib eraldada VLAN-ide kaudu. Tähelepanu tuleb siiski pöörata sellele, et välimine paketifilter ja sellega ühendatud seadmed asuksid oma alamvõrgus ja mitte nii, et VLAN-e kasutades luuakse ilma ALG-deta ühendus välise paketifiltri ja sisevõrgu vahel.



Joonis: turvaliste VLAN-ide moodustamine 3. kihi kommutaatoritega
Schicht-3-Switch – 3. kihi kommutaator

Kontrollküsimused:

- Kas VLAN-is asuvad üksnes sama kaitsevajadusega tööprotsessid või töörühmad?
- Kas tsoonid on üksteisest füüsiliselt eraldatud?
- Kas on tagatud, et väga kõrge kaitsevajaduse korral ei kasutata VLAN-e?
- Kas on tagatud, et rakenduslüüsi ees (ühendus internetiga) oleva tsooni ja selle taga asuva sisevõrgu vahel ei oleks ühendusi?
- Kas VLAN-ides kaitstakse andmeid asjakohaselt pealtkuulamise eest, näiteks krüpteerimise abil?
- Sisevõrk: kas VLAN-ide korral, mis kuuluvad erinevatele asutustele, toimub selge eraldamine (füüsiline või krüpteeringuga)?

M 5.63z GnuPG või PGP kasutamine

Algatamise eest vastutavad: infoturbeosakond, administraator

Rakendamise eest vastutavad: administraator, kasutaja

GNU Privacy Guard (GnuPG) ja Pretty Good Privacy (PGP) on levinud programmid, millega saab sõnumeid ja faile nii krüpteerida kui ka dekrüpteerida ning lisaks saab neid varustada ka digiallkirjaga (nimetatakse ka elektrooniliseks allkirjaks).

Mõlemad tarkvaratööriistad kasutavad funktsioone, mis on määratletud OpenPGP-standardis (RFC 2440). Krüpteerimise abil saab kaitsta info konfidentsiaalsust, digitaalne allkirjastamine võimaldab kontrollida, kas fail või sõnum on autentne ning kas seda on manipuleeritud. Nii GnuPG kui ka PGP abil saab lisaks täita võtmehalduse ülesandeid, nt lisada ja eemaldada võtmeid.

Krüpteerimine ja digitaalne allkiri

GnuPG ja PGP puhul kasutatakse sümmeetrilisi ja asümmeetrilisi krüptograafilisi protseduure. Sümmeetrilised, nt AES ja IDEA, on mõeldud andmete krüpteerimiseks, asümmeetrilised, nt ElGamal, RSA ja DSA/DSS, on mõeldud võtmehalduseks või allkirjade loomiseks. Mõlemad vahendid genereerivad ja kasutavad avalikke võtmeid ja privaatvõtmeid nn võtmepaarides. Iga privaatvõtme kohta on olemas täpselt üks avalik võti. Ainult avalikku võtit tundes on privaatvõtme väljaarvutamine praktiliselt võimatu. Avaliku võtmega krüpteeritud ja privaatvõtmega allkirjastatud sõnum on dekrüpteeritav ainult vastava privaatvõtmega ning seda saab kontrollida saatja avaliku võtmega. Avaliku võtme võib avalikustada igaühele. See on mõeldud selleks, et krüpteerida sõnumeid, mis on mõeldud privaatvõtme omanikule. Sõnumi volitamata manipuleerimise tõendamiseks ja seega muudatuste eest kaitsmiseks arvutab GnuPG või PGP saatja privaatvõtme abil sõnumile kontrollkoodi ehk digitaalse allkirja. Iga sidepartner saab saatja avaliku võtme abil kontrollida, kas sõnumi lõpus olev kontrollkood langeb kokku talle saadetud sõnumiga või kas sõnumit on volituseta muudetud. Tehnilisel tasandil eraldatakse turvalisuse põhjustel digitaalsete allkirjade võtmed ja krüpteerimise võtmed. See on kasutaja jaoks tavaliselt nähtav. GnuPG või PGP kasutamisel tuleks rakendada eespool kirjeldatud funktsioonide kombinatsiooni. Sõnumid/failid tuleks standardina allkirjastada saatja privaatvõtmega ja krüpteerida seejärel vastuvõtja avaliku võtmega, et tagada parim võimalik turvalisus.

Versioonid

Nii GnuPG kui ka PGP on saadaval levinumate arvutiplatvormide (Unix, GNU/Linux, Microsoft Windows) jaoks. PGP puhul on olemas ka versioonid MacOSi jaoks. GnuPG puhul on tegu vaba/avatud lähtekoodiga tarkvaraga, mille uusim versioon on hetkel 2.1.9. PGP levinud versioonid on 2.6.3i, ja 5.x kuni 8.x. Versioonidel alates numbrist 5.x on olemas graafiline kasutajaliides, kuid nende ühilduvus vanemate versioonidega pole täielik. Kuna ühilduvus vanemate versioonidega on puudulik, tuleks enne krüpteeritud sõnumite vahetamist küsida, millist PGP-versiooni sidepartner kasutab. PGP on saadaval erinevatest allikatest, lisaks on saadaval erinevate WWW, FTP või meiliserverite tasuta versioonid. GnuPG ja PGP vaheline ühilduvus ei ole täielik. Üheks põhjuseks on tarkvara-

patendid (osade PGP-versioonide poolt standardina kasutatav IDEA algoritm on patenteeritud) ja teiseks väikesed kõrvalekalded OpenPGP-standardist. RSA-patendi aegumisega jäi siiski üks oluline takistus vähemaks. GnuPG toetab RSA-d alates versioonist 1.0.3. Nende probleemide vältimiseks tuleks võimaluse korral välja valida ainult üks tarkvaratööriist. Kui see on võimatu, tuleb kasutada eranditult OpenPGP-ga ühilduvaid võtmeid. Sel moel tagatakse, et sidepartnerid, kellel on 3DES, omavad ühist sümmeetrilist algoritmi. Sellisel juhul ei esine eespoolkirjeldatud ühilduvusprobleemi, mis tuleneb IDEA kasutamisest. Lisainfot selle kohta leiate GnuPG-projekti lehekülgedelt www.gnupg.org ja www.gnupg.de korduma kippuvate küsimuste alt.

Alates PGP 5. versioonist on kasutusel vaidlusi tekitav funktsioon nimega Corporate Message Recovery (CMR). CMR pakub võimalust muuta faile või sõnumeid, mida üks isik teise jaoks krüpteeris, ka kolmanda isiku jaoks dekrüpteeritavaks. Administraator saab konfigureerimise abil muuta sellise kolmanda võtme kasutamise ka kohustuslikuks. PGP 7. versioon sisaldab veel kahte täiendavat funktsiooni, mille abil võib olenevalt olukorrast juhtuda, et turvafunktsioonidest õnnestub mööda pääseda. Üks kasutuselevõetud funktsioone on serveripõhine võtmete taastamismehhanism, millega saab kasutaja võtit edasi kasutada ka siis, kui ta on nt vastava paroolfraasi ära unustanud. Teine funktsioon on paroolfraasi vahesalvestus, et kasutaja ei peaks seda PGP erinevate osasüsteemide vahel liikudes iga kord uuesti sisestama. Sarnane mehhanism on olemas ka versioonis 2.6.3i, mille puhul saab paroolfraasi salvestada keskkonnamuutujasse. Seda mehhanismi ei tohiks kasutada.

Eriti just siis, kui GnuPG-d või PGP-d kasutatakse Windowsi operatsioonisüsteemides, tuleb arvestada sellega, et nende tarkvaratööriistade turvamehhanismidest võib operatsioonisüsteemi turvaaukusid kasutades õnnestuda mööda pääseda.

Turvaline installeerimine ja kasutamine

GnuPG ja PGP puhul kasutatakse küll turvaliseks peetud krüptograafilisi meetodeid, kuid vale konfiguratsiooni ja kasutamisvigade tõttu võib turvalisuse aste langeda. Installeerimine ja konfigureerimine ning võtmete genereerimine pole GnuPG ja PGP puhul, sarnaselt suuremale osale teistele keerukatele krüptograafilistele toodetele, mitte just kõige lihtsam tegevus. Kasutusvigade vältimiseks tuleb vastava toote ja mõningate krüptograafiliste üldkontseptsioonidega esmalt harjuda. Seepärast peaks organisatsioonis üks töötaja õppima vahendit põhjalikumalt kasutama ja olema kontaktisikuks. Ta peaks suutma teistele kasutajatele õpetada, kuidas GnuPG-d ja PGP-d turvaliselt kasutada.

Esmalt tuleb eriti hoolikalt harjutada krüpteerimist, allkirjastamist ja võtmete haldamist ning alles seejärel tohib kasutaja programmi kasutama hakata. Lisaks oleks mõistlik kogu organisatsiooni ulatuses kasutada ühte programmiversiooni,

et vältida eespool kirjeldatud ühilduvusprobleeme. Nii GnuPG kui ka PGP kohta on olemas mahukas dokumentatsioon, mis tuleb enne kasutamist läbi lugeda. Kuna kogemused on näidanud, et mitte igal kasutajal ei jätku kannatust neid lugeda, tuleks koostada kirjalik juhis, mis on kohandatud organisatsiooni eripäradega.

Nende juhtumite lahendamiseks, kus kasutajatel tekib GnuPG või PGP kohta küsimusi, millele ei leia vastuseid kaasasolevast dokumentatsioonist, on mitmeid võimalusi:

- alustuseks on internetis olemas kogumikud korduma kippuvate küsimustega (frequently asked questions, FAQ);
- uudistegrupid, nagu alt.security.pgp, de.comp.security, sci.crypt, või meililistid aitavad probleemidele kiirelt lahendusi leida;
- PGP kohta on mitmeid raamatuid.

Võtmete genereerimine

Iga kasutaja genereerib GnuPG ja PGP puhul oma võtmepaari ise. Seejuures tuleb arvestada alljärgnevaga:

- Võtme pikkus – DSA/DSS- või RSA-võtme genereerimisel saab valida erineva pikkusega võtmete vahel. Arvestage, et pikema võtme korral suureneb vastupanu dekrüpteerimisele, kuid jõudlus langeb. Võtme pikkus peaks seetõttu olema 1024 bitti.
- Paroolfraas – võtme genereerimisel tuleb sisestada paroolfraas, mis kaitseb faili volitamata juurdepääsu eest, rakendades kaitsena privaatvõtit. Sarnaselt paroolidele ei tohi ka selle äraarvamine olla kerge. Näiteks on olemas Trooja hobused, mis otsivad sihilikult privaatvõtmetega faili (SECRING.*) ja saadavad selle meiliga kõrvalistele isikutele. Liiga lihtsa paroolfraasi korral ei suuda see jõurünnetele (automaatne parooli äraarvamine) vastu panna. Seepärast peaks paroolfraas sisaldama vähemalt kümmet märki, sh erimärke. Viirusetõrjeprogrammid suudavad tavaliselt küll Trooja hobuseid avastada, kuid selle eeldus on kasutaja arvutisse installeeritud programmi (või selle andmebaasi) pidev värskendamine.
- Kasutaja-ID – avalike võtmete hulka kuulub kasutaja-ID, mis peab olema võimalikult ainulaadne ja sisaldama meiliaadressi, nt kasutaja@bsi.bund.de.
- Juhuslikud arvud – võtmete genereerimiseks vajavad GnuPG ja PGP võimalikult juhuslikke algväärtuseid. Erinevad programmid ja versioonid kasutavad nende juhuslike väärtuste genereerimiseks erinevaid väärtusi. Näiteks palutakse kasutajal sisestada mõni suvaline tekst. Siinkohal oleks parem sisestada mõni „päris” tekst, nt võib selle sama lõigu siit tekstist ümber trükkida. Klaviatuuril lihtsalt „huupi toksimine” annab enamasti halvemaid tulemusi, kuna klahvivajutuste vahele jäävad ajalised viivitused võivad olla liiga lühikesed ja regulaarsed.

Võtmete säilitamine

Privaatvõtmeid hoitakse failis SECRING.*. Turvalise töö tagamiseks on määrava tähtsusega, et tagataks selle faili sisu konfidentsiaalsus ja kaitse manipulatsiooni-

de vastu. Juurdepääs sellele failile on küll paroolfraasiga kaitstud, kuid sellegipoolest ei tohiks seda hoida kohtvõrgus, isegi mitte ebapiisavalt kaitstud autonoomsüsteemidel. Võtmerõngad (võtmekogumid) tuleks salvestada disketile, mida kasutaja peab hoolikalt hoidma. Võtmete salvestamisel tuleks eelistada kiipkaarte. Lisaks tuleks failist SECRING.* luua varukoopia ning kirja panna paroolfraas. Varukoopiat ja paroolfraasi tuleb hoida eraldi kohtades, et vältida kõvaketta rikkest või kasutusveast tulenevat privaatvõtme kaotamist. Avaliku võtmega krüpteeritud sõnumeid ei saa sel juhul enam dekrüpteerida. Paroolfraasi üleskirjutamine ja turvalises kohas hoidmine on ülimalt tähtis ja on mõeldud ainult avariiolukordadeks. Kirjutuslaua lukustatud sahtel või muud sellised „turvalised“ kohad ei ole mitte mingil juhul sobivad kohad salajase võtme või paroolfraasi hoidmiseks.

Tühistussertifikaat

Pärast võtme genereerimist tuleb genereerida nn tühistussertifikaat (revocation certificate) ja see välja printida või disketile salvestada. Sellega saab avaliku võtme tühistada, kui paroolfraas unustatakse või kui seda ei saa mõnel muul põhjusel enam kasutada. Tühistamissertifikaati tuleb hoida turvalises kohas, et avaliku võtme tühistamine ei toimuks volitusteta.

Võtmete jagamine

Selleks, et vastuvõtja saaks saatja saadetud faili digiallkirja kontrollida või et saatja saaks sõnumit kindla adressaadi jaoks krüpteerida, läheb tal vaja oma sidepartneri avalikku võtit. Selle saatmiseks on erinevaid võimalusi, nt e-posti manus või WWW-server, kuid eelnevalt peab ta siiski veenduma, et võti kuulub tõesti õigele inimesele. Krüptograafiliselt kaitstud seose loomine inimese ja tema avaliku võtme vahel toimub sertifikaatide abil, mida väljastab usaldusväärne kolmas osapool.

GnuPG ja PGP puhul saab iga kasutaja kinnitada teiste inimeste avalikke võtmeid sertifikaatidega. Kasutaja tohib avalikku võtit sertifitseerida ainult siis, kui ta tunneb võtmeomaniku identiteeti või on seda kontrollinud ja avalik võti on isiklikult edastatud. Teine võimalus on kontrollida avaliku võtme ehtsust nn sõrmejäljega (fingerprint). Selleks arvutatakse avaliku võtme alusel arvurida (räsiväärtus) ja lisatakse võtmele. Pärast avaliku võtme saatmist saab nüüd seda arvurida saatjaga võrrelda, nt telefoni teel, et pärast sõrmejälje kinnitamist saadetud avalik võti sertifitseerida.

Sertifitseerimise hierarhia – usaldusvõrk – internetiühendusega võtmeserver

GnuPG-d ja PGP-d saab põhimõtteliselt kasutada nii sertifitseerimise hierarhias kui ka usaldusvõrgus. Usaldusvõrgu puhul usaldatakse teiste kasutajate sertifikaate. Sertifitseerimishierarhias kinnitavad kõikide oma kasutajate võtmeid usaldusväärsel ja kontrollitaval viisil usaldusväärsed kolmandad osapooled, nn sertifitseerimisüksused. Ettevõttes või ametiasutuses tuleb intranetis luua sertifitseerimishierarhia. Haldaja peab sertifitseerima kõik oma organisatsioonivaldkonna või kogu organisatsiooni võtmed. Sertifitseeritud avalikud võtmed peavad olema intraneti serveril saadaval kõikidele töötajatele, juurdepääs sellele alale peab olema eranditult vaid lugemispääs (read-only). Usaldusvõrgu meetodit tuleks kasutada

ainult privaatse side jaoks. Internetis saab avalikud võtmed sisse seada nn võtmeserverites. Neid ei tohi mitte mingil juhul segi ajada sertifitseerimisüksustega. Võtmeserverid võtavad võtmed kõikjalt vastu ja suunavad nad vastava päringu esitamisel edasi. Kõigile peab olema selge, et võtmeserverilt saadud võtmeid pole server vähimalgi määral kontrollinud. Võtmeserveril oleva avaliku võtme ehtsuse kontrollimiseks tuleks kasutada juba mainitud sõrmejälge.

Avaliku võtme omaallkiri

Avaliku võtme omaallkirjaga allkirjastatakse ainult kasutaja-ID kui osa GnuPG või PGP avalikust võtmest. Selline omaallkiri võimaldab tuvastada teenusetõkestusründeid (vt G 5.28 Teenuse halvamine), kuid avaliku võtme omaallkiri ei suuda seda takistada. Kuna avaliku võtme kasutaja-ID pole krüpteeritud, on võimalik seda võltsida. Selle tagajärjeks oleks, et selle „võltsitud" võtme kasutamisel ei jõua krüpteeritud e-kirjad enam selle võtme omanikuni, kuna nad juhitakse ümber teisele e-posti aadressile. See ei ohusta krüpteeritud sõnumi konfidentsiaalsust, kuna sõnumi krüpteerimine saab toimuda ainult privaatvõtmega.

Võtmetaaste

Juhul kui krüpteerimiseks kasutatavad võtmed lähevad kaduma, pole üldjuhul ka nendega kaitstud andmed enam kättesaadavad. PGP kommertsversioonid alates versioonist 5.0 pakuvad selliseks puhuks andmete taastamise võimalust. Neid funktsioone nimetatakse võtmetaasteks (key recovery). See funktsioon aitab salvestatud, krüpteeritud andmete taastamisega vältida andmekadu olukorras, kus võti või juurdepääsuparool läheb kaduma. PGP vanematest versioonidest on avastatud ADK-juurutamise (additional decryption key) vigu, mida saab kasutada rünneteks. See puudutab ennekõike just neid PGP-versioone, mis on vanemad kui 6.5.8. Seetõttu tuleks kasutada piisavalt uut versiooni, milles on võimalikult paljud turvalisust puudutavad avastatud vead kõrvaldatud. GnuPG ignoreerib reeglina kõiki ADK-sid. Kui tahetakse kasutada PGP taastamisfunktsiooni, tuleb genereerida üks või kaks lisavõtit. Võtme genereerimisel seotakse need lisavõtmed uute genereeritud võtmetega ja kõik andmed, mis krüpteeritakse uute võtmetega, sisaldavad lisaks muule ka seansivõtme krüpteerimist ADK-dega. Nii saab avariiolukorras neid andmeid dekrüpteerida nende ADK-dega, ilma et läheks tarvis originaalvõtit. Sellega võimaldab PGP Message Recovery funktsiooni kasutada ilma taastamisinfo tsentraalse salvestamiseta.

Võtmete taastamisfunktsiooni kasutamise võib klientsüsteemi jaoks muuta vastava eelseadistuse abil sunniviisiliseks, et kasutajad ei saaks sellest funktsioonist kõrvale hiilida. Kuid sellisel juhul sõltub kogu krüpteerimise turvalisus ADK-de konfidentsiaalsusest. Kui need tulevad avalikuks, saab nende abil kõik andmed dekrüpteerida. Selle ülimalt tundliku funktsiooni kuritarvitamise vältimiseks on mõõdapääsmatu, et ADK-de kaitsmiseks tuleb kasutada väga hoolikalt valitud ja turvalises kohas hoitavaid paroole. Lisaks saab alates PGP versioonist 6.0 võtmeid tükeldada nõnda, et nende kasutamine vajab mitme inimese koostööd. Sellist nelja silma kontrolli tuleks ADK-de kasutamisel kindlasti rakendada. Täiendav kaitsemeede võib olla kasutajate hoiatamine iga kord, kui nad krüpteerivad andmeid võtmega, mis on seotud ADK-dega. Enne PGP ja võtmetaaste kasutuselevõttu tuleks omavahel võrrelda nende eeliseid ja puudusi. Ühest küljest välistatakse küll

olukord, kus võtme kaotamine tähendaks andmekadu, kuid teisalt tekib krüpteerimissüsteemile tsentraalne nõrk koht. Seepärast tuleks seda funktsiooni kasutada ainult siis, kui PGP-d kasutatakse salvestatud andmete krüpteerimiseks. Kui kasutusvaldkonnaks on ainult sideühenduste turvaliseks muutmine, võib võtme kaotamise korral paluda e-kirja uuesti saatmist. Samuti tuleks kontrollida, kas poleks parem alternatiiv hoida parooli suletud ümbrikus turvalises kohas ja luua privaatvõtme failidest varukoopiad.

Key reconstruction

Ühte lisavõimalust, kuidas lahendada probleeme, mis tulenevad võtme kaotamisest nt unustatud paroolfraasi tõttu, pakub PGP versioon nr 7. Selleks jaotatakse võti mitmeks osaks, krüpteeritakse ja salvestatakse taastamisserverisse. Salvestamisel määratleb kasutaja viis küsimuse ja vastuse kombinatsiooni. Võtme taastamiseks peab kasutaja viiest küsimusest vähemalt kolmele õigesti vastama. Selle funktsiooni oht seisneb võimaluses, et kasutajad valivad endale välja küsimused, mille vastused on kolmanda osapoole jaoks äraarvatavad või leitavad, nt sugulaste nimed või sünnikuupäevad. Tagajärjeks võib olla kolmandate isikute juurdepääs kasutaja võtmele. Kuna küsimuste ja vastuste kombinatsioonide kvaliteeti ei saa tavaliselt kontrollida, tuleks selle funktsiooni kasutamisest hoiduda. Selle asemel tuleks privaatsetest võtmefailidest luua mõnele andmekandjale varukoopia ja hoida seda andmekandjat turvalises kohas. Ka vastavat paroolfraasi tuleb hoida suletud ümbrikus (vt M 2.22z Paroolide deponeerimine).

Ainulogimine

Nimetuste ainulogimine (single sign-on) ja paroolfraasi vahesalvestus (passphrase caching) all pakub PGP alates 7. versioonist mehhanismi, mis salvestab kasutaja sisestatud parooli ajutiselt, et kasutaja ei peaks seda iga tegevuse korral uuesti sisestama. Sellega kaasneb oht, et kui kasutaja lahkub korraks oma töökohalt, avaneb volitamata isikutel võimalus kasutaja identiteedi abil dokumente krüpteerida või dekrüpteerida või ka digitaalselt allkirjastada. Kui tahetakse kasutada PGP paroolfraasi vahesalvestuse funktsiooni, tuleb seega kindlasti tagada kasutaja arvuti viivitamata lukustamine, kui kasutaja lahkub töökohalt kasvõi lühikeseks ajaks. Selleks võib kasutada näiteks Windowsi tööjaama lukustamise funktsiooni, mille eeldus on kasutaja piisavalt tugev parool, kuid rakendada on võimalik ka kasutajate autentimise kiipkaarti. Kõikidel teistel juhtudel tuleb PGP suvandite dialoogväljal (PGP options) aktiveerida paroolfraasi vahesalvestust keelav valik (Do not cache passphrase).

Kontrollküsimused:

- Kas kasutajaid õpetatakse, kuidas GnuPG-d ja PGP-d kasutada?
- Kas andmeid ja võtmeid hoitakse eraldi?
- Kas privaatvõtmetest luuakse varukoopiad?
- Kas privaatvõtmeid hoitakse turvalises kohas?

M 5.64z Secure Shell (SSH)

Algatamise eest vastutavad: IT-juht, infoturbespetsialist

Rakendamise eest vastutavad: administraator

Ilma eriliste laiendusteta võimaldavad protokollid telnet ja ftp ainult vananenud autentimismehhanisme. Tavaliselt viiakse läbi lihtne kasutajatunnuse ja parooli küsimine, mis nagu kasulik koormuski saadetakse edasi avatekstina. Järelikult ei ole kindlustatud autentimise ja kasuliku koormuse andmete konfidentsiaalsus. Sarnastel protokollidel nagu rsh, rlogin ja rcp, mis tihtipeale on koondatud mõiste r-teenused alla, on leitud sarnaseid turbepuudujääke.

„r-teenuste" asemel võib kasutada Secure Shelli (SSH), mis kasutab konfidentsiaalsuse ja tervikluse turvaliseks autentimiseks ja säilitamiseks ulatuslikke funktsioone. Selleks kasutatakse asümmeetriliste ja sümmeetriliste krüpteeringute kombinatsiooni. SSH paikneb ISO/OSI-referentmudeli 7. kihil (rakenduste kiht), samas on SSH kaudu võimalik transportida ka teisi protokolle, näiteks X-Windowsi graafilise kasutajaliidese X11-protokoll.

Hetkel põhineb SSH kolmel protokollil, mis on üles ehitatud üksteise peale ja millest igaühe jaoks on olemas Internet-Draft:

- Alumine protokoll on transpordikihi protokoll (transport layer protocol). See protokoll vastutab suurema osa SSH turbefunktsioonide eest, nimelt hosti tasandil autentimine, krüpteerimine ja andmetervikluse kaitse. Krüptograafilised algoritmid tuleb sidepartnerite vahel kokku leppida.
- Keskmine protokoll on kasutaja autentimisprotokoll (user authentication protocol). Tegemist on kasutaja tasandil autentimisega, kusjuures ka siin tuleb vastav meetod eelnevalt kokku leppida. Kui autentimiseks kasutatakse lihtsat kasutajatunnuse ja parooli edastamist, siis on selle informatsiooni konfidentsiaalsus sidekanali suhtes kindlustatud selle all asuva transpordikihi protokolli kaudu. Soovitatav on aga autentimine avaliku võtme (public key) meetodi kaudu.
- Ühendusprotokoll (connection protocol) põhineb kahel eelneval protokollil ning lubab mitme loogilise kasutajakanali üles ehitamist. Nendel kasutajakanalitel paiknevad andmed edastatakse kõik koos ühe ainsa kindlustatud SSH-ühenduse kaudu.

Kõigile Unixi operatsioonisüsteemide levinud teostustele on olemas nii SSH kliendid kui ka SSH serverid. Peale selle eksisteerib SSH kliente nii Windowsile, Mac OS-ile kui ka Java-Appletile. Põhimõtteliselt on SSH kasutamine soovitatav, kui r-teenuste funktsionaalsust kasutatakse sidekanalite kaudu, mis ei ole piisavalt kaitstud kompromiteerimise ja/või manipulatsiooni eest (näiteks interneti kaudu).

Alljärgnevalt antakse mõningad vihjed SSH turvalise kasutamise kohta:

- Erilise tähtsusega on vahendusründed. Ründaja filtreerib kogu sidepartnerite vahel liikuva informatsiooni ja edastab võltsitud avalikke võtmeid.

Kui sidepartneritel ei ole võimalik avalikke võtmeid kontrollida, saab ründaja tervet suhtlust pealt kuulata ja manipuleerida. Selleks dekrüpteerib ta vastavad andmed, loeb või muudab neid, ja lõpuks krüpteerib need teise võtmega ning saadab edasi. Seda on võimalik vältida sobiva võtme-/sertifikaadihalduse kasutamisega. SSH praktilisel kasutamisel kasutatakse tihti kompromisslahendust, mis võimaldab selle kasutamist ilma täiendava infrastruktuurita. Seejuures saadetakse hostiga ühenduse loomisel, mille avalik võti ei ole veel teada, see ebaturvalise võrgu kaudu ja salvestatakse lokaalses andmebaasis. Kõigi järgnevate ühenduste korral, mis selle hostiga luuakse, on võimalik see avalik võti andmebaasist järgi kontrollida. Turbekontseptsiooni raames tuleb välja selgitada, kas meetod, mis pakub vahendusrünnete suhtes vähendatud kaitset, on selle ülesande jaoks piisav.
- Internet-Draftsides on kindlaks määratud krüptograafilised meetmed, mis tuleb SSH teostuse poolt kasutusse anda. Vajaduse korral on võimalik teostada veel täiendavaid krüptograafilisi algoritme. Tegelikkuses kasutatavad meetodid selgitatakse välja alles ühenduse loomisel. Sobivate klient- ja serverprogrammide valimise ja vastava konfiguratsiooni kaudu tuleb kindlustada, et SSH-klient ja SSH-server lepiksid kokku krüptograafilise algoritmi suhtes, mis vastaks infoturbenõuetele.

Vältimaks turbemeetmetest möödumist, tuleks SSH kasutamisel kõik teised protokollid, mille funktsioonid Secure Shell katab, näiteks r-teenused või telnet, täielikult välja lülitada. See eeldab aga, et kõigil kommunikatsioonipartneritel on sobiv teostus. SSH vanemate versioonide kohta on teada, et need sisaldavad turbekriitilisi programmivigu. Seega tuleks kasutada versiooni, mille juures on need vead kõrvaldatud. Teatud juhtudel võib tekkida ühilduvusprobleeme programmiteostuste vahel, mille programmiversioonid on üksteisest väga erinevad. Seega tuleks vältida segakäitust. Jälgida tuleb, et SSH kasutamisel tulemüüride kaudu ei ole sisutundlik andmevoo kontroll enam võimalik.

Kontrollküsimused:

- Kas SSH-d kasutakse r-teenuse asendamiseks?
- Kas SSH jaoks kasutatakse sobivat võtme- ja sertifikaadihaldust?
- Kas kõik protokollid, mille funktsionaalsuse SSH katab, on välja lülitatud?

M 5.66z SSL-i/TLS-i kasutamine kliendis

Algatamise eest vastutavad: infoturbeametnik, IT-juht

Rakendamise eest vastutavad: administraator, kasutaja

Veebikasutuses kõige sagedamini kasutatav turvaprotokoll on SSL/TLS (Secure Socket Layer / Transport Layer Security). SSL-protokolli esimese versiooni (SSL v1.0) arendas välja Netscape. Uuemad versioonid on nimetuse TLS all muutunud erinevate RFC-de standardiks. SSL-i/TLS-i toetavad kõik tänapäevased brauserid.

SSL/TLS võimaldavad kaitsta ühendusi järgmiselt:

- krüpteerides ühenduse sisu,
- kontrollides edastatud andmete terviklust ja õigsust,
- kontrollides serveri identiteeti ja
- soovi korral kontrollides kliendipoole identiteeti.

Uue, SSL-i/TLS-iga kaitstud sideühenduse alguses toimub nn kätlus kliendi ja serveri vahel. Siinjuures lepivad klient ja server kokku krüptograafilistes algoritmides, mida rakendatakse võtmete vahetuseks, krüpteerimiseks ja tervikluse kaitsmiseks. Lisaks sellele lepivad klient ja server kokku, millist SSL-versiooni kasutama hakatakse. Seejärel saadab server kliendile oma X.509-sertifikaadi. Valikuliselt võib ka klient edastada serverile oma X.509-sertifikaadi, kui server seda nõuab. Asümmeetrilise krüpteerimismeetodi abil toimub seejärel sümmeetrilise võtme turvaline vahetamine. Tegeliku andmeedastuse krüpteerimiseks kasutatakse sümmeetrilist protseduuri, sest see suudab suuri andmehulkasid kiiremini krüpteerida. Iga tehingu korral väljastatakse mõni teine sümmeetriline võti seansivõtmena, mille abil toimub ühenduse krüpteerimine.

Kasutaja tunneb SSL-i/TLS-iga kaitstud andmeedastust võimaldavad veebilehed ära nt selle järgi, et internetiaadressi on täiendatud s-tähega (https://www. . .). Lisaks tähistab suurem osa tänapäevastest brauseritest neid lehti ka kuidagi silmatorkavamalt, nt sümboliga (võti, tabalukk jne) või internetiaadressi värvimärgistusega.

SSL-i/TLS-i kasutamine ei ole piiratud HTTP-klientide ja -serveritega. Ka protokolle, nagu SMTP, FTP, IMAP või LDAP, saab SSL-i/TLS-i kaudu krüptograafiliselt kaitsta. See eeldab siiski, et seotud kliendid ja serverid toetavad seda turbefunktsiooni.

SSL/TLS koosneb kahest kihist. Ülemisel kihil töötab SSL-i/TLS-i kätlusprotokoll. See aitab kliendil ja serveril üksteist autentida, samuti annab see järgneva andmeliikluse jaoks võtme ja krüpteerimisalgoritmi. Alumine kiht, SSL-i/TLS-i salvestusprotokoll, mis moodustab liidese TCP-kihiga, krüpteerib ja dekrüpteerib tegeliku andmeliikluse. Kuna SSL/TLS kasutab TCP-le ligipääsemiseks Socket-

liidest ja asendab selle turvalisust täiendava versiooniga, saab seda kasutada ka teiste teenuste jaoks.

Versiooni number

Olemas on mitmed SSL-i/TLS-i protokolli versioonid, nagu SSL v2, SSL v3, TLS v1.0, TLS v1.1 ja TLS v1.2. Versiooni SSL v1 ei toodud avalikkuse ette. Turvalise ühenduse tagamiseks kliendi ja serveri vahel tuleks kasutada vähemalt versiooni TLS 1.2.

TLS 1.1 pakub piisavat turvalisust, aga võrreldes versiooniga TLS 1.2 on sellel siiski mõned nõrgad kohad, nt on versioonis TLS 1.1 veel alles šifrikomplektid, mis põhinevad IDEA-l ja DES-il, versioonil TLS 1.2 enam mitte.

TLS 1.0 võib olemasolevates kliendirakendustes üleminekuna edasi kasutada, kui üleviimine versioonile TLS 1.1 või eelistatavalt versioonile TLS 1.2 ei ole kohe võimalik ja rakendada tuleb sobivaid meetmeid valitava avatekstiga rünnete vastu (nt BEAST) CBC-rakendusele. Üldiselt peaks siiski üleviimine versioonile TLS 1.2 toimuma nii kiiresti kui võimalik. **Versioone SSL v2 ja SSL v3 ei tohi enam kasutada**.

Algoritmid ja võtmepikkused

SSL-i/TLS-i puhul saab kasutada erinevaid krüptograafilisi algoritme, millel on erinevad võtmepikkused (vt lisaks M 3.23w Sissejuhatus krüptograafia põhimõistetesse). Ühenduse loomisel lepivad klient ja server kokku, milliseid protseduure seansi ajal kasutatakse.

Toodete (brauser, veebiserver, plugin jne) valiku ja sobiva konfiguratsiooni valimisega tuleb tagada, et SSL/TLS-kaitsega varustatud side puhul kasutataks ainult selliseid algoritme ja võtmepikkuseid, mis vastavad tänapäeva tehnika tasemele ja organisatsiooni turbenõuetele. Seetõttu peaksid kasutatavad šifrikomplektid toetama perfektset tulevikusalastust (perfect forward secrecy, PFS) (vt TR-02102-2). Täiendavaid juhiseid algoritmide ja võtmepikkuste kohta leiate meetmest M 2.164 Sobiva krüptoprotseduuri valimine .

Sertifikaadid

Avalike võrkude kaudu toimuva andmeside puhul on sidepartneri identiteeti raske kontrollida, sest ei saa kindlaks teha, kas nimeandmed on õiged. SSL-i/TLS-i puhul toimub sidepartneri identiteedi kontrollimine nn sertifikaatide abil. Sertifikaadid sisaldavad nende avalikku võtit, samuti täiendava üksuse kinnitust avaliku võtme ja selle omaniku vahelise seotuse kohta, ehk siis kas serveri või kliendi kohta. Sertifikaadi väärtus sõltub seega olulisel määral seda kinnitava üksuse (kannab ka nime Trustcenter või sertifitseerimisüksus) usaldusväärsusest.

Sertifikaadi ehtsust saab omakorda kontrollida kinnitava üksuse avaliku võtmega. Kõik levinud brauserid sisaldavad juba installeerimisel osade sertifitseerimisüksuste SSL/TLS-sertifikaate. Nendel sertifitseerimisüksustel on sertifikaatide väljastamiseks väga erinev turvapoliitika ja väga erinevad tingimused. Enne kui edastada turvalisuse seisukohast olulist infot SSL/TLS-kaitsega ühenduse kaudu, tuleb seega kontrollida vastava sertifitseerimisüksuse turvapoliitikat.

Uue sertifikaadi vastuvõtmisel ei tohi seda aktiveerida enne sõrmejälje kontrollimist. Sõrmejälg on kuueteistkümnendiksüsteemis arv, mis edastatakse koos sertifikaadiga. Lisaks tuleks seda edastada ka mõnda teist teed pidi ja võrrelda, sest see peab tagama sertifikaadi õigsuse.

Veebiserverite käitajad, kes tahavad oma veebilehtede kasutajatega vahetada turvalisuse seisukohast olulisi andmeid, peaksid selleks pakkuma krüptograafiliselt kaitstud võimalust, st nt SSL-i/TLS-i. Minevikus on ette tulnud ka olukordi, kus sertifitseerimisasutused on saanud kahjustada ning väljastasid seetõttu sadu võltsitud sertifikaate, sealhulgas sõnumiteenuste, võrguportaalide, muude sertifitseerimisasutuste ja anonüümsust tagavate teenuste jaoks.

Tühistamisloendite ja valideerimisprotokollidega, nagu OCSP (Online Certificate Status Protocol) saab võltsitud, manipuleeritud või vananenud sertifikaate muuta kiiresti kehtetuks. Seetõttu tuleb rakendusprogrammides, nagu veebilehitsejates ja e-posti klientides, aktiveerida sertifikaatide valideerimine. Seejuures tuleb sertifikaatide tühistamisloendite kasutamisele eelistada OCSP-d (tühistatud sertifikaatide loendid – certificate revocation lists, CRL), sest OCSP võimaldab kiiret värskendamist interneti kaudu.

Kui sertifikaati ei saa valideerida, sest OSCP-serverit ei saada kätte või ei pääseta ligi tühistamisloenditele, on kliendi seisukohast kaks võimalust: ta võib ühenduse katkestada või tõenäoliselt manipuleeritud või kehtetu sertifikaadi aktsepteerida. Otsus, mida sellistel juhtudel teha, peaks olema kooskõlas asutuse turvasuunistega.

Seansi uuendamine ja TLS-tihendus

Kliendi poolel tuleks seansi uuendamine välja lülitada. Üldist teavet sessiooni uuendamise funktsioonide kohta võib leida meetmest M 5.177 SSL-i/TLS-i kasutamine serveris .

TLS pakub võimalust edastatavaid andmeid enne krüpteerimist tihendada. See

võib kaasa tuua, et krüpteeringule võidakse sooritada kõrvalkanali ründeid krüpteeritud andmete pikkuse kaudu. Sellekohane näide on CRIME (Compression Retro Info-leak Made Easy), 2012. aastal avalikustatud kõrvalkanali rünne, mille eesmärk oli üle võtta HTTPS-seanss. Selle takistamiseks tuli TLS-tihendus välja lülitada.

Teadmiseks. SSL-i/TLS-i kasutamisel tuleb arvestada sellega, et krüpteeritud andmeid ei saa seoses aktiivsisu ja kahjurvaraprogrammidega kontrollida tsentraalselt, seega nt turvalüüsis. Sellega tuleb turvakontseptsioonis arvestada, et ei tekiks turvaaukusid. Lisasoovitusi leiate muu hulgas moodulist B 1.6 Viirusetõrje kontseptsioon .

Kontrollküsimused:

- Kas kasutatavad klient-tooted toetavad SSL-i/TLS-i turvalist versiooni?
- Kas on tagatud, et kasutatavad kliendid kasutavad krüptograafilisi algoritme ja võtmepikkusi, mis vastavad tänapäeva tehnika tasemele ja asutuse turvanõuetele?
- Kas enne seda, kui turvalisuse seisukohast olulist teavet edastatakse SSL/TLS-kaitsega ühenduse kaudu, kontrollitakse vastava sertifitseerimisasutuse turvapoliitikat?
- Kas ka SSL-i/TLS-i kasutamisel on tagatud piisav kaitse kahjulike programmide ja keelatud aktiivsisu eest?
- Kas pööratakse tähelepanu sellele, et uued sertifikaadid aktiveeritakse alles pärast sõrmejälgede kontrollimist?
- Kas on tagatud, et sertifikaatide valideerimine vastab asutuse turvasuunistele?
- Kas seansi uuendamine ja TLS-tihendus on välja lülitatud?

M 5.67z Ajatempliteenuse kasutamine

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: administraator, kasutaja

Ajatemplid võimaldavad kontrollida ja tõestada andmete terviklust. Ajatempli loomiseks arvutatakse esmalt andmetest räsifunktsiooni abil räsi, mis seejärel saadetakse päringuna ajatempliteenuse osutajale. Ajatempliteenuse osutaja kas signeerib saadetud päringu koos ajanäiduga (nn signeeritud ajatempel) või räsib päringu räsifunktsiooni abil kokku teiste (teistelt kasutajatelt) saadud päringutega ja avalikustab (publitseerib) tekkiva räsi (nn räsitud ajatempel). Ajatempel tõendab, et andmeid (esitatud kujul) ei ole ajatempli väljastamise hetkest alates muudetud.

Näiteks e-kirjade päisesse (header) lisatavat ajainfot on võimalik suhteliselt kergelt manipuleerida. Juhul kui on tarvis teada e-kirjade saatmise või kättesaamise täpset ajahetke, tuleb kasutada ajatempliteenust. Ajatempel on aega kajastav sissekanne, mille teeb neutraalne osapool ja mida ei ole võimalik võltsida. Ajatempli server lisab ajatempli andmed kas täisautomaatselt, st kasutaja jaoks läbipaistvalt, või e-kirja saatva kasutaja soovil.

Signeeritud ajatempel koosneb järgmistest komponentidest:

- ajatempli sertifikaat, milles sisaldub kaitstavate andmete räsi, õige kuupäev, õige kellaeg ja ajatempliteenuse identiteet;
- teenuse osutaja digitaalne allkiri;
- lisaandmed, sh teenuseosutajale väljastatud sertifikaat.

Räsitud ajatempel koosneb järgmistest komponentidest:

- ajatempli sertifikaat, milles sisaldub kaitstavate andmete räsi, õige kuupäev, õige kellaeg ja ajatempliteenuse identiteet;
- räsiahel, mis esitab üksteisele järgnevaid räsimisoperatsioone, mis arvutab kaitstavate andmete räsist avaldatud räsi.
- avaldatud räsi koos viitega allikale, kus räsi on avaldatud.

Tõendina eeldab signeeritud ajatempel kasutatud digitaalsignatuuri algoritmi turvalisust, turvalist privaatvõtme haldust ja teenuseosutaja usaldusväärsust. Räsitud ajatempel seevastu eeldab tõendina rakendamisel kasutatud räsifunktsiooni turvalisust ja publitseerimisel kasutatud andmekandja terviklust, kuid ei eelda turvalist võtmehaldust ega teenuseosutaja usaldusväärsust.

Ajatempli teenust saab pakkuda ja kasutada nii sisevõrgu keskkonnas kui ka internetis. Teenus võtab interneti/intraneti keskkonna serverina allkirjastatud failid või ka ainult nende allkirjad vastu ja lisab neile sünkroonitud ajatempli ning saadab vajaduse järgi kas adressaadile või tagasi saatjale.

M 5.68z Krüpteerimisprotseduuride kasutamine võrgusuhtluses

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: administraator

Kommunikatsioonivõrkude otstarve on andmete transportimine erinevate IT-süsteemide vahel. Andmete edastamine ühelt sidepartnerit teisele toimub väga harva eraldiseisva ja ainult selleks otstarbeks kasutatava sideühenduse vahendusel. Enamasti suunatakse andmed nende teekonnal läbi paljude vahepunktide. Olenevalt sidevahendist ja rakendatavast tehnoloogiast võidakse vahejaamades andmeid volitamata pealt kuulata, samuti on oht, et sellega võivad tegeleda vahendamisvõrgus asuvad kolmandad osapooled (nt kui kasutatakse Ethernet-protokolli ilma punktist-punkti-võrguühenduseta). Selleks, et kolmandad isikud ei saaks andmeid volitamata pealt kuulata, neid muuta või hiljem tagasi võrgu keskkonda sisestada (taasesitusründed), tuleb kasutusele võtta sobivad mehhanismid, mis selliseid tegevusi takistavad. Nimetatud ohtusid aitab vähendada krüpteerimine, vajaduse korral koos mõlema sidepartneri autentimisega. Viimase võimaluse kasutamine oleneb sellest, kui tugevate mehhanismidega krüpteerimisprotseduur valitakse ja kui turvalised on võtmed (vt B 1.7 Krüptokontseptsioon). Rakendused on omavahel sideühenduses reeglina sellepärast, et vahetada rakendusse puutuvaid andmeid.

Andmete krüpteerimine võib toimuda mitmel tasandil:

- Rakenduse tasand – omavahel suhtlevatel rakendustel peavad olema nii krüpteerimismehhanismid kui ka krüpteeringu lahtikodeerimise mehhanismid.
- Operatsioonisüsteemi tasand – krüpteerimise viib läbi lokaalne operatsioonisüsteem. Kõikvõimalik võrgus aset leidev kommunikatsioon krüpteeritakse kas automaatselt või soovi kohaselt.
- Võrguühenduselementide tasand – krüpteerimine toimub võrguühenduselementides (nt marsruuterites).

Erinevatel mehhanismidel on nii oma eelised kui ka puudused. Rakenduse tasandil toimiva krüpteerimise eelis seisneb tõsiasjas, et krüpteerimisfunktsiooni kontrollib täielikult vastav rakendus. Puuduseks seevastu on asjaolu, et krüpteeritud andmeside saab toimuda vaid ühe, samasuguse krüpteerimismehhanismiga varustatud partnerrakendusega. Lisaks saab mõlema partnerrakenduse vahel kasutada vastavaid autentimismehhanisme. Eelnevaga võrreldes toimub operatsioonisüsteemi tasandi krüpteerimine kõikide rakenduste jaoks läbipaistvalt. Igal rakendusel on võimalik olla teiste rakendustega krüpteeritud sideühenduses juhul, kui operatsioonisüsteemil, mille keskkonnas partnerrakendus töötab, on olemas vastavad krüpteerimismehhanismid. Selle variandi puudus seisneb tõsiasjas, et autentimisel on võimalik vastastikku autentida vaid arvuteid, aga mitte kõnealuseid partnerrakendusi.

Krüpteerivate võrguühenduselementide eelis on, et rakendused ja arvutid võivad olla ilma krüpteerimismehhanismideta; ka siin toimub krüpteerimine sidepartnerite jaoks läbipaistvalt. Sellele vaatamata toimub kommunikatsioon

kuni esimese krüpteeritud võrguühenduselemendini ilma krüpteerimata ja kujutab endast seega jääkriski. Autentimine on selle variandi puhul võimalik ainult ühenduselementide vahel – tegelikke sidepartnereid siin ei autendita.

Juhul kui läbi võrgu edastatakse konfidentsiaalseid andmeid (ka intraneti piires), on soovitatav kasutada krüpteerimismehhanisme. Kui kasutatavatel rakendustel krüpteerimismehhanisme ei ole või kui need mehhanismid on liiga nõrgad, tuleks rakendada operatsioonisüsteemi tasandil toimuvat krüpteerimist. Selleks võib kasutada protseduure, nagu SSL, mis tagab läbipaistva krüpteerimise operatsioonisüsteemi tasandil. Olenevalt turvapoliitikast võib kasutada ka krüpteerivaid võrguühenduselemente, nt juhul, kui soovitakse internetikeskkonnas luua sidepartneriga virtuaalset privaatvõrku (VPN-i), samas on vastavad mehhanismid reeglina olemas ka tulemüürisüsteemides (vt B 3.301 Turvalüüs (tulemüür)).

Krüpteeritud andmeside ja sobivate autentimismeetodite kasutuselevõtt eeldab ettevõtte või ametiasutuse turvapoliitika ulatuslikku planeerimist.

Siin peatükis kirjeldatud andmeside krüpteerimise valdkonnas tuleb enekõike arvestada järgmiste punktidega:

- Milliseid protseduure tuleks krüpteerimiseks kasutada ja millised protseduurid on olemas (nt marsruuterites)?
- Kas kasutatavad krüpteerimismehhanismid toetavad/rakendavad olemasolevaid või planeeritavaid standardeid (IPSec, IPv4, IPv6, IKE)?
- Kas turvapoliitikat arvestades on kasutamiseks välja valitud piisavalt tugevad krüpteerimismehhanismid ja piisavalt pikad võtmed?
- Kas võtmeid hoitakse turvaliselt?
- Kas võtmete genereerimine toimub turvalises keskkonnas ja kas võtmed jõuavad vajalikku rakenduskohta (arvutisse, tarkvarakomponentidesse) turvalist teed pidi?
- Kas on tarvis rakendada võtmetaaste mehhanisme?

Juhul kui sidepartnerite autentimiseks kasutatakse sertifikaate, tuleb arvestada sarnaste küsimustega.

M 5.69 Aktiivsisu tõrje

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: infoturbespetsialist

Kui brauseris kuvatakse veebilehti, pole nende sisuks sageli mitte ainult tekst, pildid ja multimeedia, vaid samal ajal ka programmikood (aktiivsisu), mille võivad käivitada olenevalt olukorrast ka eraldi pluginad. Aktiivsisu tuntud näideteks on JavaScript, Java apletid, ActiveX-i komponendid, Flash. Aktiivsisu käivitamine brauseris võib tekitada turbeprobleeme, sest seeläbi võidakse arvutisse laadida kahjulikke programme, samuti võib ründaja püüda aktiivsisu kaudu andmetele volituseta ligi pääseda. Levinud brauserites on turbemehhanismid, mis piiravad aktiivsisu pääsuvõimalusi. Sellele vaatamata tulevad ikka ja jälle ilmsiks uued puudujäägid ja avastatakse uusi võimalusi, kuidas nendest turbemehhanismidest mööda pääseda. Sisevõrgu kaitsmiseks internetist pärineva aktiivsisu vastu on võimalik rakendada erinevaid meetodeid, mida kirjeldatakse alljärgnevalt.

Aktiivsisu väljafiltreerimine tulemüüriga

See on kõige turvalisem interneti kasutamise meetod, mida ühtlasi ka kõige enam soovitatakse, sest see jätab peamise kontrolli tulemüüri hooleks. Aktiivsisu vastuvõtmise takistamiseks läheb rakenduslüüsis (Application Level Gateway, ALG) tarvis proksit, mis kontrollib, kas HTML-lehtedel leidub aktiivsisu. Aktiivsisu leidmisel tuleb see leheküljelt välja filtreerida. Sellise funktsiooniga rakenduslüüside valik on üpris lai (vt M 2.75 Sobiva rakenduslüüsi valimine). Siiski tuleb arvestada, et seda lahendust, olgugi et see on turvalisim, kasutatakse tulevikus üha vähem, sest nende veebilehtede arv, mis ilma aktiivsisuta kasutuskõlbmatuks muutuvad, aina suureneb. Aktiivsisu saab peita ka meilidesse, seega tuleks ka neid aktiivsisu suhtes kontrollida. Lisaks tuleb arvestada sellega, et aktiivsisu on vaja välja filtreerida ka TLS-i/SSL-iga krüpteeritud andmevoogudest. TLS-i/SSL-iga krüpteeritud andmevood tuleb seega võrgu piiril, nt rakenduslüüsis, lõpetada (terminate). Ka seda funktsiooni pakuvad nüüd juba küllaltki paljud tulemüüritooted.

Aktiivsisu käivitamise desaktiveerimine brauseris

Tsentraalselt hallatavates töökohaarvutites võib piirata kasutajate õigusi nii palju, et nad ei saaks enam muuta oma brauseri turbeseadistusi. Brauserid saab seadistada selliseks, et aktiivsisu nendes enam ei käivitata. Sellisel juhul pole rakenduslüüsis tarvis aktiivsisu filtreerida.

Kahjuliku koodi otsimine aktiivsisust

Nii nagu klassikaliste viirusetõrjeprogrammide puhul, on olemas ka turbetarkvara, mis kontrollib, kas aktiivsisus leidub kahjulikku koodi. Kui tarkvara tuvastab mõne ohu, takistab see juurdepääsu kahjulikule koodile. Kahjuliku koodi kontrollimise turbetarkvara saab kasutada klientsüsteemis või võrgu piiril. Siiski tuleb arvestada, et see meetod ei paku täielikku kaitset, sest võib juhtuda, et turbetarkvara ei suuda alati kahjulikku veebilehte või komponenti tuvastada. On paratamatu, et tuvastamise tõenäosus on väiksem kui 100%. Nagu klassikalisi viirusetõrjeprogramme, tuleb ka turbetarkvara ja selle andmebaase regulaarselt värskendada.

Aktiivsisu käivitamine eraldatud keskkonnas

Riskide vähendamiseks saab aktiivsisu käivitada eraldatud keskkonnas ning selleks on mitmeid tehnilisi võimalusi:

- Terminaliserver - Klientsüsteem suunab brauseri selleks otstarbeks valmis seatud eraldi terminaliserverisse, mis asub eraldatud võrgusegmendis. Klientsüsteem loob terminaliserveri protokolliga (VNC, RDP, ICA, X11 jne) ühenduse terminaliserveriga. Nii toimub brauseri kaugjuhtimine. Sidevõimalused terminaliserveri ja kohtvõrgu vahel on kasutatava võrgutehnoloogia tõttu minimaalsed.

- Virtuaalsed IT-süsteemid - Brauser pannakse tööle eraldi virtuaalses IT-süsteemis, mida saab kasutada läbi klientsüsteemi. Sidevõimalused virtuaalse IT-süsteemi ja klientsüsteemi ning kohtvõrgu vahel on tänu vastavale konfiguratsioonile minimaalsed. Seda lahendust saab ka täielikult klientsüsteemis rakendada.

- Operatsioonisüsteemi mehhanismid - Mõned operatsioonisüsteemid pakuvad võimalust protsesse üksteisest eraldada (mõnikord näiteks lisakomponentide abil). Sellised on näiteks SELinux ja AppArmor. Ka neid mehhanisme saab kasutada aktiivsisu käivitamiseks eraldatud keskkonnas.

Aktiivsisu selektiivne käivitamine

Aktiivsisu käivitamist saab piirata teatud veebilehtedega, samuti on võimalik lasta kasutajatel aktiivsisu käivitamist brauseris ise sisse ja välja lülitada. On ka pluginaid, mis muudavad sisse- ja väljalülitamise kasutajatele mugavamaks. Igapäevakasutuses õigustab see meetod end siiski vaid harva. Teatud liiki aktiivsisu, nt ActiveX-i komponendid, võivad olla väljaandja digitaalse allkirjaga. Kontrollitud ja kehtiv allkiri võib näidata komponendi päritolu. Siiski ei saa allkirjast usaldusväärselt järeldada, kas komponent sisaldab kahjulikku koodi. Soovitused:

- Aktiivsisu käivitamist tohib lubada ainult siis, kui see on vajalik ametiülesande täitmiseks.
- Aktiivsisu käivitamise pluginaid tohib installida ainult siis, kui need on vajalikud ametiülesande täitmiseks.
- Enne aktiivsisu käivitamist tuleb (tsentraalselt või lokaalselt) värskendatud turbetarkvaraga kontrollida, kas selles leidub kahjulikku programmikoodi.
- ActiveX-i tüüpi aktiivsisu tohib (kui üldse) käivitada ainult siis, kui see pärineb usaldusväärsest allikast, st aktiivsisu peab olema allkirjastatud, allkiri peab olema kontrollitud ja allkirjastaja peab olema usaldusväärne.

Riskide ja vajalikkuse vastandamisega tuleb jõuda otsuseni, kuidas aktiivsisuga ümber käia. See otsus oleks soovitatav dokumenteerida.

Täiendavad kontrollküsimused:

- kas riskide ja vajalikkuse vastandamisega jõuti otsuseni, kuidas aktiivsisuga ümber käia?

- kas aktiivsisu käivitamine on lubatud ainult siis, kui see on vajalik ametiülesande täitmiseks?

- kas aktiivsisu käivitamiseks mõeldud pluginaid installitakse ainult siis, kui need on vajalikud ametiülesande täitmiseks?

- kas aktiivsisu kontrollitakse enne käivitamist, et leida võimalikku kahjulikku programmikoodi, ning kas selleks kasutatavat turbetarkvara värskendatakse pidevalt?
- kas ActiveX-i tüüpi aktiivsisu käivitatakse (kui üldse) ainult siis, kui see pärineb usaldusväärsest allikast, st kui aktiivsisu on allkirjastatud, allkiri on kontrollitud ja allkirjastaja on usaldusväärne?

M 5.70 Aadressi tõlkimine - Network Address Translation (NAT)

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: administraator

NAT (Network Address Translation) on mehhanism, mille puhul aktiivne võrgukomponent (enamikel juhtudel marsruuter) muudab paketti edasi saates paketi IP-aadressi. Marsruuter salvestab tabelisse sisemise aadressi ja sisemise allikpordi seose välise aadressiga, sihtkoha pordi ja pordi, mille marsruuter ise muudetud paketi jaoks välja valis ning tõlgib vastuspaketid vastavalt ümber. NAT-d saab kasutada mitmel eesmärgil:

- NAT suudab takistada info hankimist lokaalvõrgu struktuuri kohta meetodil, mis võtab aluseks lokaalvõrgu IP-aadressid, kuna välisvõrgust vaadelduna on nähtav ainult NAT-lüüsi IP-aadress. Niimoodi tõkestatakse väliste ründajate jaoks muuhulgas võimalus otse sisevõrgu arvuteid rünnata.
- Lokaalvõrgus läheb reeglina tarvis rohkem IP-aadresse kui ametlikult registreeritud. NAT-lüüsi kasutades on iga võrgu jaoks ilmtingimata tarvis ainult ühte ametlikku IP-aadressi, sisemisi aadresse võib seevastu valida vastavalt soovile.

Sisevõrgu ülesehitamisel tuleks siseaadressid valida ainult nendest valdkondadest, mis on ametlikult selliseks otstarbeks ette nähtud (vt RFC 1918 - Address Allocation for Private Internets). Nimetatud valdkonnad on järgnevad:

- 10.0.0.0 - 10.255.255.255 (8-bit võrgumask)
- 172.16.0.0 - 172.31.255.255 (12-bit võrgumask)
- 192.168.0.0 - 192.168.255.255 (16-bit võrgumask)

Neid aadresse „üldises internetis“ ei marsruudita ning seetõttu tuleb need interneti lüüsis ametlikult välja jagatud IP-aadressiks ümber tõlkida.

- Mõningatel juhtudel kasutatakse sisevõrgu loomisel suvalisi IP-aadresse. Juhul kui selline võrk ühendatakse internetti, võib juhtuda, et seni kasutuses olnud IP-aadresse pole võimalik enam edasi kasutada, kuna vastavad aadressid on juba mõnele teisele institutsioonile ära antud. Selleks, et kõiki arvuteid ei peaks hakkama ümber konfigureerima, võib kasutusele võtta aadresside tõlkimise, mis muudab siseaadressid ümber välisteks ametlikult registreeritud aadressideks. Sellise lahenduse puhul võib siiski esineda probleeme nimeteisendusega, mis tähendab, et arvutitele, mille senised sisevõrgus kasutusel olnud nimed on internetis juba välja jagatud, ei saa seejärel enam internetist juurde pääseda. Sama probleem võib esineda juhtudel, kus vahetatakse interneti teenusepakkujat.

- Kahe võrgu ühendamisel, mille IP-aadressid on valitud RFC-1918 valdkonnast, võib samuti juhtuda, et tuleb rakendada aadresside tõlkimist juhul, kui mõlemas võrgus kasutatakse samu aadresse.

Siseaadressi tõlkimine üheks või mitmeks ametlikult registreeritud IP-aadressiks ja vastupidi toimub aadressitõlkimiskomponendis. Aadressitõlkimise funktsioon on olemas ka proksil, kuna proksi kasutab väliskeskkonnas ainult oma ametlikku aadressi ja saadab andmepaketid edasi vastavatele siseringi arvutitele. Marsruuterite või eraldiseisvate paketifiltrite poolt tehtav aadresside tõlkimine võib toimuda kas staatilise või dünaamilise protsessina. Aadresside staatiline tõlkimine on lihtne ja kiire. Iga sisemine aadress tõlgitakse täpselt ümber üheks välimiseks aadressiks. See eeldab muidugi, et iga siseaadressi kohta eksisteerib üks välisaadress. Sagedamini kasutatakse siiski aadresside dünaamilist tõlkimist, eriti neil juhtudel, kus sisemiste IP-aadresside arv on väliselt nähtavate aadresside omast suurem. Marsruuteris või paketifiltris peetakse vastavat liigitamistabelit, kuhu registreeritakse siseaadressid koos nende juurde kuuluva paketi pordinumbritega, mis seostatakse välise aadressi uue pordinumbriga. Sageli muudetakse väljapoole nähtavaks ainult üks IP-aadress, mis varjab pordinumbrite liigituse alusel kõiki ülejäänud sisemisi IP-aadresse.

Aadresside dünaamilise tõlkimise üheks tagajärjeks on olukord, kus internetis muutub ühenduse loomine sisevõrgu arvutiga reeglina võimatuks. Juhul kui seda võimalust on siiski tarvis säilitada, peab turvalüüsil olema kas „Destination NAT“ või „Port Forwarding“ funktsioon (vt allpool). Teatud teenused (nt traceroute või ftp) vajavad aadresside tõlkimise puhul erikohtlemist.

Välimine juurdepääs NAT puhul

Ühenduse loomiseks väljast (nt veebiserverile saadetavate päringute puhul) tõlgitakse NAT-lüüsis ümber kõik paketid, mis on suunatud teatud kindlale pordile ja edastatakse serveri vastavale pordile. Seda mehhanismi nimetatakse ka „Destination NAT“ või „Port-Forwarding“. Serveri vastuspakettidega käitub NAT-lüüs analoogselt.

Täiendavad kontrollküsimused:

- Milliseid IP-aadresse kasutatakse sisevõrgus?
- Kas NAT-d kasutatakse?
- Kas Port-Forwarding funktsiooni kasutatakse?

M 5.71z Sissetungi tuvastuse ja sellele reageerimise süsteemid

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: administraator

Tulemüüri administraatori üheks peamiseks ülesandeks on tekkivate logiandmete analüüsimine, et selle abil ründeid võimalikult operatiivselt tuvastada. Kuna andmeid on palju ja rünnete toimepanekuks on samuti suur hulk erinevaid keerukaid võimalusi, kulub selliseks tööks palju aega. Siin on abiks sissetungi tuvastamise süsteemid (ID (Intrusion Detection)) ja sissetungile reageerimise süsteemid (IR (Intrusion Response)). ID-süsteemi eesmärgiks on aidata keskmiste oskustega administraatorit, kellel ei ole süvitsiminevaid teadmisi internetiturbe valdkonnast. Süsteem võimaldab administraatoril suure hulga logiandmete hulgast ründeid tuvastada. IR-süsteemide eesmärgiks aga on automaatsete vastumeetmete kasutuselevõtt kohe pärast seda, kui mõni rünne on kindlaks tehtud.

Ideaaljuhul peaks neil programmidel analüüsimiseks piisaval hulgal infot olema ja neid peaks haldama heal tasemel administraator, et ründed ei saaks ükskõik millistest logiandmetest mitte üksnes tuvastatud, vaid et suudetaks koguda ka infot kaitsefunktsioonide tugevuse ja ohustatuse kohta ning et vajalikud vastumeetmed saaksid kasutusele võetud võimalikult kiiresti. Hetkel on siiski tegu veel valdkonnaga, mida alles tugevasti uuritakse, mis tähendab, et ka juba olemasolevatele programmidele võib pidevalt juurde tekkida märkimisväärseid parandusi. Intrusion Detection süsteeme saab jaotada kahte klassi: allkirjade analüüs ja anomaaliate tuvastus:

- Allkirjade analüüs põhineb oletusel, et paljusid ründeid on võimalik tuvastada logiandmete teatud järjekorra alusel. Üheks näiteks on nn portide skaneerimine. Eeltööna enne ründe toimepanemist selgitatakse välja, milliseid teenuseid ründe sihtmärgiks veatud arvuti võimaldab, st milliste TCP-portidega on võimalik ühendusi luua. Selle info saamiseks saadetakse teatud programmi abil üksteise järel kõikidele TCP-portidele ühenduse loomise pakett. Juhul kui ühenduse loomine õnnestub, tähendab see, et on leitud sihtmärk, kuhu on installeeritud teenus, mida saab rünnata. Sellise ründe juurde kuuluv allkiri ehk tunnus on lihtne: kõikidele TCP-portidele saadetakse üksteise järel ühenduse loomise pakette. Samas tulevad kohe ilmsiks sellist liiki ründetuvastusega seotud probleemid: millises järjekorras ja milliste ajavahemike möödudes peaksid portidele tehtavad päringud toimuma, et rünnet oleks võimalik tavapärasest tööst eristada? Praegused Portscanningu tüüpi programmid töötavad selliselt, et päringuid ei saadeta mitte kindlas järjekorras Port 1, Port 2 kuni Port n, vaid juhuslikus järjekorras. Ka pakette on võimalik saata mitte kohe üksteise järgi, vaid juhuslike ajavahemike tagant (nt 1 s, 100 ms, 333 ms, 5 s . . .). See kõik muudab allkirja koostamise raskeks. Portscanningu rünnete peenemaks variandiks on see, kui üksikuid pakette saadetakse erinevatelt allikaadressidelt. Rakendades samas ka veel eelpool kirjeldatud ajalist nihet pakettide saatmisel, on tõenäosus, et selline rünne jääb märkamata, väga kõrge.
- Anomaaliat tuvastavad süsteemid seevastu lähtuvad oletusest, et kasutajate ja arvutite tavapärast käitumist on võimalik edasi anda statistiliste näitajatena ning kõrvalekaldeid käsitletakse rünnetena. Sellekohaseks näiteks

on ajaperiood, mille vältel on kasutaja tavaliselt oma arvutisse sisse logitud. Juhtumite puhul, kus töötaja teeb oma tööd peaaegu alati esmaspäevast reedeni kella kaheksast viieni ning kõikumine on maksimaalselt 2 tundi, võib olukorda, kus tuvastatakse, et tegevus leiab aset laupäeval või kell 24.00, käsitleda ründena. Anomaaliate tuvastamise probleemiks on see, kuidas defineerida tavapärast käitumist. Teatud piirväärtuste või tõenäosusarvutustega on teatud info saamine siiski võimalik. Samas on küsitav, kas töötaja aktiivset tegevust õhtul kell 19.10 tuleks kohe käsitleda ründena. Reeglina pole kasutajate tavapärane tegevus mitte alati ühesugune, vaid muutub, mis tähendab, et süsteemi tuleb kohandada. ID-süsteem aga ei suuda iseseisvalt tuvastada, et käitumise muutumine on reeglipärane ja mitte rünne.

Seetõttu on mõttekas ID-süsteemid andmekogumise liigi põhjal alamsüsteemideks jaotada. Seda võib saavutada eraldi sniffer tüüpi programmiga kusagil võrgus (võrgupõhine ID-süsteem) või tavapärase logimisfunktsiooni osana mõnes ühendatud arvutis (hostipõhine ID-süsteem). Mõlematel on oma eelised ja puudused. Võrgupõhised süsteemid suudavad laiaulatuslikke korraga mitut arvutit puudutavaid ründeid paremini tuvastada. Ühe arvuti vastu suunatud keeruliste rünnete (nt erinevatest vaheasukohtadest tehtavate rünnete) tuvastamine seevastu on palju raskem. Lisaks ei suuda võrgupõhised süsteemid analüüsida krüpteeritud andmeid. Hostipõhiste ID-süsteemide miinuseks on aga fakt, et nende rakendamine võib nõuda arvutite logimisfunktsioonide põhjalikku muutmist. Kuna logimisandmete analüüsimisel tuleb järgida isikuandmete kaitsenõudeid ka neil juhtudel, kus analüüsimine toimub automaatselt, võib salvestamisel tekkida vajadus kasutada pärisnimede asemel pseudonüüme. Enne ID-, IR-süsteemi ja tulemüüri ühendamist tuleks arvestada järgnevaga:

- Kas tulemüüri vastu on võimalik sihipäraselt algatada rünnet, mida ID-süsteem võib eksikombel pärisründeks pidada? Selle tagajärjel IR-süsteemi poolt käiku lastav blokeering tulemüüri kaudu toimivate teenuste suhtes võib endaga kaasa tuua käideldavuse märkimisväärse languse.
- ID-, IR-süsteemi ja tulemüüri omavaheline suhtlemine tuleb dokumenteerida piisavalt läbipaistvalt. Ainult nii on võimalik igal ajahetkel hinnata, kes tulemüüri administreerib: kas IR-süsteem või administraatorid. Kahtluse korral tuleks eelistada administraatorite otsuseid.

Vältimaks ründeid ID-süsteemi enda vastu, peaksid need olema võrgust vaadelduna võimalikult nähtamatud. Kõige lihtsamaks lahenduseks on kasutada IP-aadressi, mida internetis ei marsruudita. Lisaks võib soovitada ka ARP protokolli desaktiveerimist vastava liidese jaoks, et nii ARP- kui ka IP-pakettidele jäetaks reageerimata.

M 5.72 Mittevajalike võrguteenuste desaktiveerimine (Unix)

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: administraator

Unix-süsteemi kõikide ebavajalike võrguteenuste väljalülitamiseks tuleb toimida käesolevas meetmes toodud kirjelduste järgi. Võrguteenuste sisselülitamiseks on Unixi keskkonnas kaks võimalust. Kasutada saab serveriteenust inetd , mida konfigureeritakse failis /etc/inetd.conf ning Startup-failid, mille asukohaks on /etc/rc.d/init.d või /etc/init.d . Ebavajalike teenuste väljalülitamiseks tuleb /etc/inetd.conf faili vastav rida märgistada trellidega. Standardse installatsiooni puhul on reeglina konfigureeritud ainult hädavajalikud teenused. Nende hulgas leidub aga ka teenuseid, mis võivad kujuneda ohuallikaks. Seetõttu tuleks tööle lülitada ainult minimaalne arv teenuseid, st ainult need teenused, mida süsteemil on ilmtingimata tarvis (vt M 4.95 Minimaalne operatsioonisüsteem ja M 4.97 Ainult üks teenus serveri kohta).

Teenused, mille käivitamise eest hoolitsevad Startup-failid, lingitakse alamkataloogidega / etc/rc X .d või /etc/rc.d/rc X .d , mille puhul X tähistab vastavat Unix-Runlevelit, milles Startup-fail käivitatakse. Ebavajalike teenuste desaktiveerimiseks saab ebavajalikud teenused ümber paigutada alamkataloogi, et neid oleks vajaduse tekkimisel võimalik ka uuesti sisse lülitada. See võib toimuda järgnevalt:

cd rc3.d; mkdir .s; mv S85sendmail .s/

Hetkel aktiivseid teenuseid saab tuvastada käsuga netstat -a .

Täiendavad kontrollküsimused:

- Kas Startup-failides tehtud muudatused on dokumenteeritud?
- Kellel on õigus Unix-süsteemi teenuseid lisada?
- Kas pärast igat rakendusprogrammide ja operatsioonisüsteemi koostisosade värskendust (update) kontrollitakse netstat -a käsuga, millised teenused on võrguühenduse ootel?

M 5.76w Sobivate tunnelduspro tokollide kasutamine VPN-süsteemis

Algatamise eest vastutavad: IT-juht, infoturbespetsialist

Rakendamise eest vastutavad: administraator

Andmeühenduste turve

Olukorras, kus VPN-võrgust (VPN - Virtual Private Network) luuakse juurdepääs LAN-ile, toimub see reeglina mõne välise andmeühenduse kaudu. Näiteks otsese sissevalimise puhul (Direct Dial-In) kasutatakse mõne telekommunikatsiooniteenust pakkuva operaatori võrku. Internetikeskkonnas loodava ühenduse puhul liiguvad andmed läbi internetiteenust pakkuvate operaatorite võrkude (ja võib-olla ka läbi nende koostööpartnerite võrkude). Kuna VPN-ühenduse puhul leiab aset otseühendus LAN-iga, tuleb andmete edastamiseks kasutatav võrgu andmetee muuta piisavalt turvaliseks, et oleks tagatud andmete konfidentsiaalsus, terviklus ja autentsus. Turve tagatakse andmevahetuses liikuvate andmepakettide krüpteerimisega ning vajadusel ka allkirjastamisega, mis leiab aset pärast sidepartnerite autentimist (vt M 4.34 Krüpteerimise, kontrollsummade ja digitaalallkirjade rakendamine). VPN-keskkonna sideühenduste turbe tagamiseks on loodud mitmeid protseduure ja mehhanisme, mille üheks näiteks on tunneldamine. VPN-ühenduse turvalisust tagava protseduuri valimine võib muuhulgas sõltuda järgnevatest faktoritest:

- turbenõuetest tulenevad nõuded protseduuri tugevusele (antud nõuded määravad ära nt võtmete pikkuse),
- protokollitasandil kasutatavad protseduurid,
- VPN-riistvara ja -tarkvara poolt toetatavad protseduurid.

Üldreeglid

- igal VPN-tootel on reeglina olemas ka side turvet võimaldavad standardsete protseduuride valik. Eesmärgiks peaks olema võimalikult paljude protseduuride tugi;
- andmete transportimiseks kasutatavatel protokollidel on olemas juba oma enda turvamehhanismid. VPN-toode võib neid kasutada. Mõningatel VPN-toodetel võivad lisaks olla ka veel oma protseduurid.

Turvamehhanismid põhinevad erinevatel krüptograafilistel protseduuridel. Lühikese sissejuhatuse krüptograafia põhimõistetesse leiate meetmest M 3.23 Sissejuhatus krüptograafia põhimõistetesse .

Protokolliühenduste krüpteerimine/ tunneldus

Kui kahe sidepartneri vahel luuakse krüpteeritud andmeühendus, luuakse selle ühendusega turvaline kanal. Selle kanali kaudu on võimalik kommunikatsiooniprotokolliga (nt IP-ga) edastada ükskõik milliseid andmeid. Lahendusi, kus edastatavad andmed on kommunikatsiooniprotokolli andmepaketid, nimetatakse üheks tunneliks. Protokolli, mida kasutatakse andmete krüpteerimiseks, krüpteeritud andmete edastamiseks läbi tunneli ja ühenduse haldamiseks, nimetatakse ka tunnelprotokolliks. Tunnelprotokolle saab eristada järgnevate põhimõtete alusel:

- millistele transpordiprotokollidele need toetuvad ja milline on nende protokollikihi liigitus (OSI-Layer) (vt M 4.90 Krüptoprotseduuride kasutamine ISO/OSI etalonmudeli eri kihtides),
- milliseid protokolle edastatakse läbi tunnelühenduse,

- milliste krüptograafiliste protseduuride tugi on olemas tunneli loomiseks,
- kas tunneli lõpp-punkte autenditakse ja
- kas rakendatav transpordiprotokoll võimaldab luua mitut paralleelset tunnelit.

Tunnelprotokoll vastutab peamiselt järgnevate valdkondade eest:

- tunneli või tunnelite haldamine, ühenduse loomine, säilitamine ja lõpetamine,
- krüptograafiliste protseduuride kokkuleppimine tunneli moodustamiseks: võtmevahetusprotseduur, krüpteerimisprotseduur ja allkirjastamisprotseduur,
- läbi tunneli edastatavate protokollide andmepakettide kokku- ja lahtipakkimine ning
- andmepakettide kokku- ja lahtipakkimine.

Rakendatava VPN-riistavara ja -tarkvara valikul tuleks jälgida, et toodetel oleks võimalikult paljude erinevate ja laialt levinud krüpteerimisprotseduuride tugi. Sellega saab suurendada tõenäosust, et klientsüsteem ja server suudavad omavahel sobiva protseduuri kokku leppida.

Levinud tunnelprotokollide ülevaade

VPN-i keskkonnas kasutatakse järgnevaid tunnelprotokolle:

- PPTP (Point to Point Tunneling Protocol)
- L2TP (Layer 2 Tunneling Protocol)
- IPSec (Internet Protocol Security)
- TLS/SSL (Transport Layer Security, Secure Sockets Layer)

Nimetatud protokollidel on järgnevad tooteomadused:

Tunnel-protokoll	Kiht	Transporditavad protokollid	Vajalik alusprotokoll	Toetatavate tunnelite arv	Tunneli autentimine
PPTP	2	IP, IPX, NetBEUI	IP	1	ei
L2TP	2	IP, IPX, NetBEUI	IP, X.25, Frame Relay, ATM	mitu	jah
IPSec	3	IP	IP	1	jah
TLS/SSL	4	IP, HTTP, SMTP, . . .	IP	mitu	jah

Tabel: protokollid

Praktilise rakendamise jaoks oluline aspekt on see, et kõik tunneldamise lõpp-punktid peavad toetama väljavalitud tunnelprotokolle ja kehtestatud krüptograafilisi protseduure. Järgneb levinud tunnelprotokollide lühike kirjeldus.

PPTP (Point to Point Tunneling Protocol)

PPTP on 2. kihi tunnelprotokoll. Selle ülesandeks on PPP-ühenduste (Point to Point Protocol) loomine läbi IP-võrgu. Selliselt loodud PPP-ühendusi saab kasutada nt IP-pakettide transportimiseks (tunneldamiseks). Turbealased funktsioonid nagu autentimine, võtmete haldamine ja krüpteerimine rakenduvad samuti PPP vahendusel ning sageli kasutatakse selleks MPPE-d (Microsoft Point-to-Point Encryption Protocol). Sellistest lahendustest rääkides ei eristata sageli enam puhast PPTP-d ja PPTP/PPP/MPPE kombinatsiooni. Selle tunneldusmeetodi tavapärases rakenduses on leitud turvaauke, eriti just seoses nõrkade paroolidega. Seetõttu tohib PPTP-d VPN-i lahendusena kasutada ainult koos täiendavate turvamehhanismidega.

L2TP (Layer 2 Tunneling Protocol)

Sarnaselt PPTP-ga on L2TP versiooni nr 2 (L2TPv2) otstarbeks PPP-ühenduste loomine pakettidena edastatavates võrkudes. Vastupidiselt PPTP-le saab L2TP puhul lisaks IP-le kandevvõrguna kasutada ka teisi tehnoloogiaid, nt ATM-i. Tunneldamisfunktsiooni jaoks kasutab L2TP Cisco poolt loodud protokolli L2F (Layer 2 Forwarding) protokolli mehhanisme. L2TP-l endal andmepakettide krüpteerimist võimaldavaid funktsioone ei ole. Vastav krüpteerimine peab aset leidma kas kandevvõrgus või transporditavate protokollide poolt. Sel põhjusel kasutatakse sageli L2TP ja IPSec-i (vt allapool) kombinatsiooni.

IPSec (Internet Protocol Security)

IPSec on 3. kihi protokoll, millel on olemas IP-side krüpteerimiseks ja tervikluse tagamiseks vajalikud funktsioonid. Kombineerides seda IKE-protseduuriga (Internet Key Exchange, varem ISAKMP/Oakley), saab rakendada ka automaatset võtmevahetust ja tunneldamise lõpp-punktide autentimist. IPSec-side võtmevahetuseks võib kasutada ka ettevõttelt Sun Microsystems pärinevat protseduuri SKIP (Simple Key Management for Internet Protocol). Lisaks on IPSec-il olemas ka käsitsi võtmevahetuse funktsioon. Kasutajate autentimiseks tuleb seevastu kasutada teisi protseduure. IPSec on keeruline protokoll, millel on mitmeid erinevaid valikuid ja töörežiime. Rakendatavate krüptograafiliste protseduuride spetsifikatsioon pole samuti lõplikult kindlaks määratud, nimetatakse vaid miinimumnõudeid. Seetõttu tuleb IPSec-i rakendades tagada, et sellele loodaks konfiguratsioon, mis täidaks konkreetse kasutusvaldkonna jaoks välja töötaud turbenõudeid ja võimaldaks kasutusele võtta sobivad krüptograafilised protseduurid (vt M 5.149 Turvaline välisvõrguühendus IPSec-i abil ja M 2.164 Sobiva krüptoprotseduuri valimine).

TLS/SSL (Transport Layer Security, Secure Sockets Layer)

TLS/SSL on laialt levinud protseduur, mille eesmärgiks on tagada transportimise turvalisus nt veebirakendustele või meilide edastamiseks. Ühelt polt on TLS/SSL-i abil võimalik transportida erinevaid rakendusprotokolle, nagu HTTP, SMTP, POP või IMAP. Teiselt poolt on spetsiaalsete tarkvarakomponentidega võimalik TLS/SSL-i vahendusel luu ka IP-tunnelit. Tänu selle tööpõhimõttele pole TLS/SSL-i võimalik üheselt kindla protokollikihi alla liigitada, kuid sellele vaatamata käsitletakse seda sageli 4. kihi protokollina. TLS/SSL-il on olemas autentimist, krüpteerimist ning võtmevahetust ja tervikluse kaitset võimaldavad turvafunktsioonid. Sarnaselt IPSec-iga pole selleks vajalikud krüptograafilised protseduurid spetsifikatsioonis lõplikult kindlaks määratud. Enamasti lepivad sidepartnerid protseduurid kokku iga kord, kui ühendus luuakse. Seetõttu tuleb tagada, et loodaks konfiguratsioon, mis täidaks kasutusvaldkonna jaoks välja töötaud turbenõudeid ja võimaldaks kasutusele võtta sobivad krüptograafilised protseduurid (vt M 2.164 Sobiva krüptoprotseduuri valimine , M 5.66 TLS-i/SSL-i kasutamine ja M 5.148 Turvaline välisvõrguühendus OpenVPN-i abil).

Muud tunnelprotokollid

VPN-lahenduste loomiseks ei tule kõne alla mitte ainult ülalloetletud protokollid, vaid ka kõikvõimalikud muud protseduurid. Üheks näiteks võiks olla OpenSSH kasutamine VPN-i otstarbel. OpenSSH töötati esmajoones välja kui krüpteerimist võimaldav alternatiiv telneti, ftp ja r-teenustele, kuid seda saab kasutada ka VPN-ühenduste turvamiseks. Lisaks on saadaval ka täiendavad tooted, mis kasutavad erinevate firmade endi poolt loodud tunneldus- ja krüpteerimisprotseduure. Selliseid tootjate endi loodud protseduure tuleks siiski vältida, kuna nende turbeomadusi on sageli väga raske hinnata. Nende asemel tuleks kasutada protseduure, mis lähtuvad levinud standardite avalikult kättesaadavatest spetsifikatsioonidest.

Kontrollküsimused:

- Kas rakendatav tunnelprotokoll suudab piisavalt kaitsta andmete konfidentsiaalsust, terviklust ja autentsust?
- Kas rakendatavad krüptograafilised protseduurid ja võtmete pikkus vastavad kaasaegsetele tehnilistele nõuetele?
- Kas on tagatud, et sides osalevate VPN-komponentide vahel lepitakse kokku sobivate krüptigraafiliste protseduuride kasutamine?

M 5.77z Alamvõrkude rajamine

Algatamise eest vastutavad: IT-juht, infoturbespetsialist
Rakendamise eest vastutavad: IT-juht, administraator

Ametiasutuste ja ettevõtete IT-süsteemid on reeglina integreeritud lokaalsetesse kohtvõrkudesse (LAN-id), mis on veel omakorda ühenduses teiste võrkudega. Keskmise suurusega võrkude ja suurte võrkude puhul on ainuüksi tehnilistel põhjustel vaja, et LAN jaotataks alamvõrkudeks, nt juba sellepärast, et iga alamvõrgu kohta lubatud IT-seadmete arv on piiratud või sellepärast, et kaablite kogupikkusel on omad piirid. Alamvõrkude loomine on soovitatav ka IT-turbe seisukohast.

Ühelt poolt on sellega võimalik tagada, et tundlikke andmeid käideldakse vaid teatud kindlas alamvõrgus (konfidentsiaalsus), teisalt on võimalik takistada olukorda, kus alamvõrgus esinevad rikked või selle vastu suunatud ründed võiksid ohustada teisi alamvõrkusid (terviklus ja käideldavus). Ka neil juhtudel, kus LAN-iga on võimalik luua sideühendusi väljastpoolt, tuleks kindlasti samamoodi luua vastavad alamvõrgud, et kaitsta LAN-i väljast tulevate rünnete vastu. Eriti oluline on tagada, et VPN-serverid saaksid paigutatud niinimetatud juurdepääsuvõrku. Selleks võib kasutusele võtta nt turvalüüsi täiendavad demilitariseeritud tsoonid (DMZ).

Alustuseks tuleb kindlaks määrata, milliseid IT-süsteeme tohib ühises alamvõrgus käitada ja milliseid mitte.

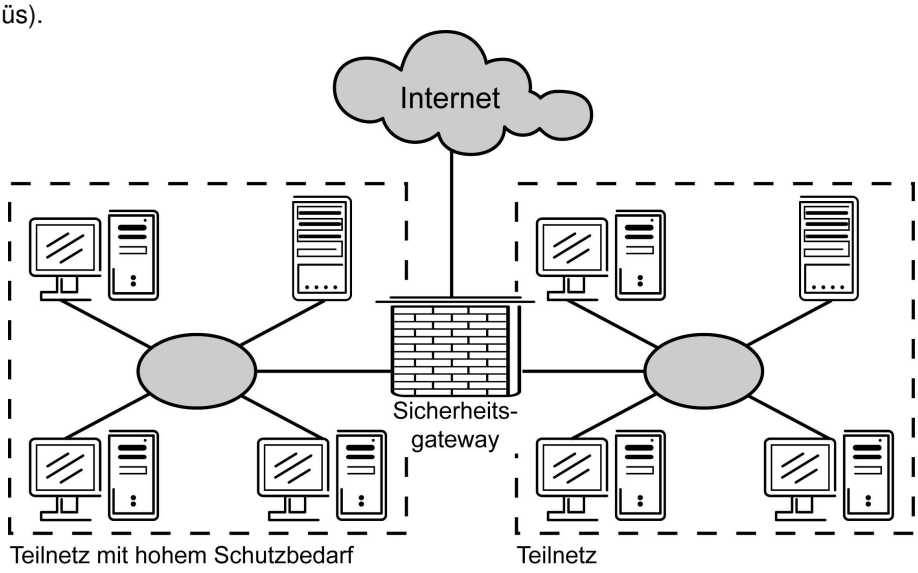
Siinkohal on soovitatav lähtuda eelnevalt väljaselgitatud turbeastmest ja toimida alljärgnevalt:

- Tundlike andmete koondamine alamvõrkude piiridesse – kõikide ühte alamvõrku kuuluvate IT-süsteemide ja nende sideühenduste turbeaste peaks konfidentsiaalsusest kui ühest põhiväärtusest lähtuvalt olema ühesugune. Sellega saavutatakse, et konfidentsiaalsete andmete käitlemine ei väljuks spetsiaalselt kaitstud alamvõrkude piiridest. Vajaminevaid kaitsemeetmeid rakendades saab keskenduda vastavatele alamvõrkudele.
- Kõrgkäideldavate süsteemide isoleerimine – IT-süsteeme ja sideühendusi, mille turbevajadus on tervikluse ja käideldavuse poolest kas kõrge või väga kõrge, tuleks võimaluse korral käitada eraldi alamvõrgus. Niimoodi tagatakse, et teistes alamvõrkudes esinevad rikked ei sega nende komponentide töötamist. Lisaks on selliste lahenduste korral võimalik tõrkeid kiiremini piiritleda ja kõrvaldada. Teise sammuna tuleb loodud alamvõrkude omavaheliseks ühendamiseks välja valida sobivad komponendid (vt M 5.13 Võrgu ühendusaparatuuri õige kasutamine).

Turvalüüside rakendamist tuleks eriti kaaluda selliste alamvõrkude omavahelisel ühendamisel, mille komponentidele kehtivad väga kõrged turbenõuded. Sellega tagatakse andmevoo sihipärane ja juhitud liikumine alamvõrku ning alamvõrgust välja.

Järgneval joonisel on toodud näide, milline võiks välja näha LAN-i tervikstruktuur

pärast seda, kui kõrgete turbenõuetega alamvõrk on muust alamvõrgust turvalüüsiga eraldatud. Lihtsustamise eesmärgil on turvalüüsi kujutatud ühe sümbolina, kuid reaalselt kuulub selle alla muidugi mitu komponenti (paketifilter, rakendusluüs).



Joonis: LAN-i tervikstruktuuri näide

Teilnetz mit hohem Schutzbedarf – kõrge turbevajadusega alamvõrk; Sicherheitsgateway – turvalüüs; Teilnetz - alamvõrk

LAN-i segmenteerimise tehnilisi nõuandeid leiate järgmistest meetmetest:

- M 5.61 Sobiv füüsiline segmenteerimine
- M 5.62z Sobiv loogiline segmenteerimine

Kontrollküsimused:

- Kas kohtvõrk on väljaselgitatud turbevajaduste põhjal jaotatud mõistlikult alamvõrkudeks?
- Kas VPN-serverid on paigutatud muust võrgust eraldatud juurdepääsuvõrkudesse?
- Kas on otsustatud, milliseid võrguühenduselemente alamvõrkude rajamiseks kasutatakse?

M 5.78z Kaitse mobiiltelefonide järgi asukoha määramise eest

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: kasutajad

Mobiilside kasutamisel on sidepartnereid tarvis tehnilistel põhjustel kättesaadavuse tagamise eesmärgil positsioneerida. Sidepartnerid edastavad infot oma asukoha kohta ka sideühenduse loomisel – kellelegi helistades. Sellist asukohainfot saavad võrguoperaatorid ja teenusepakkujad, aga võib juhtuda, et ka kolmandad osapooled kasutada isikupõhiste või seadmepõhiste liikumisprofiilide koostamiseks. Juhul kui liikumisprofiilide koostamise võimalust käsitletakse mobiiltelefonide rakendamisel ohuna, tuleks juhul kui võimalik, mobiiltelefone ja SIM-kaarte töötajate vahel sagedamini vahetada. Niimoodi muudetakse seadmete ja kaartide seostamine kindlate kasutajatega vähemalt raskemaks.

Kui liikumisprofiilides nähakse ohtu, tuleks võimaluse korral mobiiltelefone ja ka SIM-kaarte töötajate vahel sagedamini vahetada. Niimoodi muudetakse seadmete ja kaartide seostamine kindlate kasutajatega vähemalt raskemaks. Positsioneerimisi Radio Resource Location Protocol'i (RRLP) kaudu ei saa sellega siiski tõrjuda, sest kindlaks tehakse nii telefoninumber kui ka International Mobile Equipment Identity (IMEI).

Olukorras, kus on tarvis tagada, et teatud aja jooksul poleks isikute asukohta võimalik tuvastada, aitab ainult mobiiltelefoni väljalülitamine. Et päris kindel olla, tuleks telefonist eemaldada ka aku.

Kontrollküsimused

- Kas on selgeks tehtud, kas liikumisprofiilidel võib olla negatiivne mõju?

M 5.79z Kaitse mobiiltelefoni numbri tuvastamise vastu

Algatamise eest vastutavad: infoturbeametnik, IT-juht

Rakendamise eest vastutavad: kasutajad

Mobiilsidevõrgus kuvatakse tavaliselt suhtluses osalejatele kõiki telefoninumbreid. Kas seda tehakse või mitte, sõltub mobiiltelefonide tehnilistest võimalustest ning mobiiltelefonides, operaatorvõrgus ja mobiilsideoperaatorite tehtud seadistustest.

Mobiiltelefonides on võimalik helistaja numbrinäidu keelufunktsiooniga (nii ühekordselt kui ka kõikidele kõnedele) tõkestada oma telefoninumbri kuvamist kõne vastuvõtja telefonis. Nimetatud funktsioon kannab mobiiltelefonides sageli tähistust „Inkognito" või „Anonüümne". SMS-i saatmisel mobiiltelefoniga ei ole numbrinäidu keelufunktsioon tavaliselt võimalik. Voice-Mailbox'i käitumine tuleks iga juhtumi korral eraldi kinnitada, samuti ka numbrinäidu keelufunktsiooni tegevuste üldine käitumine välismaal.

Numbrinäidu keelufunktsiooni võib seadmetel, mis toetavad GSM-standardit, juhtida järgmiste GSM-koodidega järgmise kõne jaoks:

- oma telefoninumbrit näidatakse *31#telefoninumber
- oma telefoninumbrit ei näidata *31#telefoninumber

Numbrinäidu keelufunktsiooni saab aktiveerida ka võrguoperaatori kaudu.

Teatud määral pakub kaitset isikute ja mobiiltelefoninumbrite otsese seostamise vastu see, kui kasutajad vahetavad telefone ja SIM-kaarte omavahel. Niimoodi pole võimalik isikuid ja telefoninumbreid ehk mobiiltelefone jäädavalt omavahel siduda. Liigitamisvõimalus ettevõtte või ametiasutuse lõikes jääb aga siiski alles.

Lisaks helistamisfunktsioonile on võimalik isikute mobiiltelefonide numbreid välja uurida ka avalikest telefoniraamatutest, juhul, kui need on sinna sisse kantud. Mobiilside lepingut sõlmides tuleks seetõttu hoolikalt kaaluda, kas ja millises vormis tohib oma andmeid avalikes telefoniraamatutes eksponeerida. Ka asutusesisestes telefoniraamatutes ja üksikute andmepäringute (blanketid, loosimised jne) korral ei tohiks mobiiltelefoninumbreid mõtlematult avaldada.

Kontrollküsimused

- Kas vajalikel juhtudel keelatakse telefoninumber väljuvate kõnede jaoks?

- Kas avalikes telefoniraamatutes on avaldatud ainult selleks ettenähtud telefoninumbrid?

M 5.80z Kaitse mobiiltelefonidega pealtkuulamise eest siseruumides

Algatamise eest vastutavad: infoturbeametnik, IT-juht

Rakendamise eest vastutab: infoturbeametnik

Kes tahab mobiiltelefonide pealtkuulamise siseruumides kindlalt välistada, peab hoolitsema selle eest, et kaitstavasse ruumi ei võetaks kaasa ühtegi mobiiltelefoni. Kui asutuse IT-turvapoliitika ei luba mobiiltelefoniga ruumi siseneda, tuleb sissepääsude juures sellest ka selgelt märku anda. Arvestage, et teabe edastamine ilma kontrollimiseta ei anna soovitud tulemusi.

Kaitseks ei piisa ainult mobiiltelefoni väljalülitamisest või oote- või lennurežiimi seadistamisest. Kui telefone on vastavalt manipuleeritud, saab neid raadioside kaudu märkamatult sisse lülitada.

Mobiiltelefonide detektorid

Mobiiltelefonide detektorid on seadmed, mis suudavad tuvastada, kas teatud piiratud alas leidub üks või mitu mobiiltelefoni, mis lülitavad ennast edastusrežiimile (alustavad kõnet).

Olemas on aktiivseid ja passiivseid detektoreid. Passiivsed hoiatusseadmed teavitavad mobiiltelefone, mis asuvad edastusrežiimil. Seadmete tööpiirkonda on võimalik reguleerida selliselt, et tuvastamise ala piirdub alaga, mida soovitakse kontrollida. Vastava turbevajaduse korral on soovitatav need seadmed muretseda ja konfidentsiaalsete kõneluste ajaks sisse lülitada. Moodsad mobiiltelefonid ei vaja pealtkuulamiseks siiski alalist sideühendust, vaid võivad kõne salvestada ja helifaili viivitusega mobiilsidevõrgu kaudu üle kanda. Seepärast kaitsevad passiivsed mobiiltelefoni detektorid ainult teatud tingimustel ruumisiseste kõnede pealtkuulamise eest.

Selleks, et oleks võimalik tuvastada ka ooterežiimil töötavaid mobiiltelefone, peavad detektorid olema varustatud aktiivse saatjaga. Selle saatja abil saab mobiiltelefoni lülitada edastusrežiimi. Seejärel saab detektor seda tuvastada. Selle aktiivse detektori abil on võimalik tuvastada kõiki sisselülitatud mobiiltelefone. Hiljem sisse lülitatavad mobiiltelefonid peavad ennast tugijaamas registreerima ning seetõttu saab ka sellist tegevust tuvastada. Segavaid saatjaid saab rakendada ka nii, et tõkestada teatud ruumide piires raadiosidet nii tugevalt, et mobiililevi vastuvõtt muutub võimatuks.

Hetkel saab soovitada vaid passiivsete mobiilidetektorite rakendamist. Mobiiltelefone saab kasutada ka diktofonidena. Hääletud ja lennurežiimi lülitatud seadmed võivad ilma vaevata salvestada vestlusi, nii et isegi aktiivsed mobiiltelefoni detektorid ei kujuta endast sobivat vastumeedet.

Kontrollküsimused

- Kas on tagatud, et mobiiltelefone ei kasutata pealtkuulamise eest kaitstavates ruumides?

M 5.81 Turvaline andmeedastus mobiiltelefoni kaudu

Algatamise eest vastutavad: infoturbeametnik, IT-juht

Rakendamise eest vastutavad: kasutajad, infoturbeametnik

Mobiiltelefone kasutatakse kõnede tegemiseks, kuid nendega on võimalik edastada ka andmeid ja saata fakse. Mõnede selliste teenuste kasutamiseks läheb tarvis lisavarustust. Moodsad mobiiltelefonid on tavaliselt pidevalt internetiga ühendatud, et võtta vastu vestlussõnumeid või e-kirju. Kui mobiiltelefonid kasutavad LTE-standardit, viiakse iga suhtlemine ellu andmeedastusena internetiprotokolli (IP) kaudu.

Lühisõnumid

Lühisõnumitega (Short Message Service SMS) on võimalik ühest mobiiltelefonist teise või ka e-posti aadressile saata kuni 160 tähemärgi pikkuseid sõnumeid. Pikemad sõnumid jagatakse seejuures tavaliselt mobiiltelefoni poolt mitmeks lühisõnumiks. Lühisõnumite kohaletoimetamine toimub alati lühisõnumite keskuse vahendusel, mis suunab sõnumid edasi kõikidele vastuvõtjatele.

Lühisõnumeid salvestatakse telefoni mällu vaid seni, kuni telefoni mälus on veel vaba ruumi. Kui vaba salvestusruumi enam piisavalt ei ole (sageli vanemate või eriti soodsate mudelite puhul), ei ole võimalik rohkem lühisõnumeid vastu võtta. Võrguoperaatorid püüavad täiendavaid lühisõnumeid kliendile kätte toimetada vaid teatud piiratud aja jooksul. Juhul kui telefoni mälu uute sõnumite jaoks ei vabastata, kustutab võrgu operaator uued sõnumid ära.

Mõningatel juhtudel on võimalik mobiiltelefoni abil ka ise määrata, millise aja jooksul võrgu operaator lühisõnumeid oma süsteemis säilitab. Eelseadistuseks on reeglina ajavahemik 24 kuni 48 tundi. Nimetatud säilitamisaega ei ole reeglina võimalik pikendada, välja arvatud juhul, kui operaatoriga on sõlmitud sellekohane leping. Seda ei tuleks kindlasti mitte ka lühendada.

Olenevalt mobiilsideteenuseosutajast on olemas võimalus, et lühisõnumi saatja saab automaatse vastuvõtukinnituse. Selleks, et veenduda, kas sõnumid (vt G 5.27 Sõnumi salgamine) on vastu võetud, tuleks aktiveerida vastuvõtukinnitus. Sellega saab lisaks ka kontrollida, kas lühikese salvestusaja tõttu ei ole sõnum ehk sõnumikeskuse poolt kohale toimetatud (vt G 4.32 Sõnumi kaotsiminek). Vastuvõtukinnitusi tuleks mobiiltelefonis salvestatuna hoida nii kaua kui võimalik.

Lühisõnumite saatmiseks peab mobiiltelefoni vastavas menüüs olema salvestatud lühisõnumikeskuse (SMS-Gateway) number. Enamatel juhtudel on see võrgu operaatori poolt SIM-kaardil juba ette ära konfigureeritud.

Internetis on eraldi pakkumisi, et saata lühisõnumeid minimaalsete kuludega. Ründe toimepanija saab seega ilma suurema vaevata saata mobiiltelefonile suure hulga SMS-sõnumeid. SMS-rämpspostil on samasugused mõjud nagu e-posti rämpspostil (vt G 5.75 Ülekoormus siseneva meili tõttu). Postkast ehk mälu koormatakse üle ja võimalikud olulised sõnumid ei pruugi enam kohale jõuda. Seetõttu võidakse kasutajale tekitada võib-olla ka suuri väljaminekuid. Selle vastu aitab lisaks kolmandate teenuseosutajate pakkumiste lukustamisele teenuseosutaja või mobiilisideoperaatori kaudu see, et oma telefoninumbrit ei levitata liiga laialt, st nt loobutakse kandest telefoniraamatutes või kahjujuhtumi korral loobutakse mõneks ajaks SMS-ide vastuvõtmisest.

SMS-i saatjat ei ole SMS-i korral võimalik usaldusväärsel moel identifitseerida. Tuvastamiseks saab kasutada vaid saatja telefoninumbrit ning olenevalt võrgu operaatorist ja mobiiltelefoni konfiguratsioonist võib juhtuda, et neid andmeid ei edastata. Läbi interneti saadetavate lühisõnumite puhul ei saa selgest identifitseerimisest juttugi olla. Seda fakti peaksid kasutajad neile laekunud sõnumite hindamisel alati meeles pidama. Olenevalt lühisõnumi sisust on alati mõistlik saatja käest järele küsida, kas ta on ka reaalselt sellise sõnumi saatnud.

Faksid

Mobiiltelefoniga ühendatud IT-süsteemi kaudu (nt sülearvuti) saab saata ja vastu võtta fakse.

Seejuures tuleb arvestada tavapärastele faksiaparaatidele kehtivate nõuetega (vt moodulit B 3.402 Faks), ennekõike sellega, et:

- mobiiltelefoni mälu võidakse faksi vastuvõtmisega üle koormata,
- olenevalt faksi sisust on võib-olla vajalik faksist koopiaid teha, mis võib mobiiltelefonide puhul osutuda keeruliseks,
- vastavalt vajadusele tuleks mõnede faksi vastuvõtjate või saatjate telefoninumbrid tõkestada.

Lisaks sellele soovitatakse:

- pärast saatmist järele uurida, kas faks ka loetavalt pärale jõudis,
- pärast vastuvõtmist tuleks järele küsida, kas faks pärineb tõesti sellelt saatjalt,
- aeg-ajalt tuleb kontrollida programmeeritud sihtaadresse.

E-kiri

Lisaks lühisõnumitele saab mobiiltelefonidega vastu võtta ja saata ka e-kirju. Vanemate seadmete puhul on ka e-kirjade nagu lühisõnumite piirang 160 märki.

Kui võrguoperaator avab kasutaja jaoks e-posti teenuse, väljastatakse mobiiltelefonile oma e-posti aadress. Üldiselt on mobiiltelefonidel tänapäeval siiski e-posti kliendid, mis suudavad e-kirju töödelda nagu PC. Kui mobiiltelefonidel ei ole e-posti kliente, kuid on veebilehitseja, saab e-kirju tavaliselt töödelda veebiliidese kaudu.

Mõnede võrguoperaatorite puhul saab e-posti teenuseid kombineerida ka teiste teenustega. Nii näiteks on võimalik sisenevaid e-kirju arvuti poolt ette lugeda, neid on võimalik edasi saata mõnele faksiaparaadile või mõnele teisele e-posti aadressile. Väljuvaid e-kirju on võimalik mobiiltelefoniga salvestada ning saata välja audiofailina.

Nii nagu lühisõnumid ja faksid, võivad ka e-kirjad kiiresti olemasoleva mäluruumi (vanematel ja eriti soodsatel seadmetel) ammendada. Seetõttu peaks e-kirja klient olema seadistatud nii, et failimanuseid laaditakse alla üksnes siis, kui kasutaja seda selgesõnaliselt taotleb.

E-kirjaga seotud turbeprobleeme ja meetmeid on kirjeldatud moodulis B 5.3 Rühmatarkvara . Siinkohal tuleks arvestada, et mobiiltelefonides on e-kirja funktsioonid teiste e-posti rakendustega võrreldes vägagi piiratud. Samamoodi nagu SMS, on ka e-post antud kontekstis ette nähtud vaid lühikese sisuga teadete edastamiseks. Turvameetmed nagu krüpteering ja allkiri on tavaliselt võimalikud ainult nutitelefonidel. Alternatiivselt on olemas spetsiaalsed seadmed või täiendavad moodulid, millega mobiiltelefon saab edastada krüpteeritud või allkirjastatud sõnumeid.

Instant Messenger

Mõnedel mobiiltelefonidel ja enamikul nutitelefonidel on olemas Instant Messenger või seda on võimalik hiljem installeerida. Instant Messenger'iga on võimalik edastada sõnumeid, aga ka faile nagu nt fotosid, filme ja Office-dokumente. Sageli kasutatakse ka Instant Messenger'i, mis töötab Internet-Relay-Chat-(IRC)-süsteemi kaudu. Suhtlus Instant Messenger'i kaudu peaks toimuma krüpteeritult lõpp-punktist lõpp-punkti. Kasutada tohib usaldusväärseid IRC-servereid või Instant-Message-Provider'it. Sellisel juhul suureneb suhtluse usaldusväärsus võrreldes lühisõnumitega tunduvalt. Kahtlased failiedastused tuleks tagasi lükata. Instant Messenger'il on lühisõnumitega võrreldes ka see eelis, et kulud ei teki mitte sõnumite arvu, vaid andmehulga alusel. Lisaks on paljudel Instant Messenger'idel vastuvõtukinnituse funktsioon, mida tuleks ka kasutada, et seista vastu sõnumite salgamise ohule (vt G 5.27 Sõnumi salgamine).

Andmeedastus

Mobiiltelefoni saab olenevalt mudelist ühendada muu IT-süsteemiga (nt sülear-

vuti või elektroonilise märkmikuga) ja seejärel lihtsamalt ka suuremaid andmehulki üle kanda. Täiendavate seadmete ühendamiseks on mitmeid võimalusi ning loeb see, millist ühendamisviisi mõlemad seadmed toetavad.

Pistikkaart Pistikkaart (PC-Card, PCMCIA) on algselt tavapärane lahendus mobiiltelefoni ja sülearvuti ühendamiseks, mida aga tänasel päeval peaaegu enam ei kasutata. Enamik pistikkaarte ühildub samas siiski vaid ühe kindla tootja mobiiltelefonidega.

Softmodem Selle lahenduse korral kasutatakse sülearvutis pistikkaardi asemel spetsiaalset tarkvara. Mobiiltelefon ühendatakse sülearvutiga tavapärase jadaliidesega (või USB-ga). Antud lahendus on sageli odavam kui pistikkaart.

Infrapuna Infrapunaliidese kaudu võib andmeid ka ilma juhtmeta mobiiltelefonist teise seadmesse (nt sülearvutisse või elektroonilisse märkmikusse) üle kanda. Selleks peab nii mobiiltelefon kui ka teine seade toetama infrapuna ülekandestandardit IrDA-d. IrDA on ülemaailmne standard andmete edastamiseks infrapuna kaudu, kuid tänapäeval ei kasutata seda enam peaaegu üldse (vt M 4.255 Infrapunaliidese kasutamine).

Bluetooth Bluetooth on levinud standard, tänu millele saavad seadmed raadiolainete abil vahemaade 1 kuni 100 m korral (olenevalt Bluetooth-klassist) omavahel andmeid vahetada. (vt B 4.8 Bluetooth).

WLAN: Traadita-LAN-i kaudu saab mobiiltelefoni ühendada arvutivõrguga või see saab ise töötada kui nn WLAN-Hotspot („Tethering”) ja anda internetiühendust muude IT-süsteemide kasutusse. WLAN-ühendus tuleks seejuures kaitsta WPA kaudu krüptograafiliselt. Täiendavad üksikasjad WLAN-i kasutamiseks on toodud moodulis B 4.6 Traadita kohtvõrgud .

Andmete edastamisel nt sülearvutist läbi mobiilivõrgu, tuleks edastatavad andmed eelnevalt sülearvutis krüpteerida. Selleks on saadaval erinevaid lihtsalt kasutatavaid rakendusi. Andmete krüpteerimine enne nende edastamist kindlustab nende turvalisuse kogu teekonnaks saatjast adressaadini. See väljub GSM-i puhul standardse õhuliidese kaitse kaudu mobiiltelefoni ja tugijaama vahel. See on vajalik, sest krüpteering loetakse GSM-võrgu kaudu õhuliidesel katkenuks. Halva rakenduse korral ei paku krüpteering ka UMTS-iga edastamisel paremat kaitset kui edastamine GSM-iga. Kui andmed krüpteeritakse seevastu programmide poolt, mis asuvad lõppseadmel, võib sõnumeid lisaks sellele ka digitaalselt allkirjastada. Adekvaatsete krüptograafiliste protseduuride ja süsteemide valiku kohta leiate lisainfot moodulist B 1.7 Krüptokontseptsioon .

Alternatiivselt andmete krüpteerimisele pakuvad moodsad mobiiltelefonid mitme-

kesiseid võimalusi, et rajada krüpteeritud VPN-tunneleid, millega saab samuti piisavalt kaitsta andmete edastamist mobiiltelefoni ja muude võrguosaliste vahel. Alternatiivina võiks VPN-lõpp-punktina kasutada ka olemasolevat sülearvutit, mille kaudu saab mobiiltelefon luua kaitstud andmeühenduse. Kui kasutatakse VPN-i, on olemas eelis, et krüpteering on läbipaistev ja ei vaja edasist kasutaja sekkumist.

Kui mobiiltelefonil on veebilehitseja ja e-posti klient, on see nende kanalite kaudu sama haavatav kui PC. Mõtlematult allalaaditud andmed, telefonihelinad, aga ka Drive-by-tüüpi infektsioonid võivad muuta seadmed samamoodi töövõimetuks nagu statsionaarsed arvutid.

Kõikides organisatsioonides peavad eksisteerima selged reeglid andmete edastamise kohta. Andmete edastamiseks tohib kasutada ainult seadmeid, millele on väljastatud vastav luba ning kõikidele seadmetele peavad olema välja töötatud selged kasutusreeglid (vt lisaks M 2.204 Ebaturvalise võrkupääsu tõkestamine).

Selleks, et GSM-liidese kaudu toimuv andmevahetus ei tooks endaga kaasa turvariske, tuleks selle kasutamisele seada piirangud. Nii ei tohiks IT-süsteemidel, millel töödeldakse tundlikke andmeid, lubada kasutada mobiilsidekaarte või peaksid ühendused mobiilivõrgu kaudu olema alati kaitstud krüpteeritud VPN-tunnelitega. Sama kehtib ka kõikide IT-süsteemide kohta, mis on ühendatud arvutivõrku, et ei tekiks olukorda, kus tulemüüriga loodud kaitsefunktsiooni hakatakse õõnestama.

Kontrollküsimused

- Kas on olemas eeskirjad selle kohta, milliseid andmeid tohib mobiiltelefonide kaudu edastada?
- Kas on olemas eeskirjad selle kohta, milliseid liideseid tuleb kasutada ja kuidas toimub krüpteerimine?

M 5.83z Turvaline välisvõrguühendus Linux FreeS/WAN abil

Algatamise eest vastutavad: IT-juht, administraator

Rakendamise eest vastutavad: administraator

Paljudes institutsioonides on nõue, et eraldi kohtades installitud kohalikud võrgud oleksid omavahel ühendatud. Enamikel juhtudel toimub see kas renditud liinide või avaliku võrgu kaudu, mis ei ole allutatud institutsiooni kontrollile. On oht, et edastatud andmetega on võimalik manipuleerida ja neid pealt kuulata ning et ründaja esitleb ennast volitatud sidepartnerina (maskeraad). Kasutades virtuaalset privaatvõrku (Virtual Private Network - VPN), saab neid ohte vältida. Krüptograafiliste meetoditega on seejuures võimalik tagada nii andmete terviklus ja konfidentsiaalsus, kui ka teostada sidepartnerite turvaline autentimine. Linux FreeS/WAN on vabavarana saadav programmipakett Linuxi operatsioonisüsteemile, mille abil on võimalik luua IPSEC-standardiga ühilduv VPN.

Plaanimine

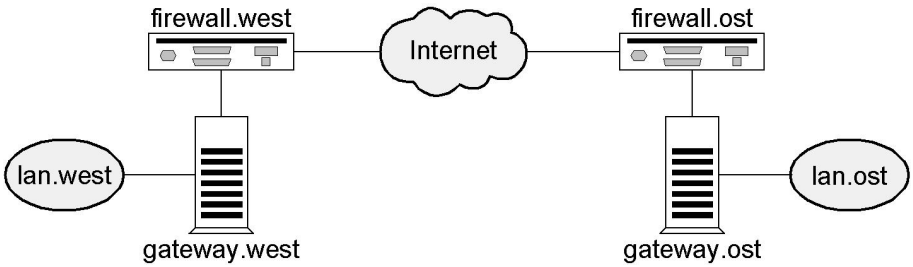
Plaanimise käigus tuleks esmalt välja selgitada, milliseid nõudeid peab sideühenduse turbeks kasutatav toode täitma. Siia hulka kuuluvad näiteks nõuded selle kohta, kas toode peab juba eelnevalt paigaldatud komponentidega koos töötama või kas peale TCP/IP on vaja transportida veel teisi protokolle. Pärast seda tuleks läbi töötada FreeS/WAN i dokumentatsioon ja selle põhjal otsustada, kas see programmipakett on antud ülesannete jaoks sobilik. Kui nii otsustatakse, tuleks kindlaks määrata ja dokumenteerida see, milliseid FreeS/WAN funktsioone milleks kasutatakse ja kuidas see olemasolevasse võrgustruktuuri paigutatakse.

Installeerimine

FreeS/WAN töötab vabavarana saadaval operatsioonisüsteemil Linux ning kasutab kerneli IP-protokollitulpa. Soovitatav on käitada FreeS/Wan i ainult selleks konfigureeritud PC-l, millel ei ole lisaks vajalikele marsruutimisfunktsioonidele aktiveeritud mitte ühtegi teist teenust (vt M 4.97 Ainult üks teenus serveri kohta). Eelkõige ei tohiks nad kasutada tulemüürifunktsioone, vaid peaksid olema tulemüürisüsteemist sõltumatud. Operatsioonisüsteemi installeerimiseks peaks kasutama Linuxi distributsiooni, mis sisaldab FreeS/WAN i. See kergendab installeerimist märgatavalt, kuna vastasel juhul tuleb Linuxi kernel tavaliselt uuesti kompileerida. Siinkohal tuleks tähelepanu pöörata FreeS/WAN i dokumentatsioonile. Linuxi distributsioonilt tuleks installeerida ainult vajalikud programmipaketid.

Konfiguratsioon

FreeS/WAN paigaldab hulga IPSEC-is defineeritud funktsioone. Seetõttu on ka vastava konfiguratsiooniga võimalik seda programmipaketti kasutada erinevates keskkondades ja erinevateks ülesanneteks. Järgneva näite põhjal selgitatakse, kuidas FreeS/WAN i on võimalik kasutada kahe interneti kaudu ühenduses oleva lokaalse võrgu side turbeks. Võrgus olevate komponentide paigutus:



Joonis: võrgus paiknevad komponendid

Institutsiooni mõlemad asukohad west ja east on internetiga ühenduses. Mõlemal pool kasutatakse seejuures mitmeastmelist tulemüürisüsteemi, mis lihtsuse mõttes on joonisel kujutatud üksiku sümbolina. gateway.west ja gateway.east on Linuxi operatsioonisüsteemi all paiknevad IT-süsteemid, mis FreeS/WAN i abiga toimivad lokaalsetele võrkudele lan.west ja lan.east lüüsidena (gateway). Mõlemal lüüsil on kaks võrgukaarti, mis ühendavad nad tulemüüri süsteemidega ja lokaalsete võrkudega eesmärgiga tagada lan.west i ja lan.east i IT-süsteemide vaheline turvaline suhtlus. Kommunikatsiooni turve peaks kõigi IT-süsteemide puhul läbipaistev olema. Tähtis on võtmehalduseks õige meetod valida. Soovitatav on kasutada avaliku võtme (Public Key) (RSA) meetodi kaudu automaatset võtmevahetust. Teiste FreeS/WAN i poolt pakutavate meetoditega võrreldes on sellel suurim turbeaste. Konfiguratsiooni esimeseks sammuks on RSA võtmepaaride loomine mõlemale lüüsile. Seda saab teostada näiteks käskluse ipsec rsasigkey abil. Võtmete pikkus peaks olema vähemalt 768 bitti. Nagu ka dokumentatsioonis märgitud, võib niimoodi moodustatud võtmeid kasutada ainult allkirjadeks, mitte aga krüpteerimiseks. FreeS/WAN i programmipaketisiseselt on see kindlustatud. Käskluse ipsec rsasigkey väljund sisaldab nii avalikku kui ka privaatset RSA-võtit. VPN-i turvalisuse säilitamiseks on määrav see, et privaatne võti ei oleks mitte mingil juhul kompromiteeritud (vt M 2.46 Krüpteerimise õige korraldus). Privaatne võti paikneb lüüsil failis /etc/ipsec.secrets, omandiõigus (ownership) ja load (permissions) tuleb märkida järgmiselt:

-rw——- root root /etc/ipsec.secrets

Avalik võti paigutatakse seevastu faili /etc/ipsec.conf (vaata all). Selles failis tehakse ka kõik muud FreeS/WAN i puudutavad seadistused. Faili vorming on selline, et mõlemal lüüsil saaks kasutada sama faili. Konfiguratsioon toimub mitmes etapis, kus seadistusi tehakse vastavalt mudelile parameeter = väärtus . Parameetrid, mis nõuavad kahe lüüsi vahelist eristamist, tähistatakse eelneva võtmesõnaga left või right. FreeS/WANi vastav instants tuvastab IP-aadressi põhjal iseseisvalt selle, milline parameeter nendest kahest neile sobib. Reeglina erinevad mõlemal lüüsil salvestatud faili /etc/ipsec versioonid ainult interface parameetri poolest näiteks seetõttu, et ühel poolel kasutatakse ethernet i ja teisel poolel tokeni ringi. Antud näite põhjal antakse järgnevalt soovitusi faili /etc/ipsec.conf konfigureerimiseks.

Lõik config setup

Selles lõigus teostatakse üldiseid seadistusi.

interfaces = ipsec0=eth0

Esmalt tuleb parameetriga interface kindlaks määrata, milliseid võrguliideseid

turvatud ühenduste loomiseks kasutatakse. Teiste liideste kaudu krüpteeritud pakette ei saadeta. Ülaltoodud näites luuakse ühendus tulemüüriga lüüsi liidese eth0 abil.

forwardcontrol = yes

Kui forwardcontrol on määratud väärtusega yes, lülitab FreeS/WAN IP-pakettide edastamise iseseisvalt sisse ja välja, kui IPSEC on siis vastavalt aktiveeritud või desaktiveeritud. Kui VPN ei ole kättesaadav, kaitseb see pakettide krüpteerimata edastamise eest. Linuxi süsteemi buutimisel tuleks kindlustada, et IP-pakettide edastamine oleks välja lülitatud enne võrguliidese aktiveerimist. Antud seadistuse teostamine sõltub kasutatavast Linuxi distributsioonist.

dumpdir =

Selleks, et FreeS/WAN i komponendid ei looks programmivea korral mälutõmmiseid (core dump), tuleks parameeter dumpdir määrata tühja väärtusega. Näiteks esineb oht, et volitamata isikud võivad nendelt mälupiltidelt salajasi võtmeid teada saada.

plutoload = %search

plutostart = %search

Deemon pluto on FreeS/WAN paketi osa ja seda kasutatakse automaatseks võtmehalduseks. Parameetritega plutoload ja plutostart määratakse, millised ühendused stardi ajal automaatselt pluto andmebaasi laaditakse või selles aktiveeritakse. Need parameetrid on otstarbekas määrata spetsiaalse väärtusega, milleks on %search. Nii laaditakse või aktiveeritakse need ühendused, mis on vastavalt märgistatud parameetriga auto .

Lõik conn west-east

Selles lõigus teostatakse seadistusi, mis kehtivad ainult ühele kindlale ühendusele, näiteks west-east.

type = tunnel

Parameetriga type määratakse selle ühenduse käitusrežiim. Kuna antud näites tuleb võrguühendus turvata kahe lokaalse võrgu vahel lüüside kaudu, tuleb kindlasti kasutada tunnel- režiimi. Transport- režiim on lubatud ainult hostilt hostile side korral ja passthrough on lubatud ainult manuaalse võtmehalduse korral.

auto = start

Kui parameetrid plutoload ja plutostart on määratud spetsiaalse väärtusega %search , siis määrab parameeter auto antud ühendusele kindlaks, kas nad laaditakse (aktiveeritakse) stardi ajal automaatselt pluto andmebaasi. Näites tahetakse ühendust koheselt käivitada, seepärast määratakse parameetri auto väärtuseks start.

auth = esp

Parameeter auto määrab, millisega kahest IPSEC-funktsioonist, sõnumi kapselturve (Encapsulating Security Payload - ESP) või IP autentimispäis (Authentication Header - AH), autentimine teostatakse. Antud juhul saab nii krüpteerimise kui ka autentimise teostada ESP-ga. See on standardseadistus.

authby = rsasig

Autentimine on soovitatav teostada digitaalallkirjade abiga RSA algoritmi kaudu (seadistus rsasig). Võrreldes „ shared secrets ” (seadistus secret) meetodiga pakub see kõrgemat turbeastet ja võimaldab lihtsamat haldust.

pfs = yes

pfs - Perfect Forward Secrecy tähendab, et minevikus edastatud teateid ei saa kompromiteerida ka siis, kui mõlema lüüsi privaatsed võtmed teada saadakse. (Tu-

levaste ühenduste turvet ei ole aga enam võimalik kindlustada.) Selle parameetri soovitatav standardväärtus on yes.

keyingtries = 0

Parameeter keyingtries määrab antud ühenduse loomise või aktualiseerimise maksimaalse kordade arvu. Soovituslik on väärtuseks määrata spetsiaalne väärtus 0, mis tähendab, et katsete arv on piiramatu. Parameetrile keyingtries vaikeseadistusega määratud väärtus 3 ei ole enamikele rakendustele piisav.

left =

right =

Parameetritega left ja right määratakse mõlema osaleva lüüsi IP-aadressid. Soovituslik on IP-aadressid numbriliselt sisse kanda ja mitte kasutada spetsiaalset väärtust %defaultroute . Võrreldes IP-aadresse, mis on vastavatele võrguliidestele määratud, tunneb FreeS/WAN ära, millise rolli (left või right) IT-süsteem endale võtab.

leftnexthop =

rightnexthop =

Parameetrite leftnexthop ja rightnexthop väärtusteks tuleb määrata vastavate komponentide IP-aadressid, mis peavad paketti ebaturvalise võrgu kaudu edasi juhtima. Antud näite korral on see komponent tulemüürisüsteemi osa. Vastavalt lokaalse võrgu aktiivsete võrguosade jaotusele ja paigutusele tuleb siinkohal aga paljudel juhtudel kanda sisse lähim marsruuter, mis interneti tulemüüri suunas teele jääb.

leftsubnet =

rightsubnet =

Nende kahe parameetri kaudu määratakse kindlaks, millised kaks alamvõrku omavahel turvaliselt suhtlevad. Antud näite korral on nendeks lokaalsed võrgud lan.west ja lan.east. Väärtused tuleb sisse kanda vormina alamvõrk/mask, näiteks 10.10.0.0/16.

leftid = @gateway.west

rightid = @gateway.east

Parameetrite leftid ja rightid kaudu jagatakse mõlemale lüüsile autentimiseks vajalikud nimed, mis on soovitatav määrata DNS-nimede vormis, etteasetatud “@” märgiga. Seeläbi takistatakse see, et FreeS/WAN teisaldab enne DNS-serverile päringu esitamist DNS-nimed IP-aadressideks.

leftrsasigkey =

rightrsasigkey =

Nende kahe parameetri abiga määratakse mõlema lüüsi avalikud võtmed. Vastavad salajased võtmed tuleb kanda sisse antud lüüsi faili /etc/ipsec.secrets.

Marsruutimine

IP-pakettide edastamiseks kasutab FreeS/WAN Linuxi marsruutimistabeleid. Käskluse route abiga tuleb seega mõlemal lüüsil tekitada reeglid, et lokaalsele või välisele võrgule määratud paketid vastava võrgukaardi kaudu edasi juhitaks.

Lüüsi kaughaldus

gateway.west ja gatewat.east ei saa antud konfiguratsiooni korral VPN-i kaudu suhelda. Turvaline tunnel transpordib andmeid ainult lan.west ja lan.east vahel. See on infoturbe seisukohast soovitatav, välja arvatud juhul, kui ühte antud kahest lüüsist tahetakse teise lüüsi kaudu hallata. Sellisel juhul tuleb failis ipsec.conf luua uus ühendus. See lisaühendus erineb west-east ühendusest selle poolest, et tal puudub parameeter leftsubnet (juhul kui gateway.west i tahetakse kaughallata

lan.east i kaudu) ehk siis puudub parameeter rightsubnet (juhul kui gateway.east i tahetakse kaughallata lan.west i kaudu).

Tulemüüri seadistused

firewall.west ja firewall.east tuleks konfigureerida nii, et mõlema lüüsi vahel oleks võimalik krüpteeritud andmepakette ja vajalikke halduspakette vahetada. Antud näite korral on selleks vajalikud järgmised reeglid:

- IP-paketid protokollnumbriga 50 gateway.west ist gateway.east i ja vastupidi on lubatud,
- UDP-paketid, port 500 gateway.west ist gateway.east i ja vastupidi on lubatud.

Kui näitest kõrvalekalduvalt määrati parameetri auth väärtuseks ah , tuleb läbi lasta ka IP-pakette protokollnumbriga 51. Kogu ülejäänud kommunikatsioon lüüsiga või lokaalse võrguga tuleb vastava tulemüürisüsteemi poolt keelustada. Kuna tulemüürisüsteem ja lüüs on realiseeritud üksteisest eraldi, ei tohiks kasutada parameetreid leftfirewall ja rightfirewall ega ka parameetreid leftupdown ja rightupdown. Ärge teostage IPSEC-pakettidele aadressiteisendust.

Tootmisandmete kasutamise keeld testimisel

Võrguaadressi ümbernimetamise (Network Address Translation - NAT) kasutamisel tuleb jälgida, et aadresside sisendus toimuks kas lüüsi ja lokaalse võrgu vahel või lüüsil endal. Üldjuhul ei ole aadresse võimalik tulemüürisüsteemi siseselt teisendada. Selle põhjuseks on see, et osa IP-pakettidest modifitseeritakse NAT-i kasutamisel nii, et IPSECI terviklusekontroll reeglina ebaõnnestub. NAT-i võib seega kasutada alles „pärast" IPSEC-lüüsi. Kui aadressiteisendus tahetakse läbi viia IT-süsteemil, millel käitatakse ka FreeS/WAN i, tuleb arvestada sellega, et nii muutub IP-pakettide töötlemine sellel IT-süsteemil väga keerukaks. Lisainformatsiooni leiate FreeS/WANi dokumentatsioonist. Ülevaatlikum ja ka lihtsamini hallatav on teostada NAT eraldi komponendil lüüsi ja lokaalse võrgu vahel.

VPN-i funktsioonitest

Enne õiget tootmises kasutamist tuleks kontrollida, kas VPN toimib nii, nagu vaja. Kahe lokaalse võrgu asemel tuleks testimisfaasis lüüsiga ühendada ainult testarvutid. Kui VPN koheselt korrektselt ei tööta, ei saa kindlustada, et tootmisandmeid edastatakse interneti kaudu kaitstult. Tuleks kontrollida, kas paketid on krüpteeritud. Nagu dokumentatsioonis kirjeldatud, on seda kõige lihtsam teha tööriistade ping ja tcpdump kaudu. Ping i abiga saab koostada kergesti tuvastatavaid IP-pakette ja tcpdumb i saab kasutada sellest lähtuva FreeS/WAN i võrguliikluse lugemiseks. Jälgida tuleb seda, et ping käsklus tuleks teostada testarvutil ja mitte lüüsis. Näitlikustavas konfiguratsioonis kaitseb VPN ainult lokaalsete võrkude vahelist andmeedastust (testifaasis on need asendatud ühe või mitme testarvutiga) mitte aga andmesidet lüüsidest või lüüsidesse. (vt ka lõiku „Lüüsi kaughaldus".) Käsklust tcpdump loodud võrguühenduse jälgimiseks saab teostada suvalisel kahe lüüsi vahel paikneval IT-süsteemil.

Juhuks, kui VPN ei tööta nii nagu vaja, näiteks ei ole kommunikatsioon üldse võimalik või võrguliiklust ei krüpteerita, võimaldab FreeS/WAN laialdasi diagnoosivõimalusi. Informatsiooni programmipaketi oleku kohta saab näiteks tühifailist /proc/net/ipsec_tncfg

Täiendavad kontrollküsimused:

- Kas FreeS/WAN i käituseks kasutatakse iseseisvaid IT-süsteeme minimaalse Linuxi operatsioonisüsteemi installatsiooniga?
- Kas on kindlustatud, et privaatsed RSA-võtmed ei välju kunagi lüüsist?
- Kas VPN-i korrektset toimimist testitakse enne selle tootmissüsteemi paigaldamist?

M 5.87 Leping kolmandate poolte võrkudega ühendamise kohta

Algatamise eest vastutavad: asutuse/ettevõtte juhtkond, infoturbeosakond
Rakendamise eest vastutavad: IT-juht, infoturbeosakond

Üha rohkem ettevõtteid ja asutusi ühendavad oma seni suletud võrgud võrgukogudeks, nn ekstranettideks. Sisevõrgu ühendamisel kolmandate osapoolte võrkudega on oluline, et enne võrkude ühendamist koostataks detailne leping (data connection agreement, DCA). Selle lepinguga tuleb kindlaks määrata, kellele ja millistel tingimustel võimaldatakse ligipääs teise võrku ning millised võrgu osad ja teenused ligipääsuks avatakse. Samuti on oluline määrata, kellele enda organisatsioonist ja millistel tingimustel antakse teatud ligipääsuõigused võõrale võrgule.

Selline leping peaks hõlmama järgmisi punkte:

- kirjeldus lepingu üldise sisu kohta;
- vastutavate isikute kindlaksmääramine (kes vastutab lepingu tingimuste täitmise eest?);
- organisatoorsete ja tehniliste probleemide ning turvalisust puudutavate juhtumitega tegelevad kontaktisikud;
- vajalik tehniline informatsioon, kusjuures kindlaks määratakse järgmised aspektid:
- milliseid teenuseid (näiteks telnet, ftp, http) kasutatakse,
- milliseid IT-platvorme, rakendusi ja andmeformaate toetatakse,
- milline kättesaadavus tuleb tagada (jõudlus, maksimaalne väljalangemismäär),
- kes ja mida tohib protokollida või peab protokollima, kuhu logiandmed paigutatakse ja kes neile ligi pääseb (eriti oluline võib see olla hädaolukordades),
- millisel määral on vajalik logiandmete regulaarne vahetamine,
- millised turvameetmed tuleb tagada.
- konfidentsiaalsuslepe (non-disclosure agreement) selle kohta, et osapooled ei tohi koostöö raames saadud informatsiooni kolmandatele isikutele edastada;
- vastutuse ja hüvitise regulatsioon (siin tuleks muu hulgas välja tuua võrguühenduse katkestamise tingimused, vastutus arvutiviiruste või rünnakute korral, leppetrahvid täitmata kohustuste eest või vastutus võõra sisu kasutamise eest);
- teabenõuete reguleerimine tekkivate turvaaukude korral;
- määratlemine, milliseid andmeid võib milleks kasutada (näiteks töötulemuste edasikasutamisel);
- kirjeldus selle kohta, kuidas lisanduvad partnerid lepinguga seotakse, näiteks läbi rakenduste ühise kasutamise või teenusepakkujana ühele lepingupoolele;
- lepingu kehtivusaeg (tehnika areneb kiirelt, mis tähendab, et ka selle kasutamise lepingut tuleb pidevalt kohandada).

Leping tuleks sõlmida lepingust kinnipidamise eest vastutavate isikute vahel. Kuna sellega on seotud ettevõte või asutuse erinevad osakonnad, tuleks eelnevalt välja selgitada, kes peaks võrguühenduse loomise eest vastutama. Mõttekas on selleks luua meeskond, kuhu kuuluvad vähemalt infoturbespetsialist, IT-juht, spetsialist ja andmekaitsespetsialist. Kriitilistesse otsustesse, näiteks kas ühendus tuleks probleemide tõttu ajutiselt sulgeda, tuleks kaasata kõik ülalnimetatud isikud, sest nende huvid võivad üksteisest suuresti erineda. Enne võrguühenduse aktiveerimist tuleks mõlemal poolel kõrvaldada kõik turvaaugud. Siinkohal tuleks leida ka viis, mis võimaldaks oma partnerite turbeastmes kindel olla, näiteks viia läbi turbekontroll või pistelised katsed kohapeal. Mitte mingil juhul ei tohi turvaaukude kõrvaldamist lükata reaalsesse käitusesse, kuna kogemused näitavad, et neil on madalam tähtsus kui näiteks tavalistel kättesaadavusprobleemidel.

Tegutsemine vahejuhtumite korral

Kolmandatele isikutele tuleks lubada ainult selliste teenuste kasutamine, mille kohta on sõlmitud leping ja mis on ilmtingimata vajalikud. See, millised enda võrgu osad kolmandatele isikutele ligipääsetavaks teha, sõltub kommunikatsioonipartnerite suhetest ja nendevahelisest usaldusest. Välismaiste partnerite korral tuleb arvestada nende riikide seadustega, mis puudutavad näiteks krüpteerimist või autoriõiguste kaitset.

Kui võrguühenduse tõttu tekib turbeprobleeme, tuleb kindlalt määratleda, kes ja millal võib ühenduse katkestada, keda tuleb informeerida ja milliseid eskaleerumise samme ette nähakse.

Kontrollküsimused:

- Kas iga võrguühenduse korral kolmanda osapoolega on olemas lepingud põhiliste raamtingimuste kohta?
- Kas kokkuleppeid ajakohastatakse nii, et arvesse võetaks ka muutunud raamtingimusi?

M 5.88 Lepingud andmevahetuse kohta kolmandate pooltega

Algatamise eest vastutavad: asutuse/ettevõtte juhtkond, infoturbeosakond

Rakendamise eest vastutavad: IT-juht, infoturbeosakond

Andmevahetus teiste ettevõtete ja asutustega võib toimuda näiteks andmekandjate või e-posti kaudu. Lisaks juba üksikute andmevahetuste korral järgitavatele turvameetmetele tuleb regulaarse andmevahetuse puhul luua kindlate sidepartneritega kokkulepped, et andmevahetus võimalikult hõlpsalt läbi viia.

Selline leping peaks hõlmama järgmisi punkte: Kes on kontaktisikud?

- kontaktisikute määramine organisatoorsete ja tehniliste probleemide ja eelkõige turvalisust puudutavate juhtumite korral;
- vajalik tehniline informatsioon, see tähendab, et määratakse kindlaks:
- milliseid rakendusi ja andmeformaate toetatakse,
- milline kättesaadavus tuleb tagada: näiteks, kui tihti tuleb e-kirju lugeda ja kui kiiresti neile vastata.

Andmete kaitse transpordil

- millised turvameetmed tuleb tagada andmevahetuse korral:
- andmeid kontrollitakse enne ja pärast andmevahetust arvutiviiruste suhtes
- kuidas kaitsta andmeid transpordikahjustuste ja volitamata ligipääsu eest (suletud mahuti, kontrollsumma, krüpteerimine),
- kuidas on krüpteerimishaldus teostatud,
- juhul kui kustutamine on vajalik, tohib saatjapoolsed andmed kustutada alles pärast korrektse kättesaamise kinnitamist saaja poolt,
- konfidentsiaalsuslepe (non disclosure agreement) ehk lepe selle kohta, et osapooled ei tohi koostöö raames saadud informatsiooni edastada kolmandatele isikutele;
- määratakse kindlaks, milliseid andmeid ja milleks võib kasutada (näiteks töötulemuste edasikasutamisel);
- kohustus täita kõiki seadusi, eeskirju ja reegleid, näiteks andmekaitse- ja autorikaitseseadus või litsentsireeglid.

Täiendavad punktid, mida sellisesse leppesse sisse viima peaks, leiate meetmest M 2.45 Andmekandjate üleandmine .

Kontrollküsimused:

- Kas kindlate sidepartneritega on olemas kokkulepped põhilistes raamtingimustes?
- Kas kokkuleppeid ajakohastatakse, et arvesse võetaks ka muutunud raamtingimusi?

M 5.89 Turvalise kanali konfigureerimine Windowsis

Algatamise eest vastutavad: IT-juht, infoturbespetsialist
Rakendamise eest vastutavad: Administraator

Windowsi domeeni arvutite vahel on vaja jagada haldusinformatsiooni. Näiteks vahetavad seda omavahel ühe domeeni domeenikontrollerid. Üldjuhul edastatakse seejuures konfidentsiaalseid andmeid, mille ülekanne peab olema turvatud. Selleks saab kasutada nn turvakanalit (Secure Channel), mida seda tuleb vastavalt turbenõuetele ja lokaalsetele iseärasustele konfigureerida. Siinkohal kasutatakse turbemehhanismidena sidepartnerite autentimist, krüpteerimist konfidentsiaalsuse säilitamiseks ja allkirju tervikluse turbeks. Turvakanali konfiguratsioon toimub grupipoliitika kaudu.

Nende konfigureerimisel on olulised järgnevad aspektid:

- Alati on kindlustatud vastastikune autentimine, kuid krüpteerimine ja allkiri võivad olla nõutud üksteisest sõltumatult. Kui sidepartner vastavat turvet ei toeta, siis seda ei kasutata. Sellisel juhul toimub kommunikatsioon ilma turvameetmeteta.
- Krüpteerimine või allkiri võivad olla määratud kommunikatsiooniühenduse loomise eelduseks. Kui sidepartner vastavat turvet ei toeta, siis ühendust ei looda. Sellest tulenevalt võib juhtuda, et kliendid ei saa ennast domeeni sisse logida. See suvand tuleks aktiveerida ainult juhul, kui krüpteerimist ja allkirjastamist toetavad nii kõik domeeni arvutid kui ka kõik tuttavate domeenide arvutid.

Konfiguratsiooniks olulised grupiparameetrid:

- turvakanal: allkirjastage turvakanali andmed digitaalselt (kui võimalik),
- turvakanal: krüpteerige turvakanali andmed digitaalselt (kui võimalik),
- turvakanal: krüpteerige või allkirjastage turvakanali andmed digitaalselt (alati),
- turvakanal: vajalik tugev seansivõti (alati tuleks kasutada krüpteeringut 128 bitti).

Need parameetrid leiate Computer Configuration | Windows Settings | Security Settings | Local Policies | Security Options alt.

Windows 7 korral on seadistused järgmised:

- domeeni liige : allkirjastage turvakanali andmed digitaalselt (kui võimalik),
- domeeni liige: krüpteerige turvakanali andmed digitaalselt (kui võimalik),
- domeeni liige: krüpteerige turvakanali andmed digitaalselt (alati),
- domeeni liige: vajalik tugev seansivõti (alati tuleks kasutada krüpteeringut 128 bitti,)
- domeeni liige: desaktiveerige arvutiparoolide muutmine (alati),
- domeeni liige: arvutiparoolide maksimumvanus (standard: 30 päeva, tavaolukorras ei tohiks suuremat väärtust kasutada.)

Need parameetrid leiate Computer Configuration | Windows Settings | Security Settings | Local Policies | Security Options alt.

Kui võrgus on lisaks Windowsi operatsioonisüsteemiga arvutitele ka teiste operatsioonisüsteemidega arvuteid, tuleks aktiveerida ainult kaks esimest suvandit. Kui aga kõikidel võrgusolevatel arvutitel on Windowsi operatsioonisüsteem, tuleks aktiveerida kõik suvandid.

Kontrollküsimused:

- Kas konfidentsiaalse informatsiooni edastamine on sobivate meetmetega kaitstud (näiteks allkirjad, krüpteerimine)?
- Kas turvaline kanal on konfigureeritud vastavalt infoturbenõuetele ja lokaalsetest oludest lähtuvalt?
- Kas konfiguratsioonil arvestati kõigi oluliste grupipoliitika parameetritega?
- Kas võrgus kasutatakse ainult selliseid servereid ja kliente, millel on Windowsi operatsioonisüsteem?

M 5.90 IPSec'i protokolli kasutamine Windowsi keskkonnas

Algatamise eest vastutavad: infoturbeametnik, IT-juht

Rakendamise eest vastutavad: administraator

Suhtlemise kaitseks pakub Windows IPSec-nõuetele vastavat rakendust. IPSec on rahvusvaheline standard, mis võimaldab IP-l põhineva suhtluse krüptograafilist kaitset. Alati tuleb iga üksikjuhtumi korral otsustada, kas suhtluse kaitsmiseks tuleb kasutada IPSec-i. Seda tuleb arvesse võtta juba Windowsi kasutamise kavandamisel ja määratleda vastava suunise abil.

IPSec hõlmab järgmisi funktsioone:

- suhtluse lõpp-punktid
- edastatavate andmete tervikluse tagamine digiallkirjadega
- edastatavate andmete või kogu IP-andmepaketi usaldusväärsuse tagamine krüpteerimisega (tunnel-režiim)

Üldised suunised sobiva krüptoprotseduuri valimiseks on esitatud meetmes M 2.164 Sobiva krüptoprotseduuri valimine . Räsimeetodina tuleks IPSec-i rakendamise korral kasutada SHA-2-perekonna algoritmi, st SHA-224, SHA-256, SHA-384 või SHA-512.

Neid toetatakse IPSec-kliendis, mis on klientidel tulemüüri osa. See funktsioon on alates Windows 7-st standardi kohane.

Selleks, et lisaks edastatavate andmete terviklusele ja usaldusväärsusele tagada andmevahetus õigete suhtluspartnerite vahel, tuleb viimased autentida.

Windowsi rakendus võimaldab suhtluse lõpp-punktide autentimiseks järgmisi protseduure:

- Kui mõlemad suhtluspartnerid asuvad samas Active-Directory-struktuuris, võib kasutada Kerberos-protokolli. Seejuures toimub tavapärane Windowsi autentimine. See protseduur põhineb sümmeetrilistel võtmetel, mida kasutatakse nn Kerberos-Tickets'ite krüpteerimiseks.
- Kasutada võib X.509-sertifikaate. Siinjuures toimub asümmeetrilistel võtmetel põhinev autentimine sertifitseerimisandmete põhjal. Üldiselt kasutatakse nn Challenge-Response-protseduuri. See kontrollib, kas autenditav kasutaja on õige privaatse võtme valduses. IPSec-funktsioon DirectAccess kasutab seda varianti. Kasutada tuleks autentimismeetodit X.509-sertifikaatidega, kui on nõutav internetipöördus, kaugpöördus ettevõtte ressurssidele, suhtlus väliste äripartneritega või ilma Kerberos-protokollita arvutite kasutamine.

Esimese IPSec-ühenduse ülesehitamise korral lepitakse suhtluspartnerite vahel kõigepealt kokku autentimiseks kasutatavate algoritmide, tervikluse kaitse ja usaldusväärsuse säilitamise suhtes ja salvestatakse nn Security Association-is (SA).

Neid SA-s salvestatud parameetreid kasutatakse kõikide tuleviku sideühenduste jaoks, kuni SA-parameetrite kehtivus lõpeb ja protseduurid uuesti kokku lepitakse. See toimub tavaliselt täiesti automaatselt IPSec-rakenduse komponentide abil.

Tegeliku krüpteerimise jaoks tuleb luua võtmed, nn Master- ja Session-Key (sessioonivõti). Tavaliselt luuakse Master-Key, millest tuletatakse kõik teised võtmed, ühe ühenduse jaoks ainult üks kord, Session-Key luuakse aga seevastu perioodiliselt mitu korda. Olemas on võimalus luua ka Master-Key perioodiliselt uuesti, mis nõuab aga suhtluspartnerite uut autentimist. Tavaliselt toimib uus autentimine automaatselt IPSec-rakenduse komponentide kaudu, nii et sellega mõjutatakse olulises osas jõudlust.

IPSec tunneb suhtluse kaitseks kaht erinevat meetodit: ESP (Encapsulated Security Payload) ja AH (Authentication Header). Alates Windows Server 2008-st ei toetata enam AH-d, sest sellel meetodil puudub sellega seotud puuduste tõttu (võrguaadresside rakendamine NAT kohta ei ole võimalik) peaaegu täielikult praktiline tähtsus.

IPSec-il põhineva suhtluse juhtimiseks pakub Windows IPSec-suuniseid (IPSec-Policies), mis määravad, milliseid IPSec-parameetreid tuleb ühenduse jaoks kasutada. Alates Windows Server 2008-st nimetatakse IPSec-suuniseid ka Ühendusturvalisuse eeskirjadeks.

Erinevate suuniste abil on võimalik saavutada,

- et IT-süsteemid aktsepteerivad üksnes IPSec-iga kaitstud ühendusi,
- et IT-süsteemid nõuavad suhtluspartneritelt IPSec-iga kaitstud ühendusi, kuid võimaldavad ka kaitsmata suhtlust, kui partner ei toeta IPSec-protokolli,
- või et IPSec-il põhinev suhtlus välistatakse.

Windows pakkus varasemates versioonides kolme eelnevalt määratletud IPSecpoliitikat, mis on alates Windows Server 2008-st välja jäetud:

- klient (ainult vastus): IT-süsteemide jaoks, mis lepivad IPSec-kaitse suhtes kokku üksnes suhtluspartnerite nõudmise korral ja muul juhul suhtluse kaitset ei kasuta.
- Server (nõuda kaitset): IT-süsteemide jaoks, mis nõuavad oma suhtluspartneritelt IPSec-kaitstud ühendusi, kuid mis aktsepteerivad ka kaitseta ühendusi, kui suhtluspartner ei toeta IPSec-i.
- Server (vajalik on kaitse): IT-süsteemide jaoks, mis loovad üksnes IPSec-kaitsega ühendusi ja lükkavad kaitsmata ühenduste soovid tagasi.

Neid eelnevalt määratletud eeskirju saab üksikasjalikult kohandada kohalikele nõudmistele. Seejuures soovitatakse kõigepealt luua koopia ja teha muudatused suunise koopial.

IPSec-poliitika raames kasutatakse nn filtrireegleid, et määratleda erinevaid IPSec-parameetreid, nt olenevalt kasutatavast logist. Näiteks saab kindlaks määrata, et HTTP jääb krüpteerimata, FTP seevastu aga krüpteeritakse. Windowsi versioonid võimaldavad IPSec-poliitikate konfigureerimist rühmasuuniste kaudu suunises Arvuti konfigureerimine| Windowsi seadistused | Täiendatud turvalisusega Windows-Firewall | Ühendamisturvalisuse eeskirjad, Windows Server 2008 puhul toimub konfigureerimine suunises Haldus | Täiendatud turvalisusega Windows-Firewall | Ühendamise eeskirjad. Alates Windows Server 2008-st ei anna Microsoft kasutada eelnevalt määratletud IPSec-suuniseid. Uute ühendusturvalisuse eeskirjade abi aitab aga nende konfigureerimisel. IPSec aktiveeritakse kas rühmasuuniste kaudu või lokaalselt võrguühenduste omaduste dialoogiaknas. Omaduste dialoogiaknas aktiveerimist saab kasutada alates Windows Server 2008-st. Siin konfigureeritakse ja aktiveeritakse IPSec ühendusturvalisuse eeskirjade loomisega Windows-Firewall'is.

Alates Windows Server 2008-st koondati lokaalse tulemüüri ja IPSec-i eeskirjade konfigureerimine liideses, et lihtsustada haldamist ja kõrvaldada vea allikad vastuolus olevatest IPSec-i tulemüüri eeskirjadest.

Üldiselt tuleb IPSec-i kasutamise korral Windowsi keskkonnas arvesse võtta järgmist:
enne IPSec-i rakendamist tuleb kontrollida, kas käivitamisega seotud jõudluse kahanemine on vastuvõetav. Teatud tingimustel tuleks kaaluda TCP/IP-Offload-Engine'iga (TOE) võrguadapterite kasutamist, et teostada arvutusmahukaid ülesandeid, mis puudutavad TCP/IP-protokollipinusid võrguadapteril, et vähendada CPU koormust.

Sessioonivõtmete tugevamaks kaitseks tuleks aktiveerida valik Perfect Forward Secrecy (PFS). See tagab, et pärast sessioonivõtme kahjustamist saab dekrüpteerida üksnes selle ainsa sessioonivõtmega krüpteeritud andmeid.

Seda on võimalik saavutada nii,

- et sessioonivõtit, mida kasutati andmete krüpteerimiseks, ei kasutata enam järgmiste võtmete loomiseks ja
- et võtmematerjali, mida kasutati ühe sessioonivõtme loomiseks, ei kasutata rohkem järgmise sessioonivõtme loomiseks.

Selle tagajärjel on küll võimalik vähene jõudluse kahanemine, kuid üldjuhul ei ole see määrava tähtsusega.

Kõrge kaitsevajadusega ühenduste jaoks võib Master-Key jaoks aktiveerida ka valiku PFS-i. See toob siiski kaasa suuremad probleemid jõudlusega kui PFS sessioonivõtmete korral, sest siinjuures tuleb iga kord läbi viia suhtluspartneri autentimine.

Igal konkreetsel juhul tuleb otsustada, milliseid mehhanisme ja meetodeid kasutatakse autentimiseks ning tervikluse ja usaldusväärsuse tagamiseks IPSeckäsitluse raames ühenduse loomise ajal. Arvestada tuleb sellega, et suhtluspartnerite vahel peab alati olema vähemalt üks protseduur, mis kaitseb mõlemat partnerit. Kui luuakse oma IPSec-poliitikad, tuleb tingimata alati määratleda niinimetatud Standardvastuse eeskiri. See kehtib siis, kui ühtegi muud poliitika filtrireeglit ei kasutata. Kui standardvastuse reegel puudub, võib ette tulla, et suhtluspartnerite vahel jääb ühendus loomata. Standardvastuse reeglit ei kasutata DirectAccess'i kasutamise korral.

IPSec-poliitika filtrireeglid võimaldavad muu hulgas ühendada IPSec-kaitse ka suhtluspartneri IP-aadressiga, nii et krüpteerimise võib aktiveerida olenevalt suhtluspartnerist.

Kui autentimiseks kasutatakse Kerberose mehhanismi, ei ole IPSec-iga autentimine kaitstud, sest Kerberos ei toimi IPSec-ühenduse raames.

Selleks, et kontrollida IPSec-ühenduse ülesehituse ja IPSec-suhtluse korrektset toimimist ning alates Windows Server 2008-st Snap-in'i täiendatud turvalisusega Windows-Firewall'i. Programmi või Snap-In'i saab kasutada veaallika piiritlemiseks, kui tekivad probleemid IPSec-ühendustega. Programm on üles ehitatud siiski suhteliselt lihtsalt, nii et seda saab kasutada üksnes esimeseks põhjuse uurimiseks.

IPSec-i tuleks muu hulgas kasutada kombinatsioonis EFS-krüpteeritud failidega (vt ka M 4.147z EFS-i turvaline kasutamine Windows 'i keskkonnas), kui neid hoitakse serveris ning need tuleb kaitstult võrgu kaudu kliendile edastada. Peale IPSec-i võib võrgusuhtluse kaitsmiseks kasutada iga muud mehhanismi, et kaitsta serveris salvestatud EFS-faile transportimisel. Kui IPSec-iga tuleb kaitsta suhtlust süsteemiga, mille operatsioonisüsteem ei ole Windows, tuleb koostalitlusvõimet ja õiget töötamist kontrollida praktilise testi abil. Ehkki IPSec-meetod on standardiseeritud, on üksikjuhtudel ka standardiseeritud meetodite puhul teatud tingimustel võimalikud ühilduvusprobleemid.

Kontrollküsimused:

- Kas on olemas IPSec-poliitika?
- Kas osalevate IT-süsteemide jõudlus on IPSec-suhtluse jaoks piisav?

- Kas aktiveeriti valik Perfect Forward Secrecy (PFS)?
- Kas kontrolliti, kas IPSec-ühenduse ülesehitus teostatakse õigesti?
- Kas on määratletud standardvastuse eeskiri?

M 5.91 Interneti-PC personaalse tulemüüri installeerimine

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: administraator

Personaalsete tulemüüride areng on mõeldud kliendi lokaalsete ressursside turbeks. Tulemüür kaitseb ametkonda või ettevõtte võrku internetist tulevate rünnakute eest. Üksnes personaalsete tulemüüride kasutamisest ei piisa.

Ainult selle tulemüüri kasutamisel ilmnevad järgmised puudused:

- kõik internetiga ühendatud kliendid tuleb tugevdada, mis tähendab, et kõik võimalikud nõrgad kohad tuleks kõrvaldada;
- nagu iga keskselt mittekasutatava tarkvara korral, on üksikute personaalsete tulemüüride protokollide haldus ja analüüs mahukas.

Hetkel saadaolevatel toodetel on veel palju arenguruumi. Tootja pakutavad turbeprofiilid on konfiguratsioonivõimalustest lähtudes praktilised. Lisaks kesksele tulemüürile on otstarbekas kasutada ka personaalset tulemüüri. Nende abiga on klientidel võimalik teostada näiteks kahjurvara kontrolli, mis edastatakse meilide, Java, Activex i või teiste sarnaste mehhanismide kaudu. Selleks võib kasutada näiteks Sandbox i mehhanismi, millega piiratakse internetist allalaaditud rakenduste (Java, ActiveX , jne) ligipääs lokaalsele süsteemile. Personaalse tulemüüriga ei ole kahjurvara kontroll enam kesksel kohal ja sellega vähendatakse tulemüürisüsteemi koormust. Eeliseks on ka see, et nii on võimalik hoiduda tulemüüril krüpteeritud andmete filtreerimisest tulenevast probleemist. Personaalseid tulemüüre on tark kasutada interneti-PCdel ehk arvutitel, mis on sisse seatud ainult interneti kasutamiseks ja millel ei ole ühendust ametkonna või ettevõtte võrguga. Tulenevalt nende toodete laialdasest funktsionaalsusest ja tehnoloogia keerukusest, tuleb kindlustada süsteemi kompetentne haldus.

Personaalse tulemüüri konfigureerimisel ja käitamisel peaks arvestama järgmiste aspektidega:

- Filtreerimine peaks olema seadistatud nii piiravalt kui võimalik. Siin kehtib põhimõte: kõik, mis ei ole otseselt lubatud, on keelatud.
- Vältimaks NETBIOSi funktsioonide väärkasutust, tuleks juhul, kui kasutatavad tulemüürid seda võimaldavad, keelustada ligipääs internetist IPportidele 137 kuni 139 ja 445.
- Pärast esmast personaalse tulemüüri konfigureerimist tuleks seadistatud filtreerimisreegleid testida, et näha, kas lubatud tegevused lubatakse ja mittelubatud tegevused keelustatakse.
- Juhul, kui interneti-PC installatsiooni niigi juba regulaarselt ei kustutata ja Image abiga uuesti ei taastata, tuleks filtreerimisreeglite õiget konfiguratsiooni pisteliselt kontrollida.
- Kui kasutatud toode seda võimaldab, tuleks personaalse tulemüüri reeglid liigitada spetsiaalsete programmidega. Nii on teatud juhtudel võimalik tuvastada ja takistada seda, et ka mõni teine programm lisaks määratud programmidele loob internetis olevate arvutitega ühendusi või võtab neid vastu.

- Kuna paljud personaalse tulemüüri kontrollmehhanismid põhinevad aktuaalsetel teadmistel, tuleb tootja avalikustatud turvapaigad ja uuendused regulaarselt installida. Seejuures tuleb tagada, et selleks vajalikud failid hangitakse usaldusväärsest allikast, näiteks otse tootjalt.
- Personaalne tulemüür tuleb konfigureerida nii, et kasutajaid ei tülitataks hulgaliste neile mõistmatute hoiatusteadetega.
- Kui kasutatav toode seda võimaldab, tuleks infoturbeseisukohast olulised juhtumid protokollida. Spetsialistid peaksid logi andmeid regulaarselt analüüsima. Jälgida tuleb juhiseid meetmes M 2.110 Andmeprivaatsuse suunised logimisprotseduurides .

Mõningad tooted võimaldavad alustada väga piirava aluskonfiguratsiooniga ja pärast seda seadistusi jooksvas käituses peenseadistada. Seejuures küsitakse kasutajalt infoturbe seisukohast oluliste sündmuste korral, millele senini reeglit ei olnud, kas see sündmus on lubatud. Näide sellise infoturbeseisukohalt olulise toimingu kohta on näiteks kindla installitud programmi pöördus internetile. Kasutaja vastustel põhinevalt tuvastab personaalne tulemüür samm-sammult soovitud konfiguratsiooni, näiteks filtreerimisreeglid. Sellise samm-sammulise konfiguratsiooni eeliseks on see, et nii vähendatakse süsteemihalduse keerukust.

Puuduseks on aga see, et kasutajad ei suuda eelteadmisteta hinnata, milline sündmus on lubatud ja milline mitte. Personaalse tulemüüri samm-sammulist konfiguratsiooni saab soovitada ainult juhul, kui kasutajatele antakse kindlad juhised selle kohta, kuidas programmi päringutele vastata, või kui see toimub administraatori juhendamisel, siis kuidas seda telefoni teel teha.

Tänaseks tegeleb personaalsete tulemüüride tootmisega suur hulk tootjaid.
Osaliselt on nende toodete kasutamine eraisikutele tasuta. Ärivaldkonnas tuleb reeglina aga soetada litsents. Personaalseid tulemüüre testitakse tihti erialaajakirjades ning testitulemuste uurimine on abiks kõige sobilikuma toote valimisel.

Kontrollküsimused:

- Kas on olemas personaalse tulemüüri kasutamise kontseptsioon?
- Kas turvaaukude kõrvaldamiseks installitakse tootja poolt avalikustatud turvapaigad ja uuendused?

M 5.92 Internet-PC turvaline Internetiga ühendamine

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: IT-juht, administraator

Spetsiaalsest kasutusalast tulenevalt on interneti-PC korrapäraseks käituseks eriti oluline turvaline internetiühendus. Seega tuleks internetiga ühendamine hoolikalt plaanida ning seejuures arvestada järgnevate aspektidega.

Sobiva internetiteenuse pakkuja (Internet Service Provider - ISP) valik

Internetiühendus toimub ISP kaudu, kes annab kasutajale vastava tehnika ja teenused. Turul tegutsevad pakkujad erinevad üksteisest teenuse mahu, kvaliteedi ja hinna poolest. Sobiva ISP valik sõltub seega internetiühenduse nõuetest:

- Kas ISP pakub soovitud ühendustehnikat (modem, ISDN, DSL jne)?
- Kas ISP täidab nõuded ribalaiusele (minimaalne, keskmine) ja interneti-ühenduse kättesaadavusele? Selle väljaselgitamiseks tuleks lugeda ka eri-alaajakirjade artikleid vastavate testide kohta.
- Kas ISP pakub vajalikke lisateenuseid (näiteks meilide või uudiste jaoks) või peab selleks kasutama veel mõne kolmanda pakkuja teenuseid?
- Kas ISP võimaldab pakutud teenustele vajalikke infoturbemehhanisme? Näiteks kas WWW ja FTP jaoks võimaldatakse proksiserverite kasutamine ja kas meile saab kasutada ka SSL-kaitsega?
- Kas ISP annab informatsiooni selle kohta, kuidas toimitakse isikuandmete või asutuse või ettevõtte kohta käiva informatsiooniga? Kas need andmed ühilduvad teie andmekaitsealaste nõuetega?
- ISP-d pakuvad internetiühendustele erinevaid hinnamudeleid. Näiteks on võimalik eristada kindla tasuga, ajast sõltuvat ja mahust olenevat maksustamist. Kas hinnamudel on interneti-PC kasutusotstarbeks sobilik?
- Vastavalt internetiühenduse kättesaadavuse nõuetele tuleks kontrollida, kas võib olla vajalik kahe või enama teenusepakkujaga lepingute sõlmimine.

Veel soovitusi sobiva interneti-tarnija valimiseks leiate meetmest M 2.176 Sobiva internetiteenuse pakkuja valimine .

Internetiühenduseks sobivate võrgukomponentide hankimine

Sõltuvalt sellest, kas internetiga ühendatakse ainult üks interneti-PC või suur hulk interneti-PCsid, esinevad selleks vajalikele riistvarakomponentidele erinevad nõudmised. Nende komponentide hankimisel peaks jälgima järgmisi aspekte:

- Kui internetiga soovitakse ühendada ainult ühte interneti-PC-d, võetakse enamikel juhtudel kasutusele kas modem või ISDN-kaart. Seadmete ja ISP sissevalimisserveri vahel esineb tänapäeval ühilduvusprobleeme harva. Modemid ja ISDN-kaardid on odavad ja tehniliste rikete korral on neid võimalik

kiiresti välja vahetada. Kõrgete kättesaadavusnõuete korral peaksid olemas olema ka asendusseadmed.

- Kui internetiga tuleb varustada hulk interneti-PCsid või vajatakse suurt ribalaiust, kasutatakse tihti spetsiaalseid marsruutereid (näiteks DSL-marsruuter). Kui ISP seadmeid ise ei paku, on ühilduvusprobleemide vältimiseks vajalik täpne seadistus. Kõrgendatud kättesaadavuse vajaduse korral tuleks uurida, kas ISP pakub selliseid teenuseid nagu marsruuteri väljavahetamine kindla aja jooksul, asendusseadme olemasolu jne.

Internetiühenduse turvaline konfiguratsioon ja käitus

Internetiühenduse turvaliseks ja reeglitepäraseks käituseks tuleb järgida järgmisi soovitusi:

- Selleks, et andmekao korral oleks ühendust võimalik kiiresti taastada ja kõrvalekalded tuvastada, tuleb kõik interneti ühendamisel tehtud konfiguratsioonid dokumenteerida.
- HTTP ja FTP protokollide kaudu tehtavate pöörduste jaoks tuleks kasutada nn proksiservereid. Need proksiserverid edastavad klientide päringud “asetäitjatena” soovitud HTTP- või FTP-serverile. Seeläbi tekib teiste hulgas eelis, et võimalikel pakettfiltritel saab restriktiivseid reegleid konfigureerida. ISP käitab reeglina vastavaid proksiservereid.
- Sageli kasutatavate ISP või internetis paiknevate serveritega (näiteks meiliserver, proksiserver jne) tuleks alati ühendust võtta IP-aadressi kaudu. See IP-aadress tuleb kõikides kaasatavates komponentides kindlalt juurutada ning seetõttu väheneb DNS-spuufingu rünnakute oht.
- Kui internetile ligipääsu kasutatakse dünaamiliste IP-aadressidega, tuleks aeg-ajalt ühendus katkestada. Sellega tagatakse, et järgmisel sissehelistamisel määratakse kliendile uus IP-aadress.. Eriti oluline on see flat rate ühenduse korral. Sellise IP-aadresside vahetamisega tehakse kindlad rünnakud raskemaks.
- Eelseadistatud paroolid, näiteks internetiteenuse pakkuja juures sisselogimisel, tuleb muuta (vt M 2.11 Paroolide kasutamise reeglid).
- Kui kasutatav operatsioonisüsteem seda võimaldab, tuleb internetiühenduse konfiguratsioonifailidele ligipääs lubada ainult vastutavatele administraatoritele.
- Kui kasutatav kommunikatsioonitarkvara või kasutatav modem, ISDN- või DSL-seade võimaldab kaughalduse kasutamist, tuleb see desaktiveerida või hästi kaitsta.
- Kui internetiühendus luuakse sissehelistamise teel, tuleks sissehelistamise number ISP juures sisse kanda.
- Kui kasutaja ennast välja logib või internetirakenduse sulgeb, peab ka modem või ISDN-seade side katkestama.
- Kui internetiteenuse pakkuja juures sisselogimise autentimiseks on võimalik valida PAP ja CHAP meetodi vahel, tuleks eelistada CHAP meetodit. Sellega välditakse autentimisandmete avatekstina edastamist.

- Kõik mittevajalikud funktsioonid (näiteks kommunikatsioonisidemete väljastpoolt aktiveerimine) tuleb välja lülitada. Sissetulevaid päringuid ei tohi vastu võtta.
- Kasutatud sihtaadresse ja seadistatud parameetreid tuleks aeg-ajalt kontrollida (vt M 5.29 Sihtaadresside ja logide perioodiline kontroll).

Täiendavad kontrollküsimused:

- Kas internetiteenuse pakkuja täidab internetiühenduse kättesaadavusele määratud nõudmised?
- Kas kõik internetiühendusega seotud konfiguratsioonid dokumenteeriti?

M 5.93 Veebibrauseri turve Internet-PC kasutamisel

Algatamise eest vastutavad: IT-juht, infoturbespetsialist

Rakendamise eest vastutavad: Administraator

World Wide Web (WWW) on kindlasti üks olulisemaid internetis pakutavaid teenuseid. Lisaks informatsiooni hankimisele kasutatakse internetti tänapäeval ka interaktiivsete teenuste (näiteks e-kaubandus ja e-valitsus) platvormina. Interneti-PCdel vajatakse seetõttu enamikel juhtudel veebiteenuste kasutamiseks brauserit ehk klientprogrammi. Brauserite tehnoloogia on väga kiiresti arenenud. Algsest funktsioonist internetist tekste ja pilte alla laadida ning kuvada on veebibrauserid muutunud veebipõhiste rakenduste eessüsteemideks. Brauserid kuvavad suurt hulka erinevaid meediaformaate ning toimivad programmide ja skriptide (aktiivsisu) käituskeskkonnana. Viimase hulka kuuluvad näiteks sellised tehnoloogiad nagu Java, Javascript ja ActiveX. Moodsate brauserite funktsionaalsust saab lisaks täiendada veel nn pistikprogrammidega (Plug-In). Suur funktsioonide hulk toob endaga kaasa nii keerukad konfiguratsioonivõimalused kui ka võimalikud turbeprobleemid.

Järgmised soovitused interneti-PCl paikneva brauseri konfigureerimiseks peaksid vastama nendele infoturbeaspektidele.

Installimine

Põhisoovitus installida ainult vajalikud tarkvarakomponendid kehtib nii brauserite kui ka arvukate pistikprogrammide kohta. Neid kasutatakse enamasti kindlate meediaformaatide, näiteks videote või raadioprogrammide kuvamiseks ja esitamiseks. Seejuures on põhiline oht selles, et pistikprogrammide konstrueerimis- või teostusvigadest tulenevalt võidakse vastavate veebilehekülgede avamisel käivitada soovimatud toimingud, näiteks lokaalsete andmete manipuleerimine või kompromiteerimine. Seepärast peaks installima ainult need pistikprogrammid, mis on igapäevatöö jaoks ka ilmtingimata vajalikud. Tarkvara nõrkusi ei ole avastatud mitte ainult pistikprogrammides vaid hulgaliselt ka brauserites endis. Neid turvaauke võidakse kasutada turbemehhanismidest möödumiseks või muu kahju tekitamiseks. Veebibrauserite tootjad avaldavad seetõttu tihti turvapaikasid, uuendusi või juhiseid nende turvaaukude kõrvaldamiseks. Süsteemi haldajad peaksid seepärast regulaarselt külastama brauseritootjate veebilehekülgi ja end ajakohaste turvaaukude kohta informeerima ning võimalusel pakutavad uuendused ja turvapaigad installima (vt M 2.35 Teabe hankimine turvaaukude kohta). Veel üheks probleemiks on väliste programmide käivitamine brauseri kaudu. Enamik brausereid võimaldab faile kohe pärast allalaadimist määratud rakendusprogrammiga avada ja käivitada. Kuna allalaaditud failid pärinevad sageli tundmatutest allikatest, on oht, et avamisel või käivitamisel käivitatakse soovimatud teostused. Põhjusteks võivad olla näiteks rakendusprogrammide puhvri ülevool või failidesse peidetud kahjulikud makrod. Riski vähendamiseks tuleks interneti-PCle installida nii vähe rakendusprogramme kui võimalik. Võõraste failiformaatide, näiteks Wordi või Exceli failid, kuvamiseks tuleks võimalusel kasutada vaatajaid (Viewer), mis makrosid ei toeta. Kõik installitud tarkvarakomponendid (näiteks pistikprogrammid, turvapaigad, uuendused ja vaatajad) tuleks hankida ainult usaldusväärsetest allikatest, näiteks otse tootjalt või ametlikelt peegelserveritelt.

Konfiguratsioon

Levinud veebibrauseritel on keerukad konfiguratsioonivõimalused. Paljud suvandid mõjutavad brauseri turvalist käitust ja sellega ka interneti-PC infoturvet. Pärast standardinstallatsiooni ei vasta brauseri seadistused tavaliselt infoturbe nõuetele.

Üksikud konfiguratsiooniseadistused tuleks seega süstemaatiliselt üle kontrollida ja vajadusel kohandada. Selle aluseks on kasutuskontsept ja interneti-PC suunised. Konfiguratsioonil tuleks arvestada järgmisi punkte. Kui internetiteenuse pakkuja (ISP) pakub proksiserveri kasutamise võimalust, tuleks seda ka kasutada. Selleks peab brauserisse kandma proksiserveri IP-aadressi ja pordinumbri. Mõnede brauserite korral tuleb see informatsioon iga toetatud teenuse jaoks eraldi sisestada. Proksiserverid toetavad reeglina vähemalt HTTP, HTTPS ja FTP teenuseid. Vajalikud IP-aadressid ja pordinumbrid tuleks võtta ISP informatsioonist või tuleks sinna esitada päring.

Aktiivsisu all mõistetakse arvutiprogramme, mida sisaldavad veebilehekülje või mis veebilehe avamisel ja vaatamisel automaatselt alla laetakse. Need arvutiprogrammid teostatakse internetikasutaja arvutis kas antud brauseri või operatsioonisüsteemi poolt. Olulised näited aktiivsisu kohta on sellised tehnoloogiad nagu Java, Javascript ja ActiveX. Nagu iga arvutiprogrammi juures, on ka aktiivsisu korral oht, et programmikood ei vii läbi ainult mõttekaid, vaid ka soovimatuid või isegi kahjulikke tegevusi. Näiteks võib aktiivsisu transportida viiruseid või Trooja hobuseid. Kahjuliku aktiivsisu eest kaitsmiseks sisaldavad brauserid mõningaid turbefunktsioone. Minevikus ilmnes tarkvaras mitmeid nõrku kohti, mida on turbefunktsioonide vältimiseks nüüd võimalik kasutada (vt M 5.69 Aktiivsisu tõrje).

Levinumates brauserites on võimalik määrata, kuidas aktiivsisuga käitutakse. Ülanimetatud põhjustest lähtuvalt tuleks aktiivsisu brauseris lubada ainult juhul, kui see on selgesõnaliselt määratletud interneti-PC kasutuskontseptis või suunistes. Sellisel juhul tuleks aktiveerida ainult tehnoloogiad, mida igapäevases töös vajatakse, näiteks Javascript.

Mõned brauserid võimaldavad isikliku informatsiooni või paroolide salvestamist, et neid ei peaks iga kord uuesti sisestama ning et neid oleks võimalik automaatselt veebiformularidesse sisestada või veebiserveri suhtes autentimiseks kasutada. Internet Explorer pakub seda võimalust märksõna Auto Completion all. Seda funktsiooni ei tohiks kasutada, sest vastasel juhul tekib oht, et paroole, isiklikku informatsiooni või informatsiooni ametkonna või ettevõtte kohta võidakse tahtmatult edastada. Mõned brauserid võimaldavad ka FTP-serveri pöördusel automaatselt

kasutajanime ja parooli edastamist. Selleks, et paroole ei edastataks tahtmatult kolmandatele isikutele, tuleks brauser konfigureerida nii, et standardina toimuvad ainult anonüümsed sisselogimised. Mõnede brauserite puhul saab konfigureerida seda, kas allalaaditud failid avatakse automaatselt või salvestatakse ning kas tuleb esitada päring kasutajale. Selleks, et faile ei avataks või käivitataks tahtmatult, tuleks see suvandi korral määrata kas käsuna Save või Ask User. Niinimetatud küpsiste abil saavad veebiserverid interneti-PCIe andmeid paigutada ja hiljem jälle kasutada. Seda funktsiooni kasutatakse tihti internetipoodides virtuaalsete ostukorvide korral. Infoturbe seisukohast ei ole küpsised enamjaolt probleemsed. Küpsiste abiga on võimalik koostada kasutajate käitumisprofiile, nii et andmekaitse seisukohalt oleks soovitatav küpsiste salvestamine desaktiveerida.

Levinumaid brausereid saab konfigureerida nii, et kasutajale esitatakse enne küpsise salvestamist veebiserveri poolt vastav päring. Vastavalt sellele, milliseid veebiteenuseid kasutatakse, võidakse kasutajat tülitada suure arvu erinevate dialoogiakendega ja seeläbi tema tööd segada. Seepärast tuleb interneti-PCI küpsistega toimimise viisi otsustamisel lähtuda konkreetsest kasutusjuhtumist.

SSL/TLS (Secure Sockets Layer/Transport Layer Security) on protokollid, millega kaitstakse krüptograafiliselt veebiserveri ja veebibrauseri vahelist ühendust. Kui server seda pakub, tuleks SSL/TLS turvet alati kasutada. See on eriti oluline isikliku informatsiooni edastamisel, näiteks kui serverilt meile alla laetakse. Sidepartnerite autentimiseks võib kasutada sertifikaate, praktikas väljastatakse SSL-sertifikaate enamasti veebiserveritele. Kui on ka vajalik kliendi autentimine, toimub see enamasti teiste meetoditega, näiteks kasutajanime ja parooli abiga (vt M 5.66z SSL-i/TLS-i kasutamine kliendis). SSL-sertifikaadi ehtsust kontrollib brauseri tarkvara enamasti sertifitseerimiskeskuse digitaalallkirja kaudu. Mõningate tuntumate sertifitseerimiskeskuste sertifikaadid antakse levinumate brauseritega juba kaasa. Mõningad serverite käitajad kasutavad aga teiste sertifitseerimiskeskuste sertifikaate, nii et SSL-sertifikaatide ehtsust ei ole võimalik otseselt kontrollida.

Kui sellele veebiserverile peab tihti ligi pääsema, tuleks vastava sertifitseerimiskeskuse sertifikaat selle kättesaadavusel brauserisse importida. Sertifikaadi ehtsuse kindlakstegemiseks tuleks enne selle importimist edastada ja võrrelda nn Fingerprint i, näiteks faksi, telefoni või meili teel. Ainult siis võivad kasutajad olla kindlad selles, et server kuulub soovitud käitajale. Veebibrauserite rünnaku ja ärakasutamise võimaluste vähendamiseks tuleks aktiveerida ainult need funktsioonid, mis on ametialaste kohustuste täitmiseks hädavajalikud.

Kasutamine

Andmed ja programmid tuleks alla laadida võimalikult usaldusväärsetest allikatest. Need võivad olla näiteks tootja või väljaandja veebilehekülg ning ametlikud peegelserverid (“ Mirrors ”). Juhul kui vastavat failiformaati on võimalik

nakatada, tuleks internetist allalaaditud failid ja programmid kontrollida viirusetõrjeprogrammi abil. Allalaaditud faile ja programme ei tohiks seega otse brauserist avada ega käivitada, vaid need tuleks eelnevalt ainult salvestada. Nagu juba üleval kirjeldatud, saab küpsiseid kasutada ka kasutajate harjumuste profiilide loomiseks. Seega, kui põhimõtteliselt on küpsiste salvestamine lubatud, tuleks need regulaarselt kustutada. Seda saab teha kas otse brauserist või vastava küpsiste salvestusfaili kustutamisega. Internetist leiab hulgaliselt jaosvara tööriistu, millega on võimalik salvestatud küpsiseid hallata. Selleks, et juba korra internetist allalaaditud lehekülgi ei peaks nende vajaminemisel uuesti alla laadima, kasutab brauser veebilehekülgede lokaalseks vahesalvestamiseks vahemälu. See vähendab interneti kasutusaega. Internetis sisseoste tehes edastatakse tihtipeale konfidentsiaalset informatsiooni, näiteks krediitkaardinumbreid. Teatud juhtudel salvestatakse see informatsioon brauseri vahemällu.

Seeläbi tekib oht, et seda informatsiooni saab vahemälust volitamata lugeda ja kuritarvitada. Kui ligipääs interneti-PCle ei ole tõhusalt turvatud, tuleks brauseri vahemälu pärast igat konfidentsiaalsete andmete edastamist kustutada. Alternatiivse võimalusena saab vahemälu funktsiooni konfiguratsiooni käigus ka täielikult desaktiveerida.

Kontrollküsimused:

- Kas kõik tarkvaraosad hangitakse usaldusväärsetest allikatest?
- Kas aktiivsisu teostamine on konfigureeritud vastavalt interneti-PC etteantud suunistele?
- Kas allalaaditud faile kontrollitakse enne nende avamist või käivitamist viirusetõrjeprogrammiga?

M 5.94 Meilikliendi turve Internet-PC kasutamisel

Algatamise eest vastutavad: IT-juht, infoturbespetsialist
Rakendamise eest vastutavad: administraator

Meil on intranetis ja internetis tähtsaim teenus. Kaasaegses büroosuhtluses kasutatakse meili tavaliste selliste sidevahendite nagu telefon, telefaks, kirjad ja teleprinter, abil tehtava suhtluse täiendamiseks või isegi asendamiseks. Samuti annab meilidele lisaväärtust võimalus saata meilile lisatud manusega kaasa erinevas formaadis faile. Seepärast kasutatakse meili tihtipeale ka rühmavara lahendusena näiteks siis, kui mitu sidepartnerit üksteise järel ühe dokumendi kallal töötavad. Tehnilisel tasandil on meilide kasutamiseks erinevaid võimalusi. Üheks võimaluseks on veebimeili kasutamine, mille pakkujaid leiab internetist mitmeid, näiteks Web.de või gmx. Need võimaldavad kasutajatel veebiliidese kaudu kasutada kõiki vajalikke funktsioone meilide vastuvõtmiseks, lugemiseks, koostamiseks, saatmiseks ja haldamiseks. Nagu iga teise veebilehekülje korral, toimub ka nende puhul kasutamine brauseri kaudu.

Veebimeili eelised:

- lisaks brauserile ei pea kliendile installima ühtegi teist tarkvarakomponenti,
- kasutaja ei ole meiliteenuse kasutamiseks kohustatud kasutama ainult ühte kindlat arvutit või kohta.

Puuduseks on aga see, et meiliteenuse kasutamise turve sõltub ainult veebimeiliteenuse pakkujast. Soovitusi veebimeili turvaliseks kasutamiseks leiate meetmest M 5.96 Veebmeili turvaline kasutamine . Meiliteenuse kasutamisel on kõige tavalisem variant vastava programmi kasutamine: näiteks Microsoft Outlook, Outlook Express, Netscape Messenger või KMail. Enamasti kasutatakse meilide allalaadimiseks kas POP3-e (Post Office Protocol Version 3) või IMAPi (Internet Message Access Protocol) protokolli. Väljuvad meilid saadetakse SMTP protokolli (Simple Mail Transfer Protocol) abiga. Selleks tuleb meiliprogrammi konfigureerimisel määrata väljaminevate ja sissetulevate meilide serverite aadressid. Soovitatav on nende serverite IP-aadressid teenusepakkujalt järgi uurida ja need kindlalt meiliprogrammis seadistada. Enne meilide teenusepakkujalt kliendile edastamist peab klient ennast üldjuhul meiliserveriga seoses autentima.

Autentimine toimub enamasti parooli abil, mis edastatakse vastavale serverile avatekstina välja arvatud juhul, kui pole kasutusele võetud täiendavaid turvameetmeid. Sellest tulenevalt esineb oht, et interneti kaudu parooli edastamisel on seda võimalik lugeda ja hiljem kuritarvitada. Selle vältimiseks tuleb kogu meiliserveriga teostatav side TLS/SSL-i abil krüpteerida. See kaitseb teid meilide edastamisel ilmneda võivate kompromiteerimise ja manipuleerimise eest. Praeguseks pakuvad paljud teenusepakkujad võimalust POP3 või IMAP pöördust TLS/SSL-i abiga turvata (vt ka RFC 2595).

Selleks, et volitamata isikud meilile ligi ei pääseks, peaks teenusepakkuja meiliserveri ligipääsuparool olema piisava pikkusega ja raskesti äraarvatav. Lisaks sellele tuleks parooli ka regulaarselt vahetada. Küsimusele, kas meiliparooli võib interneti-PCle salvestada või tuleb see iga kord uuesti sisestada, ei ole ühtset vastust. See sõltub sellest, mitu autentimisprotsessi peab kasutaja läbima (kliendil sisselogimine, sisselogimine ISP-l, jne) ja millisel määral on piiratud pahatahtliku ärakasutamise oht. Rohkem soovitusi paroolide kasutamise kohta leiate meetmest M 2.11 Paroolide kasutamise reeglid .

Mõned meilikliendid võimaldavad meile luua HTML- või rikasteksti (RTF) formaadis. HTML-formaadi korral on probleemiks, et see võib sisaldada aktiivsisu, näiteks Javascript i ja viiteid teistele internetis paiknevatele objektidele. See on juba mitmeid kordi toonud kaasa turbeprobleeme. Sellest tulenevalt ei tohiks saata HTML-formaadis meile. Kui ilmtingimata on vaja kasutada vormindatud elemente, näiteks tekstitüüp ja värv, tuleb selle asemel kasutada RTF-formaati. Klientprogrammid tuleks seega konfigureerida nii, et nad koostavad ja saadavad meile puhtas tekstiformaadis või RTF-formaadis. Sissetulevate HTML-formaadis meilide jaoks tuleks klient konfigureerida nii, et ta selliste meilide kuvamisel aktiivsisu ei täidaks. Mõned meilikliendid ei kuva HTML-formaadis meile ise, vaid käivitavad selleks eraldi vaataja (Viewer) või brauseri. Sellistel juhtudel tuleks kasutada vaatajat või brauserit, mis aktiivsisu ei täida. Lisaks sellele tuleks kindlustada, et meili lugemisel ei loodaks pöördust teistele internetis paiknevatele objektidele, näiteks eelnevalt internetiühendust katkestades. Alternatiivse võimalusena saab HTML-formaadis meile avada puhtakujulise tekstiredaktoriga (text editor). Tulenevalt meilis sisalduvatest märgenditest (tag) on tekst seejuures tihti raskesti loetav.

Mõningad klientprogrammid toetavad meilide eelvaate võimalust. Meili sisu kuvatakse nii, et kasutaja ei pea seda eraldi avama. Sellest tulenevalt tekib oht, et meilides paiknev kahjulik sisu võidakse teostada tahtmatult. Eelvaate funktsioon tuleks desaktiveerida.

Manused ehk failid, mis on lisatud meilis sisalduvale tekstile, on laialtlevinud transpordivahend arvutiviiruste, usside ja muude kahjurvarade edastamiseks. Meiliprogrammis näidatud faililaiend (.jpg,.exe jne) ei ühildu sageli tegeliku failitüübiga. On olemas tehnikaid, millega teatud programmides tegelikku faililaiendit varjata. Seega tuleks sissetulevate meilide manustesse alati kahtlustavalt suhtuda, seda eriti juhtudel, kui manus ei olnud kokkulepitud või meil tuleb tundmatult saatjalt. Enne manuste avamist või käivitamist tuleks nad salvestada ja viirusetõrjeprogrammiga kontrollida. Täitefaile ja faile, mis võivad muuta süsteemikonfiguratsiooni (nt.exe,.vbs,.reg Windowsi all või Shell Script Linuxi all), ei tohiks ilma süsteemihalduse loata käivitada. Ettevaatlik tuleb olla ka selliste manuste suhtes, millel ei ole mingit seost saatja ja temaga olevate ärisuhetega,

näiteks erootikateenuse pakkumised maksunõustajalt või meil tavalisest täiesti erinevas keeles. Sellistel juhtudel ei tohiks meilis sisalduvaid manuseid avada, vaid sellest peaks teatama kas süsteemihaldusele või infoturbespetsialistile.

Olukorra selgitamiseks võib ka saatjalt järele pärida, et välja selgitada, kuidas on antud manused tööga seotud. Windowsi all tuleks võimalusel standardrakendustena konfigureerida ainult sellised programmid, mis ei suuda makrosid või skripte teostada. Enamikele levinumatele dokumendi- ja failitüüpidele (nt wordi või exceli failid) on saadaval vastavad vaatajad (Viewer). Võimalusel tuleks täisväärtuslike rakendusprogrammide, näiteks Microsoft Office, installeerimisest loobuda. Vaikeseadistuse merge asemel tuleks.reg failitüübi standardrakenduseks konfigureerida redaktor (editor). Vastasel juhul kantakse failis paiknevad Registry sissekanded topeltklõpsu või faili teistsuguse avamise korral interneti-PC Registry sse. Konfiguratsioonimuudatusest tulenevalt võidakse teiste hulgas desaktiveerida ka turbeseadistusi. Failitüüpide standardrakendusi saab Explorer is muuta dialoogivälja View | Options | File types kaudu. Meili teel edastatakse paljudel juhtudel informatsiooni, mille konfidentsiaalsust ja terviklust tuleb saatjalt saajale edastades kaitsta. Selleks võib kasutada krüpteerimist ja digitaalallkirju. Siinjuures on problemaatiline, et erinevad meilide krüptograafilise turbe meetodid (nt S/MIME, GnuPG (PGP) ja MailTrusT) ei ole üldse või on ainult osaliselt omavahel ühilduvad. Seega tuleb enne meilide krüpteerimist või digitaalallkirja kasutamist sidepartneriga kokku leppida, millist meetodit või milliseid meetodeid kasutatakse (vt M 5.63z GnuPG või PGP kasutamine). Selleks vajalikke tarkvarakomponente pakutakse levinumatele meiliprogrammidele pistikprogrammidena. Kui meilide krüpteerimiseks kasutatakse mitut erinevat pistikprogrammi, tuleb jälgida, et ei tekiks tehnilisi probleeme siis, kui need ühte meiliprogrammi installitakse.

Sissetulevate meilide kättesaamisel või lugemisel võimaldavad levinumad meiliprogrammid kättesaamis- ja lugemiskinnituse päringu võimalust. Kättesaamiskinnituseks peab saaja server toetama DSN-standardit (Delivery Service Notification), lugemiskinnituseks peab meiliklient toetama MDN-standardit (Message Disposition Notification). Meilikliendist sõltuvalt on seda võimalik seadistada nii, et see vastab kinnitusnõudele alati, mitte kunagi või ainult kindlate saatja(te) korral. Infoturbeseisukohast ei ole sellised kinnitusteated üldjuhul probleemsed. Seoses reklaammeilidega, mida saadetakse suurele hulgale meiliaadressidele, võib see funktsioon olla aga soovimatu. Saatja näeb, et vastav meiliaadress on olemas ja võib-olla ka seda, et tema reklaammeili loeti.

Sissetulevaid või väljaminevaid meile saab mõnedel meiliklientidel soovi korral automaatselt eelnevalt kindlaksmääratud meilisaajale või levimisnimistusse saata, näiteks pimekoopiana (Blind Carbon Copy - BCC). Netscape Messenger 4.7 korral leiate selle funktsiooni Preferences | Mail & Newsgroups | Copies & Folders | BCC to other alt. Seda funktsiooni tuleks kasutada ainult juhul, kui on kindlustatud, et kõik isikud, kes sellele meiliaadressile ligi pääsevad, tohivad sissetulevaid ja väljaminevaid meile lugeda. Vastasel juhul on oht, et konfidentsiaalseid and-

meid edastatakse tahtmatult kolmandatele isikutele. Mõnede Windowsi operatsioonisüsteemide versioonide korral antakse kaasa programm Outlook Express. Kui seda programmi ei vajata, näiteks kasutate mõnda muud klientprogramm või veebimeiliteenust, tuleks Outlook Express deinstallida. Kõikide interneti-PCl paiknevate tarkvarakomponentide korral tuleb kindlustada, et kõik kättesaadavad infoturbeseisukohast olulised turvapaigad ja uuendused installitakse samaaegselt.

Kontrollküsimused:

- Kas meiliserveri pöörduse parooli vahetatakse regulaarselt?
- Kas meile koostatakse ja saadetakse ainult puhtas tekstiformaadis ja RTF-formaadis?
- Kas sissetulevates meilides olevad manused kontrollitakse enne nende avamist ja käivitamist viirusetõrjeprogrammiga?

M 5.95 E-kaubanduse turve Internet-PC kasutamisel

Algatamise eest vastutavad: IT-juht, infoturbespetsialist

Rakendamise eest vastutavad: administraator

Internetti ei kasutata tänapäeval enam mitte ainult informatsiooni hankimiseks ja suhtlemiseks, vaid üha enam ka äritegevuse ja haldustegevuse teostamiseks. (näiteks online- tellimused, panga- või väärtpaberitehingud ja e-riigi teenused). E-kaubanduse ja e-valitsuse teenustel on enamasti kõrgem turbeaste kui tavalisel interneti kaudu informatsiooni hankimisel. Eelkõige tuleb kindlustada see, et online -tehingud ja -tellimused oleksid interneti-PCl töötlemisel ja internetis edastamisel manipuleerimise eest kaitstud.

Kui interneti-PCd kasutatakse ka ekaubanduse ja e-valitsuse teenuste kasutamiseks, tuleks järgida järgmisi soovitusi.

Enne, kui võtate interneti teel ühendust mõne teenusepakkujaga, tuleks kontrollida, kas tema andmekaitse- ja infoturbepõhimõtted vastavad teie nõudmistele. Sellekohast infot peaks leidma teenusepakkuja veebiserverist. Arvutiviiruste, Trooja hobuste ja muu kahjurvara eest kaitsmiseks tuleb installida

viirusetõrjeprogramm, mille andmebaasi pidevalt uuendatakse. Rohkem sellekohaseid soovitusi leiate moodulist B 1.6 Viirusetõrje kontseptsioon ja M 4.3 Viirusetõrjeprogrammide kasutamine .

E-kaubanduse ja e-valitsuse kasutamiseks vajalikud andmed ja konfiguratsioon tuleb regulaarselt varundada (vt M 6.79 Andmete varundamine Internet-PCde kasutamisel). Vastasel juhul on oht, et rakendust ei ole Interneti-PC rivist väljalangemisel või tahtmatul kustutamisel võimalik koheselt taastada või pole võimalik teha järeldusi teostatud toimingute kohta. Kui kasutamiseks on vaja spetsiaalseid tarkvaraosi, näiteks Online Banking programme, tuleks need hankida ainult usaldusväärsetest allikatest, võimalusel otse pakkujalt või tootjalt. Nendele tarkvaraosadele tuleb regulaarselt teostada otsinguid selgitamaks, kas on saadaval turbe seisukohast olulisi turvapaikasid või uuendusi, mis tuleb kindlasti installida. Enne installimist tuleb tarkvara ja uuendused viiruste suhtes kontrollida. Kui interneti-PCd kasutatakse pidevalt e-kaubanduse ja e-valitsuse teenusteks, tuleks sellele arvutile määrata kindel kasutaja ja seda arvutit ainult selleks otstarbeks kasutada. Vastasel juhul on oht, et hiljem ei ole võimalik välja selgitada, milline kasutaja mida tegi. Paljude e-kaubanduse ja e-valitsuse rakenduste korral kasutatakse klientprogrammina veebibrauserit.

Reeglina kasutatakse andmeside turbemehhanismina TLS/SSL-protokolli. Seejuures kaitstakse andmete konfidentsiaalsust ja terviklust krüptograafiliste

vahenditega.

TLS/SSL-ühendus tuntakse brauseris ära selle abil, et aadress (URL) ei alga mitte http: -ga, vaid https: -iga ja rohkem levinud brauseritel kasutatakse vastava ühenduse märkimiseks ka erilist sümbolit, näiteks suletud tabalukku. Veebipõhiseid e-valitsuse ja e-kaubanduse teenuseid tuleks kasutada ainult TLS/SSL-i kaudu. Teenusepakkuja peaks kogu veebirakenduse TLS/SSL-i kaudu kättesaadavaks tegema. Tuleb jälgida, et kasutataks brauserit, mis toetab tugevaid krüptograafilisi meetmeid, eriti 128-bitilist võtmepikkust. Mõningate vanemate brauserite korral ei ole see ekspordipiirangutest tulenevalt võimalik.

TLS/SSL-i protokollide korral kasutatakse veebiserverite autentimiseks sertifikaate. E-kaubanduse ja e-valitsuse teenuste TLS/SSL-i kaudu kasutamisel peaksid kasutajad serveri sertifikaadi kehtivust pisteliselt kontrollima, et veenduda, kas see on tõesti soovitud serveriga ühendatud. Kasutajad tuleb veebibrauseri kasutamiseks koolitada ning neile tuleb anda juhiseid, kuidas nad kindla installatsiooni ja konfiguratsiooni korral kontrolli teostada saavad.

Kontrollküsimused:

- Kas kasutatakse viirusetõrjeprogrammi ning kas selle andmebaasi uuendatakse regulaarselt?
- Kas e-kaubanduse ja e-valitsuse teenuste andmed salvestatakse regulaarselt?
- Kas kasutatakse tugevat krüpteerimist toetavat brauserit?

M 5.96 Veebmeili turvaline kasutamine

Algatamise eest vastutavad: administraator, kasutaja

Rakendamise eest vastutavad: kasutaja, administraator

Kõik ettevõtted ei käita enda meiliserverit, vaid osad kasutavad selleks välise teenusepakkuja teenuseid. Seejuures on veebimeil lihtne ja kasutajasõbralik variant, et teenusepakkujate veebiserverite kaudu meiliteenuseid kasutada. Veebimeiliks nimetatakse kõiki internetil põhinevaid meiliteenuseid, mille korral on kasutamiseks vajalikud ainult brauser ja internetiühendus. Siia kuuluvad näiteks hot.ee ja mail.ee teenused. Veebipõhised meiliteenused lubavad meilidele ligipääsu asukohast ja internetiteenuse pakkujast sõltumata. Veebimeili teenusepakkuja juures registreerimisel tuleb tavaliselt esitada kasutaja nimi ja aadress, soovitud meiliaadress ja parool. Mõned teenusepakkujad nõuavad registreerimise kirjalikku kinnitust. Valitud parooli kasutatakse edasistel sisselogimistel autentimiseks. Kasutaja saab endale kas ühe või mitu meiliaadressi ning kasutajakonto meilide vastuvõtmiseks, töötlemiseks ja saatmiseks. Veebimeiliteenuse pakkujate hulk on suur ja paljud neist pakuvad isegi tasuta teenuseid. Tähelepanu tuleb pöörata sellele, et need ei erine mitte ainult funktsionaalsuse (näiteks postkasti suurus, faks, sms, rämpspostifilter, jne), vaid ka turbeastme poolest ning lisaks võib osade puhul esineda suuri turvaauke. Seetõttu tuleks teenusepakkuja valikul olla väga ettevaatlik ning eriti tähtsad on järgnevad aspektid:

- Üldised äritingimused peaksid olema ülesleitavad ja kättesaadavad, peale selle peaksid need olema arusaadavad ega tohiks sisaldada vastuvõtmatuid tingimusi. Infoturve peab olema tagatud. Klient ei peaks olema sunnitud nõustuma oma isikuandmete edastamisega, mille tõttu võidakse talle saata reklaammeile. Lisaks selle tuleks õigeaegselt teatada teenuste või hinnapoliitika muutumisest, et klientidel oleks piisavalt aega reageerimiseks (näiteks sissetulevate meilide ümberjuhtimine, postkastide varundamine).
- Kättesaadavus - Palju reisivatele inimestele on oluline postkastide ülemaailmne kättesaadavus. Peale selle tuleks testida, kui kaua võtab aega meilide saatmine ja vastuvõtmine.
- Lisaks pakkumise kasutajasõbralikkusele tuleks uurida, kas on olemas näiteks online -abi, korduma kippuvad küsimused või muud dokumentatsiooni. Samuti tuleks välja selgitada klienditoe kättesaadavus ja kompetents (meili, telefoni või faksi teel).
- Turvalisuse hindamisel tuleks jälgida tehnilisi ja organisatsioonilisi turvameetmeid:
- Kasutajakontole peaks olema võimalik ligi pääseda krüpteeritud ühenduse kaudu, näiteks SSL-i kaudu;
- Meile peaks olema võimalik krüpteerida või digiallkirjastada;
- Klientide autentimine - Näiteks tuleks uurida, kas toimub uute klientide isikukontroll, kas on võimalik ennast vale nime ja aadressiga sisse logida või kas on võimalik valida eksitavaid meiliaadresse, nagu support@... jne . Klientide identiteet tuleks posti teel kindlaks teha;
- Igaüks võib kunagi mõne parooli unustada. Kui klienditukke helistades väljastatakse ilma suurema uurimiseta uus parool, pole see mitte kasutajasõbralikkus, vaid märk kontrolli puudumisest. Sisse tuleks viia mõistlikud turvakontrollid;

- Veebimeili teenustele ligipääsemiseks ei tohiks nõuda aktiivsisu aktsepteerimist (Java, JavaScript, ActiveX);
- Sissetulevate ja väljaminevate meilide viiruskontroll peaks olema iseenesestmõistetav;
- Võimalik peaks olema spämmi filtreerimine.

Mõningaid punkte peab jälgima ka veebimeili teenuste kasutamisel:

- Veebimeiliteenustele ligipääsemiseks mõeldud parool peaks olema sobivalt valitud ehk siis piisavalt pikk (vähemalt kaheksakohaline) ja piisavalt keeruline (numbrid, tähed ja erimärgid). Parooli tuleks regulaarselt vahetada. Mitte mingil juhul ei tohi see olla arvutisse salvestatud või arvuti lähedusse asetatud . Lisateavet paroolivaliku kohta leiate meetmest M 2.11 Paroolide kasutamise reeglid .
- Kasutajakontole ligipääsuks tuleks kasutada SSL-i.
- Meil peaks olema krüpteeritud või digiallkirjastatud. Selleks on tavaliselt vajalik vastuvõtjaga läbi rääkida, millised on krüptograafilised meetodid ja programmid, mida mõlemad pooled kasutavad.
- Isegi kui teenusepakkuja viirusekaitset lubab, tuleks manused enda arvutil viiruste suhtes kontrollida.
- Sissetulevaid meile peaks regulaarselt lugema. Tähtsad meilid tuleks lokaalselt salvestada. Lisaks tuleks postkaste regulaarselt korrastada: juba lokaalselt salvestatud või ebaolulised meilid tuleks kustutada. Peale selle tuleks postkastide sisu regulaarselt lokaalsetele andmekandjatele salvestada ning ka lokaalselt salvestatud meilid tuleb vastavalt turvata.
- Selleks, et lokaalse PC teised kasutajad ei pääseks veebimeilile ligi, tuleks veebimeilist väljuda alati “logi välja” nupu või mõne sarnase mehhanismi kaudu.

HTML-formaadis meilid võivad põhjustada turberiski (vt G 5.103 Veebimeili väärkasutus). Vältida tuleks HTML-formaadis või aktiivsisuga meilide saatmist. Teenusepakkuja peaks aktiveerima võimaluse, et sissetulevates meilides paiknevad võimalikud aktiivsisud alati filtreeritaks. Selleks, et kasutaja ei avaks teadmatult HTML-formaadis meile, tuleks kasutada meiliklienti, kes antud meilid vastavalt märgistab.

Täiendav kontrollküsimus:

- Kas veebimeiliteenuste kasutamine on reguleeritud?

M 5.98 Kulukate sissehelistusnumbrite kasutamise tõkestamine

Algatamise eest vastutavad: infoturbeosakond

Rakendamise eest vastutavad: IT-juht, administraator

Tasulised internetiteenused arveldatakse telefoniarve kaudu sellega, et kasutajad suunatakse spetsiaalsete sissehelistamisprogrammidega tasulistele telefoninumbritele. Nendeks võivad olla näiteks 0900 numbrid. Selleks kasutatavad Webdialer id on programmid, mis loovad arvutile uue internetiühenduse.

Pärast allalaadimist ja installimist ühendab Dialer end internetiga. Tavaliselt katkestatakse selleks ajaks olemasolev internetiühendus. (See toimib ainult tavalise telefoniühenduse korral, mitte aga DSL-i või teiste sarnaste süsteemide kasutamisel.) Pärast seda on selle ühenduse kaudu võimalik esitada päring tasulisele sisule. Tekkivate kulude suurusel on määravaks, millise numbri Webdialer valis. Suured kulud võivad tekkida nii sissehelistuskorrast kui ka ajaühikust olenevalt.

Algselt oli see mõeldud lihtsa ja anonüümse maksevõimalusena internetis, kuid viimasel ajal kuritarvitatakse seda üha enam selleks, et interneti-PCde kasutajate teadmiseta sinna selliseid Webdialer eid installida. Neid Webdialer eid saab märkamatult installida Trooja hobuste kaudu või mõne veebilehe külastamisel. Ilma kasutajate teadmiseta ja ilma vastava vastutasuta tekitatakse suuri kulutusi.

Et end selliste probleemide eest kaitsta:

- tuleks kasutajaid teavitada, mis Webdialer id on ja kuidas selline kahjurvara levib;
- peaks telekommunikatsioonieettevõttelt nõudma iga interneti-PC kohta eraldi ühenduste tõendeid;
- tuleks kaaluda kallite telefoninumbrite, nagu 0900 numbrite üldist keelustamist, või kindlate numbriblokkide keelustamist;
- tuleks aktiivsisu, võimalusel eelkõige ActiveX, desaktiveerida.

Üldiselt ei tohiks installida programme, mis lubavad väidetavalt tasuta või kiiremat ühendust kahtlase sisuga veebilehekülgedele.

M 5.100 Exchange'i süsteemi siseneva ja väljuva side kaitse

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: administraator

Rühmatarkvaraserver suhtleb rühmatarkvaraklientide, veebilehitsejate, telefonirakenduste ja muude rakendustega ning teiste rühmatarkvarasüsteemidega. Andmevahetus leiab aset ka rühmatarkvara erinevate süsteemikomponentide vahel. Sideks kasutatakse kohtvõrku ja/või välisvõrke. Kõikidel juhtudel edastatakse andmeid, mida on tarvis kaitsta. Need ei hõlma üksnes kasutajate identifitseerimiseks kasutatavaid andmeid (nt kasutajatunnust ja parooli), vaid tööalaseid ja erakasutuse korral ka isiklikke andmeid. Seetõttu tuleb otsustada, milliseid kaitsemehhanisme peaks andmeside turvamiseks rakendama. Rühmatarkvarasüsteemidesse sisenevad ja nendest väljuvad kaitset vajavad andmed peaksid võimaluse korral olema alati krüpteeritud. Andmete kaitsmiseks saab kasutada erinevaid krüpteerimismeetodeid. Seetõttu tuleks esmalt välja selgitada, milline meetod on oma kulude ja kasuteguri poolest kõige parem. Otsus tuleb arusaadavalt dokumenteerida.

IPSeci kasutamine

IPSec võimaldab andmeside üldist turvet IP-tasandil: kõik andmepaketid krüpteeritakse ning tagatakse nende terviklus. IPseci kasutamisel Microsoft Exchange'i süsteemides on omad eelised. Kuna IPSeci turve põhineb operatsioonisüsteemil, pole Microsoft Exchange'i süsteemi tarvis muul viisil konfigureerida.

Meilivahetuse turbe tagamiseks saab valida erinevate lahendusvariantide vahel:

- Füüsilisel tasandil on mõeldav linkkrüpteerimine, kuid üldjuhul on seda väga raske ellu viia.
- Võrgutasandil saab kasutada virtuaalset privaatvõrku (VPN).

Internetiprotokolli IP suure leviku tõttu kasutatakse siin enamasti kas IPSeci või muid VPN-lahendusi. IPSec võimaldab turvata IP-ühendusi erinevate asukohtade vahel, erinevate lõppseadmete vahel ning ka lõppseadmete ja asukohtade vahel.

Võtmehalduseks saab kasutada kindlalt eelkonfigureeritud võtmeid (preshared keys) ja ka avaliku võtme infrastruktuure (PKI). Exchange'i andmeside turvamiseks IPSeciga peavad kõik meilide marsruutimises osalevad arvutid suhtlema omavahel läbi IPSeci. Ainult Windowsil põhinevates võrkudes on IPSec standardina juba saadaval, st lisalitsentse ei ole tarvis.

Sellest hoolimata tuleb siiski arvestada täiendavate konfigureerimistöödega (vt M 5.90 IPSec'i protokolli kasutamine Windowsi keskkonnas).

TLS-i/SSL-i kasutamine

SSL-i võib soovitada üldjuhul kõikide HTTP-põhiste pöörduste jaoks. See kehtib ka Microsoft Exchange'i süsteemi komponentide ja teiste, SSL-i turvet võimaldavate komponentide vahelise siseside kohta. Microsoft Exchange Serveri ja klien-

tide vaheliste edastuskanalite krüpteerimine on kõikide kasutusjuhtude korral kas soovitatav või isegi kohustuslik. Eriti puudutab see tundliku teabe edastamist läbi ebaturvaliste andmesidekanalite, nt läbi interneti. Microsoft Exchange'i keskkonnas tuleks selleks kindlasti kasutada kas SSL- või TLS-protokolli (vt M 5.66z SSL-i/TLS-i kasutamine kliendis). SSL-i/TLS-i valikulise või kohustusliku kasutamise üle otsustades tuleks lähtuda pöördusi tegevate klientide asukohast ja edastatavate andmete turbevajadusest. Edastuskanali krüpteerimist rakendades saab kasutada ka nõrgema toimega autentimismehhanisme, nt paroolil põhinevat autentimist, kus parool on loetav.

Klient-server-andmeside turve

Kui Microsoft Outlooki klient on konfigureeritud töötama Exchange'i kliendina, saab side ka turvata. Seevastu kui Microsoft Outlook kasutab Exchange'i serveri poole pöördumiseks ainult internetiprotokolle (POP3, IMAP4, SMTP, NNTP), tuleks ühenduste turvamiseks kasutada TLS-i. Sama põhimõte kehtib ka teiste meiliserveritega seotud pöörduste kohta. SSL-i/TLS-i rakendamise vajadus võib tuleneda ka sellest, kui Exchange'i serverile on tagatud juurdepääs Outlook Web Accessiga (OWA). Sel juhul tuleb edastuskanalite krüpteerimisfunktsiooni rakendada veebilehitseja ja (siin vajaliku) IIS-serveri vahel. HTTP-protokolli kaudu saab kasutada erinevaid Microsoft Exchange'i süsteemi teenuseid. Klientpöörduste juurdepääs postkasti sisule lahendatakse enamasti HTTP-ga. HTTP-teenuste konfiguratsioon peab olema alati turvaline, st pöördused, mis kannavad endas konfidentsiaalset infot, peavad olema kaitstud SSL-i/TLS-iga ning sisse tohib lülitada ainult need teenused, mida läheb reaalselt tarvis. Kõige suuremate ohtudega on seotud järgmised HTTP abil kättesaadavad RPC-liidesed.

RPC-liides

RPC-liidest tuleb üldjuhul alati turvata SSL-iga (vt M 2.481 Exchange'i kasutuse planeerimine Outlook Anywhere'i jaoks).

WebDAV-liides

WebDAV-protokoll (Web-based Distributed Authoring and Versioning) võimaldab failisüsteemiga sarnanevat juurdepääsu andmetele, kasutades selleks HTTPprotokolli.

Kuna Exchange'i puhul võib WebDAV-pöörduse sihtpunkt olenevalt olukorrast olla ka kliendi lokaalne failisüsteem, tuleb seda failisüsteemi kaitsta volitamata juurdepääsude eest. Siinkohal tuleb keskenduda eelkõige WebDAV-ga pakutavate andmete turbele. Kui ründajal õnnestub WebDAV-ga luua juurdepääs lokaalsele failisüsteemile, saab ta seeläbi ette valmistada uusi ründeid. Seetõttu peaks juurdepääsu WebDAV-le võimaldama ainult autentimist ja SSL-i rakendades.

Lisaks tuleb alati silmas pidada, et volituste väljastamise kord oleks range.

Server-server-andmeside turve

Server-server-andmesidet tuleb Exchange'i puhul krüpteerida juhul, kui konfidentsiaalsete andmete edastamiseks kasutatakse ebaturvalisi võrke või kui serveris aset leidev autentimine põhineb loetavatel paroolidel. Krüpteerimismehhanismide valik sõltub kasutatavatest Exchange'i konnektoritest. Seega tuleb kon-

nektorite valimisel arvestada ka sellega, milliseid krüpteerimismehhanisme need võimaldavad.

Teadetepõhise andmeside turve

Praktikas kasutatakse meilide turvamiseks sageli programme, mille aluseks on S/MIME ja OpenPGP. S/MIME võtmehaldus eeldab avaliku võtme infrastruktuuri (PKI) kasutamist. Seevastu PGP kasutab avatud võtmehaldust ja tsentraalset PKId ei vaja. Kolmandate tootjate turbetooted põhinevad enamasti kas ühele või ka mitmele meilikliendile mõeldud plug-in -lahendustel (vt M 5.110z Meili kaitse SPHINXi (S/MIME) abil). Turbelahendusi pakutakse ka failisüsteemi jaoks, nt saab Shelli laiendustega faile ükshaaval krüpteerida ja signeerida. Sel moel turvatud faile võib saata meilides manustena.

Avaliku võtme infrastruktuur

Microsoft Outlookil on meilide krüpteerimiseks sisse ehitatud S/MIME-l põhinev krüpteerimismehhanism. See mehhanism rakendab avaliku võtme infrastruktuuri usaldussuhteid kas omaenda Windows Enterprise CA-ga (Certification Authority) või mõne võõra CA-ga. CA genereeritud juursertifikaadid peavad olema süsteemi jaoks kättesaadavad. Selleks tuleb kõikide Outlooki klientide jaoks usaldusväärseks liigitatavad juursertifikaadid konfigureerida tsentraalselt Windowsi grupipoliitikaga.

Täiendavad turbemeetmed

PKI turvalise käituse tagamiseks tuleb võtta järgmisi meetmeid:

- rakendatavate komponentide turve;
- sertifikaaditühistusnimistute kasutamine (Certificate Revocation List – CRL). Microsoft Exchange Serveri üldtuntud süsteemikomponentide kõrval tuleb turvata ka selliseid komponente, mida kasutatakse Exchange'i jaoks vajalike krüpteerimis- ja signeerimisfunktsioonide käitamiseks. Olukorras, kus soovitakse tühistada kas ühte või ka mitut kasutajasertifikaati, tuleb arvesse võtta sertifikaaditühistusnimistu kehtivusaega. CRL on soovitatav pärast tühistamist avalikustada kohe, mitte oodata järgmise planeeritud avalikustamiseni. Siinkohal tuleb arvestada, et uue CRL-i avalikustamisega ei muutu vana nimistu automaatselt kehtetuks, mis tähendab, et need kliendid, kellel on kehtiv CRL juba olemas, ei ole kohustatud uut nimistut kasutama. Seetõttu on soovitatav valida CRL-idele võimalikult lühike kehtivusaeg, mis sunniks kliente võimalikult sageli enda CRL-i uuendama.
- Outlook Web Accessi kasutamist võimaldatakse standardselt kõikidele meilikasutajatele. Outlook Web Accessi turvalise konfiguratsiooni loomiseks võib rakendada juurdepääsupiiranguid ja juurdepääsuobjektide segmenteerimist, vt ka „Understanding Security for Outlook Web App: Exchange 2010 Help".
- Outlook Anywhere'i (varem: RPC-over-HTTP) käsitletakse dokumendis „Understanding Outlook Anywhere: Exchange 2010 Help".
- ActiveSynci käsitletakse dokumendis „Understanding Client Access: Exchange 2010 Help".
- Alates versioonist Exchange 2010 puudub tarkvaral WebDAV liidese tugi.

- Transpordiserverite turvamist TLS-iga kirjeldatakse dokumendis „TLS - Functionality and Related Terminology in Exchange 2010: Exchange 2010 Help”. - TLS-il põhineva turbe desaktiveerimisest on soovitatav hoiduda.
- Unified Messagingi serverite turvet käsitletakse dokumendis „Securing Unified - Messaging Network Traffic: Exchange 2010 Help”.
- Client Accessi serverile ja teistele Exchange’i serverite serverirollidele kehtivaid nõudeid kirjeldatakse dokumendis „Securing Client Access Servers: Exchange 2010 Help”.

Kontrollküsimused:

- Kas Exchange’i süsteemide jaoks on vastu võetud selged otsused, milliste meetmetega tagatakse siseneva ja väljuva side turve?
- Kas Microsoft Exchange’i süsteemidesse saadetavad ja nendest väljuvad konfidentsiaalsed andmed krüpteeritakse?
- Kas olemasolevad WebDAV liidesed on muudetud turvaliseks?

M 5.108z Rühmatarkvara või meilisüsteemi krüptograafiline kaitse

Algatamise eest vastutavad: administraator, infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator, kasutaja

Rühmatarkvarasüsteem suhtleb rühmatarkvaraklientide, brauserite, telefoni, suhtlusrakenduste ja teiste rühmatarkvarasüsteemidega. Andmeid vahetatakse ka rühmatarkvarasüsteemi komponentide vahel . Suheldakse kohaliku võrgu ja/või välisvõrkude kaudu . Kõigil juhtudel kantakse üle kaitsmist vajavaid andmeid. Tegemist pole mitte ainult kasutaja tuvastamiseks kasutavate andmetega (näiteks k asutajanimi ja parool), vaid ka ärilise infoga , mistõttu tuleb otsustada, milline kaitsemehhanism suhtluse turvamiseks valida. krüpteerimine ja digiallkirjad on mõeldud terviklikkuse ja konfidentsiaalsuse ning elektrooniliselt edastatavate sõnumite salgamatuse kaitseks. Et elektroonilist suhtlust (nt e-kirja) ei saaks teel muuta ega pealt kuulata, tuleb see krüptograafiliselt turvata. Konfidentsiaalsuse tagamiseks võib kasutada krüptimist ning terviklikkuse, autentsuse ja tagasivõetamatuse tagamiseks võib kasutada digiallkirja. Üldiselt saab rühmatarkvara ja meilide krüptograafiliseks kaitseks kolm viisi.

Võrgust võrku

Sel puhul turvatakse ühendust ühest võrguühenduspunktist teise näiteks VPN-i (virtuaalse privaatvõrgu, vt B 4.4 Virtuaalne privaatvõrk (VPN)) kaudu.

Eelis: kindlaksmääratud krüpteerimine toimib k asutaja sekkumisest olenemata. Paljude kasutajate asemel tuleb koolitada vaid mõnda administ raatorit.

Puudused: individuaalseid seadistusi pole näiteks digiallkirjade puhul võimalik teha. Lisaks saab seda lahendust rakendada ainult üksikute, varem kindlaksmääratud suhtluspartneritest koosnevate rühmade puhul.

Tegemist on hea lahendusega siis, kui geograafiliselt eraldatud organisatsioonid või selle osad soovivad sageli turvalise kanali kaudu suhelda.

Klient-veeb/meiliserver: näiteks TLS/SSL, proksilahendus

Proksilahenduse puhul krüptitakse või dekrüptitakse iga meil meiliserveris ning edastatakse kliendile avatekstina .

Eelis: toimib meilikliendist olenemata . Meiliklientidele pole vaja täiendavaid krüptimisprogramme installeerida .

Puudused: proksilahenduste puhul võib konfigureerimine keeruline olla. TLS/SSL-lahenduste puhul võib esineda palju vigu.

Kliendilt kliendile ehk „lõpust lõpuni”

Kliendilt kliendile ühenduse krüptograafilise turbe puhul kasutatakse meiliklientidele integreeritud või seal hiljem installeeritavaid funktsioone (näiteks pistikprogramme). Selle poolest tuntud tooted on GnuPG või PGP. Et nad ka tegelikult oodatud turvalisust pakuksid, tuleb nende kasutamisel pöörata tähelepanu hulgale raamtingimustele .

Paljudele meiliklientidele on krüpteerimise ja digiallkirja võimalus juba sisse ehitatud. Selle eeliseks on, et taolisi funktsioone saab kasutada ilma lisakulutusteta ja asutuse sees toimuvat meililiiklust saab otse kaitsta. Puuduseks on, et mõnikord on kasutusel krüptograafiliselt nõrgad meetodid või rakendused. Samuti esineb tihti ühildamatust teiste meiliklientidega. Alternatiivina on olemas terve rida krüpteerimise ja digiallkirja jaoks mõeldud lisatooteid. Eelis: tooteid saab valida nii, et nad vastaksid just asutuses kehtivatele tingimustele ja turbenõuetele. Puuduseks on, et alati ei ole kõigi meiliprogrammide jaoks tooteid olemas. Meiliprogrammi uuendamise puhul ei ole kindel, kas pistikprogramm veel toimib või on ka seda vaja uuendada . Võib juhtuda, et sellised krüpteerimisprogrammid ei ühildu vas-

tuvõtja lehel asuvate sarnaste programmidega. Kuna kliendilt-kliendile-turve põhineb alati sellel, et igale kasutajale tuleb anda krüptograafilised võtmed , on vaja keskset võtmehaldust, mis peab tagama võtmete regulaarse vahetamise , alalise kehtivuse ning turvalise installeerimise ja salvestamise , nii et neile pääseksid ligi ainult volitatud isikud. See muudab aga protsessi keerukamaks (vt M 2.46 Krüpteerimise õige korraldus). Milliseid kriteeriume (näiteks funktsionaalsus, kasutajasõbralikkus, koostalitlusvõime , majanduslikkus, tehtud turvalisusuuringud) sobiva krüptograafilise programmi valimisel silmas pidada, on kirjeldatud moodulis B 1.7 Krüptokontseptsioon .

Rühmatarkvarasüsteemide vahel kaitsmist vajavate andmete ülekandmisel peab kaitse olema adekvaatne . Selleks võib rakendada erinevaid meetmeid, ent tuleb otsustada, millised meetmed milliste raamtingimuste puhul sobivad, ja o tsus dokumenteerida.

Täiendavad kontrollküsimused:

- Kas on olemas meili krüptograafilise kaitse kontseptsioon ?
- Kas kasutatakse adekvaatseid krüpteerimis- või signeerimismeetodeid ?
- Kas kasutajaid või administraatoreid koolitatakse krüptimistoodetega ümber käima ?

M 5.109z Meiliskanneri kasutamine meiliserveril

Algatamise eest vastutavad: administraator, infoturbespetsialist

Rakendamise eest vastutavad: administraator

Turvalisuse tõstmiseks peaks kesksele meiliserverile olema installeeritud mällu paigutatud viirustõrjeprogrammiga meiliskanner (kutsutakse ka meilivalvuriks), mis kontrollib sisenevate ja väljuvate meilide ning eelkõige nende manuseid rämpsposti, arvutiviiruste ja muud laadi kahjurvara suhtes. Lisaks meiliserveril meilivalvuri sisseseadmisele võib internetti mineval liidesel sisse seada ka nn SMPTlüüsi, millega kontrollitakse sisenevaid ja väljuvaid meile. Internetiühendus peab siis olema selline, et kõik SMPT-ühendused jookseksid üle SMTP-lüüsi. Meiliskannerid töötavad kahel täiesti erineval põhimõttel. Store-and-Forward -skanner võtab esmalt meili vastu ja kasutab siis oma mehhanisme meili liigitamiseks. Pärast liigitamist otsustab skanner, mida meiliga edasi teha (kustutada, märgistada,...). Selle meetodi eeliseks on, et kiri võetakse kõigepealt vastu ning siis on aega seda rahulikult kontrollida. Samas on see ka puuduseks, kuna juriidilisest vaatepunktist on kiri vastu võetud ning seetõttu esineb kohustus see kasutajale edasi saata. Online -skanner kontrollib meili ja üritab seda liigitada juba vastuvõtmisel.

Kui skanner teeb kindlaks, et meil võib olla soovimatu, võib ta sellest kohe keelduda ning meil jääb saatja vastutusele. Selle meetodi eeliseks on, et kasutajaid ei kuhjata erinevate märgistuste või karantiiniteadetega üle. Puuduseks on aga, et vale liigituse korral ei saa meili enam lokaalselt kätte. Kiri paikneb saatja juures ning ei kasutajal ega administraatoril ole võimalik sellele ligi pääseda. Praktilises töös kasutatakse tihtipeale nende kahe meetodi segu. Võrgus või pärast meili vastuvõtmist kasutatavad filtrid tuleb vastavate eeskirjadega kindlaks määrata ja juhatusega kooskõlastada. Sama tähtis on väljuvate meilide kontroll. Ühest küljest on nii võimalik sisevõrgu nakatumist vältida või avastada see enne suurema kahju tekkimist. Teisest küljest kaitseb see ametiasutust või ettevõtet võimaliku mainekahju või isegi kahjuhüvitamisnõude eest, mis võivad tekkida siis, kui viirustega saastatud meilid edastatakse äripartneritele. Väljuvate meilide skannerite puhul tuleb kindlaks määrata, mis juhtub meilidega, millel on tuvastatud viirus. Sellisel juhul peaks vähemalt administraatori juures käivituma alarm.

Rämpsposti tuvastamine

Enamik meilivalvureid pakuvad „kahtlaste" meilidega tegelemiseks laialdasi seadistusvõimalusi. Näiteks on võimalik sellised meilid kustutada, märgistada, edastada või „karantiiniserverile" vahesalvestada, kuniks on selgunud, kas meili sisu on ohutu või mitte. Veel üks võimalus on potentsiaalselt ohtlikud manused eemaldada ja kiri ise vastava teatega saajale edasi saata. Vastavad meiliskannerid toetavad meilides spämmitunnuste tuvastamiseks erinevaid mehhanisme.

Suhtluses osalevate võõraste IP-aadresside mõju vähendamiseks kasutatakse esimese sammuna tihti Black- ja Whitelist 'e. Näiteks on olemas nimekirjad, mis annavad ülevaate sellest, kas mõni IP-aadress on varem soovimatuid meile saatnud või kas selle IP-aadressi taga on kehtiv meiliserver. Peale selle on olemas nimekirjad, mis annavad teavet selle kohta, kas IP-aadressi taga olev meiliserver käitub vastavalt RFC-le või kas see paikneb sissehelistamisvõrgus. Neid nimekirju

kasutatakse tihtipeale selleks, et suhtlus IP-aadressidega juba varakult lõpetada ja vältida ühegi meili vastuvõtmist. Nimekirju hooldavad teenusepakkujad ning neid pakutakse nii tasuta kui ka tasuliste variantidena. Selliste listide kasutamisel tuleb arvesse võtta, et nad võivad olla vigased.

Võib juhtuda, et ettevaatmatusest satub nimekirja mõni äripartner, mistõttu ei ole enam võimalik sellelt äripartnerilt meile saada. Lisaks tuleb arvestada, et sellise nimekirja pakkujal on võim otsustada, millistelt partneritelt asutus tulevikus meile vastu võtta saab. Selliste listide pakkujad teevad seda tihti DNS-serverite kaudu (nn DNSBL, DNS-based Blackhole Lists). Kui meiliskanneri teenusepakkuja kasutab sellist DNSBLi, saadab meiliskanner kõigi sisenevate meilide IP-aadressid DNSCL-i kasutajale. Vastusena saab meiliskanner teate, kas vastav IP-aadress on listis või ei. Selle meetodi kaudu saab DNSBL-i kasutaja kõigi asutusega suhtlevate meilisüsteemide IP-aadressid. Nii on tal võimalik koostada ulatuslikke meilikommunikatsiooniprofiile. Selle probleemi vältimiseks on soovitatav kasutada Blacklist 'i lokaalseid koopiaid. Paljud teenusepakkujad annavad klientide kasutusse andmekogukoopiad (tasuline). Enne Blacklist 'ide kasutamist tuleb analüüsida nendega kaasnevaid riske. Tekkivaid ohte tuleb vastavate ettevaatusabinõude või teenusepakkujaga sõlmitud lepingute abil minimeerida.

RFC-vastavustest

Veel üks tähtis kontrollsamm on RFC vastavus SMTP-dialoogi ajal. Tuleb kontrollida, kas infot edastav meiliserver annab endast märku kehtiva nimega (HELO/EHLO), kas serveri IP-aadressi saab DNS-i kaudu tagasi teisendada, kas nime teisendamine annab jälle sama IP-aadressi, kas meili saatja ja saaja süntaks on õige ning kas meili saaja üldse eksisteerib. Rämpsposti saatjad tekitavad siin sageli nii palju vigu, et mitmed meilid tuleb vastavustestis kõrvale jätta. Et enda meile selliste vigade tõttu ei blokitaks, tähendab see aga teiselt poolt, et administraator peab oma süsteemid seadistama vastavalt RFC-le.

Meili sisu kontrollimine

Kahjurvara tuvastamine

Järgmise sammuna kontrollitakse tihtipeale meilide sisu. V õtmesõnade või teiste rämpspostile omaste tunnuste järgi soovimatute meilide tuvastamiseks kasutatakse allkirjal põhinevaid filtreerimissüsteeme. Sageli toimivad filtrid punktisüsteemi alusel. Kui filtreerimissüsteem registreerib kindla negatiivse omaduse, jagatakse selle eest kindlad punktid. Kõigi negatiivsete omaduste punktid liidetakse seejärel kokku ning need moodustavad näitaja meili soovimatuse tõenäosuse kohta. Filtrid, mis selle tarvis seadistada tuleb, muutuvad pidevalt. Visioon iseseisvalt töötavast meiliskannerist jääbki aga visiooniks.

Filtreerimissüsteemid peavad olema võimelised muutuma vastavalt tegelikule rämpspostimaailmale ning administraator peab neid käsitsi seadistama. Igal mei-

liskanneril peaks olema üks või isegi mitu moodulit, mille abil tuvastada kahjurvara. Tuvastatud viirustega meile ei tohiks edasi saata, vaid tuleks vahesalvestada.

Ohtlike manustega ümberkäimine

Potentsiaalselt ohtlike manustega, milles sisenemise hetkeks kahjurvara ei leitud, ümberkäimiseks tuleb kõigepealt kindlaks määrata eeskirjad, kus sätestatakse, millised failitüübid asutusele kahjulikud on või millised failitüübid kindlasti kahjutud on. Väga kriitiliselt tuleks siinkohal analüüsida täiteprogrammidega manuste edastamise vajadust. Pärast juhiste kindlakstegemist on võimalik tegevus vastava Blacklist 'i või Whitelist 'i abiga ellu viia.

Blacklist 'i korral liigitatakse nimekiri „keelatud" failivormingute alla, mida ei tohi mingil juhul väljuva meili manusena kasutada ning mida ka sisenevate meilide korral ei aktsepteerita. Whitelist on piirav lähenemisviis, mille korral lubatakse manusena ainult failitüüpe, mis on lisatud lubatud failitüüpide nimekirja. Back- või Whitelist 'ide kindlaks määramisel tuleks jälgida, et saavutatakse mõistlik kompromiss turvalisuse ja funktsionaalsuse vahel. Liiga nõrgad seadistused võivad viia selleni, et sisevõrku satub kahjurvara, kuid liiga range seadistus võib samas takistada tootlikkust. Kuna krüpteeritud meile ei ole võimalik automaatselt kontrollida, tuleb kindlaks määrata, kuidas krüpteeritud meilide korral käituda (vt B 1.6 Viirusetõrje kontseptsioon ja B 1.7 Krüptokontseptsioon).

Töötajate teavitamine, personaliosakonna osalemine

Töötajaid tuleb teavitada kehtivatest reeglitest ja sellest, et meile skannitakse automaatselt. Kui tehakse otsus, et meile skannitakse meiliserveril automaatselt, tuleks kaasata ka personalihaldus ja infoturbespetsialist. Riigist ja asutuse tüübist (ametiasutus või firma) olenevalt tuleb võib-olla arvestada teistegi õigusaktidega.

Ei asenda lokaalset viirustõrjeprogrammi

Viirustõrjeprogrammidest ei tohiks tööarvutites loobuda isegi siis, kui meiliserverile on installeeritud meilivalvur. Kuigi praeguseks edastatakse suurim osa viirustest ja kahjurvarast meili teel, on pahatahtlike programmide levitamiseks ikkagi veel palju teisi viise, näiteks USB-mälupulk, mõni muu irdkandja või failide veebist allalaadimine.

Kriisiplaan ülekoormuse vastu

Meetmed meiliskanneritele

Meile edastavad süsteemid peavad sageli toime tulema töödeldavate andmemahtude äkilise suurenemisega. Isegi siis, kui asutus on süsteemi töövõimekuse ülima täpsusega välja arvestanud, saabub ikkagi hetk, mil süsteem on üle koormatud. Nende hetkede jaoks tuleb koostada kriisiplaan. Kriisiplaan peab kindlaks määrama, kuidas on võimalik samm-sammult meiliskanneri funktsionaalsust tugevdada ja seega töötlusmahtu vähendada, ning milline on sellise tegevuse mõju suhtlusele. Kuna mõju on tihtipeale seotud piirangutega, tuleb juhatusele nendest piirangutest teada anda ning kriisiplaani vastavalt ühtlustada. Kriisiplaani praktilist toimimist peaks varem harjutama ja vajadusel tuleb seda kohandada. Näitlikustava

kriisimeetmena olgu välja toodud, et meiliskannerit on võimalik konfigureerida nii, et see lubaks ainult kindlaksmääratud sidepartnerite vahelist suhtlust. Kõik teised (uued) sidepartnerid lukustatakse kriisiplaani aktiveerimise ajaks välja.

Kontrollküsimused:

- Kas kesksel meiliserveril jookseb integreeritud, mälus paikneva viirustõrjeprogrammiga meiliskanner?
- Kas soovimatute meilide vastu on tõhus kaitse?
- Kas meilide skannimiseks vajalike üksikute filtreerimismeetodite valikul kontrolliti neid kriitiliselt?
- Kas töötajaid on teavitatud meilide kontrollimisest ja sellest, kuidas seda tehakse?
- Kas meiliskannerile määrati kriisiplaan ja kas juhtkond kinnitas selle?
- Kas meiliskanneri kriisiplaani läbiviimist harjutatakse?

M 5.110z Meili kaitse SPHINXi (S/MIME) abil

Algatamise eest vastutavad: infoturbeosakond, administraator

Rakendamise eest vastutavad: kasutajad, administraator

Meilide kasvava tähtsuse tõttu tuleb võtta meetmeid, mis tagaksid e-kirjade konfidentsiaalsuse ja siduvuse. Seda on võimalik saavutada meilide krüptotoodete ja digitaalsete allkirjade laialdase kasutamise abil. Elektrooniline allkiri tagab seejuures selle, et e-kiri tuleb näidatud saatjalt ja et seda pole muudetud. Informatsiooni krüpteerimine tagab, et meili saab lugeda vaid selle õiguspärane vastuvõtja.

Krüptoprotseduurid

Tootjast sõltumatu interoperatiivsuse saavutamiseks kasutatakse projekti SPHINX raames eranditult tooteid, mis põhinevad tööstuslikel standarditel S/MIME ja MailTrusT. Standardid kasutavad meilide kaitseks erinevate krüptoprotseduuride kombinatsioone. Sümmeetrilise meetodina kasutatakse andmete krüpteerimiseks 112-bitise võtmepikkusega 3DES-algoritmi. Elektroonilise allkirja ja krüpteerimise jaoks kasutatav avaliku võtme meetod on vähemalt 1024-bitise võtmepikkusega RSA-algoritm. SHA-1 on soovitatav räsialgoritm, mida kasutatakse sõnumi ühetähenduslikuks kujutamiseks määratava pikkusega. Krüptovõtmete isikutele jaotamist reguleeritakse digitaalsete sertifikaatidega. Sertifikaat on elektrooniline dokument, mis sisaldab peaasjalikult avalikku võtit ja võtmeomaniku nime. Sertifitseerimiskeskus (trustcenter) tõendab oma elektroonilise allkirjaga võtme ja isiku vahelist seost. SPHINXi raames kasutatakse ITU soovitusel X.509 versiooni 3 standardiseeritud sertifikaate. Kommunikatsioonipartneritevaheline usaldus seisneb sisuliselt usalduses digitaalsete sertifikaatide vastu ja kõikide selles sisalduvate andmete usaldusväärsuses. Avaliku halduse jaoks on juba paljud sertifitseerimiskeskused sertifikaate välja andnud.

Nimetatud usalduskeskusi kontrollib kõrgemalseisev juursertifitseerimiskeskus ja neid liidab avaliku halduse taristu (public key infrastructure, PKI). Sellega alluvad kõik väljastatud sertifikaadid kõikides infoturbe küsimustes IT etalonturbe standardile. Kodanike ja firmadega kontakti saamiseks integreeriti haldus-PKI Euroopa sertifitseerijate portaali Bridge CA, mis seob omavahel usaldusväärselt sõltumatuid PKI-sid. Usalduse tagamise järgmine nõue on kasutaja salavõtme kaitse. Selleks võib salajase (või isikliku) võtme salvestada kas spetsiaalsesse faili või kiipkaarti. Üldiselt nimetatakse seda faili või kiipkaarti isiku turvakeskkonnaks (personal security environment, PSE). PSE-d on krüptograafiliselt kaitstud ja neid on võimalik aktiveerida vaid parooli abil kasutamiseks. Parooli ja faili või kiipkaardiga turvalise ümberkäimise eest vastutab omanik.

Turvaline installeerimine ja kasutamine

SPHINX-toodete näol on tavaliselt tegemist nn pistiktoodetega. Koos kindlalt tunnustatud krüptoprotseduuridega täiendavad need olemasolevat meilitoodet. Vale konfiguratsiooni või vale kasutamise tõttu võib aga turvalisuse tase väheneda. SPHINX-toodete konfiguratsioon ei ole nagu enamikul keerulisematest krüptotoodetest iseennast selgitav. Et haldusvead sisse ei hiiliks, tuleb läbi viia kasutatava SPHINX-toote alane koolitus. Ettevõtetes ja asutustes peaks IT üks haldustöötaja läbima SPHINX-tooteid puudutava koolituse ning olema kättesaadav tehnilise nõustajana. Et kasutajad hakkaksid uute funktsioonide rakendamisest aru saama,

tuleb lahti seletada mõned krüptograafilised põhimõisted. Vaja on läbi viia sertifikaadi taotlemise ja SPHINX-toote kasutamise alane koolitus. Ettevõtetes ja asutustes tuleks valitud kasutajad SPHINX-toodete kasutamise alal välja õpetada ja need omakorda võiksid oma teadmisi teistele edasi anda. Eelistada tuleks tootja- või müüjakoolitust.

Enne programmi kasutamist tuleks eriti harjutada allkirjastatud ja krüpteeritud meilide saatmist või vastuvõtmist. Soovitatav on, et organisatsiooni sees kasutataks ühtset SPHINX-toodet, parem veel kui ühtset programmiversiooni. Sellega on võimalik hoida administreerimisele, koolitusele, hooldamisele ja tarkvara hooldusele tehtavad kulutused madalatena. Iga SPHINX-toote juurde kuulub ulatuslik dokumentatsioon, mis tuleks enne toote kasutamist läbi lugeda. Enne kasutajatele kättejagamist tuleks see kohandada organisatsiooni iseärasustega. Sellega on võimalik saavutada suurem aktsepteeritavus toote juurutamisel.

Võtmete deponeerimine

Isiklikke võtmeid deponeeritakse isiku turvakeskkonnas (PSE). Turvalisuse seisukohalt on määrava tähtsusega, et PSE sisu jääks usaldusväärseks ja et see oleks kaitstud manipuleerimise eest. Kasutatav parool tuleb luua meetmes M 2.11 Paroolide kasutamise reeglid kirjeldatud reeglite järgi ja deponeerida turvaliselt. Parooli tahtmatu või tahtlik edasiandmine võimaldab teistel isikutel anda parooli omaniku nimel elektroonilist allkirja. Kui PSE on fail, räägitakse soft PSEst. See on parooli abil krüptograafiliselt kaitstud. Seda ei ole soovitatav salvestada võrgudraividele, sest muidu on vaja rakendada täiendavaid turvameetmeid. Võtmete salvestamisel tuleb eelistada kiipkaartide kasutamist. Aga ka kiipkaartide korral tuleb kasutatav parool turvaliselt deponeerida.

SPHINX-toodetega kasutatavatest kiipkaartidest ei saa teha koopiat. Soft PSEst tuleb teha turvakoopia ning märkida üles parool. Turvakoopia ja parool tuleks säilitada turvalises kohas, parim oleks seda teha eraldi. Nii on võimalik tagada, et kõvaketta purunemise või vale kasutamise korral ei lähe PSE kaduma. Krüpteeritud sõnumeid ei ole PSE kadumise korral enam võimalik dešifreerida. Parooli üleskirjutamisse ja turvalises kohas deponeerimisse tuleks seejuures suhtuda kui kriitilisse tegevusse, mis on vajalik vaid hädaolukorras. Suletud kirjutuslaua sahtlit või mõnda muud taolist „turvalist” kohta ei soovitata mitte mingil juhul PSE või parooli säilitamiseks.

Võtmete jagamine

Et sõnumi vastuvõtja saaks kontrollida faili saatja elektroonilist allkirja või et saatja saaks sõnumi ühele kindlale vastuvõtjale saatmiseks krüpteerida, on tal vaja oma suhtluspartneri digitaalset sertifikaati. Selle võib ta saada mitmel erineval moel, näiteks meili lisana või spetsiaalselt internetiserverilt (kataloogist), mõnikord ka WWW-serverilt. SPHINX-tooted toetavad kasutajat digitaalsete sertifikaatide kontrollimisel. Enamike toodete puhul peab kasutaja esimesel vastuvõtmisel oma suhtluspartneri sertifikaadi käsitsi meiliaadressi juurde paigutama. Lisaks suhtluspartneri sertifikaadile on automaatseks kontrolliks vaja ka selle välja andnud usaldusekeskuse sertifikaati. Vajalikud sertifikaadid edastatakse tavaliselt allkirjastatud meililisadena. Juursertifitseerimiskeskuse sertifikaat peaks juba olemas olema või

olema IT-teenuse kaudu eelinstalleeritud.

Selleks, et kasutaja oma sertifikaadi kätte saaks, nõutakse temalt taotlust ja identifitseerimist. Mõlemad toimingud saab läbi viia registreerimiskohas. Asutustes, firmades ja organisatsioonides võib neid enamasti leida siseteenistusest või töökaitsest. Usalduskeskuste filiaalides on registreerimiskohad enamasti olemas. Registreerimiskohas kontrollitakse sertifikaadi saamiseks tehtud avalduste õigsust ja identifitseeritakse kasutaja isik teenistus- või isikutunnistuse alusel. Ka väljaantud kiipkaardid saab reeglina sealt. Soft PSEde puhul toimub kättetoimetamine elektrooniliselt, enamasti meili teel.

Kontrollküsimused:

- Kas kasutajaid koolitatakse SPHINX-toodetega ümber käima?
- Kas administraatoreid valmistatakse ette SPHINX-toote konfigureerimiseks ja tehnilise toe pakkumiseks?
- Kas registreerimiskoht on sisse seatud ja vajalik personal ülesande täitmiseks valmis?
- Kuidas on korraldatud soft PSE ja parooli turvakoopiate deponeerimine?
- Kas kasutajad saavad turvameetmeid ja protseduure puudutavat koolitust?
- Kas kasutajaid on informeeritud sertifikaadi taotlemise ja sulgemise protseduuridest?

M 5.111 Marsruuterite pääsuloendite konfigureerimine

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: Administraator

Marsruuterite ja kommutaatorite laialdasi pöördusvõimalusi seadmete kasutamiseks ja haldamiseks saab kontrollida pääsuloendi (Access Control List - ACL) abiga. Ligipääsu saab määrata üksikutele arvutitele või võrkudele, lisaks saab määrata ka pöördusmeetodi. ACL-iga määratakse, millised arvutid või võrgud marsruuterile või kommutaatorile erinevate teenuste (näiteks TELNET, SNMP, HTTP, jne) kaudu ligi pääsevad. Järgnev näide näitab Cisco marsruuteri vastavat pääsuloendit TELNETi teenuse ligipääsupiiranguks lüüsile endale:

- access-list 102 permit tcp host 163.183.200.22 any eq 23 log
- access-list 102 permit tcp host 163.183.200.24 any eq 23 log
- access-list 102 deny ip any any log

Pääsuloendi kindlaks määramine peab vastama infoturbe suuniste nõuetele. Eelkõige tuleks määrata tegutsemisviis juhuks, kui ühtegi spetsiifilist reeglit ei esine. Sellega seoses on olemas kaks põhilist lähenemisvõimalust: „Mis ei ole keelatud, on lubatud” (Blacklist) ja „Mis ei ole lubatud, on keelatud” (Whitelist). Konfigureerimisel tuleks eelistada piiravat Whitelisti lähenemist, sest ainult puhtal Blacklisti lähenemisel tekivad varem või hiljem lüngad. Pääsuloendi abiga saab kontrollida nii pöördust lüüsile endale kui ka üle lüüsi toimuvat andmesidet. Marsruutereid kasutatakse lokaalsetes võrkudes ja laivõrkudes pakettfiltritena. Marsruuter kontrollib sellisel juhul ühendatud alamvõrkude suunda ja andmesidet liidese kohta (inbound ja outbound). Ühendusest sõltuvatele protokollidele (näiteks TCP) on lisaks võimalik defineerida pääsuloend (ACL), mis arvestab ühenduse olekut. See võimaldab määrata, et teatud ühendused on läbi marsruuteri lubatud ainult ühes suunas (näiteks Telnet -ühendus „seestpoolt väljapoole”). Seejuures laseb marsruuter vastassuunas läbi ainult need paketid, mis on vastuspaketid juba olemasolevale ühendusele, aga samas lükkab tagasi paketid, millega üritatakse ühendust luua keelatud suunas. Ühenduseta protokolle (nt UDP) on tavaliste pakettfiltritega raske turvata. Seepärast kasutatakse selleks tihtipeale Stateful Inspection System i. Seejuures peab süsteem tabelit, milles salvestatakse, kas ja kust kindla ajaperioodi jooksul lubatud pakett (näiteks DNS-päring) kindlale aadressile saadeti. Kui antud ajaperioodil registreeritakse mõni pakett vastassuunas, siis tõlgendatakse seda kui vastust salvestatud päringule ning see lastakse läbi. Kindla päringuta paketid keelatakse. Reeglina analüüsitakse pääsuloendis järgmisi kriteeriume:

- paketi allikas (IP-päises paiknev IP-aadress),
- paketi sihtkoht (IP-päises paiknev IP-aadress),
- kasutatav protokoll ja võimalusel ka pordinumber (näiteks port 80/TCP HTTP-le või 25/TCP SMTP-le).

Probleemide korral (näiteks konfiguratsioonivigade või rünnakukatsete tuvastamisel) tuleb pääsuloendid (ACL) konfigureerida nii, et keelatud ühenduskatsed

protokollitakse. Selleks tuleb igale pääsuloendi sissekandele lisada vastav protokollikäsklus. Niimoodi saab logifailidest väärtuslik andmeallikas, tänu millele on võimalik probleemidega ja rünnakutega võrgus paremini toime tulla. Pääsuloendi (ACL) loomine peab vastama infoturbe suuniste nõuetele. Võimalusel tuleks luua mallid (Templates), mida on võimalik pidevalt kasutada ning mida peab ainult vähesel määral modifitseerima. Pääsuloendi (ACL) kasutamisel tuleb arvestada teatud jõudluse kaoga. Mõnikord on see isegi keeruliste reeglite juures unarusse jäetav, kui aga marsruuter juba suure koormusega käitatakse, tuleks enne pääsuloendi laiendamist kontrollida, kas seade suudab neid laiendatud reegleid veel üleüldse töödelda. Cisco marsruuteri pääsuloendi väljavõttest lähtuvalt on järgnevalt ära toodud mõningad filtreerimisreeglid. Lähtutakse sellest, et tegemist on inbound ligipääsuga. Järgmised teenused tuleks koheselt lubada, ülejäänud ühendused tuleks keelata:

- SMTP sisesele MEILISERVERILE
- TELNET ühele sisesele TELNETi SERVERILE
- HTTP sisesele VEEBISERVERILE
- HTTPS sisesele VEEBISERVERILE
- access-list 103 permit tcp any any established
- access-list 103 permit tcp any host MAIL-SERVER eq smtp
- access-list 103 permit tcp any host TELNET-SERVER eq telnet
- access-list 103 permit tcp any host WEB-SERVER eq www
- access-list 103 permit tcp any host WEB-SERVER eq 443
- access-list 103 deny ip any any log

Täiendavad kontrollküsimused:

- Kas pääsuloendite loomine viidi läbi infoturbe poliitikast lähtuvalt?
- Kas pääsuloendi funktsionaalsust kontrolliti?
- Kas mittelubatud ühendused protokollitakse?

M 5.112 Marsruutimisprotokollide turvaaspektide arvestamine

Algatamise eest vastutab: IT-juht, infoturbe spetsialist

Elluviimise eest vastutab: administraator

Autentimine

Ideaalina peaks kasutama vaid selliseid marsruutimisprotokolle, mis toetavad marsruutimisinfo vahetamisel marsruuterite turvalist autentimist. Niipea kui marsruutimistabelitelt saadetakse värskendus, peab toimuma marsruutimisvärskenduse saatnud marsruuteri autentimine. Sellega saavutatakse olukord, kus marsruuter töötleb vaid usaldusväärsest allikast (marsruuterilt) pärit usaldusväärset marsruutimisinfot. Autentimata marsruutimisinfo vahetamisel on võrgu turvalisus autoriseerimata või tahtlikult võltsitud marsruutimisvärskenduse tõttu ohustatud. Turvalisust on võimalik tõsta pääsuõiguste reeglistiku (Access Control Lists) sisseseadmisega, nii et ainult kindlaks määratud IP-aadressidega IT-süsteemid tohiksid marsruutimisinformatsiooni vahetada. Dünaamilisi marsruutimisprotokolle tuleks kasutada vaid turvalistes võrkudes. Demilitariseeritud tsoonides ei tohi neid kasutada. Kui näiteks ründajal õnnestub demilitariseeritud tsoonis marsruutimisinfo vahetamisel andmepakette lugeda, saab ta sellest teadmisi asutuse võrgustruktuuri kohta. Demilitariseeritud tsoonides tuleks selle asemel registreerida staatilisi marsruuterid. Marsruutimisinfo vahetamisel toetavad autentimist järgmised marsruutimisprotokollid:

- Border Gateway Protocol (BGPv4)
- Open Shortest Path First (OSPFv2)
- Marsruutimisinfo protokolli versioon 2 (RIPv2)
- Enhanced Interior Gateway Protocol (EIGRP)
- Intermediate System-to-Intermediate System (IS-IS)

Marsruutimisvärskendusi saatva marsruuteri autentimine saavutatakse võtme (parooli) väljavahetamise teel. See võti peab teada olema kõigile osalevatele marsruuteritele. Võtme määrab marsruuteri konfigureerimisel kindlaks administraator. Neid võtmeid tuleks regulaarselt muuta.

Krüptograafiline autentimine

Erinevate marsruutimisprotokollide puhul tuleb vahet teha klaarteksti autentimise ja krüptograafilise autentimise vahel. Soovitatav on kasutada vaid krüptograafilist autentimist toetavaid marsruutimisprotokolle. Krüptograafilisel autentimisel kasutatakse reeglina räsifunktsiooni MD5. Tegeliku võtme asemel saadetakse selle meetodi korral autentimiseks välja nn Message-Digest (sõnumilühend). Sõnumilühend luuakse küll võtme abil, kuid võtit ei saadeta võrgu kaudu. Sellega võetakse ära võtme võrgus lugemise võimalus. Võtmehalduse suhtes on vaja silmas pidada, et võtmete jagamine ja uuendamine toimuks nii, et volitamata isikud ei kuuleks neid pealt ega saaks neid lugeda.

Krüptograafilist autentimist toetavad järgmised protokollid:

- Border Gateway Protocol (BGPv4)

- Open Shortest Path First (OSPFv2)
- Marsruutimisinfo protokolli versioon 2 (RIPv2)
- Enhanced Interior Gateway Protocol (EIGRP)
- Intermediate System-to-Intermediate System (IS-IS)

Nõuanne: MD5 räsialgoritmis on leitud krüptograafilisi kitsaskohti. Seepärast tuleks võimalusel kasutada tugevamat algoritmi. Paremaid räsialgoritme kui MD5 ei toeta aga marsruutimisprotokollid ja -tooted veel täielikult. RFC 4822 määrab üksikasjaliselt kindlaks, kuidas on SHA-perekonda kuuluvaid räsialgoritme võimalik RIPv2 korral autentimiseks kasutada. IPSec'i tagasipöördumise kaudu on põhimõtteliselt võimalik tugevamaid räsialgoritme kasutada ka OSPFv3 (OSPF for IPv6) korral. MD5 tuntud kitsaskohtadele vaatamata pakub ka MD5-l põhinev autentimine ühtekokku kõrgemat turvalisuse taset kui klaarteksti autentimine.

Võtmehaldus

Mõned marsruutimisprotokollid pakuvad võtmehaldust niinimetatud võtmejadade kasutamisega. Üks võtmejada koosneb tervest reast kindlaksmääratud võtmetest. Marsruuterid kasutavad võtmeid rotatsiooniprotsessis. See vähendab võtmete väljaluuramise võimalust. Võtmejadas oleval võtmel on kehtivusaeg vaid teatud kindlaks määratud ajaks. Seejuures on tähtis, et marsruuteritel oleks kindel kellaaeg, et võtme vahetamine toimuks sünkroonselt. Seda on võimalik reguleerida asutuse NTP-serveri kaudu. Ideaalina peaks asutuse NTP-server olema ühendatud raadiokellaga. Võtmehaldust toetavad järgmised protokollid:

- Marsruutimisinfo protokolli versioon 2 (RIPv2)
- Enhanced Interior Gateway Protocol (EIGRP)

Järgnev tabel annab turvatehnilisest vaatepunktist ülevaate marsruutimisprotokollide kõige erinevamatest autentimisega seotud tunnustest.

Protokolli nimi	Autentimine	Klaartekst	Räsifunktsioon	RFC-protokollid
RIPvI	Ei			RFC 1058
IGRP	Ei			Proprietaarne (Cisco)
RIPv2	Jah	Jah	Jah	RFC 2453, 4822
EIGRP	Jah		Jah	Proprietaarne (Cisco)
OSPFv2	Jah	Jah	Jah	RFC 2328
IS-IS	Jah	Jah	Jah	RFC 1195, 5304
BGPv4	Jah		Jah	RFC 4271

Tabel: autentimine erinevate marsruutimisprotokollide kasutamisel

Täiendavad kontrollküsimused:

- Kas on tagatud, et marsruutimisprotokollide kasutades ei imbuks teave asutuse sisevõrgu kaudu välja?

- Kas demilitariseeritud tsoonides (DMZ) loobutakse dünaamiliste marsruutimisprotokollide kasutamisest?
- Kas selgelt piiritletud marsruutimisdomeenid on defineeritud?
- Kas vastavalt kaitsevajadusele on marsruuterite autentimise vajalikkuse kohta otsus tehtud?

M 5.115z Veebiserveri integreerimine turvalüüsi koostisse

Algatamise eest vastutavad: IT-juht, infoturbeosakond
Rakendamise eest vastutavad: infoturbeosakond, administraator

Veebiserveri integreerimine turvalüüsi on paljudel juhtudel kriitiline, kuna veebiserver esitab võrgu ribalaiusele tihti kõrgeid nõudmisi. Lisaks kättesaadavuse tagamisele on kaitseks sihilike rünnakute eest tähtis ka serveri asukoha õige valik, kuna veebiserverid on hästi äratuntavad ja selle tõttu eriti ohustatud ning kuna veebiserverite programmides esines minevikus tihti turvalünki.

Järgnevalt kirjeldatakse kolme lahendust, mille abil on võimalik veebiserverit turvalüüsi integreerida:

- Integreerimine ilma pöördproksit (reverse proxy) kasutamata
- Integreerimine, mille käigus kasutatakse pöördproksit, mille eesmärgiks on veebiserveri koormuse vähendamine
- Integreerimine pöördproksi ning lisakaitse abil teise paketifiltri näol

Kõigil kolmel juhul ei paigaldata serverit ALG, vaid paketifiltri taha, kuna teatud tingimustel võib ALG süsteemi kogujõudlust tunduvalt vähendada. Seetõttu on soovitused rakendatavad ka sel juhul, kui võetakse tarvitusele vaid üks lihtne turvalüüs (koosneb ainult ühest paketifiltrist). Veebiserverit ei tohi mitte mingil juhul paigutada asutuse sisevõrku. Kõrgendatud turvanõuete korral võib siiski olla vajalik kasutada veebiserveri kaitseks oma ALG-d, mis kaitseb veebiserverit ja sellel käitatavaid veebirakendusi teatud liiki rünnete eest (Cross-Site Scripting, Command Injection ja muud taolised). Vastavaid ALG-sid on olemas erinevatelt pakkujatelt. Keerukamate veebirakenduste korral soovitatakse kasutada sarnast ALG-d.

Ilma pöördproksita (reverse proxy) veebiserver

Kui veebiserveri enda turvalisusele ei esitata erinõudeid ning kui server saab sissetulevate päringutega probleemideta hakkama, on võimalik paigutada veebiserver välise paketifiltri demilitariseeritud tsooni (DMZ). Vastavate paketifiltri reeglite abil tuleks tagada, et veebiserver oleks väliste rünnete eest kaitstud nii palju kui võimalik. Lisaks sellele tuleks täiendavate paketifiltri reeglite abil hoolitseda selle eest, et ründaja saaks isegi pärast veebiserveri edukat kompromiteerimist teha nii vähe kahju kui võimalik. Soovitused on kokku võetud järgmises tabelis.

Allikas
Eesmärk
Otsus
Märkused
Üldine teave
Veebiserver
Välisvõrk ja sisevõrk
Lubada ainult pakette, mis kuuluvad teise arvuti poolt algatatud ühenduse juurde
Veebiserver vastab vaid päringutele. Oma ühendusi ei ole vaja üles ehitada
Veebiserveri side internetiga

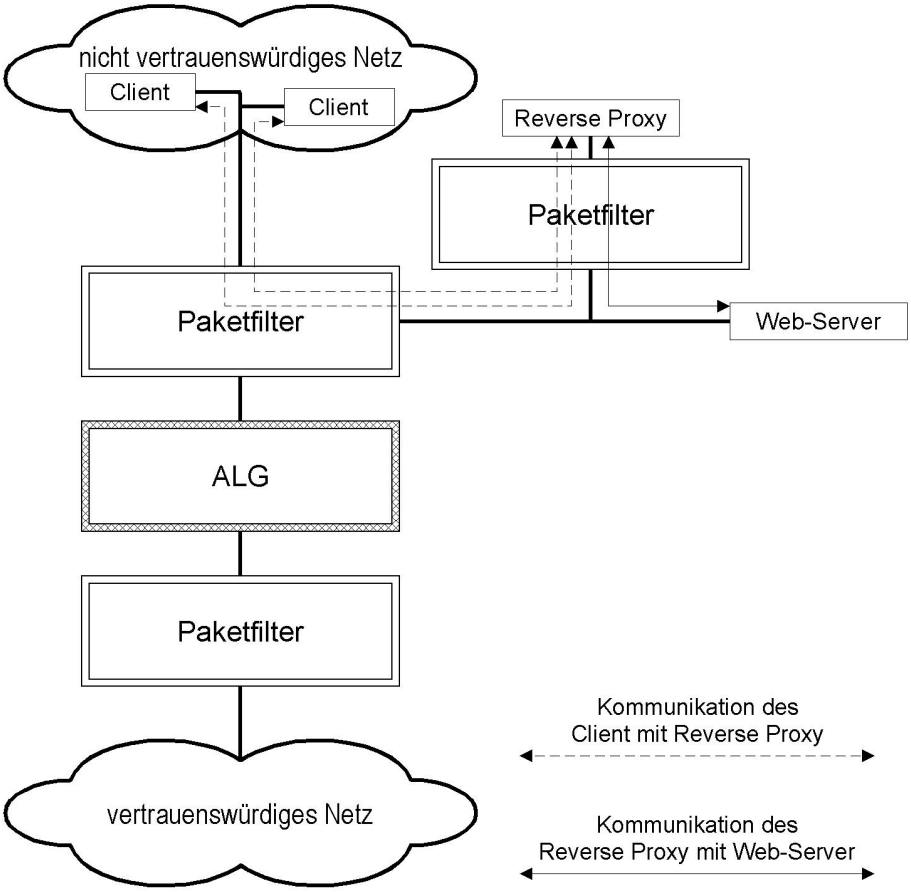
Välisvõrk
Veebiserveri port 80
lubatud
Port 80 on standardport
Välisvõrk
Veebiserveri teised pordid
keelatud
Veebiserveri side sisevõrguga
Sisevõrk
Veebiserveri port 80
lubatud
Veebiserveri kasutamine ka sisevõrgust
Sisevõrk (vajadusel piirang haldusvõrguna)
Veebiserver: port 22(SSH)
lubatud
Administreerimine ja andmete edastamine toimuvad SSH ja SCH kaudu.
Sisevõrk
Veebiserveri teised pordid
keelatud
Logimine
Veebiserver
Loghost UDP-port 514
lubatud
Logiandmete ülekandmine loghosti.

Seejuures lähtutakse asjaolust, et veebiserveri haldus sisevõrgust toimub SSH-ühenduse kaudu ning et veebiandmed kantakse veebiserverile turvakoopiaprotokolli (SCP) kaudu. Edasi lähtutakse sellest, et veebiserveril ei kasutata domeeninimede teenust (DNS). Nimede teisendamine ei ole tavapäraseks käituseks vajalik. Juurdepääsustatistika või muude järelduste tegemiseks võib see vajadusel toimuda hiljem. Veebiserverile laekuvad logiandmed saadetakse üle võrgu oma loghosti juurde (vt M 4.225z Logiserveri kasutamine turvalüüsis). Kuna veebiserveri algatatud ühendused ei ole lubatud, on veebiserverit kompromiteerinud ründaja tegevust võimalik otsustavalt pidurdada. Enamasti on ründajal pärast sissemurdmist ründe jätkamiseks vaja teisi tööriistu, mida ta laeb välisvõrgu arvutilt. Kui see ei ole paketifiltri reeglite tõttu võimalik või on oluliselt raskendatud, võib juhtuda, et väiksemate oskustega või vähem otsusekindlad ründajad (näiteks Script Kiddies – skriptijuntsud) mõnikord isegi katkestavad ründe. Kui veebiserveri haldus või veebiandmete ülekandmine veebiserverile toimub teisiti, tuleks kasutatud protokollide jaoks rakendada vastavaid paketireegleid.

Pöördproksiga (reverse proxy) veebiserver

Esimesel juhul moodustavad veebiserveri kogu koormuse sissetulevad päringud. Kui veebiserver tuleb sissetulevatest sõnumitest vabastada, võib kasutusele võtta pöördproksi, mis vastab sagedasti korduvatele päringutele oma vahemälust ning vähendab sellega veebiserveri koormust. Võimalikult suure läbilaskevõime saavutamiseks on vajalik paigutada veebiserver ja pöördproksi ühte ja samasse demilitariseeritud tsooni. Juurdepääs mitteusaldusväärsest võrgust peaks olema lubatud vaid pöördproksile, otsepääs veebiserverile mitteusaldusväärsest võrgust peaks olema välise paketifiltri abil takistatud.

Veebiserver ja pöördproksi eraldi demilitariseeritud tsoonides
Enamasti ei ole pöördproksid välja töötatud eelkõige turvalisuse aspekte silmas pidades. Seetõttu tuleks vajadusel pöördproksi veebiserverist teise paketifiltriga eraldada. See tõstab veebiserveri turvalisust, võib aga teiselt poolt viia käsutuses oleva ribalaiuse vähenemisele. Sel viisil saab pöördproksi võimaliku kompromiteerimise korral ära hoida soovimatud ründed pöördproksilt veebiserverile (näiteks haldusportidele). See lahendus on kujutatud järgneval joonisel.



- Mitteusaldusväärne võrk
- Klient
- Pöördproksi
- Paketifilter
- Veebiserver
- ALG
- Usaldusväärne võrk
- Kliendi andmevahetus pöördproksiga
- Pöördproksi andmevahetus veebiserveriga

Joonis 1: veebiserveri integratsioon pöörd-puhverserveri (caching proxy) ja teise paketifiltri kasutamisega veebiserveri täiendavaks kaitseks See lahendus on võrdväärne sellega, kui pöördproksi ja veebiserver paigaldataks välise paketifiltri

erinevatesse demilitariseeritud tsoonidesse. Täiendava filtriastme kasutamine sõltub konkreetsest kasutusmudelist.

Kontrollküsimused:

- Kuidas on veebiserver turvalüüsi integreeritud?
- Kas kaitseks rünnete eest veebirakendustele kasutatakse täiendavat ALGd?

M 5.116z Meiliserveri integreerimine turvalüüsi koostisse

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: infoturbeosakond, administraator

Meiliserveri integreerimisel turvalüüsi koostisesse on mõeldavad kaks stsenaariumit. Esimesel juhul lähtub kõik sellest, et teha meiliteenus kättesaadavaks ainult ühele usaldusväärsele võrgule, teisel juhul tuleb meiliteenus teha kättesaadavaks mitmele usaldusväärsele võrgule. Mõlemal korral käitatakse usaldusväärsetes võrkudes võrgusiseseid meiliservereid. Usaldusväärse võrgu siseselt kasutatakse meiliserverit Aliase andmebaasi halduseks, millega kõik kasutaja-aadressid ühtsesse formaati teisendatakse, võimalusel POP või IMAP deemonina või ka teise meilisüsteemi ülemineku lüüsina (näiteks X.400). Kõik võrgusisesed meilid saadetakse sellele serverile ja sealt vajadusel välise meiliserveri kaudu edasi välisvõrku. Võrgusisese meiliserveri kasutamine on soovitatav mitmel põhjusel:

- Võrgusiseste arvutite vahelised meilid ei välju usaldusväärsest võrgust, kuna nende edastamine toimub siseste meiliserverite kaudu.
- Kui sisest meiliserverit kasutatakse samaaegselt rühmavara serverina (Groupware Server), võib see ALG-d mõttetult koormata.
- Sellisel juhul on rühmavaraserver aga paremini rünnakute eest kaitstud, kuna ta paikneb ebausaldusväärsest võrgust kaugemal.

Soovitatav on sisevõrgus paiknevaid meili- ja rühmavaraservereid kaitsta lisaks vähemalt paketifiltreerimisreeglitega, et tagada ka kaitse sisevõrgus volitamata ligipääsu eest. See vastab serveri paigutamisele sisemise pakettfiltri eraldi demilitariseeritud tsooni (Demilitarized Zone - DMZ). Eriliste sisevõrgu infoturbe nõuete korral tuleks see kindlasti teostada. Erinevalt veebiserveritest, mida soovitatakse turvalüüsis paigutada võimalikult välisvõrgu lähedale, soovitatakse selle paigutuse kohaselt meiliserver paigutada välisvõrgust võimalikult kaugele. Põhjuseks on asjaolu, et sellisel juhul on võimalik võrgusiseseid meile saata ka siis, kui interneti-ühendus peaks katkema.

Ühe usaldusväärse võrgu ühendamine

Kui meiliserverit tahetakse kasutada ainult ühe usaldusväärse võrgu jaoks, piisab võrgusisesest meiliserverist. ALG toimib siinkohal võrgusisesele meiliserverile „ Smart Hostina”.

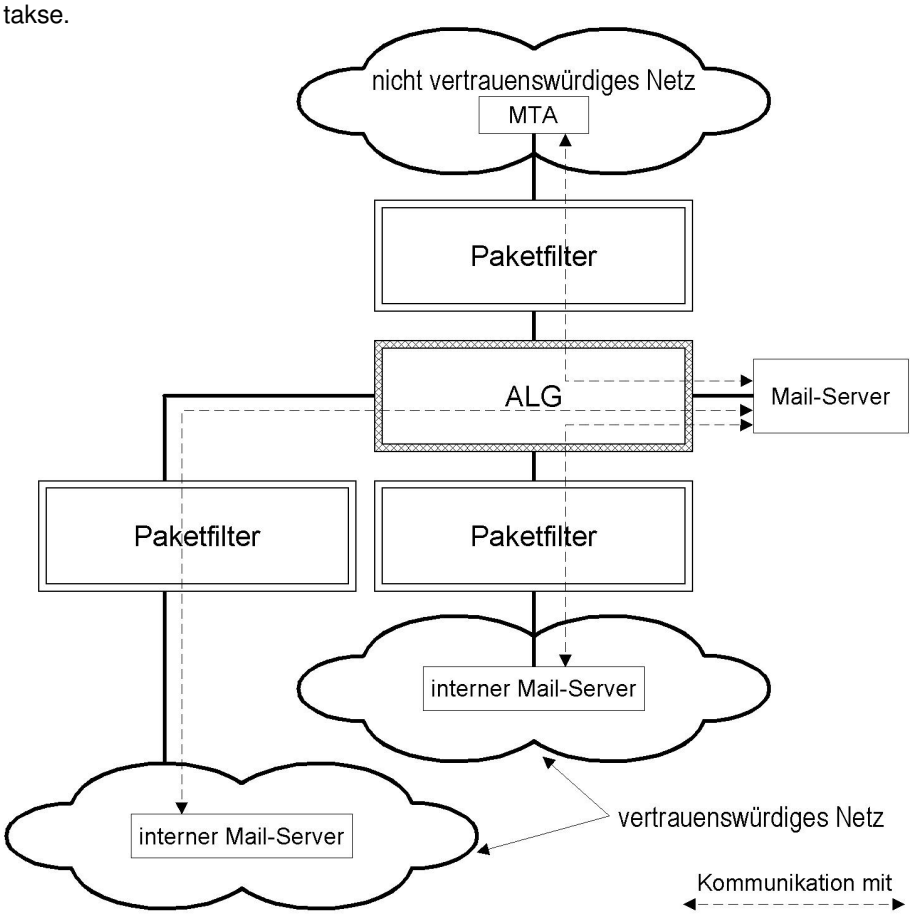
Smart Host

Smart Host on arvuti, üle mille jooksevad kõik ühe võrgu meilid. Kui ALG on konfigureeritud võrgusisese meiliserveri Smart Host ina, ei pea väljaminevate meilide võrgusisene meiliserver välja selgitama, milline meiliserver on vastuvõtudomeen, vaid ta saadab meili lihtsalt Smart Host ile edasi, mis võtab endale ülesandeks õige saaja meiliserver välja selgitada. Selleks võib taaskord olla Smart Host (näiteks interneti teenusepakkuja juures) ning kui ALG-d kasutatakse sisevõrgus Smart Host ina, siis see üldjuhul ka nii on. Smart Host i nimetatakse vahel ka Mail Relayks. Sissetulevate meilide korral toimib ALG kas meilikeskusena, mis võtab vastu kõik sissetulevad meilid ja edastab need siis võrgusisesele meiliserverile või Smart Host ina välisele meilikeskusele.

Mitme usaldusväärse võrgu ühendamine

Kui ühte turvalüüsi kasutatakse mitme usaldusväärse võrgu jaoks, näiteks ühise internetiliidesena organisatsiooni eri osadele, ei ole ülalkirjeldatud lihtne ülesehitus enam võimalik. Meilide saatmine ja vastuvõtmine peaks selle stsenaariumi

korral olema kaheastmeline. Endiselt peaks usaldusväärsetes võrkudes kasutama eraldi meiliservereid, mille kaudu on võimalik võrgusiseseid meile otse saata. Lisaks sellele on otstarbekas DMZ-i paigutada keskne meiliserver, mis toimib usaldusväärsetele võrkudele keskse Mail Exchanger ina ning mis teostatakse väliste meilide kaudu. Sõltuvalt tootest võib selline DMZ-s paiknev meiliserver olla juba ALG-ga integreeritud. Järgmine joonis näitab sellist ülesehitust kahe usaldusväärse võrguga, millel mõlemal on sisene meiliserver ja mis on ühendatud mitteusaldusväärse võrguga (näiteks internet). Mõlemad sisesed meiliserverid on vastutavad erinevate (alam-) domeenide eest, see tähendab, et DMZ-is paiknev meiliserver otsustab, millisele sisesele meiliserverile sissetulevad meilid edastatakse.



Joonis 1: Siseste MTA-de ja meiliserveri paigutamine kahe usaldusväärse võrgu ühendamiseks (ALG liidesel DMZ-i tuleb sisse seada kaks SMTP-porti, näiteks virtuaalsete IP-aadresside abiga) (nicht vertrauenswürdiges Netz – ebausaldusväärne võrk; Paketfilter – pakettfilter; (interner) Mail-Server – (sisene) meiliserver; vertrausenswürdiges Netz – usaldusväärne võrk; Kommunikation mit – side).

Sissetulevad välised meilid läbivad MTA järgmiselt:

1. mitteusaldusväärses võrgus paiknev MTA (saatja või interneti teenusepakkuja juures);

2. DMZ-s paiknev MTA See otsustab, millisesse kahest usaldusväärsest võrgust (millisele MTA-le) meil saata tuleb;

3. Meiliserver vastavas usaldusväärses võrgus.

Väljuvad meilid läbivad MTA-d vastupidises järjekorras.

Meiliserver lihtsate turvalüüside korral

Kui kasutatakse ainult lihtsat turvalüüsi, mis koosneb pakettfiltrist, on soovitatav ühendada meiliserver pakettfiltri DMZ-ga. Puuduva ALG tõttu on meiliserveri kaitse välise kompromiteerimise eest väiksem. Meiliserveri paigutamine DMZ-i pakub kompromiteerimise korral sisevõrgule suuremat kaitset kui meiliserveri paigutamine otse sisevõrku. Kui siseste meilide saatmine peab olema võimalik ka välise (interneti) ühenduse katkemise korral, võib meiliserveri tõsta sisevõrku ja lisaks paigutada pakettfiltri DMZ-i meiliedastusagent (MTA), mis toimib seal Mail Exchanger ina. See lahendus on nii öelda segu üleval kirjeldatud keerukatest lahendustest.

Täiendavad kontrollküsimused:

- Kuhu on meilserver paigutatud?
- Millised sideühendused on lubatud?

M 5.117z Andmebaasiserveri integreerimine turvalüüsi koostisse

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: infoturbeosakond, administraator

Andmebaasiserverite paigaldamisel pöörduseks ebausaldusväärsest võrgust on võimalik eristada kahte põhilist kasutusvõimalust:

1. andmebaasi andmetele ligipääs veebi ees-süsteemi kaudu,

2. otsene ligipääs andmebaasi andmetele (näiteks SQL-iga).

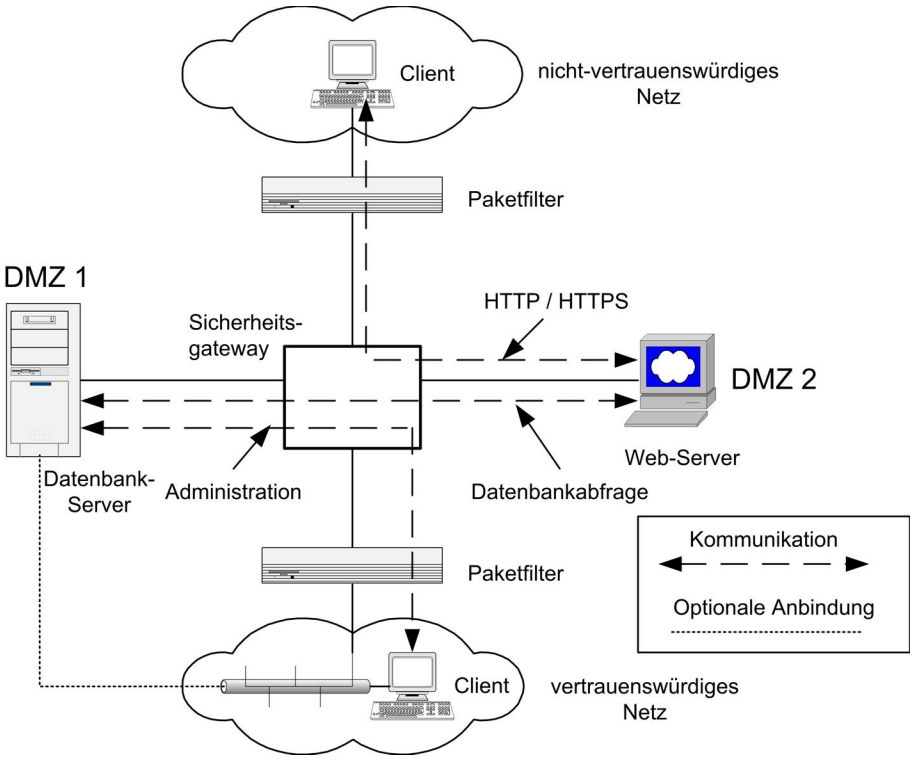
Järgnevas kahes lõigus kirjeldatakse mõlemat kasutusjuhtumit.

Ligipääs veebi ees-süsteemi kaudu

Veebiserver ja andmebaasiserver peaksid paiknema erinevates DMZ-des, et veebiserveri kompromiteerimise korral oleks ikkagi olemas andmebaasiserveri kaitse ALG (Appliation Level Gateway) proksi kaudu. Proksikaitse on aga minimaalne, näiteks kaitstakse andmebaasiserveri TCP/IP pinu (stack). Lisaks saab ründeid takistada TCP/IP päiste andmete põhjal. Kui kindlaid turbenõudeid ei esine, võib server ka veebiserveriga ühes DMZ-s paikneda. Ülesehitus ja kommunikatsioonisidemed on sellisel juhul järgmised:

- Internetist toimub ligipääs veebiserverile ainult HTTP või HTTPS-i kaudu. Pöördused on ALG poolt vastavalt kaitstud.
- Veebiserveril jooksev rakendus teisaldab päringud vastavateks andmebaasipäringuteks, teostab andmebaasis päringu ja valmistab vastavalt ette tulemuse.
- Andmebaasiarvuti, andmebaasisüsteemi haldus ja andmebaasis paiknevate andmete hooldus toimuvad sisevõrgust vastavate turvatud ühenduste kaudu.

Need ühendused on kujutatud järgmisel joonisel.

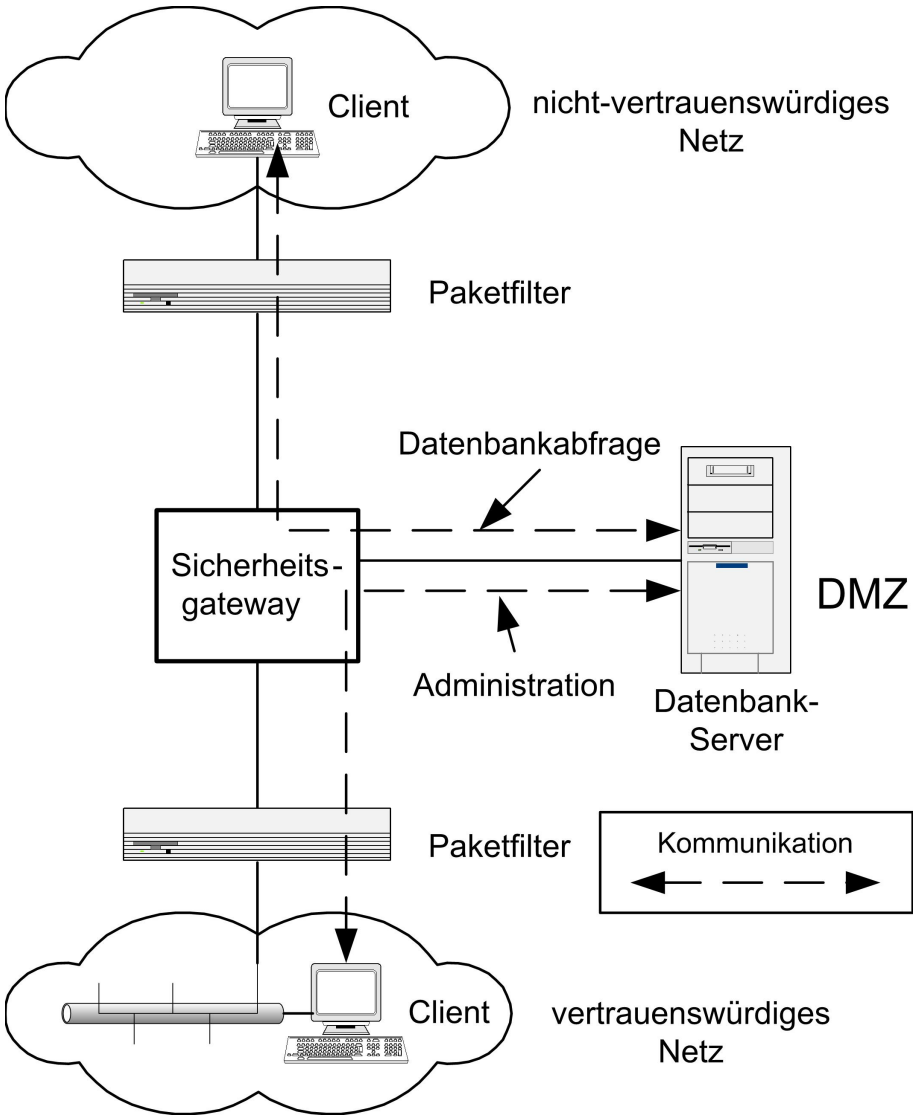


Joonis 1: Pöördus andmebaasile, kasutades veebi ees-süsteemi (nicht-vertrauenswürdiges Netz – ebausaldusväärne võrk; Paketfilter – pakettfilter; Sicherheitgateway – turvalüüs; Web-Server – veebiserver; Datenbank-Server – andmebaasiserver; Administration – haldus; Datenbankabfrage – andmebaasile esitatud päring; Kommunikation – side; Optionale Angindung – lisaühendus; vertrausenswürdiges Netz – usaldusväärne võrk)

Mitteusaldusväärses võrgus paiknev klient saab veebiserverile esitada päringuid ainult veebilehekülje kaudu, otsene pöördus andmepangale ei ole võimalik. Selle ülesehituse korral on peale transpordikihi turbe oluline ka see, et veebiserveril paiknev päringuid ja juhtumeid töötlev rakendus oleks turvaliselt programmeeritud ega võimaldaks rünnakuid andmebaasile (näiteks SQL Injection). Kui veebi ees-süsteemi kaudu peab saama vastavas andmebaasikeeles (näiteks SQL) esitada otseseid andmebaasipäringuid, tuleks ligipääs veebi ees-süsteemile teostada ainult HTTPS-i kaudu.

Otsene pöördus

Kui andmebaasile ligipääs toimub otse ebausaldusväärse võrgu kaudu, tuleks server paigutada eraldi DMZ-ti. Kuna andmebaasi protokollidele on vähe prokse, on TCP- või UDP- Relay kasutamine vältimatu.



Joonis 2: Otsene pöördus andmebaasile (nicht-vertrauenswürdiges Netz – ebausaldusväärne võrk; Paketfilter – pakettfilter; Sicherheitgateway – turvalüüs; Administration – haldus; Datenbankabfrage – andmebaasile esitatud päring; Datenbank-Server – andmebaasiserver; Kommunikation – side; vertrausenswürdiges Netz – usaldusväärne võrk)

Kuna andmebaasipäringute protokollidele puuduvad turvaproksid, mille abil neid kontrollida, on esmalt tutvustatud veebi ees-süsteemiga lahendus reeglina kõige turvalisem variant. Sõltuvalt andmebaasi andmete turbevajadusest, on väliseks pöörduseks soovitav kasutada nö tegeliku andmebaasi asemel eraldiseisvat andmebaasi, mis sisaldab antud andmete koopiaid ja mida kindlate intervallide tagant selle nö tegeliku andmebaasiga sünkroniseeritakse.

Täiendavad kontrollküsimused:

- Kuidas teostatakse andmebaasi päringuid?

- Kui kasutatakse veebi ees-süsteemi: kas on võimalik teostada otseseid päringuid andmebaasile? Kas pöördus HTTPS-i kaudu turvatakse?
- Kui on võimalik otsene pöördus andmebaasile: kas kasutatakse vastavat turvaproksi?

M 5.118z DNS-serveri integreerimine turvalüüsi koostisse

Algatamise eest vastutavad: IT-juht, infoturbeosakond
Rakendamise eest vastutavad: IT-turvaosakond, administraator

Domeeninimede teenust (Domain Name Service - DNS) kasutatakse arvutinimede teisaldamiseks IP-aadressideks ja vastupidi ning see võimaldab näha informatsiooni võrgus olevate arvutisüsteemide kohta. See informatsioon (näiteks teave DNS-serveri või Mail Exchanger i kohta domeenile) on osaliselt vajalik korrektseks internetiühenduseks. Samas võivad DNS-informatsiooni kasutada ka võimalikud ründajad, et rünnakut ette valmistada. Kui arvutil on näiteks nimi “mssq101”, võib ründaja sellest eeldada, et tegemist on Microsofti operatsioonisüsteemiga arvutiga, millel jookseb Microsoft SQL-server. DNS-i korral tuleks seega teostada siseste ja väliste nimede eraldamine.

Sisene DNS-informatsioon tuleks ebausaldusväärse võrgu eest peita. Sisevõrgus paikneval arvutil ei tohiks ka siis väljastpoolt tuvastatavat DNS-nime olla, kui tal on nö avalik IP-aadress. Kui sisevõrgus kasutatakse RFC 1918 aadressiruumi (address spa) IP-aadresse, tuleb need nii või teisiti sisese nimeserveriga teisendada. Iseäranis just DNS-serveri programmide puhul ilmnes minevikus turvaaukude tõttu probleeme. DNS-informatsiooni erilise tähtsuse tõttu ja seepärast, et suur osa rünnakutest toimub DNS-i tarkvarale, on DNS-informatsiooni kättesaadavaks tegemisel ja kasutamisel vajalik eriline ülesehitus.

DNS-server kolmeastmelises turvalüüsis

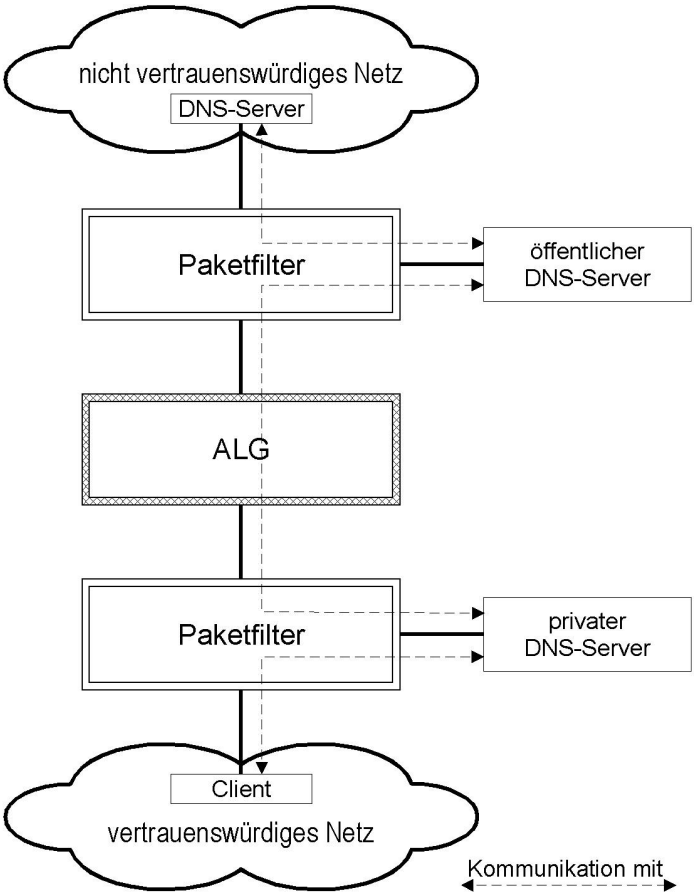
DNS-i turvaliseks kolmeastmelisse turvalüüsi integreerimiseks on võimalik kasutada järgmisel joonisel näidatud ülesehitust, mille korral ei toimu otsest ühendust usaldusväärses võrgus paikneva kliendi ja ebausaldusväärses võrgus paikneva DNS-serveri vahel (või vastupidi).

Kasutatakse kahte üksteisest eraldiseisvat DNS-serverit:

Väliselt kättesaadavat informatsiooni sisaldav avalik DNS-server paigutatakse välise pakettfiltri DMZ-i. See on seadistatud usaldusväärse võrgu domeeni “ Primary Nameserver ”-ina ning sisaldab ainult ilmtingimata vajalikku informatsiooni, näiteks:

1. välise meiliserveri nime ja IP-aadressi (MX sissekanne).
2. infoserveri nime ja aadressi, mis avalikkusele informatsiooni pakub. Siinjuures tuleb eristada serverit, mis on paigutatud kas ALG ette või taha. ALG ette asetatud serverite korral tuleb sisse kanda serveri enda aadress, ALG taha paigutatud serverite korra aga ALG enda aadress.
3. “privaatne” DNS-server paigutatakse sisemise pakettfiltri DMZ-i. See sisaldab informatsiooni sisevõrgus olevate arvutite kohta. Sisevõrgus olevatele arvutitele kantakse see server sisse DNS-serverina: kõik usaldusväärse võrgu kliendid kasutavad ainult privaatset DNS-serverit (näiteks Unixi arvutite korral sissekannetega failis /etc/resolv.conf l). Kui usaldusväärses võrgus

paiknev klient vajab DNS-informatsiooni ebausaldusväärsest võrgust, esitab ta DNS-päringu privaatsele DNS serverile. “ Forwarder ina” kasutab see avalikku DNS-serverit päringuteks, mis puudutavad väliseid nimesid. Otsene ligipääs privaatsele DNS-serverile ebausaldusväärsest võrgust tuleks pakettfiltrireeglitega keelustada, nii et usaldusväärse võrgu DNS-informatsioon oleks nähtav ainult usaldusväärses võrgus.



Joonis 1: DNS-serveri integreerimine usaldusväärse ja ebausaldusväärse võrgu turvaliseks kommunikatsiooniks. (nicht vertrauenswürdiges Netz – ebausaldusväärne võrk; Paketfilter – pakettfilter; öffentlicher/privater DNS-Server – avalik/privaatne DNS-server; vertrausenswürdiges Netz – usaldusväärne võrk; Kommunikation mit – side)

Kasutatav pakettfilter tuleb konfigureerida nii, et serverite vahel oleks lubatud ainult DNS-teenus, see tähendab DNS-port 53 lähte- või sihtpordina (sõltuvalt vaatlemissuunast). Avalikust DNS-serverist ei tohiks sisevõrku lubada mitte ühtegi ühendust. Serveri haldus peaks toimuma vastavalt turvatud ühenduste (SSH) kaudu. Järgmises tabelis kirjeldatakse võimalikku ligipääsureeglistikku, mida on võimalik vastavate pakettfiltrireeglite kaudu teostada. Seejuures lähtutakse sellest, et haldus toimub sisevõrgust SSH-ühenduse kaudu ja DNS-i kandevprotokollina kasutatakse UDP-d. Logiandmed kantakse Syslog i kaudu logiserverile.

Allikas
Siht
Otsus
Märkus
Avalike DNS-serverite kommunikatsioon internetiga
Välivõrk
Avalik DNS-server
UDP-port 53
lubada
DNS päringud ja vastused avalikust võrgust
Välivõrk
Avaliku DNS-serveri teised pordid
keelata
Väline DNS-server
DNS-server internetis, port 53 TCP ja UDP
lubada
DNS-serveri kaudu väliste nimede kustutamine
Väline DNS-server
Kõik teised internetiühendused
keelata
Välise DNS-serverite kommunikatsioon sisevõrguga
Väline DNS-server
Kõik ühendused sisevõrku
keelata
Sisevõrk (piirang ainult haldusvõrgule)
Avalik DNS-server port 22 (SSH)
lubada
Haldus ja andmeside toimuvad SSH ja SCP kaudu
Sisevõrk
Kõik teised pöördused avalikule DNS-serverile
keelata
Sisevõrgust tulev DNS-päring toimub sisese serveri kaudu
Tabel: ligipääsureeglite konfiguratsioon

DNS-server lihtsas turvalüüsis

Kui kasutatakse ainult lihtsat turvalüüsi (pakettfiltrit), soovitatakse ikkagi kahe eraldatud DNS-serveri rakendamist. Kui need kaks DNS-serverit paigutatakse pakettfiltri eraldi DMZ-desse, saab kasutada ülalkirjeldatud reegleid. Kui kahe eraldi DMZ sisseseadmine on liiga mahukas või ei ole seda võimalik teha tehnilistel põhjustel, võib kasutada ka lihtsamaid konstruktsioone. Need pakuvad aga nõrgemat kaitset ning seetõttu tuleb vastaval juhul otsustada, kas antud turbeaste on vastuvõetav või mitte. Igal juhul tuleks pakettfiltri DMZ-i paigutada avalik DNS-server. Sisene DNS-server võib antud juhul paikneda sisevõrgus. Kui sisemiseks ja välimiseks nimeteisenduseks on kasutada ainult üks DNS-server, tuleks see paigutada pakettfiltri DMZ-i. Sellisel juhul tuleks võimalusel DNS-serveri programm konfigureerida niimoodi, et eristuksid päringud, mis tulevad sisevõrgust ja välisvõrgust ning vajadusel edastataks erinevad andmed. See lahendus pakub piisava turbe ainult väikestele ja madala turbeastmega võrkudele.

Domeeni registreerimine väliste teenusepakkujate juures

Selle alternatiivse variandi korral salvestatakse tähtis DNS-informatsioon välise teenusepakkuja juures. Erinevus eelnevalt kirjeldatud stsenaariumiga on välise DNS-serveri ärajätmine. Välisvõrgust tulevaid DNS-päringuid DNS-informatsiooni kohta sisevõrgus ei saadeta organisatsioonisisesele DNS-serverile, vaid need saadetakse välise teenusepakkuja DNS-serverile, mille poolt neile ka vastatakse.

DNS-nimede või IP-aadresside päringute korral loob sisene DNS-server üle turvalüüsi ühenduse välisvõrgus paikneva DNS-serveriga. Ka selle integratsioonivariandi korral tuleks väliselt pakkuda ainult kõige vajalikumat DNS-informatsiooni, näiteks meiliserveri ja ALG nimi ja IP-aadress. Eriti ohutute organisatsioonisiseste kasutajate korral võib sisest DNS-serverit käitada sisese pakettfiltri DMZ-i asemel ka sisevõrgus, mis omakorda lihtsustab (kuigi ainult vähesel määral) pakettfiltri haldust. Selle variandi eelisteks on madalad investeerimiskulud ja turvalüüsi integreerimise lihtsustatus. Lisaks on võimalik teenusepakkujal kasutada lisasüsteeme, mis organisatsioonisisese lahenduse korral tihtipeale puuduvad.

Kontrollküsimused:

- Millisele võrguinformatsioonile saab DNS-i kaudu väljast päringuid esitada?
- Milline on valitud DNS-serverite paigutus?
- Millised sideühendused on DNS-serverile lubatud?

M 5.119z Veebi-, rakendus- ja andmebaasiserveritega veebirakenduse integreerimine turvalüüsi koostisesse

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: infoturbeosakond, administraator

Keerukate veebirakenduste (näiteks e-valitsuse rakenduse või online -kaupluse) käsutusse andmiseks on nende rakenduste kõrgendatud kaitsevajaduse tõttu vajalik rakendada täiendavaid kaitsemeetmeid. Järgnevalt esitletakse sellise erijuhtumi korral rakendatavat standardülesehitusega veebiserverist, rakendusserverist ja andmebaasiserverist koosnevat veebirakendust.

Kahe ALG ja paketifiltriga arhitektuur

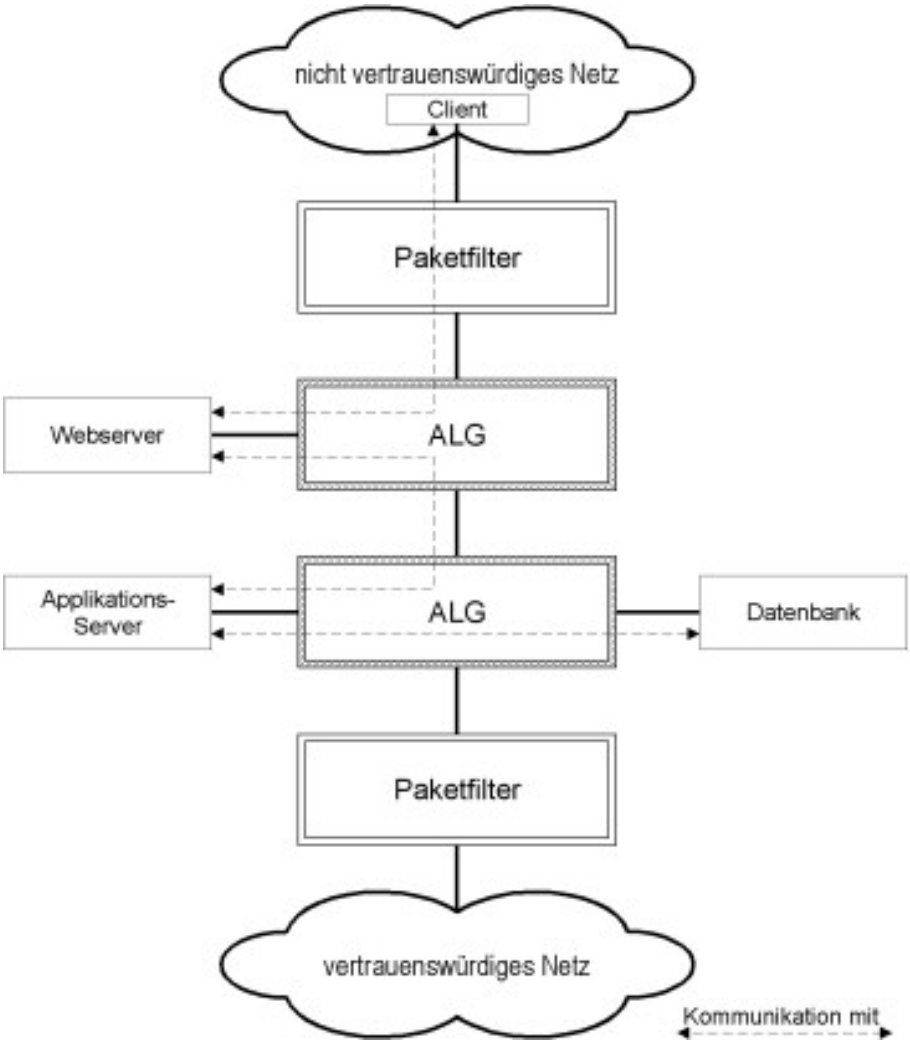
Turvalüüs on selliselt paigaldatud, et kõik serverid on ALG abil üksteisest eraldatud. Sellega hoitakse ära volitamata sissetungimised ühelt serverilt teisele ning kontrollitakse kasutuses olevaid protokolle. Mitteusaldusväärsest võrgust pärinevate rünnete eest parima kaitse pakkumiseks on veebiserver kaitstud nii paketifiltri kui ka ALG-ga. Ülesehitus on valitud selline, et iga server saaks rakendusega seoses ühenduse maksimaalselt kahe sideliiniga, mis on kaitstud vastavate ALG-dega. Järgnev tabel annab ülevaate sideliinidest.

Server	Side	Protokoll	Märkus
Veebiserver	välisvõrgu kliendiga	HTTPS	Krüpteeritud ühenduse saab lõpetada juba ALG juures Vaata ka M 5.115 Veebiserveri integreerimine turvalüüsi
Veebiserver	rakendusserveriga	Rakendusspetsiifilised programmid, näiteks SOAP; RPC, Corba jt.	Protokollide jaoks on samuti olemas turvaproksid
Rakendusserver	andmebaasiserveriga	Andmebaasiprotokoll	Vaata ka M 5 117 Andmebaasiserveri integreerimine turvalüüsi

Tabel: sideliinid

Lisaks on sisevõrgust administreerimiseks vajalikud veel juurdepääsuõigused. Neid tohib vastavalt kaitstud protokollide kaudu (näiteks SSH) anda üksnes administreerimisarvutitele. Kontrollida tuleks, kas asutuse sees tegutseva pahategija ründe ennetamiseks võiks füüsilisest ühendusest usaldusväärse võrguga täielikult loobuda.

Järgnev joonis näitab veel kord kirjeldatud arhitektuuri. Lubatud sideliinid on sisse kantud.

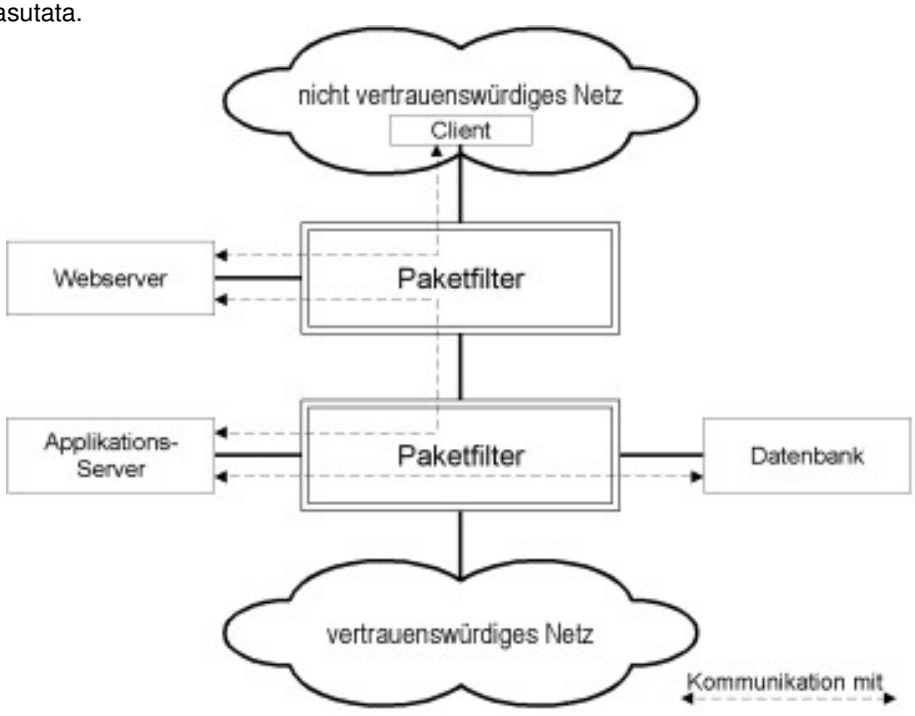


Mitteusaldusväärne võrk
Klient
Paketifilter
Veebiserver
ALG

Rakendusserver
Andmebaas
Usaldusväärne võrk
Side (millega)
Joonis 1: tüüpilise veebiserverist, rakendusserverist ja andmebaasist koosneva veebirakenduse ülesehitus.

Lihtsustatud arhitektuur ilma ALG-deta

Kui rakenduse kaitseks ei ole vaja esitada erinõudeid, võib loobuda ka ALG-de kasutamisest ning paigaldada veebiserver välise paketifiltri demilitariseeritud tsooni, rakendus- ja andmebaasiserver aga sisemise paketifiltri eraldi asuvatesse demilitariseeritud tsoonidesse. Kommunikatsioonisuhteid piiratakse sel juhul vaid vastavate paketifiltri reeglitega. Sellisel juhul puudub aga võimalus kontrollida kommunikatsiooni sisu. Kui loobutakse ALG-st kliendi ja veebiserveri vahel r everse-http-proxy), ei ole enam võimalik kontrollida mitteusaldusväärsest võrgust tulevate http-päringute vastavust http-spetsifikatsioonidele ega testida ebatavalist sisu (teatud kontekstis). On igati soovitatav kasutada kliendi juurdepääsuks veebiserverile vähemalt vastavat ALG-d (reverse-http-proxy). Järgnev joonis näitab lihtsustatud arhitektuuri kahe paketifiltriga. Kommunikatsioonisuhted on kirjeldatud nii, nagu eespool olevas tabelis, kuid protokolliga sobivaid turvaproksisid ei kasutata.



Mitteusaldusväärne võrk
Klient
Veebiserver
Paketifilter
Rakendusserver
Andmebaas
Usaldusväärne võrk
Side (millega)

Joonis 2: tüüpilise veebiserverist, rakendusserverist ja andmebaasist koosneva veebirakenduse ülesehitus ilma ALG-sid kasutamata.Seda, kas kasutuses olevale veebirakendusele piisab lihtsustatud ülesehitusest, tuleb iga üksikjuhtumi puhul eraldi välja selgitada. Otsuse vastuvõtmisel tuleb arvestada töödeldavate andmete kaitsevajadust, ning mitte mingil juhul ei tohi otsuse langetamisel lähtuda vaid kulutustest. Otsus ja selle vastuvõtmise põhjused tuleb dokumenteerida ning tingimuste võimalikku muutumist tuleb regulaarselt kontrollida. Arhitektuuri jätkuvat vastavust turvanõuetele tuleb tagada eriti veebirakenduste muutuste ja laienduste korral

Otsustamisel võiks lähtuda järgmistest punktidest:

- Veebirakendustele, millele on juurdepääs vaid suhteliselt usaldusväärsest võrgust, pakub enamasti küllaldast kaitset ka lihtsustatud ülesehitus.
- Kui veebirakenduse näol on tegemist rakendusega, millele pääseb juurde interneti kaudu või mille töödeldavad andmed on kõrge kaitsevajadusega, tuleks veebiserveri kaitseks internetist pärinevate rünnete eest kasutada vähemalt üht reverse-http-proxyt.
- Kui andmebaasiserveril, mis kuulub veebirakenduse juurde, käitatakse veel teisi andmebaase, tuleks otsustamisel arvestada ka nende andmete kaitsevajadusega. Sel juhul tuleb erilist tähelepanu pöörata andmebaasiserveri turvalisele ja hoolikale konfigureerimisele. Sel juhul on andmebaasile juurdepääsu ärahoidmiseks tungivalt vajalik kasutada turvaproksit.

Täiendavad kontrollküsimused:

- Milline arhitektuur on veebirakenduse jaoks valitud?
- Kas otsustuskriteeriumid on dokumenteeritud ja arusaadavad?

M 5.120 ICMP-protokolli käsitlus turvalüüsis

Algatamise eest vastutavad: Infoturbespetsialist

Rakendamise eest vastutavad: Administraator

Interneti kontrollsõnumiprotokolli (Internet Control Message Protocol - ICMP, spetsifitseeritud RFC 792) kui transpordikihi protokolli ülesandeks on vea- ja diagnoosiinformatsiooni transportimine IP jaoks. Süsteemisiseselt töötleb ja käivitab selle IP, TCP või UDP. ICMP-protokoll teab erinevateks otstarveteks mitmeid erinevaid nn. uudistetüüpe. Paljude kasulike funktsioonide kõrval on ICMP-s ka mõningaid selliseid uudiste tüüpe, mille abil on ründajatel võimalik hankida olulist informatsiooni võrgu kohta või mille kaudu on võimalik sooritada rünnakuid (vt G 5.50 ICMP-protokolli väärkasutus). Kahjuks ei ole ka radikaalne lahendus, milleks oleks ICMP blokeerimine turvalüüsis, rahuldav, kuna seetõttu ei ole teatud funktsioonid enam kättesaadavad. Käskudest nagu *ping* ja *traceroute* võib küll tavalistel töökohaarvutitel ja serveritel loobuda, aga ICMP globaalne blokeerimine turvalüüsis võib viia raskesti diagnoositavate mõjutusteni. Sellest tulenevalt tuleks mõelda sellele, et nii turvalüüsis ja vajadusel ka lokaalsel pakettfiltril tuleks võimaluse olemasolul teostada ICMP selektiivne filtreerimine. Seejuures tuleb arvestada arvuti kasutamiskohta (server või töökohaarvuti), turbevajadust ja eraldi olevate arvutite korral ka turvalüüsis teostatud meetmeid. Näiteks võib sisevõrgu jaoks lubada suurema hulga uudistetüüpe kui välisvõrgu jaoks.

ICMP teadet *Echo Request* (teatetüüp 8) edastatakse näiteks programmide poolt nagu käsureatööriist *ping* selleks, et teada saada, kas arvuti on põhimõtteliselt kättesaadav. Selle peale vastab arvuti *Echo Reply* ga (teatetüüp 0). Kui välisvõrgust tulev ICMP *Echo Request* lastakse sisevõrku, võib ründaja seda kasutada sisevõrgu “kaardistamiseks”. ICMP teade *Destination Unreachable* (teatetüüp 3) luuakse näiteks siis, kui võrk või arvuti ei ole kättesaadavad ning seda on võimalik kuritarvitada kõigi ühenduses olevate arvutite ühenduse katkestamiseks. Vaatamata sellele on teade *Destination Unreachable* vajalik ülemiste kihtide protokollide tööks. Näiteks on *Subtyp “Fragmentation Needed but the Don’t Fragment Bit was Set”* (teatetüüp 3, kood 4) tähtis kindla ühenduse maksimaalselt edastatava paketi suuruse väljaselgitamisel (*Path MTU Discovery).* ICMP teade *Redirect* (teatetüüp 5) edastatakse siis, kui lüüs tuvastab, et paketti on võimalik saata otse teise lüüsi juurde, mis tähendab, et siiani kasutati pikemat teekonda. Lühim teekond sisestatakse saatja marsruutimistabelisse. Ründajad saavad seda kuritarvitada üle ründearvuti marsruutide konfigureerimiseks. Seepärast tuleks ICMP *Redirect* teated turvalüüsis blokeerida. Teiste teadete puhul tuleb kaaluda, kas väljuvat informatsiooni on võimalik rünnakuks kuritarvitada.

Arvuti sisevõrgus

Järgnev tabel näitab turvalüüsi võimalikku seadistust, mis eraldab organisatsiooni sisevõrgu internetist. Need seadistused kujutavad endast enamikel juhtudel arvestatavat kompromissi turvalisuse ja funktsionaalsuse vahel:

ICMP teade	Sissetulevad	Väljuvad	Märkus
Echo Request (tüüp 8)	blokeerida	lubada	

Echo Reply (tüüp 0)	lubada	blokeerida	Võimaldab koos sellest ülevalpool paikneva seadistusega seestpoolt väljapoole „pingimist”, aga mitte vastupidi.
Destination unreachable (tüüp 3)	lubada	lubada	Vajadusel täpsem eristus vastavalt teatekoodile
Time exceeded (tüüp 11)	lubada	lubada	Vajadusel blokeerige väljuvad teated
Redirect (tüüp 5)	blokeerida	blokeerida	
Teised tüübid	blokeerida	blokeerida	

Tabel 1: ICMP sisevõrgus paiknevatele arvutitele

Kuna pingimine ei ole võrgu töös väga olulisel kohal, tuleks ka normaalse turbevajaduse korral mõelda *Echo Request* ja *Echo Response* täielikule sulgemisele. Kõrgemate infoturbenõuete korral tuleks väljuvate ICMP-tüüpide arvu veelkord vähendada.

„ Avalikud” serverid DMZ-is

Serveritele, mis paiknevad turvalüüsi demilitariseeritud tsoonis (DMZ) ja mis pakuvad avalikult ligipääsetavaid teenuseid, peaks olema lubatud lisauudistetüübid. Kaitse sisevõrgu struktuuri „väljanuhkimise” eest ei mängi siinkohal rolli, kuna need arvutid peavad nii või teisiti olema väljastpoolt kättesaadavad. Järgmist tabelit võib kasutada sellekohase pidepunktina:

ICMP teade	Sissetulevad	Väljuvad	Märkus
Echo Request und Echo Reply (tüübid 0 ja 8)	lubada	lubada	
Destination unreachable (tüüp 3)	lubada	lubada	Vajadusel täpsem eristus vastavalt teatekoodile
Time exceeded (tüüp 11)	lubada	lubada	
Source Quench (tüüp 4)	lubada	blokeerida	
Redirect (tüüp 5)	blokeerida	blokeerida	
Teised tüübid	blokeerida	blokeerida	

Tabel 2: ICMP “avalikele” serveritele DMZ-s

Turvalüüsi komponendid

Turvalüüsi komponendid peaksid tavalisele võrguliiklusele olema nii nähtama-

tud kui võimalik. Seepärast on nende süsteemide korral soovitatav mitte ühtegi ICMP teadet luua, ei iseseisvalt ega ka vastusena saabuvatele ICMP teadetele. Niivõrd kui vastavad konfiguratsioonivõimalused on olemas, on tark need seadistused antud süsteemis ka teostada. Vastasel juhul tuleks vastavad paketid välises pakettfiltris blokeerida.

ICMP kasutamine eriliste infoturbenõuete korral

Eriliste infoturbenõuetega IT-süsteemides ja võrkudes on soovitatav kõik ICMP teated blokeerida, ainsaks erandiks võiks olla uudistetüüp 3, uudistekood 4 ("*Fragmentation Needed but the Don't Fragment Bit was Set* "). See erand väldib probleeme nn " *Path MTU Discovery* ga"(Kindla ühenduse maksimaalse võimaliku paketisuuruse määramine).

ICMP sisevõrgus

Samuti on ICMP otstarbekas ka sisevõrgus kas täielikult või osaliselt blokeerida. Turvalüüsidel, mis eraldavad eriti kõrge turbevajadusega võrku tavalise turbevajadusega võrgust, on soovitatav seoses ICMP-ga kasutada samu seadistusi, mida kasutatakse sisevõrgu eraldamisel internetist.

ICMP ja *Stateful* Inspection

Mõned pakettfiltrite või turvalüüside tootjad võimaldavad oma toodetel ka ICMP jaoks teatud sorti Stateful Inspection it teostada. Lähtuvalt ICMP kasutusotstarbest ei ole see Stateful Inspection i jaoks aga väga sobilik. Vastava konfiguratsiooni vigasuse ja võrdlemisi väikese kasu tõttu ei ole soovitatav vastavaid suvandeid aktiveerida.

Täiendavad kontrollküsimused:

- Kuidas toimitakse ICMP-ga turvalüüsis?
- Milliseid ICMP teateid lastakse väljast sisse?
- Milliseid ICMP teateid lastakse seest välja?

M 5.121 Turvaline side mobiilseadme ja töökoha vahel

Algatamise eest vastutavad: IT-juht, infoturbe spetsialist

Rakendamise eest vastutavad: administraator, kasutajad

Mobiilsete lõppseadmete, näiteks süle- ja pihuarvutite kaudu on tihti ka reisil olles vajalik juurdepääs andmetele internetis või asutuse sisevõrgus. Selleks kasutatakse reeglina avalikke kommunikatsioonivõrkusid. Kuna ei asutus ega mobiilne töötaja saa avaliku kommunikatsioonivõrgu kasutamisel andmete konfidentsiaalsuse, tervikluse ja käideldavuse säilimist vajalikul määral mõjutada, on informatsiooni kaitseks vajalik rakendada täiendavaid meetmeid.

Üldiselt peab mobiilse lõppseadme ja asutuse LANi vahel andmete edastamisel olema täidetud järgmised turvanõuded:

- Edastatavate andmete konfidentsiaalsuse tagamine. Andmete piisavalt turvalise krüpteerimise kaudu edastamisel tuleb tagada, et ka kommunikatsiooni pealtkuulamise korral ei oleks võimalik teha järeldusi andmete sisu kohta. Selle juurde kuulub lisaks sobivale krüpteerimisprotseduurile ka sobiv võtmehaldus koos perioodilise võtmevahetusega.
- Edastatavate andmete tervikluse tagamine. Kasutatavad edastusprotokollid peavad võimaldama ülekantavate andmete muutuste äratundmist ning tekkinud muutuste kõrvaldamist. Sellised muutused võivad tekkida näiteks edastusvigade (tehnilised probleemid) või ründajapoolse teadliku manipuleerimise tõttu. Lisaks sellele võib andmete tervikluse tagamiseks olla otstarbekas kasutada digitaalseid allkirju.
- Andmete autentsuse tagamine. Andmete ülekandmisel peab olema võimalik usaldusväärselt kindlaks teha, kas kommunikatsioon leiab aset õigete osapoolte vahel. Sellega välistatakse teesklust või vahendusründeid. Selleks peab toimuma kommunikatsioonipartnerite vastastikune autentimine (näiteks digitaalsete sertifikaatide abil).
- Andmeedastuse jälitatavuse tagamine. Kommunikatsioon jälitatavaks muutmiseks on võimalik kasutada logimisfunktsioone, mille abil on hiljem võimalik kindlaks teha, millised andmed millal ja kellele üle kanti. Selleks vajalike mehhanismide tugevus sõltub edastatavate andmete kaitsevajadusest. Adekvaatsete meetodite ja süsteemide valikust ja kasutamisest annab ülevaate moodul B 1.7 Krüptokontseptsioon .

Kui mobiilseid lõppseadmeid kasutades on vajalik avalike võrkude kaudu asutuse ressurssidele juurde pääseda, on tungivalt soovitatav kasutada virtuaalset privaatvõrku (VPN). Vastavaid tooted pakuvad erinevad tootjad ning need on olemas praktiliselt kõigi kasutatavate platvormide jaoks. Juurdepääsu kõrge kaitsevajadusega andmetele ja süsteemidele ei tohi ilma vajalikke turvameetmeid rakendamata võimaldada.

Kui soovitakse juurde pääseda internetirakendustele, mille abil toimub tundlike andmete, näiteks isikuandmete, siseinformatsiooni või kontoandmete edastamine, on krüpteerimiseks vajalik kasutada vähemalt SSLi (vt M 5.66z SSL-i/TLS-i kasutamine kliendis).

Side teiste IT-süsteemidega

Mobiilsete lõppseadmete, näiteks süle- või pihuarvutite kasutamisel on tihti vajalik vahetada andmeid ka teiste IT-süsteemidega, näiteks äripartneritega. Ka juurdepääsuks internetile on tihti vajalik ühendus teiste IT-süsteemidega. See võib toimuda mitmel viisil, olenevalt sellest, milliseid tehnikaid osalevad seadmed toetavad, näiteks infrapuna- Bluetooth -, WLAN- või GSM-liideste kaudu. Sel juhul peaks ühelt poolt turvaliselt toimuma edastustehnikate kasutamine (lähemat teavet leiab infoetalonturbe vastavatest moodulitest), teiselt poolt peaksid aga oma IT-süsteemid olema turvaliselt konfigureeritud.

Nende hulka kuuluvad mobiilsete klientide korral turvameetmed, näiteks pääsukaitse, kasutaja autentimine, viirusetõrje, personaalne tulemüür, operatsioonisüsteemi tasandil failidele ja ressurssidele kitsendustega pääsuõiguste andmine, lokaalne krüpteerimine jne. Kui on vajalik ühendada mobiilne lõppseade võõrasse võrku või internetti, tuleks süsteemi põhimõtteliselt kaitsta personaalse tulemüüriga (vt M 5.91 Interneti-PC personaalse tulemüüri installeerimine).

Võõraste IT-süsteemide kasutamine

Võõra IT-süsteemi kasutamisel, näiteks internetikohvikus või näiteks failide vahetamiseks loodud ühenduse korral võõraste IT-seadmetega, peaksid kõik kasutajad teadlikud olema, et nimetatud süsteemid on ebaturvalised. Mitte mingil juhul ei tohi eeldada, et need on vabad kahjurvarast (näiteks arvutiviirustest või Trooja hobustest). Lisaks sellele tuleb alati järele mõelda, kas ja kuhu tundlik informatsioon võiks olla salvestatud, näiteks ajutistesse failidesse veebiproksi või brauseri vahemälus. Kõrge kaitsevajadusega andmetele või IT-süsteemidele ei tohiks sellistelt mitteturvalistelt süsteemidelt juurdepääsu olla.

Kõikides organisatsioonides peaks olema selgelt reguleeritud, millistele andmetele võib reisil olles juurdepääs olla, millistele mitte. Kõigile IT-kasutajatele peaks eelkõige selge olema, millistel tingimustel tohib toimuda andmevahetus välisvõrkude kaudu või otse võõraste IT-süsteemidega (vt M 2.217 Teabe, rakenduste ja süsteemide hoolikas liigitamine ja käitlus ja M 2.218 Andmekandjate ja IT-komponentide kaasavõtmise protseduurid).

Kontrollküsimused:

- Kas andmete edastamisel on andmed küllaldaselt kaitstud?
- Kas andmete vahetamisel pööratakse piisavat tähelepanu oma IT-süsteemi kaitsele?

M 5.122 Sülearvuti turvaline ühendamine kohtvõrguga

Algatamise eest vastutavad: administraator, infoturbeosakond

Rakendamise eest vastutavad: kasutajad, administraator

Sülearvutid kui mobiilsed IT-seadmed on rohkem ohustatud kui statsionaarsed IT-süsteemid, mille käitamine toimub vaid kontrollitud keskkonnas. Seetõttu on tähtis kindlaks määrata, milliseid eeskirju tuleb täita sülearvutite ühendamisel LANvõrku, et kahjurvara tõttu ei häiritaks LAN-võrgu ja teiste sellega ühenduses olevate IT-süsteemide turvalist käitamist. Kui sülearvuti pärast välisvõrgus kasutamist uuesti ettevõtte või asutuse võrku ühendatakse, tuleb kõigepealt aktuaalseid viiruste signatuure kasutades põhjalikult kontrollida, ega sülearvuti ole nakatunud.

Kui sülearvutid ühendatakse mobiilsel kasutamisel otse internetti, on tingimata vajalik neid kitsendustega konfigureeritud personaalse tulemüüri abil võrgust pärinevate rünnete eest kaitsta. Kaitseks kõikide võimalike rünnete eest ei piisa ainult viirusetõrje programmist. Samuti on vajalik hoida sülearvuti tarkvara ajakohasena ning installeerida õigeaegselt vajalikud turvapaigad. Enne töövõrku ühendamist on otstarbekas kontrollida, kas personaalne tulemüür, teised turvaprogrammid ja turvapaigad sülearvutis on aktuaalsed. Soovitatav on kontroll läbi viia automaatselt vastavate tööriistade abil, nii et turvalisusega seotud puuduste korral saaks juurdepääsu sisevõrgule blokeerida.

Sülearvutile installeeritud interneti-rakendusprogrammide, eelkõige brauserite ja meiliklientide käitamine peaks toimuma turvaliste sätetega (vt M 5.45 Veebibrauserite turvaline kasutamine ja M 5.57 Rühmatarkvara/meiliklientide turvaline konfiguratsioon). Eelseadistatud suvandite muutmine kasutaja poolt tuleks administratiivselt keelata. Lisaks sellele võiks kasutada tööriistu, mis piiravad brauseri funktsionaalsust, nii et selle käivitamine toimuks liivakasti (Sandbox) taolises keskkonnas.

Sertifikaadid/MAC-aadressid

Tuleb tagada, et iga suvaline sülearvuti ei omaks juurdepääsu LAN-võrgule. Enne, kui sülearvuti saab juurdepääsuõiguse LAN-võrgule, peab olema läbi viidud selle edukas autentimine autentimisserveri suhtes. Kontrollimaks, millised seadmed saavad põhimõtteliselt võrgupääsuõiguse, võiks näiteks kasutada seadmete sertifikaate või MAC-aadresse. Siinjuures tuleb aga silmas pidada, et MACaadresse on võimalik võltsida ning seetõttu ei saa neid autentimisel ainsa kriteeriumina kasutada.

Pääsupiirangud

Peab olema tagatud see, et VPNi kasutaja omaks LAN-võrgu serveritel juurdepääsu vaid tööülesannete täitmiseks vajalikele teenustele. Selle tagamine võiks toimuda näiteks kasutajast lähtuva autentimisega rakendustasandil ning paketifiltrite abil toimuva andmeedastuskontrolliga (ainuüksi paketifiltrite kasutamine ei ole IP-aadresside võltsitavuse tõttu piisav).

VPN

Välisvõrgus olevalt sülearvutilt peaks juurdepääs sisevõrgule toimuma eranditult kaitstuna VPN-ga. Kui asutus võimaldab tööga seotud meilide päringut veebi meililahenduse abil interneti kaudu, tuleb tagada, et meilide ülekandmine serverilt sülearvutile toimuks eranditult krüpteeritult (näiteks SSLi abil). Igatahes ei pea seejuures olema hästi kaitstud mitte ainult transpordikanal, vaid ka lõppsüsteem ise. Sülearvutit on võimalik kompromiteerida, kui lisaks VPN-le kasutatakse samal ajal ka standardprotokolle, näiteks HTTP või SMTP protokolle Internetis. Seetõttu tuleks sülearvutid võimalusel selliselt kaitsta, et olemasoleva VPN-ühenduse korral sisevõrguga ei oleks võimalikud teised ühendused (Split -tunneldus).

Seejuures tuleb tagada, et kõik kliendi saadetavad andmepaketid läheksid tunnelisse ning et aktsepteeritaks vaid läbi tunneli tulnud andmepakette. Seejuures tuleb ka jälgida, et lisaks VPN-ga kaitstud sülearvuti pääsule sisevõrku ei oleks samal ajal võimalikud teised võrgupääsud. Eriti tähtis on, et VPN-pääsude kasutamise ajal ei oleks sülearvutil aktiveeritud WLAN ega Bluetooth. Täiendavaid nõuandeid andmeedastuse turvalisuse tagamiseks leiab meetmest M 5.76w Sobivate tunnelduse protokollide kasutamine VPN-süsteemis . Mobiilne IT-süsteem võib kergesti sattuda valedesse kätesse. Ühendus sisevõrguga (tunneli rajamine) ei tohiks seetõttu toimuda automaatselt, vaid alles pärast autentimist.

DHCP

Dünaamilise hostikonfiguratsiooni protokolli kaudu jagatakse IP-põhistes võrkudes nendega ühendatud klientidele automaatselt välja ajutised IP-aadressid ning marsruuterite ja DNS-serverite info, nii et kasutaja ei pea internetiühenduse saamiseks arvutit enam konfigureerima. Kui DHCP on aktiveeritud, määratakse IT-süsteemile automaatselt kehtiv IP-aadress kohaliku võrguga ühendusse astumiseks ning sellega luuakse ka vaba juurdepääs kõigile ühiskasutuses olevatele kataloogidele ja draividele. Kui seda ei soovita, tuleks ühelt poolt DHCP sülearvutil deaktiveerida, kui seda ei vajata (sel juhul toimuks IP-aadresside jagamine käsitsi). Teiselt poolt tuleks IP-aadresside jagamisel lisaks MAC-aadressi kaudu kontrollida, kas kliendile tohib võrgupääsu anda.

Interneti kasutamine

Tuleb kindlaks määrata, kas sülearvutid tohivad astuda otseühendusse internetiga. Kriitiliseks punktiks seejuures on, et sel juhul hiilitakse mööda asutuse turvalüüsidest ja -mehhanismidest, mis võib endaga kaasa tuua turvaprobleeme.

On erinevaid võimalusi leida lahendus, mille valikul tuleks arvestada turvanõuete ja kasutuskeskkonnaga:

- Interneti otseühenduse keelamine. Selle lahenduse eeliseks on, et see on kõige lihtsamini rakendatav. Sellega kaasnevad aga ka kõige suuremad piirangud, mistõttu ei ole seda kerge läbi suruda.
- Erinevate kasutajatunnuste kasutamine. Operatsioonisüsteemi tasemel tuleks sel juhul rakendada kaht erinevat kasutajatunnust, üht üldiseks tööalaseks kasutamiseks ning teist internetile juurdepääsu saamiseks. Internetitunnusel peaksid olema vaid minimaalsed õigused.

- Erinevate partitsioonide/operatsioonisüsteemide installatsioonide kasutamine. Selle lahenduse korral kasutatakse erinevaid partitsioone, mis on näiteks erinevate operatsiooni- ja failisüsteemide kaudu võimalikult kindlalt eraldatud. Mida tugevam on eraldamine, seda kergem on takistada töökeskkonna kahjustamist internetist pärit kahjurvara või millegi muu taolisega.
- Virtuaalsed masinad. Sel juhul toimub interneti otsekasutamine üksnes üle operatsioonisüsteemi, mida käitatakse virtuaalses masinas (näiteks User Mode Linux , UML). Virtuaalse masina kaudu eraldatakse kasutatav brauser tegelikust hosti operatsioonisüsteemist tugevamini kui ilma virtuaalset masinat kasutamata. Selle variandiga kaasneb siiski jääkrisk, et kahjurprogramme, näiteks JavaScripti abil looduid, on võimalik kopeerimise ja kleepimise abil hosti operatsioonisüsteemi ja virtuaalse operatsioonisüsteemi vahel edasi-tagasi kopeerida. Hosti operatsioonisüsteem võib sel juhul järgmise VPN-ühenduse korral ebaturvalises seisundis olla.
- Alglaadimise CD-plaatide kasutamine. Selle lahenduse korral luuakse interneti kasutamiseks kirjutuskaitstud seadmelt, näiteks CD-ROM-ilt, internetivõimeline töökeskkond, mille kasutatavus on piiratud sellega, et vajalik IP-teave kantakse sisse käsitsi. Selleks võib kasutada näiteks Knoppix 'it, täielikult CD-lt käivitatavat funktsioneerimisvõimelist GNU/Linux-tarkvara kombinatsiooni (vaata ww.knoppix.org (undefined link to 'ISKE_kataloogid/7_Kataloog_M/M5/ww.knoppix.org')).
- Internetipääs ainult üle VPNi (üle Intraneti ja üle asutuse turvalüüsi interneti). Selle lahenduse eeliseks on, et ohtlikud materjalid sorteeritakse välja.

VPN-kasutamise autentimine

Enne VPNi ülesseadmist tuleks kontrollida kasutaja autentsust, rakendades selleks tugevaid autentimisprotseduure. Tugevad autentimisprotseduurid on näiteks ühekordsete paroolide või challenge-response mehhanismi kasutamine.

Logimine

Serveri teenuste kasutamine peaks logimise abil jälitatav olema. Seejuures peaks olema võimalik ka ära tunda, kas juurdepääs sülearvutilt serverile toimus ettevõttest või asutusest või väljastpoolt.

Ajutised andmed

Tuleks tagada, et kogu VPN-ühenduse loomist võimaldav vahesalvestatud autentimisteave kustutataks automaatselt pärast VPNi kasutamist. See kehtib nii tahtlikult kui ka tahtmatult lõpetatud VPN-ühenduste kohta. Lisaks sellele tuleks näiteks brauseril põhinevate SSL-VPN-ühenduste korral kogu vahesalvesti desaktiveerida, et ei toimuks autentimisteabe ajutist salvestamist, mis muudaks VPN-ühenduse taasloomise ründaja jaoks kergemaks.

Kontrollküsimused:

- Kas on olemas eeskirjad sülearvutite turvaliseks ühendamiseks LAN-iga?
- Kas kõik sülearvutid on kahjurkoodi ja võõrvõrkudest teostatud rünnete eest hästi kaitstud?
- Kas operatsioonisüsteemi ja installeeritud tarkvara uuendatakse pidevalt?

- Kas on olemas eeskirjad selle kohta, kas ja mil viisil tohib sülearvutitelt luua internetiühendust?
- Kas kõikide interneti-rakendusprogrammide käitamine toimub turvaliste sätetega?
- Kas on tagatud, et LAN-võrku saavad sisse logida vaid volitatud sülearvutid?
- Kas sülearvutite pääs VPNi kaudu välisvõrgust sisevõrku on kaitstud?

M 5.123 Võrgusuhtluse kaitse Windowsis

Algatamise eest vastutavad: infoturbe spetsialist, administraator

Rakendamise eest vastutavad: administraator

Windowsi taristu turvalisus ei sõltu ainuüksi üksikute süsteemide turvalisest konfiguratsioonist ja käitlusest. Kogu turvalisus sõltub olulisel määral ka võrgusuhtluse turvalisusest, mis omakorda sõltub muu hulgas sideliinide (allkirjad, krüpteerimine) kaitsest ning kasutatud autentimisprotseduuridest. Üldine reegel on, et olemasolevate liideste võrgukomponendid, mida ei kasutata (näiteks failide ja printerite ühiskasutusse andmine Microsofti võrgus), tuleb eemaldada. Hinnang selle kohta, millised võrguprotokollid eemaldada tuleks, tuleb anda konkreetseid asjaolusid arvestades igal üksikjuhul eraldi.

Turvaline kanal

Kliendi suhtlus domeenikontrolleriga toimub niinimetatud turvakanali kaudu, mida kasutatakse ka autentimisandmete edastamiseks. Turvakanali andmed krüpteeritakse seansivõtme abil. Selle kanali rajamiseks kasutatakse kliendi arvutikontot (haldamine toimub automaatselt Windowsi poolt). Arvutikonto parooli regulaarsed muutused on seetõttu turvakanali kaitsmisel olulise tähtsusega (vaata M 5.89 Turvalise kanali konfigureerimine Windowsis).

Suhtluse allkirjastamine ja krüpteerimine

Kõik andmed, mille edastamine toimub turvakanali kaudu, tuleks allkirjastada ja krüpteerida. Standardile vastavalt toimub see ainult siis, kui mõlemad suhtluspartnerid kasutavad samu protseduure. Kui üks partneritest ei toeta krüpteerimist või allkirjastamist, toimub suhtlus kaitseta (suunised Domeeni liige: Turvakanali andmed digitaalselt allkirjastada (kui võimalik) ja Domeeni liige: Turvakanali andmed digitaalselt krüpteerida (kui võimalik) Arvutikonfiguratsioon | Windowsi sätted | Turvasätted | Lokaalsed direktiivid | Turvasuvandid). Kui aktiveeritakse suunis Domeeniliige: Turvakanali andmed digitaalselt krüpteerida või allkirjastada (alati), tuleb suhtlus allkirjastada või krüpteerida. Kui mõlemad partnerid ei toeta samu protseduure, siis ühendust ei looda. SMB-protokoll (Server Message Block) ei toeta mitte ainult vastastikust autentimist, vaid võimaldab ka SMB-pakettide allkirjastamist.

Autentimise ja allkirjastamise abil on võimalik ära hoida vahendusründeid. SMBallkirjade konfigureerimiseks valige Arvutikonfiguratsioon | Windowsi sätted | Turvasätted | Lokaalsed suunised | Turvasuvandid järgmiste suuniste alusel:

- Microsofti võrk (Klient): Suhtlus digitaalselt allkirjastada (kui server nõustub),
- Microsofti võrk (Klient): Suhtlus digitaalselt allkirjastada (alati),
- Microsofti võrk (Server): Suhtlus digitaalselt allkirjastada (kui klient nõustub),
- Microsofti võrk (Server): Suhtlus digitaalselt allkirjastada (alati).

Vastavalt standardile ei ole SMB-pakettide allkirjad Windowsi all kohustuslikud, aktiveeritud on vaid suunis Microsofti võrk (Klient): Suhtlus digitaalselt allkirjastada (kui server nõustub). Suhtlus allkirjastatakse ainult juhul, kui SMB-serveril on pakettide allkirjastamine aktiveeritud. On ka võimalus muuta allkirjastamine kohustuslikuks. Selleks on vaja aktiveerida ülejäänud eespool loetletud suunised. Suuniste aktiveerimine SMB-suhtluse allkirjastamiseks võib mõju avaldada ühilduvu-

sele klientide, teenuste ja rakendustega. Seetõttu on enne nende sätete aktiveerimist vajalik läbi viia ühildumistestid. Kõik kolmandate tootjate SMB-serverid ei toeta autentimise käigus paroolide krüpteerimist. Juhul, kui sellise serveriga võetakse SMB-protokolli abil ühendust, võib parooli ülekandmine toimuda krüpteerimata, kui aktiveeritud on suunis Microsofti võrk (Klient): Krüpteerimata parool saata kolmandate tootjate SMB-serverile. Igatahes ei tohiks kaitseta paroolide edastamist lubada, st nimetatud suunis ei tohi olla aktiveeritud. Windows võimaldab rakendustasandil määrata kindlaks suhtluseks vajaliku sessiooni minimaalse turvalisuse (näiteks RPC-komponentide vahel). Järgmisi suvandeid on võimalik valida mõlemates suunistes - Võrgu turvalisus: sessiooni minimaalne turvalisus NTLM-SSP-l põhinevatele klientidele (kaasa arvatud turvalised RPC-kliendid) ja Võrgu turvalisus: sessiooni minimaalne turvalisus NTLM-SSP-l põhinevatele klientidele (kaasa arvatud turvaline RPC-server) , valides Arvutikonfiguratsioon | Windowsi sätted | Turvasätted | Lokaalsed suunised | Turvasuvandid:

- nõutav sõnumite terviklus,
- nõutav sõnumite konfidentsiaalsus,
- nõutav Mv2-sessiooni turvalisus,
- nõutav 128-bitine krüpteerimine.

Vastavalt standardile ei määrata kindlaks miinimumsuvandeid. Kui kõikidel arvutitel käitatakse kliendi operatsioonisüsteeme ja serveri operatsioonisüsteeme, tuleb suvandid aktiveerida NTLMv2-autentimiseks ja 128-bitiseks krüpteerimiseks.

Tugev autentimismehhanism

Autentimisprotseduuride kvaliteedil on turvalisuse tagamise seisukohast võrku logimisel samuti tähtis osa. Ühtekokku on võimalik kasutada kolme autentimismehhanismi: LM, NTLMv1 ja NTLMv2. Parimat kaitset pakub NTLM-protokolli versioon 2. Täielikes Windowsi võrkudes tuleks kasutada ainult NTLMv2, mis on kõige turvalisem meetod. Vanemate protokollide kasutamisest tuleks nende nõrkade külgede tõttu loobuda. Selleks tuleb juurdekuuluvas suunises Arvutikonfiguratsioon | Windowsi sätted | Turvasätted | Lokaalsed suunised | Turvasuvandid | Võrgu turvalisus: LANi haldaja autentimise tasand seadistada väärtus Ainult NTLMv2 vastused saata\ LM& NTLM keelduda. Paroolide muutmisel tuleks LAN-halduse räsiväärtuste salvestamine desaktiveerida. Selleks aktiveeritakse suunis Arvutikonfiguratsioon | Windowsi sätted | Turvasätted | Lokaalsed suunised | Turvasuvandid | Võrgu turvalisus: LAN-halduse räsiväärtuste salvestamist ei toimu järgmiseks paroolide muutmiseks.

Anonüümne juurdepääs

Anonüümne juurdepääs võrgu kaudu ei tohiks põhimõtteliselt võimalik olla (niinimetatud NULLSESSIOON). See funktsionaalsus tuleb välja lülitada, aktiveerides suunised Võrgupääs: anonüümset SID-/nimede tõlkimist mitte lubada, Võrgupääs: anonüümset SAM-kontode loendamist mitte lubada ja Võrgupääs: anonüümset SAM-kontode ja ühiskasutuste loendamist mitte lubada (valides Arvuti sätted | Windowsi sätted | Turvasätted | Lokaalsed suunised | Turvasuvandid).

Suunis Võrgupääs: anonüümsetele kasutajatele kõigi volituste andmine tuleb desaktiveerida. Windows 7 on anonüümsetele kasutajatele kõigi volituste andmine juba standardsättena desaktiveeritud.

Võrguside turvamine DirectAccessiga

Alates versioonidest Windows 7 ja Windows Server 2008 R2 võimaldab DirectAccessi funktsioon klienti püsivalt loogiliselt infokoosluse võrku ühendada, olenemata sellest, mis liiki võrguühendust kasutatakse. Võrguside kliendi ja teiste Windowsi domeeni kuuluvate arvutite vahel luuakse selle funktsiooni korral tunneldatud ühendusega. Tunnelit saab kasutada nii välisvõrkudest sisevõrgu suunal kui ka infokoosluse võrgu sees. Tunnel toimib seni, kuni Windowsi süsteemil on olemas võrguühendus. DirectAccessi kasutamisel rakendab klient ühenduse loomiseks infokoosluse võrguga sertifikaati ning ühendus luuakse juba siis, kui kasutaja end sisse logib. Seetõttu võetakse näiteks GPO värskendused ja uued poliitikad üle juba enne, kui kasutaja end oma konto alt sisse logib.

Pärast kasutaja sisselogimist aset leidvale andmesidele ei ole aluskonfiguratsioonis turvameetmeid üldse ette nähtud. Krüpteerimiskaitse rakendub üksnes klientide arvutite autentimisprotsessile. Seetõttu tuleks andmeedastust turvata sertifikaadipõhise IPSeciga. Selleks läheb tarvis PKI-d, mis tuleks üles ehitada infokoosluse võrgus. IPSeci konfigureerimisel tuleb järgida meedet M 5.90 IPSec'i protokolli kasutamine Windowsi keskkonnas . Windowsi klientides ei ole DirectAccessi jaoks eelseadistatud läbivalt ühesugust turvalogimist.

Seirevõimalusi leiab muu hulgas ka järgmistes asukohtades:

- gpedit.msc |. . . | Advanced Audit Policy Configuration | Logon/Logoff | IPSec. . .
- perfmon.exe | Performance Monitor | Available Counters (nt IPHTTPS, Teredo, IPSec, WFP).

Nende protokollide töömaht võib väga kiiresti kasvada ning arvuti töövõimet kahandada. Seetõttu tuleb turbeseadistused kõigepealt hoolikalt läbi kaaluda, arvestades nii DirectAccessi serverikomponentide kui ka infokooslusele kehtestatud nõuetega. Klientides tuleb tagada logimine.

Kontrollküsimused:

- Kas eemaldatud on kõik olemasolevate liideste võrgukomponendid, mida ei kasutata?
- Kas arvutikonto parooli muudetakse regulaarselt?
- Kas kõik andmed, mille edastamine toimub turvakanali kaudu, allkirjastatakse ja krüpteeritakse?
- Kas anonüümset juurdepääsu võrgust takistatakse?
- Kas autentimiseks ja 128-bitiseks krüpteerimiseks on suvand NTLMv2 aktiveeritud, kui kõikidel arvutitel käitatakse kliendi operatsioonisüsteeme ja serveri operatsioonisüsteeme?

- Kas on tagatud, et ka vanemad kliendid saavad autentimiseks kasutada NTLMv2 meetodit (näiteks vastavate hoolduspakettide või täiendava tarkvara installeerimisega)?
- Kas anonüümsetelt pääsudelt võrgu kaudu on ära võetud volitus „igaüks”?
- Kas turvasätteid on testitud ning kontrollitud nende ühildumist teenuste ja rakendustega?

M 5.124 Võrgupääsu korraldus nõupidamis-, ürituse- ja koolitusruumides

Algatamise eest vastutavad: IT-juht, infoturbeosakond
Rakendamise eest vastutavad: administraator

SAP-süsteem on lokaalse võrgu kaudu ühenduses SAP-klientide, brauserite, rakenduste ja teiste SAP-süsteemidega. Ka SAP-süsteemikomponentide vahel toimub andmevahetus. Kõikidel juhtudel edastatakse andmeid, mis vajavad kaitset. Need pole üksnes andmed kasutajate autentimiseks (näiteks kasutaja nimi ja parool, SSO-piletid, SAPSSO2- Cookie), vaid ka äritegevust puudutavad andmed, mille töötlemine toimub funktsioonide käitamisel. Seetõttu tuleb otsustada, kas ja millist kaitsemehhanismi tuleks suhtluse kaitseks kasutada.

Suhtlusmeetodid võib jagada peamiselt järgmistesse klassidesse:

- RFC-side: sel juhul edastatakse andmed klaartekstina. RFC-l põhinevad protokollid, näiteks DIAG, mida kasutavad SAP GUI-kliendid, pakivad andmed kokku. See pole siiski kaitsemehhanism. Lisaks sellele saab pakkimismehhanismi välja lülitada.
- HTTP-l põhinev side: andmete edastamine toimub klaartekstina.
- TCP/IP-side: andmete edastamine toimub klaartekstina.

Kaitset vajavate andmete edastamisel SAP-süsteemilt ja SAP-süsteemile tuleb need krüpteerida. Andmete kaitseks on võimalik kasutada erinevaid meetodeid. Seetõttu tuleb otsustada, milline meetod on kulusid ja efektiivsust silmas pidades kõige soodsam. Otsus tuleb jälitatavalt dokumenteerida.

IPSec'i kasutamine
IPSec pakub sideside üldist kaitset IP-tasandil. Kõik andmepaketid krüpteeritakse ja nende terviklus tagatakse. Selle meetodi eeliseks on, et SAP-süsteemi tasandil ei ole vaja enam täiendavat konfigureerimist teostada, kuna IPSec-kaitse konfigureeritakse operatsioonisüsteemi tasandil. Kui SAP-süsteemide käitamine toimub täielikes Windowsi võrkudes, on IPSec standardile vastavalt ja ilma lisakuludeta (näiteks litsentside muretsemiseks) olemas. Tekivad vaid administreerimiskulud konfigureerimise läbiviimiseks (vt M 5.90 IPSec'i protokolli kasutamine Windowsi keskkonnas). IPSec'i kasutamisel on kaitstud nii ABAP- kui ka Java-protokollistiku side.

SNC kasutamine
SAP-süsteemis on sideside võimalik kaitsta SNC (Secure Net-work Communications) abil. SNC on siiski ainult standardiseeritud liides, nii et SNC-ga ühilduvad arhiivid (ka SNC-arhiiv, SNC-moodul või SNC-juurutis) tuleb täiendavalt omandada, litsentseerida ja installeerida. SNC pakub erinevad kaitsetasemeid. Peamiselt pakutakse siiski ainult autentimist ja krüpteerimist. Olenevalt SNC-arhiivist on võimalik kasutada erinevaid algoritme. SNC pakub sideside üldist kaitset SAPsüsteemi tasandil.

SNC-juurutuste muretsemisel tuleb silmas pidada järgmist:

- Milliseid algoritme pakutakse? Valida tuleks piisavalt turvalised algoritmid ja piisava pikkusega võtmed. Firmaomaseid ja avalikkusele tundmatuid krüpteerimisprotseduure tuleb vältida.
- Milline on hinna- ja litsentsimudel? Suurtele ettevõtetele või asutustele võivad tekkida märkimisväärsed kulutused.
- Autentimine toimub SNC kasutamisel väljaspool SAP-süsteemi. Kuidas toimub SNC-kasutajate haldamine? Kas kasutajaid peab haldama eraldi tööriistade abil või integreeritakse nad olemasolevatesse haldusstruktuuridesse (näiteks LDAP-server, Windows Active Directory)?

SAP-süsteem annab tasuta käsutusse SNC-juurutused, mis on Windowsi all kasutatavad, kuid võimaldavad vaid autentimist. Siin on võimalik valida NTLMil ja Kerberosel põhinevate variantide vahel. SNC kaitseb kasutamisel ABAB- ja Java-protokollistiku sideside, tuleb aga iga kord eraldi konfigureerida. Teavet SAPdokumentatsiooni allikate kohta SNC-konfiguratsiooniks pakub meede M 2.346 SAP dokumentatsiooni kasutamine .

SSLi kasutamine
HTTP-põhiste pääsude jaoks on põhimõtteliselt soovitatav kasutada SSL-i. See kehtib ka sisesideside puhul SAP-süsteemi komponentide ja teiste komponentide vahel, mis pakuvad SSL-kaitse võimalust (näiteks LDAP-juurdepääs). Kuna SSL kasutab krüpteerimismehhanisme, SAP aga ei anna erinevate ekspordi/impordi eeskirjade tõttu erinevates riikides välja standard-krüpteerimismehhanisme, tuleb krüptoteek (SAP Cryptographic Library , SAP Cryptolib) täiendavalt installeerida. SSL-tugi ABAP- ja Java-protokollistikule tuleb eraldi installeerida. SSL räägib kasutatud kaitsemeetodi dünaamiliselt suhtluspartnerite vahel läbi. Seetõttu tuleks nõrgad meetodid lubatud meetodite nimekirjast (nn Cipher-Suite) kustutada.

Kontrollküsimused:

- Kas kaitset vajavate andmete edastamine SAP-süsteemilt ja SAPsüsteemile toimub krüpteeritult?
- Kas HTTP-põhise sideside käigus kasutatakse SSL-protokolli?

M 5.125 SAP-süsteemi siseneva ja väljuva side kaitse

Algatamise eest vastutavad: IT-juht, infoturbeosakond
Rakendamise eest vastutavad: administraator

SAP-süsteem on lokaalse võrgu kaudu ühenduses SAP-klientide, brauserite, rakenduste ja teiste SAP-süsteemidega. Ka SAP-süsteemikomponentide vahel toimub andmevahetus. Kõikidel juhtudel edastatakse andmeid, mis vajavad kaitset. Need pole üksnes andmed kasutajate autentimiseks (näiteks kasutaja nimi ja parool, SSO-piletid, SAPSSO2- Cookie), vaid ka äritegevust puudutavad andmed, mille töötlemine toimub funktsioonide käitamisel. Seetõttu tuleb otsustada, kas ja millist kaitsemehhanismi tuleks suhtluse kaitseks kasutada.

Suhtlusmeetodid võib jagada peamiselt järgmistesse klassidesse:

- RFC-side: sel juhul edastatakse andmed klaartekstina. RFC-l põhinevad protokollid, näiteks DIAG, mida kasutavad SAP GUI-kliendid, pakivad andmed kokku. See pole siiski kaitsemehhanism. Lisaks sellele saab pakkimismehhanismi välja lülitada.
- HTTP-l põhinev side: andmete edastamine toimub klaartekstina.
- TCP/IP-side: andmete edastamine toimub klaartekstina.

Kaitset vajavate andmete edastamisel SAP-süsteemilt ja SAP-süsteemile tuleb need krüpteerida. Andmete kaitseks on võimalik kasutada erinevaid meetodeid. Seetõttu tuleb otsustada, milline meetod on kulusid ja efektiivsust silmas pidades kõige soodsam. Otsus tuleb jälitatavalt dokumenteerida.

IPSec'i kasutamine
IPSec pakub sideside üldist kaitset IP-tasandil. Kõik andmepaketid krüpteeritakse ja nende terviklus tagatakse. Selle meetodi eeliseks on, et SAP-süsteemi tasandil ei ole vaja enam täiendavat konfigureerimist teostada, kuna IPSec-kaitse konfigureeritakse operatsioonisüsteemi tasandil. Kui SAP-süsteemide käitamine toimub täielikes Windowsi võrkudes, on IPSec standardile vastavalt ja ilma lisakuludeta (näiteks litsentside muretsemiseks) olemas. Tekivad vaid administreerimiskulud konfigureerimise läbiviimiseks (vt M 5.90 IPSec'i protokolli kasutamine Windowsi keskkonnas). IPSec'i kasutamisel on kaitstud nii ABAP- kui ka Java-protokollistiku side.

SNC kasutamine
SAP-süsteemis on sideside võimalik kaitsta SNC (Secure Net-work Communications) abil. SNC on siiski ainult standardiseeritud liides, nii et SNC-ga ühilduvad arhiivid (ka SNC-arhiiv, SNC-moodul või SNC-juurutis) tuleb täiendavalt omandada, litsentseerida ja installeerida. SNC pakub erinevad kaitsetasemeid. Peamiselt pakutakse siiski ainult autentimist ja krüpteerimist. Olenevalt SNC-arhiivist on võimalik kasutada erinevaid algoritme. SNC pakub sideside üldist kaitset SAPsüsteemi tasandil.

SNC-juurutuste muretsemisel tuleb silmas pidada järgmist:

- Milliseid algoritme pakutakse? Valida tuleks piisavalt turvalised algoritmid ja piisava pikkusega võtmed. Firmaomaseid ja avalikkusele tundmatuid krüpteerimisprotseduure tuleb vältida.
- Milline on hinna- ja litsentsimudel? Suurtele ettevõtetele või asutustele võivad tekkida märkimisväärsed kulutused.
- Autentimine toimub SNC kasutamisel väljaspool SAP-süsteemi. Kuidas toimub SNC-kasutajate haldamine? Kas kasutajaid peab haldama eraldi tööriistade abil või integreeritakse nad olemasolevatesse haldusstruktuuridesse (näiteks LDAP-server, Windows Active Directory)?

SAP-süsteem annab tasuta käsutusse SNC-juurutused, mis on Windowsi all kasutatavad, kuid võimaldavad vaid autentimist. Siin on võimalik valida NTLMil ja Kerberosel põhinevate variantide vahel. SNC kaitseb kasutamisel ABAB- ja Java-protokollistiku sideside, tuleb aga iga kord eraldi konfigureerida. Teavet SAPdokumentatsiooni allikate kohta SNC-konfiguratsiooniks pakub meede M 2.346 SAP dokumentatsiooni kasutamine .

SSLi kasutamine
HTTP-põhiste pääsude jaoks on põhimõtteliselt soovitatav kasutada SSL-i. See kehtib ka sisesideside puhul SAP-süsteemi komponentide ja teiste komponentide vahel, mis pakuvad SSL-kaitse võimalust (näiteks LDAP-juurdepääs). Kuna SSL kasutab krüpteerimismehhanisme, SAP aga ei anna erinevate ekspordi/impordi eeskirjade tõttu erinevates riikides välja standard-krüpteerimismehhanisme, tuleb krüptoteek (SAP Cryptographic Library , SAP Cryptolib) täiendavalt installeerida. SSL-tugi ABAP- ja Java-protokollistikule tuleb eraldi installeerida. SSL räägib kasutatud kaitsemeetodi dünaamiliselt suhtluspartnerite vahel läbi. Seetõttu tuleks nõrgad meetodid lubatud meetodite nimekirjast (nn Cipher-Suite) kustutada.

Kontrollküsimused:

- Kas kaitset vajavate andmete edastamine SAP-süsteemilt ja SAPsüsteemile toimub krüpteeritult?
- Kas HTTP-põhise sideside käigus kasutatakse SSL-protokolli?

M 5.126 SAP RFC liidese kaitse

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: administraator

Remote Function Call (RFC) on ABAP pinu jaoks primaarne kommunikatsiooniliides, mis tagab süsteemist-süsteemi-kommunikatsiooni. RFC-andmesidet toetab ka Java pinu, rakendades selleks Java Connector' it (JCo). Täiendavat viiteid SAP dokumentidele, mis käsitlevad RFC-andmesidet, leiate meetmest M 2.346 SAP dokumentatsiooni kasutamine .

RFC-volituste väljastamispiirangud

RFC võimelisi ABAP-programme (nimetatakse ka RFC toega komponentideks) juhitakse volitusobjektiga S_RFC. Iga RFC toega komponent eeldab vastavalt funktsioonidele täiendavaid volitusi, mida kontrollitakse läbi täiendavate volitusobjektide. Kuna aga nende käivitamine toimub enamasti läbi võrgu, kujutab RFC-liides endast SAP süsteemile ohtu, sest võimaldab seda distantsilt rünnata. Seetõttu tuleb RFC-volituste andmist planeerida ning kehtestada vajalikud piirangud. Volitusobjektiga S_RFC saab juhtida seda, millistele RFC-funktsioonikomponentidele on kasutajal võimalik ligi pääseda. Samas kehtivad aga volitusobjektile järgnevad olulised piirangud:

- piiranguid saab kehtestada ainult funktsioonigruppidele, kuna toetatakse ainult väärtust RFC_TYPE = „FUGR“.
- parameetri RFC_NAME, mis sisaldab puudutatud funktsioonigruppide loetelu, kontrollimine on piiratud kaheksateistkümnele märgile. Pikema loetelu sisestamine on küll võimalik, aga kontrollitakse siiski vaid esimest kaheksateistkümmet märki.

Juurdepääsu on seega võimalik väljastada vaid kõikidele ühe funktsioonigrupi sisse jäävatele funktsioonikomponentidele ning sõltuvalt olukorrast tuleb selleks luua isegi mitu volitust. Enamatel juhtudel ei tohiks S_RFC volitus võimaldada juurdepääsu kõikidele RFC-komponentidele. Vältida tuleks seadistust RFC_NAME="*". Sellega lülitatakse sisse juurdepääs RFC toega funktsioonimoodulitele, mida SAP süsteemis eksisteerib ühtekokku mitu tuhat. Niimoodi luuakse automaatne juurdepääs ka äsja installeeritud rakenduste ja moodulite RFC toega komponentidele. RFC-funktsiooni edukas käivitumine sõltub aga omakorda veel ka juurdepääsuõiguse kontrollimisest, mida teostab RFC-funktsioon iseseisvalt. RFC-volituste planeerimisel tuleb arvestada, et eksisteerivad erinevad RFC-tüübid (nt sünkroonsed ja asünkroonsed). Seetõttu tuleb juba planeerimisel arvestada ka erinevate tüüpidega. Java pinu jaoks ei ole S_RFC volitus oluline. Väljuvaid RFC-pöördusi saab piirata volitusobjektiga S_ICF, mis reguleerib juurdepääsu sihtpunktidele (vt M 4.263 SAP sihtpunkti kaitse).

Java pinu RFC

Java Connector (JCo) loob Java pinu jaoks võimaluse kasutada kommunikatsiooni toimimiseks RFC-d. Standardina kasutatakse sellises lahenduses süsteemikomponendist siiski vaid väljuvaid RFC-Call 'e (Java pinu kasutatakse RFC-Client funktsioonis). Pöördused leiavad aset kas oma ABAP pinus (nt selleks, et muuta käideldavaks ABAP pinu kasutajad ja rollid) või pöördutakse läbi sihtpunktide teistesse SAP süsteemidesse või välistesse RFC-serveritesse. Java Connector' i rakendamisel tuleb arvestada järgnevaga:

- Java pinu kasutab ABAP pinusse pöördumiseks (ABAP pinu) kasutajat SAP-JSF. Viimane tuleb installeerimistööde käigus varustada tugeva parooliga.
- Java pinus olevaid sihtpunkte (Destination-Service ’it) tuleb kaitsta volitamata juurde pääsude eest.
- Java pinu RFC-server-programmide puhul tuleb arvestada järgnevaga:
- RFC-serverid tuleb juurutada oma programmidega. RFC-serveri-instantse saab luua JCo-programmeerimisliidesega.
- JCo-RFC-Server-Implementation pakub ainuüksi puhtaid RFC-kommunikatsioonifunktsioone. Eriti oluline on see, et volituste kontroll ja haldamine toimuks enda juurutatud programmiga.

RFC-kommunikatsiooni kaitsmine SNC-ga

Olukorras, kus turbevajaduste analüüsist selgub, et kommunikatsiooniteid, kus kasutatakse RFC-d, on tarvis kaitsta, võib soovitada SNC-d. Täiendavat infot selle kohta leiate meetmest M 5.125 SAP-süsteemi siseneva ja väljuva kommunikatsiooni kaitse .

„ Trusted System“-suhete turvaline kasutamine

SAP süsteemide vahel on võimalik sisse seada ka usaldussuhted, mille puhul ei pea kasutajad RFC-pöörduse korral enam parooli sisestama. Pöörduse korral kontrollib usaldav SAP süsteem (Trusting System), kas pöördus on saanud alguse usaldusväärsest SAP süsteemist (Trusted System ’ist). Volitusobjektiga S_RFCACL on võimalik sihtsüsteemis juhtida seda, millised kasutajad tohivad ilma paroolita pöördusi töösse võtta. Muu hulgas on võimalik eristada SAP System-ID-d (SAPSID), mandanti ja pöördust tegevat transaktsiooni. Reeglina tuleb arvestada järgnevaga:

- Trusted System suhteid tuleks ellu rakendada vaid pärast küllaldast analüüsi ja riskide hindamist.
- Volitusobjektil S_RFCACL ei tohi olla määratlemata, “*” sisaldavaid seadistusi.
- RFC-sihtpunktidesse, mis lõpevad usaldavates SAP süsteemides, ei tohi salvestada kasutajainfot, kuna sellisel juhul pole usaldavates süsteemides enam võimalik eristada pöördusi tegevaid kasutajaid.

RFC-klient-programmid: sideinfo faili konfigureerimine

RFC-klientidele saab failiga „sideinfo“ luua globaalse konfiguratsiooni, mis juhib RFC-juurdepääsusid. Sellesse faili on võimalik lisada ka autentimisandmed, mida kasutatakse RFC-pöörduste (täpsemalt: selle aluseks oleva CPIC-kommunikatsiooni) loomiseks. Kõik andmed salvestatakse faili loetava teksti kujul. Seetõttu tuleb siinkohal arvestada järgnevaga:

- sideinfo faili kasutuselevõttu tuleb hoolikalt kaaluda.
- sideinfo failis sisalduvaid andmeid saavad kasutada kõik lokaalsed RFC-klient-programmid.
- sideinfo faili ei tohi salvestada autentimisinfot. Sisselogimise andmeid peab kasutaja käest küsima klientsüsteemi programm.
- Kasutajatel, kes käivitavad RFC-klient-programme, tohib sideinfo failile olla ainult lugemisõigusega juurdepääs. Kirjutusõigusega juurdepääsusid tohib võimaldada ainult volitatud administraatorile.

Sideinfo faili saab SAP süsteemis kasutada mitmes kohas ning on oluline rõhutada, et seda rakendab ka SAP Gateway .

Väliste (non-SAP) RFC-serverite turvaline kasutamine

RFC Software Development Kit -i (RFC SDK) abiga on võimalik koostada selliseid RFC-serveri-programme, mis pakuvad oma funktsioone RFC vahendusel. Väliste RFC-server-programmide rakendamisel tuleb arvestada järgnevaga:

- Välises RFC-serveris ei saa kasutada SAP standardseid turvamehhanisme ega protseduure (autentimist, autoriseerimist, haldamist).
- Saadaolevad turvamehhanismid sõltuvad eranditult juurutatud RFC-serveri-programmist.
- Kasutajaid ja volitusi saab hallata kas serveri-programmiga või väliste komponentidega. Võimalikud on ka sellised juurutused, mis võimaldavad RFC-funktsioone kasutada kõikidel pöördujatel, ilma kontrolle teostamata.

Seetõttu tuleks iseseisvalt loodavate programmide ning soetatava tarkvara puhul pöörata tähelepanu sellele, et soovitud turbenõudeid ka reaalselt täidetaks. Välise RFC-serverite installeerimisel tuleb arvestada, et installeeritaks vaid RFC-raamatukogu. Eriti oluline on tagada, et RFC baasil toimivate programmide arendamiseks kasutatav Software Development Kit (RFC SDK) poleks täies mahus installeeritud ega ligipääsetav. Selle peab tagama tarkvara levitamise protsess. Arvutites, kuhu tuleb installeerida RFC SDK, (nt arendustööks kasutatavates arvutites), tuleks juurdepääs „bin“-kataloogis (standardne andmetee: /Sap/rfcsdk/bin) asutavatele programmidele piirata SDK-installatsioonile. Programme on võimalik lisaks kõigele muule kasutada ka RFC-pöörduste tegemiseks SAP süsteemidesse (startrfc) või RFC-serverite käivitamiseks (rfcexec). Arvutite, kuhu on installeeritud RFC SDK, juurdepääsuvõimalused SAP süsteemidele (nt tootmisele) tuleb piirata võrgu tasandile.

secinfo faili konfigureerimine SAP Gateway jaoks

Välised RFC-server-programmid registreerivad end reeglina SAP süsteemi-komponendis SAP Gateway , mis tegeleb klient-pöörduste vahendamisega välistele RFC-server-programmidele. Neid on võimalik väljast laekuvate nõudmiste korral selgelt käivitada ka SAP Gateway poolt. Juurdepääsu- ja käivitamisvõimalusi, mis on saadaval välistele pöördujatele, juhitakse konfigureerimisfailiga secinfo . Seda faili ei looda automaatselt, mistõttu tuleb see kindlasti luua käsitsi. Olukorras, kus seda faili ei eksisteeri, ei rakendu ka mitte mingisugused piirangud, mis tähendab, et suvalisel isikul, kellel on vastav tehniline juurdepääs, on võimalik SAP Gateway -arvutis käivitada ükskõik millised programmid. Alustuseks piisab ka tühja faili loomisest, mis tagab, et volitusi ei eksisteeri. Seejärel võib hakata konfigureerima volitusi ja juurdepääsupiiranguid. Fail tuleb paigutada SAP Gateway data -kataloogi, täpsemalt Gateway -instantsi alla (standardne andmetee: /usr/sap//data). Olukorras, kus väliseid RFC-server-programme reeglina ei rakendata, on alternatiiviks profiiliparameetri „gw/rem_start“ kasutamine seadistusega „DISABLED“.

Täiendavad kontrollküsimused:

- Kas RFC-volitused läbisid planeerimisfaasi?
- Kas välja on jagatud minimaalsed RFC-volitused?
- Kas RFC-ühendustes, mille kaudu edastatakse tundlikku infot, kasutatakse kaitse otstarbel SNC-d?

- Kas juurdepääs RFC SDK installatsioonidele on piiratud?
- Kas on olemas secinfo fail?

M 5.127 SAP Internet Connection Framework (ICF) kaitse

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: administraator

SAP süsteemi hulka kuuluv Internet Connection Framework (ICF) võimaldab ABAP-pinu funktsioonidele ligi pääseda HTTP baasil toimivate pöördustega. Sellele lisaks toetab ICF ka Simple Mail Transport Protocol' i (SMTP-d). Kasutada on võimalik erinevaid teenuseid (Services). Teenuste ülesehitus on hierarhiline ja sarnaneb failisüsteemide puustruktuurile. HTTP-juurdepääsutee (URL-pathi osa) määratleb puustruktuuris kajastuv andmetee. ICF-i haldamiseks kasutatakse transaktsiooni SICF. ICF-i puhul tuleb arvestada järgnevalt loetletud soovitustega. Täiendavaid viiteid SAP dokumentatsioonidele leiate meetmest M 2.346 SAP dokumentatsiooni kasutamine .

Aktiivsed ICF-teenused

Sisse tuleks lülitada ainult vajalikud teenused. Iga aktiveeritud teenuse puhul peab olema teada, mis on selle funktsioon. Iga teenuse kohta on soovitatav lühidalt üles märkida, millist funktsiooni see täidab ning kas seda tohib sisse lülitada või mitte. Pärast SAP süsteemi installeerimist on kõik ICF-teenused desaktiveeritud. Sellele vaatamata on soovitav olukord siiski üle kontrollida. Kontrollida tuleks ka pärast värskenduste (updates) ja uute ICF-teenuste installeerimist. Teatud ICF-objekti täieliku ICF-puuhierarhia korraga aktiveerimist tuleb vältida. Teenused tuleb alati aktiveerida ühekaupa.

SSL-kaitse

ICF-teenuste juurdepääsude konfigureerimisel saab iga teenuse kaupa eraldi määrata, kas pöörduse andmeside peab olema SSL-iga kaitstud või mitte. Enamatel juhtudel võib SSL-i aktiveerimist teenuste jaoks koguni soovitada (vt M 5.125 SAP-süsteemi siseneva ja väljuva kommunikatsiooni kaitse), kuna see aitab andmeid kaitsta volitamata avalikustamise eest. Kuna ICF-objekti jaoks seadistatud omadused päranduvad alampuus edasi, piisab juurte sõlmpunktide konfiguratsiooni kohandamisest.

Autenditud juurdepääsud

Iga ICF-teenuse jaoks tuleb defineerida, millise autentimise variandiga sellele juurdepääsu võimaldatakse. Eriti kehtib see iseseisvalt loodud lahenduste kohta. Kasutajate autentimiseks on üldjuhul soovitav kasutada järgnevat konfiguratsiooni:

- anonüümsed sisselogimisandmed: jätta väärtused sisse kandmata
- Turvanõuded: SSL
- Basic Authentication : standardne SAP-kasutaja.

Juhul kui teenustele peab ligi pääsema anonüümselt, tuleb sisselogimisandmed loetleda valdkonnas „Anonüümsed sisselogimisandmed“. Kõik anonüümsed pöördused leiavad sellisel juhul aset sisse kantud kasutaja alt. Sellisel juhul tuleks rakendada eranditult tehnilisi, Service -tüüpi kasutajaid. Dialoogkasutajaid ei tohiks rakendada. Tuleb arvestada, et ICF-objekti jaoks defineeritud anonüümse juurdepääsu sisselogimisandmed kehtivad ka kõikidele alampuus asuvatele alamobjektidele. Erinevate objektide jaoks defineeritud erinevad sisselogimisandmed (nt klient, kasutaja, keel), mis seostuvad puu andmetee raames ühe kindla objektiga, võivad ka omavahel kattuda. Reeglina toimub pärast mõne ICF-teenuse, nt

Business Server Pages Application' i, (BSP) käivitamist alati ka tavaline, rakenduste poolt kasutatavate volitusobjektide kontroll.

ICF-haldus

Haldusalaseid transaktsioone SICF (ICF teenuse haldus) ja SMICM (ICF-Monitor) tuleb kaitsta volitamata juurdepääsude eest (volitusobjekt: S_TCODE). Tootmissüsteemides ei tohiks kasutada funktsioone, mis võimaldavad detailselt logida klientsüsteemide päringuid (nt Debugging, Trace, Runtime Analysis, Recorder). Veaolukordi tuleks uurida testimis- ja vastuvõtusüsteemis.

ICF-pääsuõigused

Isikud, kes kasutavad ICF-teenused, ei tohiks samaaegselt SAP süsteemile ligi pääseda dialoogliidese (SAPGui) kaudu, et vastavaid isikuid saaks liigitada Service-kasutajate alla. ICF-teenuste pääsuõigusi tuleks väljastada piirangutega. Volituste kontrollimiseks rakendatakse volitusobjekti S_ICF. ICF-teenuste juurdepääsuõiguste kontrollimiseks tuleb valida järgnev konfiguratsioon:

- andmevälja ICF_FIELD tuleb sisestada väärtus „SERVICE".
- andmevälja ICF_VALUE tuleb sisestada märgijada, mis on vastava ICF-teenuse jaoks sisse kantud asukohas „Service-Data/Service Options/SAP-Authorizations". Juhul kui mitme teenuse jaoks on sisestatud sama märgijada, saab juurdepääsu kõikidele nendele teenustele juhtida ühe volitusega (vt lisaks M 4.263 SAP sihtpunkti kaitse).

Vealehekülgedel kajastuvad andmed

ICF-teenuste veateadete leheküljed ei tohi sisaldada siseinfot. Eriti kehtib see enda poolt väljatöötatud teenuste kohta.

Täiendavad kontrollküsimused:

- Kas aktiveeritud on ainult vajalikud ICF-teenused?
- Kas iga teenuse kohta on teada sellele kehtivad autentimisnõuded?
- Kas juurdepääs ICF-haldusele on piiratud?
- Kas ICF-pääsuõiguste planeerimisel ja konfigureerimisel arvestatakse piirangute kehtestamise vajadusega?

M 5.128 SAP ALE (IDoc/BAPI) liidese kaitse

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: administraator

Application-Link-Enabling liidest (ALE) kasutatakse kommunikatsioonioistarbelise mehhanismina, et integreerida omavahel kas mitmete SAP süsteemide või muude väliste süsteemide erinevaid tööprotsesse. Selle liidesega transporditakse saatva ja vastuvõtva süsteemi vahel tööandmeid ja süsteemiandmeid (nt tsentraalselt toimiva kasutajahalduse korral). Andmed töödeldakse vastuvõtvates süsteemides automaatselt. Sel põhjusel tuleb ALE-liidest kaitsta. Siinkohal tuleb arvestada järgnevaga:

- ALE kasutab andmeedastuseks RFC-protokolli (täpsemalt: transaktsioonilist RFC-d, tRFC-d). Seetõttu tuleb ellu rakendada kõik RFC-d käsitlevad turvameetmed (vt M 5.126 SAP RFC liidese kaitse).
- Kaitsta tuleb saatva süsteemi ALE-sihtpunkte, kuna neisse peab talletama autentimisinfot (vt M 4.263 SAP sihtpunkti kaitse).
- Vastuvõtva süsteemi ALE-volitusi tuleb jagada piirangutega (vt M 4.261 Kriitiliste SAP volituste turvaline rakendamine).
- ALE-administraatorivolitusi tohib anda ainult volitatud administraatoritele.
- Vastuvõtvas süsteemis ei tohi eksisteerida ALE-administraatoriõigusi nendele kasutajatunnustele, mis on saatvates süsteemides sisse kantud ALE-sihtpunktide jaoks.
- Saatvates süsteemides ALE-sihtpunktide jaoks sisse kantud kasutajatunnused peavad vastuvõtvas süsteemis eksisteerima „Communication“-tüüpi kasutajatunnustena.
- Tavakasutajatel ei tohi olla mitte mingisuguseid ALE-volitusi.
- Väliste, mitte-SAP süsteemide jaoks tuleb ALE-liidese kasutamiseks vajalikud autentimisandmed turvalisel moel salvestada. Juurdepääs vastavale infole tohib olla kas ainult süsteemikomponentidel või ALE-administraatoritel.

Täiendavaid viiteid infole ALE-liidese turvaliseks muutmise kohta leiate meetmest M 2.346 SAP dokumentatsiooni kasutamine .

Täiendavad kontrollküsimused:

- Kas ALE-liides on turvaliseks muudetud?
- Kas välistes mitte-SAP süsteemides asuvad ALE-autentimisandmed on salvestatud nii, et need on volitamata juurdepääsude eest kaitstud?

M 5.129 SAP süsteemide HTTP teenuste turvaline konfiguratsioon

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: administraator

HTTP-liidese kaudu saab kasutada erinevaid SAP süsteemi teenuseid. SAP dokumentatsioonid leiate meetmest M 2.346 SAP dokumentatsiooni kasutamine . HTTP-d kasutatakse reeglina juurdepääsuks Java pinu funktsioonidele ja rakendustele. ABAP pinule HTTP-ga ligipääsemiseks tuleb kasutusele võtta Internet Connection Framework (ICF). HTTP-liidese konfiguratsioon peab olema üldjuhul alati turvaline, st pöördused, mis kannavad endas konfidentsiaalset infot, peavad olema kaitstud SSL-iga ning sisse tohib lülitada ainult need teenused, mida ka reaalselt tarvis läheb. Suuremate ohtudega on seotud järgnevad, HTTP abil kättesaadavad liidesed:

- SOAP-liides
- WebDAV-liides
- Content-Server -liides

SOAP-liides

Simple Object Access Protocol (SOAP) on protokoll, mis võimaldab kasutada Web -teenuseid. SAP süsteemi SOAP-liidese puhul tuleb arvestada järgnevaga:

- SOAP-liidesele (ABAP pinus ja Java pinus) tohib ligi pääseda alles pärast autentimist.
- SOAP-juurdepääsu tuleb turvata SSL-iga.
- ABAP pinus on olemas SOAP teenus, mis võimaldab käivitada RFC toega komponente (ICF-path: /sap/bc/soap/rfc). Juhul kui see on sisse lülitatud, saab HTTP vahendusel käivitada RFC-komponente. Niimoodi minnakse mööda tulemüüri kaitsefunktsioonist, mis peab turvama SAP süsteemi RFC-porti. Seetõttu tohib seda teenust sisse lülitada vaid koos piisavate turvameetmete rakendamisega. Sama kehtib ka XML-i baasil toimiva RFC-teenuse kohta (ICF-path: /sap/bc/xrfc).
- Java pinu poolt pakutav kaitse, WS-Security (Web Service Security , W3C ja OASIS-e standardkogumik), kehtib ainult SOAP-teate sees edastatavate andmete suhtes. Seetõttu ei ole rakenduse tasandil võimalik kontrollida, kas andmed edastati läbi autenditud või autentimata ühenduse. Olukorras, kus saatja identiteet on oluline, tuleks seetõttu autentimisandmeid kontrollida rakenduse raames. Selleks peavad SOAP-teated sisaldama ka autentimisandmeid. Andmeid tuleb kaitsta volitamata juurdepääsu eest.

Reeglina peab ka SOAP-i vahendusel käivitatud rakendus ise tagama oma turvalisuse, rakendades vastavat volituste kontrollimist.

WebDAV-liides

WebDAV-protokoll (Web-based Distributed Authoring and Versioning) võimaldab failisüsteemiga sarnanevat juurdepääsu andmetele, kasutades selleks HTTP-protokolli. WebDAV-juurdepääsuvõimalust võib pakkuda nii ABAP kui ka Java pinu vahendusel, eeldusel, et rakendatakse sobivaid tooteid või rakendusi. ABAP pinu puhul sobib selleks näiteks Knowledge Warehouse (KW, ICF-path: /sap/bc/kw/fs),

Java pinu puhul aga nt komponent nimega Collaboration Management (CM, SAP Enterprise Portal Component). Kuna WebDAV-pöörduse sihtpunktiks võib sõltuvalt olukorrast olla ka lokaalne failisüsteem, tuleb failisüsteemi kaitsta volitamata juurdepääsude eest. Siinkohal on küll esmatähtis WebDAV-i poolt pakutavate andmete kaitse, kuid teisalt, kui ründe toimepanijal tekib nõnda juurdepääs lokaalsele failisüsteemile, võib see luua pinnase, millelt saab hakata ette valmistama uusi ründeid. Seetõttu peaks juurdepääsu võimaldama ainult koos autentimisega ning SSL-i rakendades. Lisaks tuleb alati silmas pidada ka volituste väljastamist.

Content-Server -liides

Content-Server -liidesega on võimalik ligi pääseda dokumendiarhiividele (Repositories). Juhul kui liides on kaitseta, saab hankida andmeid ja dokumente saadaolevate dokumendiarhiivide kohta. Tuleb arvestada järgnevaga:

- Content-Server -liidese (ICF-path /sap/bc/contentserver) võib aktiveerida ainult siis, kui seda reaalselt tarvis läheb.
- Juurdepääs peaks olema võimalik alles pärast autentimist ning kasutada tuleb SSL-i.
- Administraatoriliidese juurdepääs peab kohustuslikus korras nõudma parooli sisestamist. Selleks tuleb faili ContentServer.ini parameetrile „AdminSecurity“ anda väärtus „1“.
- Tuleb arvestada, et SAP süsteemi sees tuleb administreerimiseks kasutada transaktsiooni CSADMIN (samuti ICF-seadistusi) ning väljaspool SAP süsteemi (nt ini -faili).

Täiendavad kontrollküsimused:

- Kas HTTP-serverile on tagatud baasturve?
- Kas aktiveeritud on ainult vajalikud teenused ning kas mittevajalikud teenused on desaktiveeritud?
- Kas SOAP-liides on turvaliseks muudetud?
- Kas saadaolev WebDAV-liides on turvaliseks muudetud?
- Kas Content-Server -liides on turvaliseks muudetud?

M 5.130 Salvestisvõrgu (SAN-i) kaitse segmenteerimise abil

Algatamise eest vastutavad: infoturbeosakond

Rakendamise eest vastutavad: administraator

Storage Area Network 'i loomiseks kasutatakse tihti Fibre-Channel tehnoloogiat (FC-SAN). Süsteem koosneb ühest või mitmest kommutaatorist, salvestamise alamsüsteemidest nagu kettaalamsüsteemidest või varundamisseadmetest nagu nt lindiajamitest. Üks või mitu kommutaatorit, mis on omavahel ühendatud, moodustavad struktuuri (fabric).
Kommutaatorite külge ühendatakse serverid, mille salvestiruum seotakse SAN-i ressurssidega. Salvestamise alamsüsteeme, servereid ja nende operatsioonisüsteeme on võimalik üksteisest sõltumatult siduda ka mitmete erinevate ressurssidega. Nii nt on võimalik siduda erinevate serveritega erisuguseid, ühe salvestisüsteemi (loogilisi) salvestamisressursse, teisalt jällegi on võimalik ühe serveriga siduda mitmeid (ruumiliselt teineteisest eraldatud) salvestuskomponente, et tekitada serveri ja selle rakenduste tarbeks liiasus.

Seetõttu tuleb kohandada SAN-i salvestusressursside haldamist ja volituste väljastamist. Tuleb tagada, et andmed ei hävineks vale juurdepääsu tagajärjel ning et serverid töötaksid SAN-is vaid sellise salvestusühikute lõiguga, mida nad võivad pidada „isiklikuks". Selle saavutamiseks jagatakse SAN kas segmentideks või gruppideks, et omavahel saaksid suhelda ainult ühisesse segmenti kuuluvad seadmed.

Segmentideks jaotamine toob endaga kaasa muuhulgas järgnevad eelised:

- Salvestikomponente, mille puhul on esinenud koostalitlusprobleeme, saab nõnda rakendada teineteisest lahutatud segmentides.
- Oluliste rakendustega on võimalik ühekaupa siduda porte, et tagada vajalik ribalaius.
- Tundlikke andmeid on võimalik teistest paremini isoleerida.
- Parem skaleeritavus, kuna uued lõppseadmed ei saa kõikide teiste seadmetega kohe piiramatult suhtlema hakata.

Mõistliku segmenteerimise tagamiseks tuleks luua SAN-ressursside liigitamise kontseptsioon. SAN-ressursside kehtiv liigitus peab olema alati dokumenteeritud ning avariijuhtumitel peab see käepärast olema. Ressursside kehtivat liigitust peab saama hõlpsasti ja ülevaatlikult tuvastada administreerimistööriistade abil.

FC-SAN-die segmenteerimine

FC-SAN-is kasutatakse seadmete süsteemisiseseks haldamiseks ja liigitamiseks identifikaatorit World Wide Names (WWN). Teatud määral sarnanevad need Ethernet-võrguadapterite MAC-aadressidega. FC-SAN-i segmenteerimine leiab aste tsoonidesse jagamise teel (zoning). Zoning -funktsioone konfigureeritakse SAN-i kommutaatorites. Tsooni alla võivad liikmetena kuuluda server, salvestamise alamsüsteemid ja teised kommutaatorid.

Soft Zoning

SAN-seadmetel on olemas kindel WWN. Soft Zoning funktsiooni puhul luuakse tsoonid WWN-ide grupeerimise teel. Switch -pordid ja SAN-seadmed liigitab

tsoonide alla SAN-i süsteemisisene nimeserver. Olukorras, kus mõni SAN-seade logib ennast struktuuri (fabric), edastab nimeserver ainult samasse tsooni kuuluvate seadmete WWN-e.
Soft Zoning on paindlik lahendus, kuna see ei sõltu paigaldatud kaablitest. Seetõttu pole selle protseduuri puhul tarvis teha sissekandeid SAN-seadmete asukohtade muutumise kohta. Samas tuleks siiski arvestada, et andmete edastamist kehtivatesse WWN-idesse ei ole võimalik tõkestada. Kuna mõningad operatsioonisüsteemid salvestavad enda sisse ka WWN-e ja hoiavad neid vahemälus (cache), võib juhtuda, et selline süsteem võib luua ühendusi salvestisüsteemidega, mida administraator ei ole vastava tsooni alla liigitanud. Sellega võivad kaasneda andmekaod.
Soft-tsoneerimise riski peaks analüüsima just eriti kaitset vajavate andmete korral ja otsustama, kas see on asutuse jaoks vastuvõetav või mitte.

Hard Zoning

Hard Zoning defineeritakse reeglina läbi portide, mõnikord ka WWN-mehaanika abil. Mõiste Hard Zoning tuleneb sellest, et protsess on sageli tihedalt seotud SAN-kommutaatori lülitustega (ASIC-dega), st riistvaraga. Soft-Zoning seevastu teostatakse kõikidel tasanditel riistvaraga. Hard Zoning protseduuri tähistatakse sageli veel ka nimega Port-Zoning. SAN-i segmenteerimine tagatakse sellega, et SAN-kommutaatorite marsruutimistabelitesse luuakse tsoonid eranditult kommutaatorite pordinumbrite baasil. Selle tagajärjel kuuluvad ühtsesse tsooni täpselt need seadmed, mille portide numbrid on liigitatud ühise tsooni alla. Staatiline liigitus kehtestab olukorra, kus erinevatesse tsoonidesse kuuluvate portide vahel andmesidet ei toimu.

Kehtiv piirang, mille kohaselt tuleb riistvara konfiguratsioonis aset leidvad muudatused ja SAN-seadmete asukohtade muutumine tabelisse sisestada käsitsi, on praktikas peaaegu alati jõukohane. Kuna salvestivõrkude puhul esineb sagedasi muudatusi suhteliselt harva, tuleks andmekadude vältimiseks eelistada Hard Zoning või mõnda muud, teiste tootjate sarnast protseduuri. Lisaks tuleks igasse tsooni koondada alati ainult väikseim võimalik arv seadmeid.

Kuna volitamata isikute füüsiline juurdepääs riistvarale on tavaliselt keeruline, peetakse Hard-tsoneerimise saavutatavat turbeastet kõrgemaks kui Soft-tsoneerimise kaudu saavutatavat turbeastet. Suurema kaitsevajadusega andmete korral tuleks seetõttu rakendada Hard-tsoneerimist. Suurenenud turvalisus peaks aga olema mõistlikus suhtes suuremate kuludega.

Hard- ja Soft-tsoneerimise kombinatsioon

Kirjeldatud tsoneerimismeetodite kombineerimine toimub tsoonide moodustamisega üheselt mõistetavate WWN-ide abil, määrates samal ajal sellise rühma kommutaatoritele spetsiifilised pordinumbrid. See võimaldab takistada kõiki spetsiifilisi ründeid.

Sellega kaasnev halduskulu suureneb vastavalt tsoneerimisvariantide eraldatud

kasutamise suhtes. Seda varianti soovitatakse seetõttu ainult eriti suure kaitsevajaduse korral või ka madalama kaitsevajaduse korral, kui kulutused end õigustavad.

LUN Binding ja Masking

SAN-i kuuluvad kõvaketta alamsüsteemid võimaldavad kettaid kasutada loogiliste ühikutena (logical units). Ühikuid on võimalik adresseerida nende LUN-ide (Logical Unit Number) alusel. Selleks, et iga arvuti, mis kuulub mõnda tsooni, mille hulka kuulub ka kõvaketta alamsüsteem, ei näeks kõiki selle süsteemi loogilisi või füüsilisi kettaid, saab kasutada LUN Binding ja LUN Masking protseduuri. LUN Binding seob LUN-idele tehtavad pöördused kindlalt salvestisüsteemide teatud Fibre Channel Port idega ja võimaldab seeläbi LUN-ide adresseerimiseks kasutada ainult teatud kindlaid võrgujuurdepääse. LUN Masking protseduuri puhul defineeritakse lisaks eelnevale ketaste alamsüsteemides veel ka juurdepääsutabelid, kuhu kantakse juurdepääsu omavate serverite kindlad WNN aadressid. Kõik ülejäänud (maskeeritud) kettad on arvutitele nähtamatud. Niimoodi mõjub ühe SAN-ühendusega arvuti vigane konfiguratsioon või vale käsitsemine ainult nendele ketastele, mis on selle arvuti jaoks nähtavad. Serverite ja salvestisüsteemide liigitamisel SAN-is tuleks alati Zoning ja LUN Masking funktsiooni omavahel kombineerida.

Virtuaalsed SAN-id (VSAN-id)

Sarnaselt sellele, kuidas on võimalik segmenteerida LAN-e, moodustades virtuaalseid osavõrke (VLAN-e), on võimalik segmentideks jaotada ka SAN-e. Selline lahendus avardab Zoning -kontseptsiooni ja võimaldab ühelt poolt paremini kaitsta nii andmete kui ka rakenduste juurdepääse ning teisalt ära hoida rikete laiema leviku, piirates rikete mõju kindlale võrguosale.

VSAN-i puhul ühendatakse omavahel mitu porti ja seeläbi ühe Fibre Channel Fabric' u mitu lõppseadet üheks virtuaalseks struktuuriks (fabric). Niimoodi luuakse ühes ja samas füüsikalises võrgu infrastruktuuris mitu virtuaalselt teineteisest lahutatud struktuuri. Kommutaator võib antud lahenduses kuuluda korraga mitmesse SAN-alamvõrku. Iga VSAN-i jaoks seatakse sisse eraldi Fabric -teenused nagu nimeserver ja Zoning. Seega ei piira VSAN-id lisaks puhtale Zoning -funktsioonile mitte ainult lõppseadmete vastastikust nähtavust, vaid ka Fabric -konfiguratsioonide vastastikust nähtavust.

Zoning -funktsioon toimib lahutamisest sõltumatult VSAN-is. Tsoon ei saa ennast laiendada korraga mitme VSAN-i peale. Zoning -funktsiooniga reguleeritakse seametevahelist juurdepääsu ja andmevoogu. Lisaks on VSAN-iga võimalik alamvõrgus pakutavaid teenuseid isoleerida ning VSAN-i piires „kapseldada". Juhtudel, kus rakendatakse vaid Zoning -funktsiooni, moodustab kogu salvestivõrgu riistvara kokku ühe ainsa „Turvadomeeni". Olukorras, kus salvestivõrgu võrguriistvaras konfigureeritakse VSAN-id, jaotatakse riistvara erinevatesse loogilistesse „Turvadomeenidesse". Niisuguse domeeni sees saab seejärel kasutusele võtta „domeenisisesed" mehhanismid nagu Zoning ja Port Binding.

iSCSI segmenteerimine

iSCSI salvestivõrgu segmenteerimine toimub sarnaselt sellega, kuidas ühen-

datakse läbi FC-SAN-i külgeühendatud seadet. Erinevus seisneb serveri ja salvestiseadme vahelise ühenduse liigitamises. iSCSI-HBA (Host Bus Adapter) varustatakse tähistusega “Initiator” ja salvestiseadme port saab tähistuse „Target“. Mõlemad pooled seotakse omavahel kaasasoleva haldustarkvaraga, mis võtab aluseks kummagi IP-aadressi. Ühenduse loomise turvamiseks ja selleks, et tagada initsiaatori (=serveri) ja sihtmärkide (=kõvaketaste) autentsus, kasutatakse turvaprotokolle nagu CHAP (Challenge Handshake Authentication Protocol) või iSNS (Internet Storage Naming Service).

Liigitus, kuidas jaotuvad kõvakettad kõvaketaste alamsüsteemisides külgeühendatud arvutite suhtes, võib baseeruda nagu FC-SAN-ides kas LUN Binding või LUN Masking funktsioonil.

iSCSI kasutamisel soovitatakse rakendada nn võrguadaptereid koos TCP/IP Offload Engine’iga (I/OAT). Need vabastavad serveri intensiivsetest arvutustoimingutest tegelike iSCSI-andmete lahtipakkimisel TCP/IP-pakettidest.

Kontrollküsimused

- Kas SAN-ressursside liigitamise kohta serverite suhtes on olemas kirjalik kontseptsioon?
- Kas hetkel kehtiv tsoneerimiskonfiguratsioon on dokumenteeritud ning kas see on hädaolukordade jaoks käepärast?
- Kas ajakohane ressursside jaotus on haldustööriistade kasutamisel lihtsalt ja ülevaatlikult äratuntav?
- Kas turbenõuete ja halduskulude põhjal otsustati, millist segmenteerimist millises olukorras kasutatakse?

M 5.131 Windows Server 2003 IP-protokollide kaitse

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: administraator

Pärast standardset installeerimist on aktiveeritud TCP/IP-pinu. Eelseadistatud turvaseaded on kompromiss, kus ühel poolel asub turvalisus ning teisel poolel ühilduvus vanemate versioonidega ja avatus teiste süsteemide suhtes. Sellest piisab vaid väga üksikutel juhtudel ning sedagi ainult suurte piirangutega, mistõttu tasuks kaaluda alusseadistuste viimist kõrgemale turbeastmele. Täiendavaid seadistusi selleks, kuidas ennetada Denial-of-Service -tüüpi ründeid, leiate meetmest M 4.279 Windows Server 2003 laiendatud turvaaspektid . Alates versioonist Windows Server 2003 koos remondipaketiga Service Pack 1 rakendab Turvakonfiguratsiooni abiline (SCW) Denial-of-Service -tüüpi rünnete ennetamiseks (vt G 4.22 Tüüptarkvara turvaaugud või vead) teatud laiendatud seadistusi mõningate rollide puhul automaatselt (vt M 2.366 Windows Server 2003 turvamallide kasutamine).

Internet Protocol Suit 'i kommunikatsiooniprotokollid

Mõningaid TCP/IP-pinu protokolle saab soovi korral konfigureerida. Tegu on operatsioonisüsteemi turvastruktuuriga integreeritud protokollidega, kuid nende integreerimise kvaliteet on väga erinev ning need ei taga sageli piisavat autentimist ega ka tervikluse kaitset. Pärast standardset installeerimist on kõik Windows Server 2003 süsteemi ebaturvalised protokollid konfigureerimata. Juhul kui installeeritakse mõni vabalt valitav protokoll, tuleb konfigureerida vastavalt selle rakendusalale ja soovitud turbeastmele ka andmevahetuse turvet tagavad mehhanismid (nt krüptograafilised funktsioonid ja autentimisfunktsioonid). Ülevaate Internet Protocol Suit 'i protokollidest erinevate Windows Server 2003 valdkondade lõikes leiate infosüsteemide etalonturbe abivahendite alt. Nendes materjalides antakse ka nõuandeid vastavate protokollide turvaliseks rakendamiseks. Eriti suurel määral mõjutavad Windows-Server-2003 infrastruktuuri turvalisust ja stabiilsust protokollid, mis tegelevad IP-aadresside laialijagamisega (DHCP) ja nimeteisendusega (DNS ja WINS). Nende tarbeks tuleb kasutusele võtta sobivad kontseptsioonid, milles arvestatakse iga valdkonna erivajadustega. Täiendavat abimaterjali vajaliku turbeastme saavutamise kohta leiate infosüsteemide etalonturbe abivahendite alt. Ülejäänud protokollitüüpe nagu IP-Routing -, Multicast - ja Quality-of-Service -protokolle (QoS) rakendatakse juhtudel, kus server on konfigureeritud spetsiaalsete rollide tarbeks. Ülejäänud juhtudel tuleks need välja lülitada. Turvalise käitamise tagamiseks kehtib reegel:

- välja tuleb valida kõige paremini sobiv protokoll ning kõik ülejäänud protokollid tuleb desaktiveerida.
- Eriti hoolikalt tuleb tervikluse ja krüpteeritud autentimise eest seista Windows-Server-2003-keskkonna rakenduskihi protokollide puhul, kasutades võimalusel kas NTLMv2-e või Kerberost.
- Kõrgema kaitsevajaduse puhul tuleb kasutajaandmed krüpteerida.
- Soovitud protokolli rakendamine tuleks defineerida IT-kooslusele ja puudutatud IT-süsteemidele kehtivas poliitikas, mis peaks sõnastama lisaks ka turvanõuded.
- Juhul kui mõni soovitud protokoll ei peaks vastama Windows Server 2003 keskkonna turvanõuetele, tasuks kaaluda IPSec 'i kasutuselevõttu (vt M 5.90 Protokolli IPSec kasutamine Windowsi keskkonnas).

Dokumentatsioon

Kõik aktiivsed võrk-protokollid tuleb välja selgitada. Olukorras, kus serveri konfigureerimiseks on kasutatud SCW malli, piisab minimaalse dokumentatsiooni loomiseks vastavast mallist. Iga protokolli kohta tuleb dokumenteerida efektiivsed autentimis- ja krüpteerimismeetodid, samuti protokolli kasutusvaldkond.

Täiendavad kontrollküsimused:

- Kas serveri TCP/IP-pinu on piisavalt DoS-rünnete vastu kaitstud?
- Kas ebaturvalised protokollid on konfigureerimata?
- Kas kõik ebavajalikud võrk-protokollid on välja lülitatud?
- Kas DHCP, DNS ja WINS protokollide turbevajadusi on hinnatud erinevalt, lähtudes nende kasutusvaldkondadest ning kas nende protokollide joaks on välja töötatud ja ellu rakendatud sobiv infrastruktuuri kontseptsioon?
- Kas kõik valikulised IP-protokollid on piisavalt turvatud, nt autentimise ja krüptograafiliste protseduuridega?

M 5.132 Windows Server 2003 WebDAV turvaline kasutamine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: IT-juht, administraator

Kasutuselevõtu planeerimine

Web Distributed Authoring and Versioning (WebDAV) võimaldab juurdepääsu Windows 2000 Serveri/Windows Server 2003 failidele läbi HTTP-toega võrguühenduse. Windows Server 2003 keskkonnas on WebDAV parem lahendus kui FTP eelkõige seetõttu, et see võimaldab Windows-kasutajakontosid kaitstult autentida. WebDAV-liides on olemas ka mõningatel lisadena saadavatel serverirakendustel nagu nt Microsoft Exchange Server ja Windows Sharepoint Services . Sobivad WebDAV-Clients leiate meetmest M 4.282 Windows Server 2003 IIS põhikomponentide turvaline konfiguratsioon . WebDAV kasutuselevõtu planeerimisel tuleb arvestada vähemalt järgnevate punktidega:

- Serveritel läheb tarvis IIS-i (Internet Information Services).
- WebDAV-i ühiskasutused võimaldavad klientsüsteemis faile töödelda otse serveris (sellel järgneb failide automaatne tõkestamine), kuid käivitatavaid programme ei saa otse serverist käivitada. Üldjuhul tuleb esmalt testida, kas planeeritud klienttarkvara suudab WebDAV-ühendusega töötada või mitte. Kas WebDAV-i juurdepääs (intranet/extranet/internet) on kõigile nähtav? Või kasutatakse seda ainult aeg-ajalt LAN-i keskkonnas, nt administraatoritöödeks? Loetletud küsimused mõjutavad autentimisprotseduuri turvanõudeid (nt anonüümne, baas-autentimine https-i, Kerberose vms vahendusel jne), samuti kasutajate haldust. Muu hulgas puudutavad need ka serveri üldist turvet. Vastusena võib selguda, et WebDAV-i on tarvis pakkuda internetikeskkonnas, võimaldades anonüümset juurdepääsu ning et arvestama peaks suure külastajate arvuga. Sellistel juhtudel tuleks serverit kaitsta meetmetega, mis kehtivad avalikele veebiserveritele. Üheks disaini puudutavaks aspektiks on siinkohal asjaolu, et Windows Server 2003 puhul tuleb WebDAV aktiveerida samas serveris, kus hoitakse soovitud faile. Turvalüüside ja demilitariseeritud tsoonide (DMZ) kasutusvaldkonna seisukohalt vaadelduna ei ole failiserverit ja WebDAV-serverit võimalik teineteisest lahutada. Analüüsi tulemusel võib ka selguda, et aeg-ajalt peab keegi administraatoritest võimalikult kiiresti Active-Directory -domeeni Helpdesk -serverist alla laadima Softwareimage-faili. Sellistel juhtudel võiks administraator WebDAV-ühiskasutuse sisse seada vastavalt tekkivale vajadusele ning ennast domeeni-kasutajakonto (Kerberos-autentimise) kaudu WebDAV-ühiskasutuse ajami tähemärgistusega ühendada. Juhul kui Windows Server 2003 IIS põhikomponentide turvaline konfiguratsioon on juba ellu rakendatud, on täiendavate tööde maht väike.
- Kas andmed peaksid olema andmeedastuse käigus krüpteeritud? Kõige lihtsam ja samas ka kõige turvalisem meetod end-to-end tüüpi krüpteerimise sisseseadmiseks on turvaline kanal HTTPS-i vahendusel, mille konfigureerimine leiab aset IIS-is. Samas ei toeta aga kõik WebDAV-kliendid optimaalselt HTTPS-i. Alternatiivse lahendusena võib kaaluda ka VPN-i või IPSec-i, kuid tuleks arvestada, et nendega seotud töö ja vaev on tunduvalt suurem kui nendest johtuv turvalisuse kasv. Kõikidel juhtudel tuleb valida protseduur, mis tagaks end-to-end tüüpi krüpteerimise.

- Olukordades, kus krüpteerimiseks pole võimalik kasutada turvalist kanalit (HTTPS), peavad planeeritavad WebDAV-kliendid toetama vähemalt Digest -tüüpi autentimist või integreeritud Windowsi autentimist (NTLMv2 või Kerberos). Sama kehtib ka juhtudel, kus HTTPS-i asemel rakendatakse VPN-i. Vastasel juhul ei ole autentimisprotseduuri võimalik piisavalt kaitsta.
- Pärast Windows Server 2003 standardset installatsiooni on Webclient-Service turvakaalutlustel desaktiveeritud. Soovitame seda standardseadistust mitte muuta ning loobuda serveris selle kasutamisest. Administraatoritöödeks, et lihtsalt faile edastada, piisab WebDAV-ühiskasutusse pääsemiseks HTTP/HTTPS-brauserist. HTTP/HTTPS-brauseri autentimismehhanismidele ja krüpteerimisele kehtivad samad nõuded nagu WebDAV-kliendile (enamik brausereid toetavad punktis nr 4 loetletud autentimismehhanisme).

Ajamite tähemärgistuste ja krüpteerimise kasutamine

Windows XP-s on olemas WebDAV-Redirector , mis suudab WebDAV-ühiskasutuse siduda ajami tähemärgistusega. See võib osutuda kasulikuks vanemate programmidega ühildumise seisukohast. Kuid sellele vaatamata ei toimi vastav sidumine HTTPS-ühenduste kaudu. Olukorras, kus on korraga tarvis kasutada ajamite tähemärgistust ja HTTPS-i, tuleb selleks rakendada kolmandate tootjate programme. Kindlasti ei ole soovitatav kasutada krüpteerimata ühendust vaid HTTP vahendusel. Alternatiivina HTTPS-ile on võimalik edastatavaid andmeid krüpteerida ka EFS-iga. Andmed krüpteeritakse klientsüsteemis ning edastatakse seejärel krüpteeritud kujul serverisse, kus need salvestatakse krüpteeritud kujul. Selline lahendus tuleb kõne alla vaid Windows 2000/XP keskkonnas, eeldusel et faili suurus ei ületa 60 megabaiti. EFS-iga krüpteerimist ei ole soovitatav kasutada tavalises IT-keskkonnas, kuna see toob endaga kaasa täiendavad riskid (vt G 4.54 Turbe kadu krüptofailisüsteemi (EFS) kasutamisel kasutamisel ning sõltuvalt olukorrast tuleb võib-olla rakendada veel ka lisameetmeid (vt M 4.278 EFS-i turvaline kasutamine Windows Server 2003 keskkonnas).

Täiendavad kontrollküsimused:

- Kas Webclient on serveris desaktiveeritud?
- Kas WebDAV-juurdepääs on kooskõlas autentimis- ja krüpteerimispoliitikatega?
- Kas WebDAV-serveri Internet Information Services (IIS) konfiguratsioon on piisavalt turvaline ja vastab kasutusvaldkonnast tulenevatele nõuetele?

M 5.133 IP-kõne signaliseerimisprotokolli valik

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: IT-juht, administraator

VoIP lahenduse puhul transporditakse juhtimisandmeid ja tegelikke kõneandmeid üldjuhul teineteisest lahus, rakendades erinevaid edastusprotokolle. Juhtimisandmed, nt seisundiinfo „hõivatud“, edastatakse signaliseerimisprotokolliga, nt H.323 või SIP (Session Initiation Protocol). Kõneandmete edastamise eest vastutab seevastu meediatranspordiprotokoll, reeglina RTP (Real-Time Transport Protocol). Protokolle, mis ei eralda juhtimisandmeid meediaandmetest, leidub väga vähe, nt IAX (InterAsterisk eXchange). Signaliseerimisprotokolle on erinevaid. Kuna need protokollid ei ühuldu omavahel, moodustab nende väljavalimine tähtsa osa VoIP-võrgu ülesehitamisest. VoIP-komponendid, millel pole mitte ühtegi ühist protokolli, saab omavahel suhtlema panna vaid turvalüüsiga. Turvalüüsi, mis peab suutma ühe protokolli käsklused teise protokolli ümber tõlkida, on väga kulukas ja tülikas rakendada. Seetõttu tuleks jälgida, et võimalusel rakendataks vaid ühte signaliseerimisprotokolli. Rakendatavate VoIP-komponentide valik mõjutab suurel määral signaliseerimisprotokollide valikut, kuna paljud VoIP-komponendid toetavad vaid üht kindlat signaliseerimisprotokolli. Turvalisuse seisukohast on protokollidevahelised erinevused küllaltki teisejärgulised. Väljavalitud signaliseerimisprotokoll tuleb dokumenteerida. Järgnevalt käsitletakse enamlevinud signaliseerimisprotokolle H.323 ja SIP. Lisaks protokollidele tutvustatakse veel ka igasuguseid helistamiseks hädavajalikke VoIP-komponente.

H.323

Protokolligrupp H.323 kirjeldab reaalajas tekkivate andmete (video, audio, andmete) edastamist pakettidele orienteeritud transpordivõrkudes. H.323 töötati algselt välja ISDN-i D-kanali protokolli Q.931 rakendamiseks IP-l põhinevas võrgus. Protokolligrupi sees on defineeritud protokollid H.225.0, H.245 ja H.450 ning H.235. Protokollis H.323 kirjeldatakse signaliseerimisprotokollide raamistikku, protokollis H.225.0 kirjeldatakse reaalset signaliseerimist, protokollis H.245 käsitletakse kõneinfo edastamise kontrollimist ning protokollis H.450 reaalset helistamisfunktsiooni. Võimalik olemasolev H.235 tugi aitab kaitsta signaliseerimise terviklust ja konfidentsiaalsust. Täpsemat asjakohast infot leiate International Telecommunications Unionist (ITU-st), mis tegeleb protokollide kehtestamisega. Audio- ja videoandmed edastatakse UDP kaudu, faksiandmed UDP või TCP abil. Enne nimetatud, reaalajas tekkivate andmete edastamist, luuakse lõpp-punktide (terminalide) vahel nn loogilised RTP- ja RTCP-kanalid. H.323-kommunikatsioonis võivad osaleda järgmised komponendid:

- H.323-kommunikatsiooni kasutajapoolsed lõpp-punktid on terminalid. Vastavad lõppseadmed on reeglina varustatud valjuhäältdi ja mikrofoniga ning võimaldavad kasutajal luua ühendust mõne teise kõnepartneriga. Lõppseadmetevaheline otseühendus on võimalik vaid juhul, kui on teada nende IP-aadress.
- Haldamise eesmärgil kasutatakse Gatekeeper ’eid. Kuna otseühenduse loomine on terminalide vahel võimalik vaid siis, kui teatakse IP-aadresse, töötab Gatekeeper H.323-võrkudes tsentraalse juhtkomponendina.

- Multipoint Control Unit (MCU) võimaldab korraldada konverentse, st kõnesid, milles osaleb enam kui kaks helistajat. Võimalikku kasutatavasse MCU-sse jooksevad kokku kõikide kõnepartnerite meediavood.
- Üleminekud teistesse võrkudesse teevad teoks turvalüüsid, tegeldes samaaegselt kasutajaandmete ja signaliseerimisandmete kohandamisega. Turvalüüsid vahendavad nt IP-telefonivõrkude ja teenuseid edastatavate telefonivõrkude vahel.

H.323 kõige suuremaks puuduseks on protokolli keerukus. Suur arv erinevaid protokolle muudab H.323 väga ebaülevaatlikuks ja raskes. Süsteemi keerukus muudab raskeks vigade tuvastamise ning võib tekitada lisakulusid. Veel üheks miinuseks on asjaolu, et paljude uuemate toodete puhul on tootjad otsustanud SIP-i kasuks.

Session Initiation Protocol (SIP)

SIP on Internet Engineering Task Force 'i (IETF-i) loodud, tekstil põhinev klient-server-sessioonisignaliseerimisprotokoll, mida kasutatakse multimeediateenuste ühendusel loomise ja lõpetamise juhtimiseks ning mida kirjeldatakse dokumendis RFC 3261. Lisafunktsioonid nagu videokonverentsid, Instant Messaging , jagatud arvutimängud ja muud rakendused eeldavad SIP-spetsifikatsiooni laiendamist. Neid kirjeldavad eraldi RFC-d. Multimeedia-sõnumitevoog nagu nt telefonikõne rääkimisandmed moodustatakse RTP-ga. Signaliseerimist kaitstakse praktikas tihti SSL-i ehk TLS-iga (Transport Layer Security) või IPSec-iga. SIP-i adresseerimise skeem sarnaneb tugevasti meiliaadressidega (sip:username@providername.org). Lokaliseerimisega tegeleb DNS (Domain Name System). SIP toetab punktist-punkti-IP-ühendusi ja punktist-mitmesse-punkti-IP-ühendusi. SIP-pakettide lihtne, loetaval tekstil põhinev disain ja vähene keerukus on põhjused, miks SIP on hakanud aina laialdasemalt levima. SIP vahendusel toimivas kommunikatsioonis võivad osaleda järgmised VoIP-komponendid:

- lõppseadmed (telefon, tarkvaratelefon, turvalüüs) kannavad nimetust UA (User Agents). User Agent saab täita kliendi, st serveri rolli. Kõne alustaja töötab kui User Agent
- Server (UAS), helistatav töötab kui User Agent Client (UAC). SIP-lõppsüsteem sisaldab alati mõlemat funktsiooni.
- Location Server hangib vastava päringu korral soovitud kõnepartneri IP-aadressi. Identifitseerimise aluseks saab võtta kasutajanime.
- Kasutajate sisselogimist ja registreerimist võimaldab Registrar . Selleks logib lõppseade ennast oma tunnuse (kasutajanime, parooliga) ja oma SIP-aadressiga Registrar -i sisse. Registrar edastab lõppseadme aadressi (IP-aadressi) Location Server -ile, mille all ta on avalikult kättesaadav. Selle registreerimise põhjal on lõppseadet võimalik lokaliseerida.
- SIP-Proxy võtab enda kanda vahendajarolli, kes signaliseerimisteateid töötleb või edasi suunab. User Agent saadab päringu SIP-proksile. SIP-hakkab päringut interpreteerima ja adresseerib selle pärast vastavat töötlemist User Agent 'ile. Vajaduse korral tegeleb SIP-proksi teate muutmisega.

Vaatamata sellele, et SIP on standardiseeritud, interpreteerivad VoIP-komponentide tootjad seda tihti siiski erinevalt. Puuduv koostalitlusvõime viib selleni, et kui VoIP-võrkudes on korraga kasutusel erinevate tootjate komponendid, ei saa kõiki VoIP-funktsioone siiski täielikult kasutada. Kõige enam on sellest puudutatud autentimisfunktsioonid selliste süsteemide vahel, mis tegelevad lisaväärtusteenuste krüpteerimise ja osutamisega. Seetõttu tuleb VoIP-komponentide juurde muretsemise käigus kindlasti kontrollida nende koostalitlusvõimet olemasolevate komponentidega.

Rakendades SIP-d tulemüüri ehk NAT-keskkonnas, tuleb lisaks arvestada täiendavate eripäradega. Lõppseadmed, mis asuvad NAT-keskkonnas, suudavad nt väljaspool NAT-keskkonda asuvate VoIP-süsteemidega suhelda ainult suure vaevaga (vt M 5.137 NAT kasutamine IP-kõne puhul).

Täiendavad kontrollküsimused:

- Kas on dokumenteeritud, millist signaliseerimisprotokolli toetavad olemasolevad VoIP-komponendid?
- Kas toodete soetamisel analüüsitakse ka seda, kas uued komponendid toetavad juba rakendatud signaliseerimisprotokolli?

M 5.134 IP-kõne turvaline signaliseerimine

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: IT-juht, administraator

IP-kõne puhul on meediavoogude kaitsest tunduvalt olulisem see, kuidas tagada signaliseerimisandmete terviklus ja konfidentsiaalsus. Üheks võimaluseks, kuidas seda lahendada, on signaliseerimisandmete transportimine läbi krüpteeritud VPN-kanalite. Täiendavaid võimalusi pakub lisaks ka sisseehitatud kaitsemehhanismidega signaliseerimisprotokollide rakendamine. VoIP-signaliseerimise ühed olulisemad protokollid on SIP ning H.323 raamistikku kuuluvad H.225 (Setup -signaliseerimine) ja H.245 (loogiliste kanalite loomine). Järgnevalt kirjeldatakse nende signaliseerimisprotokollide turvamehhanisme. Lisaks äsja loetletud protokollidele eksisteerib veel ka teisi signaliseerimisprotokolle nagu IAX2, millel puuduvad oma turvamehhanismid. Samas on olemas ka veel spetsiaalsed signaliseerimisprotokollid, nt MGCP, millega juhitakse Media Gateway 'sid, millel ei ole samuti oma turvamehhanisme. Selliste protokollide turve tuleb seetõttu tagada sobivate meetmetega rakenduskihis.

H.235

Läbi Framework H.323 kulgevat signaliseerimist saab enamasti kaitsta turvamehhanismidega, mis töötavad transpordi- või edastuskihis (nt SSL ja TLS või IPSEC). Selliseid signaliseerimisprotokollist sõltumatuid mehhanisme võib kasutada kõrgendatud turvanõuetega keskkondades. Signaliseerimise tervikluse ja konfidentsiaalsuse kaitseks on võimalik rakendada lisaks ka protokolli H.235, mis võib tavalise kaitsevajaduse rahuldada isegi ainukese meetmena. Tarvis on otsustada, kas ja kuidas tuleks hakata signaliseerimist H.323 protokolliga kaitsma. Vastav otsus tuleb dokumenteerida. Protokollis H.235 defineeritakse laiaulatuslikud turvamehhanismid, mille otstarbeks on kaitsta H.323 baasil toimuvat helistamist. Väljatöötatud mehhanismid puudutavad ennekõike helistamise signaliseerimist (H.225/Q.931) ja juhtkanalit (H.245), samuti meediavoo turvalisust. Protokollis H.235 käsitletakse kõiki süsteemikomponente, mis on krüpteeritud H.245 kontrollkanali või krüpteeritud loogilise kanali lõpp-punktid, usaldusväärsete komponentidena ning seetõttu tuleb neid ka vastavalt autentida. Usaldusväärsete ja autentimist vajavate süsteemikomponentide näideteks on turvalüüsid (gateways). Välja tuleks valida üks järgnevatest autentimismeetoditest:

- autentimine sümmeetrilise krüptograafilise meetodiga, rakendades ühist, eelnevalt kindlaks määratud saladust (näiteks parooli). Krüptograafiliste meetoditena võib rakendada kas sümmeetrilisi krüpteerimisprotseduure või Keyed-Hash -funktsioone, kusjuures ühist saladust kasutatakse vastavalt kas sümmeetrilise krüptograafilise võtmena või tuletatakse sellest krüptograafiliselt turvalisel moel.
- sertifitseeritud avalikel võtmetel ja allkirjastatud teadetel põhinev autentimine.
- Iga sellist protseduuri on võimalik juurutada alates kahest teatest, rakendades ajatempleid või Challenge-Response -protokollina alates kolmest teatest, rakendades juhuslikke Challenge 'eid.

- Diffie-Hellman -võtmekokkuleppimisprotokoll koos valikulise (optional) krüpteerimisega: esimeses faasis rakendavad mõlemad sidepartnerid Diffie-Hellman -võtmekokkuleppimisprotokolli, mis baseerub sertifitseeritud avalikel võtmetel. Selle käigus loodav ühine sümmeetriline võti läheb kasutusse valikulises teises autentimisfaasis, mis tegeleb reaalse autentimisega ning baseerub sümmeetrilisel krüpteerimisel.

H.235 raames on olemas ka täiendav mehhanism (Media Anti-Spam), mille abil saavad RTP-pakettide vastuvõtjad edukalt kontrollida, kas RTP-pakett on autentne ning kas see pärineb autoriseeritud saatjalt. Selleks arvutatakse RTP-paketi valikuliste väljade baasil välja lühike MAC (Message Authentication Code), mida vastuvõtja kontrollib enne seda, kui alustab RTP-paketi reaalset töötlemist. MAC-i saab arvutada kas krüpteerimisalgoritmiga või Keyed-Hash -funktsiooniga. Vastav mehhanism kaitseb DoS-rünnete vastu, mida põhjustavad avalikuks tulnud RTP-portide vastu suunatud RTP-Flooding ja SPIT ning kui vähegi võimalik, tuleks see mehhanism sisse lülitada. Juhul kui VoIP-Gateway' d ei toeta kommunikatsiooni läbi H.235, on tungivalt soovitatav turvalüüsi juurdepääsu, mis põhineb IP-aadressidel ja H.323-identiteetidel, piirata nii palju kui võimalik. Selleks on soovitatav kasutusele võtta Gatekeeper ning lubada VoIP-turvalüüsile juurdepääsu ainult režiimis „Routed Mode“. Vastupidiselt režiimile „Bridged Mode“, mille puhul osaleb Gatekeeper ainult autentimises ja registreerimises, toimub kogu signaliseerimine „Routed Mode“ režiimis eranditult Gatekeeper' i vahendusel.

SIP

Üheks keskseks probleemiks signaliseerimisprotokollide nagu SIP turvaliseks muutmisel on asjaolu, et signaliseerimisprotsessi on sageli kaasatud mitmed erinevad komponendid (lõppseadmed ja serverid), mille funktsioon näeb ette signaliseerimisteadete teatud osade lugemist või koguni muutmist. Sel põhjusel ei ole ka võimalik kasutada lihtsalt lõpp-punktist lõpp-punkti (end-to-end) turvamehhanisme, vaid peab tingimata tegema rakenduse eripärast tingitud muudatused. Sel põhjusel soovitab SIP-standard kasutada turvamehhanisme kihtides, mis asuvad rakenduskihist allpool. Selliste meetmetega tagatakse siiski vaid SIP-komponentide (UA, Proxy -, Registrar -, Redirect - ja Location-Server) vaheline kommunikatsioon, mida nimetatakse sageli ka „Hop-by-Hop“-turvalisuseks. Täiendavale argumendile „Hop-by-Hop“-turvamehhanismide kasuks viidatakse standardis SIP 2.0, mille kohaselt tuleb servereid niikuinii teatud piirides usaldada. Siinkohal tuleb siiski selgelt eristada signaliseerimise usaldamist ja meediatranspordi, st kõneandmete usaldamist. Kõrgendatud turbenõuete korral tuleb seetõttu välja selgitada, kas meediatranspordi turvamiseks on tarvis kasutusele võtta täiendavad, olukorrale vastavad lõpp-punktist lõpp-punkti turvamehhanismid. Sama kehtib nt ka SRTP võtmevahetuse kohta.

Kõrgete turbenõuete korral tuleks SIP-ga signaliseerimist kaitsta SSL-i või TLS-iga (Transport Layer Security). SIP-spetsifikatsioon RFC 3261 näeb ette, et kõik konformsed SIP-serverid (Proxy-Server , Redirect-Server , Location-Server ja Registrar-Server) peavad toetama TLS-protokolli koos vastastikuse autentimise ja ühesuunalise autentimisega. Lõppseadmed peaksid oma kommunikatsiooni Proxy -, Redirect - ning Registrar -serveritega kaitsma TLS-iga.

Täiendav kontrollküsimus:

- Kas signaliseerimisandmed edastatakse krüpteeritud kujul?

M 5.135 Turvaline meediatransport SRTP abil

Algatamise eest vastutavad: IT-juht, infoturbespetsialist

Rakendamise eest vastutavad: IT-juht, administraator

Real-Time Transport Protocol (RTP) leiab rakendust meediaandmete edastamisel IP-kõne raames ning Real-Time Streaming Protocol (RTSP) otstarve on nende andmete kontrollimine. Mõlemad protokollid on varustatud oma turvamehhanismidega, mis pakuvad kaitset IP-kõnede pealtkuulamise ja nendega manipuleerimise vastu. RTP/RTCP täiendusteks on SRTP/SRTCP, mis võimaldavad kasutada ka edastamisele suunatud turvamehhanisme. IP-kõnede kasutamisel tuleks kaaluda, kas kasutajaandmeid oleks mõttekas kaitsta SRTP/SRTCP-ga. Vastav otsus tuleb dokumenteerida.

Ülevaade

SRTP-d saab IP-kõnedes kasutada RTP baasil toimuva meediaedastuse konfidentsiaalsuse ja autentsuse tagamiseks ning kaitseks Replay -tüüpi rünnete vastu (teadete uuesti sisselugemise vastu). See võimaldab turvalist Unicast - ja Broadcast -edastust. Transportimiseks paigutatakse RTP/RTCP-paketid SRTP/SRTCP-pakettide sisse.

Võtmehaldus

Protokoll SRTP defineerib ühe Master -võtme ning iga korra jaoks ühe sessioonivõtme krüpteerimise ja autentimise tarbeks. SRTP-l puudub 128 biti pikkuse Master -võtme genereerimiseks ja haldamiseks iseseisev mehhanism. See tuleb tagada teiste standarditega, nt MIKEY-ga (Multimedia Internet Keying). Juhul kui kasutatakse SRTP-d, tuleb määratleda, milliste ajavahemike möödudes peab aset leidma ühelt poolt Master -võtme ja teiselt poolt sessioonivõtme vahetamine.

Krüpteerimine

Olukorras, kus IP-kõne tarbeks kasutatakse SRTP-d, tuleks reeglina sisse lülitada sümmeetriline krüpteerimisprotseduur AES-CTR (Advanced Encryption Standard - Counter Mode). Viimane sobib nii lõpp-punktist lõpp-punkti kui ka lõikude kaupa („Hop-by-Hop“) krüpteerimiseks.

Autentsus ja terviklus

RTP-sõnumite autentsust ja terviklust saab tagada SRTP funktsiooniga HMAC-SHA1, kombineerides seda lisaks vastava sessioonivõtmega. Edastatava kontrollsumma soovitatavaks suuruseks on siinkohal 80 bitti. Seda arvestades tuleb 160 biti pikkune HMAC-SHA1 kontrollsumma vähendada 80 bitini. Selline kohandamine vähendab ühelt poolt küll edastatavate SRTP-pakettide suurust, teiselt poolt aga langeb selle tagajärjel sõnumite tervikluse kaitse. Seetõttu tuleks vastav kohandamine sisse lülitada vaid erandjuhtudel. Alternatiivsete lahendustena võib rakendada funktsioone, mis põhinevad mõnel muul tunnustatud Hash -algoritmil. Valikuid tehes tuleb arvestada, et mõnedes levinud Hash -algoritmides on tuvastatud krüptograafilisi puudusi (vt M 2.164 Sobiva krüptoprotseduuri valimine). Hash -funktsiooni valikut tuleb põhjendada ning langetatud valik dokumenteerida. Samasugune turvamehhanism on ette nähtud ka SRTCP jaoks. SRTP võimaldab rakendada nõrgemat autentimist (nt 32-bitist) ehk siis võimaldab sõnumeid ka mitte autentida, nt selliste rakenduste tarbeks, mille puhul on ülimalt ebatõenäoline, et ründe toimepanijal õnnestub krüpteeritud sõnumiga manipuleerida, nii et hilisem dekrüpteerimine annaks tulemuseks arusaadava sisuga teate. Kui vähegi võimalik, ei tohiks RTP-pakettide autentimiseks nõrgemat autentimismeetodit kasutada. Kõrgemate turbenõuete puhul tuleks RTCP jaoks sisse lülitada eelpool kirjeldatud HMAC-SHA1-kontrollsummal põhinev kaitse.

Kaitse Replay -tüüpi rünnete vastu (teadete uuesti sisselugemise vastu)

SRTP pakub kaitset Replay -tüüpi rünnete vastu, mille puhul toimub esmalt kinnipüütud RTP- või RTCP-pakettide salvestamine ning seejärel nende korduv saatmine, eesmärgiga panna muuhulgas toime Denial of Service tüüpi ründeid. Teadete korduva sisselugemise tõkestamiseks peab eksisteerima tervikluse kaitse ja teadete autentimine. SRTP-pakettide vastuvõtja peab sellisel juhul nn Replay -nimekirja, mis sisaldab eelnevalt vastu võetud autentsete pakettide tunnusnumbreid. Eelnevalt tuleb kindlaks määrata maksimaalselt lubatud salvestatud tunnusnumbrite arv. Uue paketi vastuvõtmisel töötatakse vastav nimekiri läbi, et otsida võimalikke kokkulangevusi, ning kui neid esineb, jäetakse vastavad paketid kõrvale. IP-telefonide puhul, mille mälumaht on väike, tuleb Replay -nimekirja pikkust käsitelda turvet puudutava parameetrina, millega tuleb kõrgendatud turbenõuete kehtimisel kindlasti arvestada. Replay -nimekirja mahtuvus tuleb valida nii suur kui vähegi võimalik ja vastav otsus tuleb dokumenteerida.

Võtmehaldus MIKEY-ga

MIKEY (Multimedia Internet KEYing) kirjeldab reaalaja-multimeediakommunikatsiooni võtmehaldust ning võimaldab rakendada võtmevahetust, samuti täiendavaid turvaparameetreid sideosaliste vahel. VoIP lahendustes saab MIKEY-it kasutada Master -võtme vahetamiseks ja täiendavate turvaparameetrite rakendamiseks, mis peavad tagama lõppseadmete vahelise turvalise SRTP-edastuse. MIKEY ei sõltu baasina toimivast signaliseerimisprotokollist nagu H.323-st või SIP-st. Lisaks toetab MIKEY erinevate sidesessioonide ja kommunikatsiooniprotokollide võtmete ja turvaparameetrite paralleelset vahetust. Seetõttu on võimalik RTP- ja RTCP-ühendusi turvata teineteisest lahutatult. MIKEY kommunikatsioonisessioonide liitmise kontseptsioon võimaldab kasutada mitme paralleelse sessiooni jaoks ühist Master -võtit. Niimoodi on võimalik nt efektiivsemalt turvata VoIP-konverentse.

Juhul kui VoIP-d on tarvis turvata krüptograafiliste mehhanismidega, tuleb ennast kurssi viia VoIP-süsteemide poolt toetatavate võtmevahetuse protseduuridega. Vastavate protseduuride hulgast tuleb välja valida sobiv lahendus ja langetatud valik tuleb dokumenteerida.

Täiendavad kontrollküsimused:

- Milliste ajavahemike möödudes leiab SRTP kasutamise korral aset võtmevahetus?
- Milliseid Hash -algoritme rakendatakse ja kui pikk on kontrollsumma?
- Kuidas leiab aset kõnepartnerite vahel toimuv võtmevahetus?

M 5.136 IP-kõne teenuse kvaliteet ja võrguhaldus

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: IT-juht, administraator

Võrguhaldus on tähtsal kohal VoIP-teenuse turvamiseks vajalike meetmete ahelas. Lisaks kaitsele rünnete vastu peab võrguhaldus peamiselt tagama käideldavuse ja teenuse kvaliteedi. Niimoodi on võimalik vähendada erinevaid riske nagu ülekoormusest tingitud avariisid.

DiffServ ja Class-of-Service vastavalt standardile IEEE 802.1p

IP-võrkudes rakendatavate teenuste kvaliteedi tagamisel on üheks oluliseks aspektiks nn diferentseeritud teenused, Differentiated Services (DiffServ). DiffServ' i puhul jaotatakse andmevood ühekaupa klassidesse, võttes aluseks neile kehtivad teenuse kvaliteedi nõuded. Tehniliselt rakendub see IP-andmepakettide IT-päise väljas TOS (Type Of Service). Erinevate klassidega seotakse IP-päise TOS-välja teatud väärtused. Vastavalt TOS-välja väärtusele koheldakse andmepaketti võrgu sõlmpunktis kas prioriteetselt või mitteprioriteetselt. Teenuse jaoks piisava kvaliteedi tagamiseks turvakihi raames võetakse DiffServ 'ile vastav markeering ja kantakse see Ethernet-raami sisse väljale Class of Service (CoS). CoS-bittide kasutamine on kehtestatud standardiga IEEE 802.1p. Täiendava, Ethernet-raami sisese markeeringu eesmärgiks on mõjutada pakettide edastamist Layer -2-seadmetes nagu kommutaatorites, mis ei tegele IP-päise (Layer 3) analüüsimisega. DiffServ 'i kasutades tuleb tagada, et andmepakettide markeering vastaks täpselt sellele DiffServ -klassile, mis on vastava kommunikatsiooniliigi jaoks ette nähtud. Siia alla kuulub muu hulgas ka kontroll, kas kommunikatsiooniliigil on õigus reserveerida eelistatud ressursse ning kas andmepakettide tegelik markeering langeb kokku ette nähtud klassiga (Policing).

Juhul kui VoIP-võrgud toetavad Differentiated Services mudelit, tuleb see juurutada täies mahus, ilma lünkadeta. Olukorras, kus DiffServ -võrgus puudub nt Policing , on rakendustel võimalik oma andmepakette märgistada lubamatult kõrge prioriteediga, mille tagajärjel võib kõnevoogudes ilmneda massilist pakettide kaotsiminekut ning kõnefunktsiooni kasutamine võib muutuda võimatuks. Tahtlikud sekkumised ei ole DiffServ -võrkudes kasutatavate VoIP-teenustele siiski mitte ainukesed ohud. Võrgukomponentide vale dimensioneerimine võib ühendustes ja võrguressurssides (marsruuterite protsessorites, tulemüürides) tekitada punktülekoormusi, mille tagajärjel võib teenuse kasutamine seiskuda.

Overprovisioning

IP-kõne funktsioone kasutades jäetakse andmevoogude markeeringud tihti tähelepanuta. Arvatakse et moodsad kohtvõrgud nagu WAN-id on piisavalt üledimensioneeritud, et vältida ummikute tekkimist ootejärjekordade sees. Seda teoreetilist lähtepunkti nimetatakse Overprovisioning . Overprovisioning tähendab, et võrgus toimub pidev monitooring, et selgitada välja võimalikud kitsaskohad. Siinkohal tuleb märkida, et ühenduse kitsaskohaks ei ole alati ilmtingimata kanali andmekiirus. Kitsaskohaks võib osutuda ka marsruuteri CPU-jõudlus, kommutaatori põhiplaat või ka tulemüüri läbilaskevõimsus. Seetõttu osutub määravaks CPU koormuse ja võrkude kõikide ühenduste järjepidev monitoorimine, samuti perioodilised analüüsid, teostades nt aktiivseid mõõtmisi ühesuuna-viivituste kohta. Overprovisioning põhimõtet järgides tuleb arvestada, et see meetod ei suuda siiski garanteerida kõnerakenduste kindlat kvaliteeti. Kõikvõimalikud väited ja hinnangud saavad tugineda pigem eelneval kogemusel ja eelnevalt kogetud andmetel. Uute rakenduste nagu nt videokonverentside või Grid-Computing 'u kasutuse-

levõtt võib võrkude käitumist kardinaalselt muuta. Overprovisioning meetodi rakendamisel võivad ennekõike tugevasti kannatada VoIP-rakendused, sest tekivad suured andmevood.

MPLS

MPLS-i (MultiProtocol Label Switching) võib kasutada WAN-ides, et isoleerida kõneühenduste jaoks kasutatavad garanteeritud ribalaiusega kanalid ülejäänud andmesidest. Sellega on võimalik Overprovisioning põhimõtet rakendada MPLS-kanalite lõikes. Kuna VoIP-andmesides esineb andmekiiruse kõikumist vähem kui ülejäänud IP-andmesides, tuleb lähtuda sellest, et VoIP-kanaleid on võimalik rohkem täita kui neid kanaleid, kus VoIP-andmesidet edastatakse koos ülejäänud andesidega. Tuleb siiski arvestada, et MPLS-i peamine eelis seisneb teenuse paremas kvaliteedis, kuid andmeedastuse konfidentsiaalsust ja terviklust suudab see kaitsta vaid vähesel määral. MPLS-kanalite andmepaketid varustatakse sarnaselt VLAN-Tagging 'uga täiendava päisega (header) ning nende edastamine toimub krüpteerimata kujul koos kogu ülejäänud andmesidega. Seetõttu on võimalik neid kanaleid, sarnaselt Ethernet-andmesidele, sobivate sniffer 'ite abil teatud võrgus asuvates komponentides nii pealt kuulata kui ka nendega manipuleerida.

Traffic Shaping

Traffic Shaping 'ut rakendatakse kohtvõrkude ja laivõrkude turvalüüsides eesmärgiga piirata teatud andmesideliikide, st üldjuhul teisejärguliste andmesideliikide, andmekiirust. Sellekohasteks näideteks on andmete ülekandmine, nt FTP-ühendustes, mille puhul on ajalised nihked vastuvõetavad. Kogemused näitavad siiski, et juhtudel, kus Traffic Shaping 'u kriteeriumitena rakendatakse eranditult andmepakettide pordinumbreid, on nendest meetmetest kerge mööda hiilida.

Resource Reservation Protocol (RSVP)

Resource Reservation Protocol (RSVP) on ette nähtud lõpp-punktist lõpp-punkti signaliseerimise andmevoogude teenusekvaliteedi tagamiseks. RSVP loodi algselt nn Integrated Services (IntServ) rakendusena IP-võrkudes, et tagada vastupidiselt DiffServ 'ile ühtlane teenusekvaliteet. RSVP kasutuselevõtmine selle algsel kujul eeldab, et kõik edastussõlmed, operatsioonisüsteemid ja rakendused peavad seda protokolli toetama. Hetkel on nii operatsioonisüsteemide kui ka rakenduste tugi ebapiisav või olematu. Seetõttu ei tule RSVP ja IntServ 'i kasutamine VoIP jaoks hetkel kõne alla.

Täiendav kontrollküsimus:

- Milliseid meetmeid rakendatakse ülekoormuse vältimiseks?

M 5.137 NAT kasutamine IP-kõne puhul

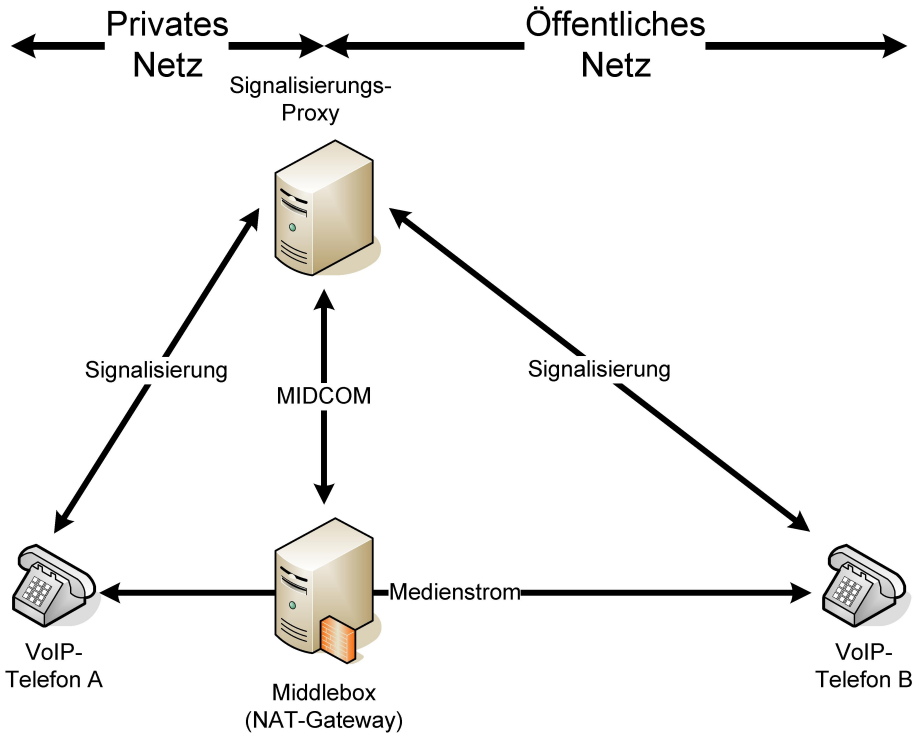
Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: IT-juht, administraator

NAT (Network Address Translation) võimaldab tõlkida privaatseid/siseseid IP-aadresse ümber avalikeks/välisteks IP-aadressideks. Sellise aadresside teisendamise käigus tõlgitakse vastava NAT-Gateway abil privaatsed allika-IP-aadressid ja sinna juurde kuuluvad privaatsed allikapordid ümber avalikeks allika-IP-aadressideks ja avalikeks allikaportideks. Selleks, et NAT-Gateway suudaks tagastuspakette ehk sissetulevaid pakette, mis on adresseeritud avalikule IP-aadressile, edasi suunata õigele sisemisele hostile, peab see vastavat liigitamistabelit, kus kajastub info avalike IP- aadresside/portide ja privaatsete IP-aadresside/portide vastavuse kohta. NAT abil toimub meediavoo UDP- või TCP-päises allika-IP-aadressi ja allika-pordinumbri modifitseerimine. Signaliseerimisteate teateosas kajastuvat allika-IP-aadressi ja allika-porti seevastu ei muudeta. Selle tulemusel ei ole andmevoogusid võimalik saata ühelegi VoIP-telefonile, mis asub NAT-Gateway' st tagapool. Internetis asuvatel VoIP-seadmetel ei ole võimalik meediavoogusid saata ühelegi VoIP-telefonile, mis asub tagapool NAT-Gateway' d selle pärast, et privaatset IP-aadressi interneti suunas ei marsruudita. Järgnevates lõikudes kajastatakse võimalusi, kuidas rakendada VoIP-funktsioone NAT-keskkonnas.

MIDCOM

MIDCOM tähendab lahtiseletatult Middlebox Commmunications ning selle on välja töötanud IETF, kes pakub lahendusi VoIP kasutamisega tekkivatele NAT- ja Firewall -probleemidele. MIDCOM-süsteem koosneb Middleboxist ja serverist, mille ülesandeks on Middlebox 'i juhtimine ja konfigureerimine. Juhtimisserveriks on VoIP-server (H.323- Gatekeeper , SIP-Proxy , jne.), mis asub signaliseerimise andmeteel ja jälgib SDP-andmete (Session Description Protocol) andmevahetust. Nende andmete põhjal juhib server MIDCOM-protokolli vahendusel Middlebox 'i (NAT-turvalüüsi, tulemüüri), mis tegeleb seoste sissekandmisega NAT-tabelisse ja vastavate portide avamisega. Järgneval joonisel on visandatud MIDCOM-i arhitektuur.



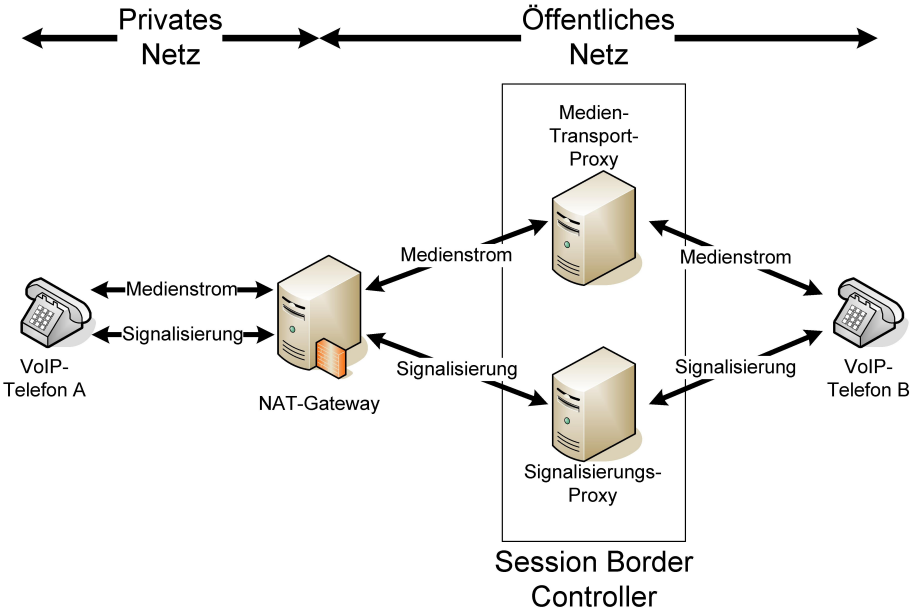
Joonis: MIDCOM-i arhitektuur

Privates Netz – privaatvõrk; Öffentliches Netz – avalik võrk; Singalisierungs-Proxy – signaliseerimisproksi; Signalisierung – signaliseerimine

Kuna juhtimisserver peab ise internetiga suhtlema, tuleb ka juhtimisserverit kaitsta tulemüüriga. Juhtimisserveri vastu suunatud rünne võib õnnestumise korral muuta võimalikuks täiendavad ründed, nt selle poolt kontrollitava Middlebox 'i (NAT-turvalüüsi, tulemüüri) vastu. Selle tagajärjel võivad tekkida märkimisväärsed kahjud.

Session Border Controller

Kuna MIDCOM on veel väljaarendamise staadiumis, on mitmed tootjad hakanud turule tooma erinevaid lahendusi, mille abil saab leevendada NAT- ja Firewall-probleeme. Vastavad Session Border Controller 'id pakuvad sageli lisafunktsioone nagu SLA-de (Service Level Agreements) seire, kõne vastuvõtu juhtimine (Call Admission Control) ja hinnateavitus (Billing). Vastavaid süsteeme pakutakse nii eraldiseisvate seadmete kui ka serverite kujul. Järgneval joonisel kujutatakse Session Border Controller 'i võimalikku rakendust, mis koosneb ühest signaliseerimisproksist ja ühest RTP-proksist.



Joonis: Session Border Controller 'i võimalik rakendus

Privates Netz – privaatvõrk; Öffentliches Netz – avalik võrk; Mediantransport-Proxy – meediatransportimisproksi; Singalisierungs-Proxy – signaliseerimisproksi; Signalisierung – signaliseerimine; Medienstrom - andmevoog

Kogu andmeliiklus (signaliseerimine ja andmevood) toimib antud näites Session Border Controller 'i baasil. VoIP-telefon B ei tea, milline on VoIP-telefoni A tegelik IP-aadress.

UPnP

UPnP (Universal Plug and Play) on tööstuslik standard, mille kasutamine levib eriti jõudsalt kodustes majapidamistes. UPnP-arhitektuuriga soovitakse lihtsustada arvutite ja lõppseadmete (nt printerite, skannerite, WLAN-i pääsupunktide) liitmist ühtsesse võrku. UPnP vahendusel saavad rakendused teada NAT-Gateway avaliku IP-aadressi, saavad ette anda kasutatavad NAT-liigitused ja pärast sessiooni lõppu vastavad liigitused eemaldada. Võimalik on määrata ka nn Lease Time , mis määrab kindlaks NAT-liigituse kehtivusaja. Juhul kui mitu NAT-Gatewayd lülitatakse järjest üksteise taha, muutub NAT-läbipääs UPnP-ga võimatuks.

STUN

STUN-iga (Simple Traversal of User Datagram Protocol (UDP) Through NATs) saavad need lõppsüsteemid, mis asuvad NAT-Gateway taga, välja selgitada oma avaliku IP-aadressi ning neil avaneb võimalus teada saada turvalüüsi NAT-liigitus. Symmetric NAT-d STUN siiski ei toeta. NAT-liigitused edastatakse VoIP puhul signaliseerimisprotokolliga, nii et sissetulevad RTP-vood adresseeritakse vastava NAT-liigituse põhjal edasi, eesmärgiga jõuda välja VoIP-telefonini, mis asub NAT-Gateway taga. Paljud VoIP-telefonid toetavad STUN-tehnoloogiat juba praegu ning see kajastub ka enamike VoIP-teenusepakkujate tootevalikus.

TURN

TURN (Traversal Using Relay NAT) võimaldab NAT-Gateway või tulemüüri taga asuvatel süsteemidel vastu võtta sisenevaid TCP- ja UDP-ühendusi. Samaaegselt tõkestatakse selle funktsiooni kasutus avalikult ligipääsetavate serverite tarbeks nagu veebiserverid või meiliserverid, lubades iga IP-aadressist ja pordist koosne-

va kombinatsiooni kohta vaid üht sessiooni ühe partneriga (peer). Vastupidiselt STUN-ile võimaldab TURN sissetulevaid ühendusi vastu võtta ka neil süsteemidel, mis asuvad sümmeetrilise NAT-Gateway taga. TURN on lihtne klient/server-protokoll ning selle autentimine kasutab paroole.

ICE

Kuna TURN-i puhul juhitakse kõik meediavood läbi TURN-serveri, on mõttekas TURN-serverit kasutada vaid siis, kui sissetulevate ühenduste vastuvõtmine STUN-iga osutub võimatuks. Üheks meetodiks, kuidas võimaldada SIP jaoks NAT-läbipääs, võttes aluseks mitu SDP vahendusel avalikustatud aadressi ja rakendades selleks protokolle STUN, TURN, RSIP ja MIDCOM, on ICE (Interactive Connectivity Establishment). Lähtutakse põhimõttest, et kliendi käsutuses on mitu aadressi (nt STUN-i või TURN-i abil õpitud aadressid), mille vahendusel klient võtab vastu meediavoogusid. Kuna lõppsüsteemid ei tea, milline aadress toimib, asutakse neid aadresse üksteise järel kontrollima, et selgitada välja nende prioriteet, kusjuures esimesena asutakse testima kõige kõrgema prioriteediga aadressi. Prioriteedid määratletakse kõige madalamate kulude ja QoS (Quality of Service) maksimumväärtuste baasil ning seejärel reastatakse need üksteise järel üles SDP-s. ICE on küll konstrueeritud SIP tarbeks, kuid töötab ka RTSP ja H.323-ga ning võimaldab lõppseadme käitamist viisil, mis ei sõltu NAT-keskkonnast.

Juhul kui LAN ühendatakse internetti läbi NAT-Gateway, on soovitatav langetada otsus ühe esitletud mehhanismi kasuks. Vastav otsus tuleb dokumenteerida.

M 5.138z RADIUS serverite kasutamine

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: administraator

Suurtes võrkudes tuleks võimalusel kindlasti kasutada autentimisservereid, nt RADIUS-servereid. RADIUS (Remote Authentication Dial-In User Service) on klient-server-protokoll, mida rakendatakse kasutajate autentimiseks, autoriseerimiseks ja nende üle arvepidamiseks (AAA-System) eesmärgiga tagada ühenduste tsentraliseeritud turve. Selle protokolli kirjeldusi leiate erinevatest RFC-dest, neist kõige olulisem on RFC 2865. Autentimisserveri eesmärgiks on tagada, et sisevõrkudele pääseksid ligi vaid volitatud kasutajad, lisaks on võimalik tõkestada juurdepääs teatud lõppseadmetele. Selle tagamiseks toimub esmalt identifitseerimine, nt kasutajatunnuse baasil ning sellele omakorda järgneb autentimine, nt parooliga. Nimetatud andmete edastamine peab toimuma krüpteeritud kujul. Selleks kasutatakse tihti EAP protokolli (Extensible Authentication Protocol). Autentimise aluseks võetakse EAP puhul pordid ning protseduur põhineb standardil IEEE 802.1X. See tähendab, et juurdepääs võrgule avaneb alles pärast seda, kui klient on ennast RADIUS-serveris üheselt identifitseerinud. Rakendatavaid autentimisservereid tuleb sobival moel turvata (vt M 4.250 Keskse võrgupõhise autentimisteenuse valimine).

RADIUS-serveri ja RADIUS-kliendi vaheliste Shared Secrets andmete kaitseks tuleb valida piisavalt pikad keerulised krüptograafilised võtmed. Siinkohal võib, juhul kui töökorralduslikud meetmed seda võimaldavad, iga RADIUS-klient-serversuhte jaoks kasutada erinevat Shared Secret' it. Erinevate komponentide võimalikult kõrge koostalitlusvõime tagamiseks tuleks RADIUS-e jaoks kasutada komponente, mis vastavad RFC-dega RADIUS-ele kehtestatud nõuetele. Autentimisprotokollid ja arveldamisprotokollid tuleks salvestada eraldiseisvasse andmebaasisüsteemi. RADIUS-kommunikatsioon tuleks piirata pordile 1812 või 1813. Portide 1645 ja 1646 kasutamisest tuleks võimalusel loobuda. Ülejäänud pordid tuleb sulgeda, juhul kui see on tehniliselt võimalik. Serveri RADIUS-kommunikatsioon tuleks piirata serverile teadaolevatele ja autenditud RADIUS-klientidele.

Kõrge kaitsevajaduse korral, mis nõuab autentimisandmete suurt konfidentsiaalsust, on RADIUS-kommunikatsiooni kaitseks soovitatav kasutusele võtta IPSec, kuid see ei tähenda, et RADIUS-e enda kommunikatsioonikaitsemehhanismidest võiks loobuda. Kirjeldatud valdkonna puhul tuleks lisaks kaaluda veel ka liiasusega RADIUS-serveri kasutuselevõtmist. Ettekirjutused, millist infot kajastatakse RADIUS-serveri autentimispäringule saadetavas vastuses, peaksid kehtestama võimalikult suured piirangud. Vältida tuleks kindlasti lubatud sisselogimisaegade, MAC-aadressi ja end sisse logiva RADIUS-kliendi pordi tüübi, samuti RADIUS-kliendi IP-aadressi ja autentimiseks kasutatava EAP-meetodi kajastamist.

Täiendavad kontrollküsimused:

- Kuidas kaitstakse autentimisinfot andmeedastuse raames?
- Kuidas kaitstakse RADIUS-serverit võimalike rünnet eest?

M 5.139 Traadita kohtvõrgu turvaline ühendamine kohtvõrguga

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: administraator

WLAN-komponentide kasutamise peamiseks eesmärgiks on sageli mugav ja mobiilne ühendumine teiste võrkudega. Selleks võivad osutuda teised WLAN-id, aga ka oma institutsiooni olemasolevad LAN-id. Siinkohal tuleks arvestada kahe järgneva turvaaspektiga:

- rakendatavaid WLAN-komponente on tarvis kaitsta võimaliku väärkasutuse eest võõrastes võrkudes ning
- sisemist LAN-i on tarvis kaitsta väljastpoolt tuleva väärkasutuse vastu.

Olukordades, kus WLAN-i soovitakse ühendada LAN-iga, tuleb üleminekut kaitsta vastavalt sellele, kumma poole turbevajadused on kõrgemad. Harilikult on selleks LAN. WLAN-i ühendamiseks LAN-iga on enamasti valida kahe võimaluse vahel:

- esimese variandina on võimalik üritada luua olukord, kus WLAN-i turbeseisund vastaks olemasoleva traadiga kohtvõrgu turbeseisundile. Selle saavutamiseks peab enamikel juhtudel laiendama standard-WLAN-komponentidega integreeritud turvamehhanisme, nt tuleb kasutusele võtta tugevamad krüpteerimisalgoritmid, samuti tuleb küllaldaselt vaeva näha täiendavate turbemeetmete juurutamisega.
- teise variandina on võimalik valida pragmaatilisem lähenemisviis, mille puhul lähtutakse sellest, et nii raadiolevis edastavad andmed kui ka WLAN-komponendid ei vasta LAN-i turbeastmele. Seetõttu tuleb WLAN-ist alguse saavaid pöördusi käsitleda nagu internetist pärinevaid pöördusi, mistõttu tuleks neid lubada ainult turvalüüsi vahendusel. Soovitatav on valida see lähenemine.

Mida kvaliteetsemalt suudetakse turvata õhuliidest ja Distribution System 'i aktiivseid komponente, seda vähem tuleb vaeva näha üleminekut LAN-i võimaldavat liidese kaitsmisega. Kõikidel juhtudel peab üleminekupunktis olema võimalik WLAN-kommunikatsiooni täielik tõkestamine sisese LAN-i suhtes, niipea kui on tuvastatud WLAN-i vastane rünne. Broadcast -domeenide efektiivse lahutamise tagamiseks peab WLAN-i ja LAN-i Distribution System 'i ühenduselemendiks olema vähemalt Layer-3-Router . Eri mehhanismide kasutamine, nt dünaamilise paketifiltri kasutamine marsruuteri asemel tuleb läbi kaaluda kasutusotstarbest lähtuvalt, võttes arvesse kehtivad turbevajadused.

Kõrgendatud kaitsevajaduse korral tuleks täiendava meetmena parandada ka autentimise turvet, võttes kasutusele nt EAP-TLS-i, et võimaldada vastastikust tugevatoimelist autentimist WLAN-klientide ja LAN-i keskkonnas asuva autentimisserveri vahel.

Täiendavad kontrollküsimused:

- Kas LAN on täiendava turvalüüsiga WLAN-i suhtes kaitstud?
- Kas juurdepääs LAN-ile läbi WLAN-i on hädavajalik ja soovitud lahendus? Kas vastav otsus on dokumenteeritud?

M 5.140 Traadita kohtvõrgu jaotussüsteemi ehitus

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: administraator

Jaotussüsteem (Distribution System) on võrk, mis ühendab omavahel pääsupunkte (Access Points) ning liidab need omakorda täiendava infrastruktuuri, nt traadiga võrgu külge. Enamikel juhtudel on võimalik eristada kahte liiki jaotussüsteeme:

- Kaabliühendusega jaotussüsteem. Kõikide pääsupunktide vahel ning pääsupunktide ja muu infrastruktuuri vahel on kaabliühendused.
- Juhtmevaba jaotussüsteem. Pääsupunktide vahelised otsesed kaabliühendused ei ole hädavajalikud. Kõige olulisemad kaablid on pääsupunktide elektrikaablid.

Mõlemal juhul peab pääsupunktide vaheline kommunikatsioone alati toimuma krüpteeritud kujul, et tagada edastatavate andmete konfidentsiaalsus. Kaabliühendustega jaotussüsteemides saab selleks otstarbeks rakendada nt IPSec-VPN-tunnelit, juhtmevaba jaotussüsteemi korral, mis vastab standardile IEEE 802.11i, on lisaks võimaik rakendada CCMP-d. Juhtmevaba jaotussüsteemi puhul on lisaks konfidentsiaalsuse ja tervikluse kaitsele väga oluline ka käideldavus ning seetõttu tuleks sellistes süsteemides kasutusele võtta meetmed, mis suudaksid tõkestada võimalikke Denial-of-Service -tüüpi ründeid. Kitsaskohti aitavad kiiresti leida ja vastumeetmeid rakendada juhtmevabad sissetungi tuvastussüsteemid (Wireless Intrusion Detection Systems) ja regulaarsed turvakontrollid. Jaotussüsteemi ülesehitamisel tuleb muuhulgas vastu võtta põhimõtteline otsus, kas turvakaalutlustest lähtuvalt on tarvis üles ehitada või tööle lülitada iseseisev infrastruktuur, st kas sisemise LAN-i infrastruktuuri on tarvis hakata füüsiliselt segmenteerima või mitte. Alternatiivse lahendusena võib kaaluda, kas vajaduste katmiseks piisab võib-olla VLAN-ide loogilisest segmenteerimisest.

Loogiline jaotussüsteem.

Olukorras, kus jaotussüsteemi tarbeks seatakse sisse füüsiline infrastruktuur, on määrava tähtsusega see, kui suureks osutuvad teenindamist vajavad vahemaad. Enamikel juhtudel ühendatakse omavahel kas Layer -2- või Layer -3-kommutaatorite abil kokku mitu pääsupunkti ning tavapäraselt skaleeritakse see kas 12, 24 või 48 pordi peale iga kommutaatori kohta. Seega, kui jaotussüsteemi loomiseks on tarvis omavahel ühendada nt 100 pääsupunkti, läheb selleks tarvis kolme kuni kümmet kommutaatorit. Tsentraalses serveriruumis ei ole enamasti võimalik rakendada lahendust, mille puhul saaks pääsupunktid otse kommutaatorite külge ühendada, mistõttu tuleb kommutaatorid laiali jagada terve territooriumi peale, mida soovitakse WLAN-iga varustada. Siinkohal tuleb tagada, et kommutaatorid oleksid piisavalt kaitstud väliste juurdepääsude eest ning sõltuvalt jaotussüsteemi käideldavusnõuetest tuleks võib-olla sisse seada liiasusega kommutaatorid. Eraldiseisva füüsilise infrastruktuuri rajamine nõuab seevastu suuremaid investeeringuid ja muudab hädavajalikuks täiendavate turvameetmete rakendamise. Loogilise segmenteerimise puhul luuakse pääsupunkte läbiva andmevoo kontrollimiseks traadiga LAN-i keskkonnas virtuaalsed LAN-id (VLAN-id). Juhul kui WLAN-kliente soovitakse segmenteerida jaotussüsteemi raamides, peab pääsupunktis aset leidma täiendav WLAN-kliendi liigitamine VLAN-i alla. Loogilise jaotussüsteemi konfigureerimine olemasoleva LAN-infrastruktuuri raames on käitamiste ja käideldavuse tagamise seisukohast omajagu problemaatiline ning

eeldab ülimalt hästi koolitatud administraatorite olemasolu. Olukorras, kus kogu LAN- ja WLAN-infrastruktuuri puhul on tarvis tagada tavapärane käideldavus, on VLAN-ide konfigureerimine selleks vastuvõetav tegevus. Niipea aga, kui on tarvis saavutada kõrge käideldavus, pole VLAN-ide rakendamine jaotussüsteemide tarbeks enam soovitatav.

Täiendavad kontrollküsimused:

- Kas on tarvis luua kaabliühendusega jaotussüsteem või juhtmevaba jaotussüsteem? Kas otsus on dokumenteeritud ja hoiule pandud?
- Kas on tehtud füüsiline või loogiline segmenteerimine? Kas see otsus on samuti dokumenteeritud ja hoiule pandud?

M 5.141 Regulaarsed traadita kohtvõrgu turvakontrollid

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: administraator

Regulaarsete ajavahemike möödudes, vähemalt kord kuus, tuleks läbi viia WLAN-i turvakontroll. Traadita kohtvõrke tuleb regulaarselt WLAN- ja võrguanalüsaatoritega kontrollida, et teha kindlaks, kas süsteemis leidub võib-olla turvaauke nagu nõrku paroole, ebapiisavat krüpteerimist või aktiivseid SSID-Broadcast 'e. Lisaks tuleks otsaida ka ilma volituseta installeeritud WLAN-e.

Network Analyzer programmid

Teenuse kvaliteedi ja turvalisuse seireks on nii WLAN-ides kui ka teistes võrkudes palju abi spetsiaalsetest tööriistadest. Traadita kohtvõrkude turvaliseks käitamiseks on ülimalt oluline, et saaks kontrollida, kas etteantud turvapoliitikatest peetakse kinni ning kas WLAN on käideldav või mitte. Viimase alla kuuluvad ka jõudlusnäitajate mõõtmised ja veaanalüüsid. Kasulikud on muidugi ka sellised tööriistad, mis loovad ülevaate kõikidest aktiivsetest WLAN-is osalejatest ning seni tuvastatud võrgus osalejatest. Võrguanalüüsi- ehk sniffer -programmid loevad andmevoogusid ja analüüsivad edastatud andmepakette erinevate seadistatavate väärtuste suhtes. Sellised programmid suudavad leida andmepakettidest teatud malle ja oskavad analüüsida marsruutimisandmeid. Võrku analüüsivaid programme tuleks rakendada regulaarselt järgmistel eesmärkidel:

- volitamata WLAN-ide tuvastamine institutsiooni piires,
- hädavajalike turvamehhanismide sisselülitamise regulaarne kontroll,
- leviaukude tuvastamine ja raadiosidevõrkude signaali kvaliteedi analüüsimine.

Traadita kohtvõrgu infrastruktuuri seire

WLAN-infrastruktuuri seire võib kõige lihtsamas variandis toimida nõnda, et ühes spetsiaalse tarkvaraga varustatud WLAN-kliendis viiakse läbi pisteline kontroll, mis hõlmab kogu varustatavat territooriumit ning annab olukorrast ülevaate. Sellise kontrollimeetodiga saab nt tuvastada volitamata pääsupunktide käitamist. Parema kontrollitulemuse annavad siiski WLAN-Management-Systems -tüüpi lahendused, mille abil tuleks regulaarselt läbi viia järgnevad kontrollid:

- võõrseadmete, eriti võõraste pääsupunktide tuvastamine.
- Wireless Site Surveys analüüsid, st uuringud eesmärgiga tuvastada WLAN-i kattumisi, andmekiirust, ribalaiust QoS jne.
- Sisselogimisaegade logi.
- WLAN-võrguelementide konfiguratsiooni seire.

Wireless Intrusion Detection System 'ite kasutamine

Olukorras, kus planeeritakse kasutusele võtta pääsupunktil põhinev juhtmevaba sissetungi tuvastamise süsteem (IDS), tuleks esmalt otsustada, kas selle tarbeks ehitatakse üles mõõtmist võimaldav infrastruktuur või lülitatakse igapäevaselt kasutatavas võrgus olevad pääsupunktid ja WLAN-kliendid teatud intervallide möödudes mõõtmisrežiimi. Kui vastav süsteem ei kata kogu seire alla kuuluvat valdkonda, pole võimalik WLAN-i vastu toime pandavaid ründeid raadiolevi tasandil

tuvastada. Lisaks selle tuleb ka veel arvestada, et nii pääsupunkt kui ka WLAN-klient ei suuda mõõtmisrežiimis töötades andmeid edastada, mis tähendab, et mõõtmisrežiimis tuleb leppida jõudluse langusega ning võib-olla ka käideldavuse langusega. Igapäevaselt tööks kasutatavate pääsupunktide käitamine mõõtmisrežiimis Scan-Mode tekitab lisaks ka veel olukorra, kus teatud aja jooksul pole seire teostamine õhuliideses võimalik. Kõikidel juhtudel, kus võetakse kasutusele Intrusion Detection Systems või koguni Intrusion Prevention System (IPS), tuleb välja selgitada või mõõtmiste abil defineerida, milline on WLAN-i tavapärane kommunikatsioonialane käitumine (vt M 5.71 Sissetungi tuvastuse ja sellele reageerimise süsteemid).

Hoiatuste ja vigade käsitlemine

WLAN-i haldamise raames peavad eksisteerima protseduurid hoiatuste ja vigadega toimetulemiseks. Selleks peavad administraatorid tegelema järgmiste ülesannetega:

- hoiatusteadete tähtsuse ja sisu analüüs, nt sagedased ebaõnnestunud autentimiskatsed mõnes pääsupunktis ,
- veaotsingu statistika analüüs,
- meetmete rakendamine turvaintsidendi kahtluse korral,
- alarmi piirväärtuste kohandamine WLAN-kasutuse muudetud väärtustega.

Penetratsioonitest

Turvakontrolli raames võib WLAN-i kitsaskohtade leidmise eesmärgil kasutada ka penetratsiooniteste. Testimisega tuleks saavutada täpne ülevaade turvameetmetest ja sellest, kas need suudavad ka reaalselt vastu pidada rünnetele, mille vastu need kasutusele on võetud. Penetratsiooniteste tuleks teha vähemalt kord iga poole aasta tagant, hiljemalt üks kord aastas.

Dokumentatsioon

Turvakontrolli läbi viies peavad administraatorid iga sammu dokumenteerima, nii et need oleksid (nt kahtluse korral, et tegu on süsteemi kompromiteerimisega) ka hiljem arusaadavad. Turvakontrolli tulemused tuleb dokumenteerida, võimalike kõrvalekallete puhul tuleb välja selgitada nende põhjus.

Täiendavad kontrollküsimused:

- Kas administraatoreid on juhendatud, millised hoiatuste ja vigadega toimetulemise protseduurid tuleb läbida, juhul kui on tegemist WLAN-i vastu suunatud ründega?
- Kas WLAN-i turvakontrolli tegemine ja tulemused dokumenteeritakse?

M 5.142 IT-kaabelduse vastuvõtmine

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: IT-juht

Juhtmestikku tohib vastu võtta ainult siis, kui kõik vajalikud tööd on tehtud, teostaja on vastuvõtu võimalikkusest teatanud ja tellijapoolsed kontrollid pole mingisuguseid vastuvõetamatuid puudusi tuvastanud. Ajaliselt tuleks vastuvõtu tähtaeg valida selline, et vastuvõtuks vajaminevate kontrollimistööde ettevalmistamiseks jääks piisavalt aega. Kõikide tellitud tööde täitmist kinnitatakse tavaliselt osutatud teenuste hindamise alusel. Lisaks arve õigsusele ja teenuse tegelikule mahule tuleb vastuvõtu käigus kontrollida ka IT-turvalisuse aspekte.

Kontrollide ettevalmistamisel oleks mõistlik arvestada järgnevate punktidega:

- Kontrollida tuleb kõikide paigalduse juurde kuuluvate dokumentide täielikkust ja tõesust.
- Esmajoones tuleb kontrollida mõõtmisprotokollide tulemusi. Vastuvõtmise käigus tehtava kontrollmõõtmise jaoks on soovitatav valida eriti silmatorkavad mõõtmistulemused.

Vastuvõtmine hõlmab järgnevaid kontrolle ja tegevusi:

- Kontrollitakse, kas põhiplaani, asendiplaani ja lülituskappide plaanidesse tehtud sissekanded vastavad tegelikkusele.
- Kontrollitakse, kas tarneid on tehtud piisaval arvul ja piisava kvaliteediga.
- Kontrollitakse, kas teenused on oskuslikult teostatud. Pisteliste kontrollidega on soovitav täpsemalt kontrollida andmepesade paigaldust, kaablite painderaadiusi ja trassidesse paigaldust.
- Silmatorkavad mõõtmistulemused, mida vastuvõtmisel tuvastatakse, tuleks üle mõõta.
- Vastuvõetud süsteemiosad, puudused ja tarvilikud täiend- ja jääktööd tuleb protokollida.
- Puuduste kõrvaldamiseks ning järel- ja jääktööde tegemiseks määratakse kindlad tähtajad, millest tuleb ilmtingimata kinni pidada.
- Kindlaks määratakse garantiitingimused ja garantiitähtajad.

Soovituslik on vastuvõtuprotokoll ette valmistada kontrollnimekirjana. Kontrollnimekiri peaks sisaldama ka punkte tööruumide üldnõuete kohta, mis ületavad meetmete piire, et fikseerida süsteemi üldseisund ja kvaliteet. See aitab kaasa süsteemide ülevaatlikule kasutamisele ja ennetab avariisid. Need punktid ei ole IT-juhtmestiku vastuvõtuks olulised ja edastatakse hiljem vastutavale osakonnale. Vastuvõtu kontrollnimekirjad tuleks kujundada selliselt, et need dokumenteeriks muuhulgas juba ka installeerimist ja kasutuselevõttu ning protokolliks tööde vastuvõtmise ettevalmistavaid meetmeid. Kontrollnimekirjade pikkus tuleks piirata miinimumini. Seega tasuks nimekirjas sisalduvaid punkte analüüsida, vajadusel täiendada ja ebaolulised punktid eemaldada. Osalejad ja vastutajad peavad vastuvõtuprotokollile andma õiguslikult siduvad allkirjad. Pärast vastuvõttu tuleb

kontrollida puuduste kõrvaldamist ning järel- ja jääktööde teostust. Kui lepingud ja seadused seda võimaldavad, tuleks arveid aktsepteerida alles selle järel. Täiendavalt tuvastatud märkused tuleb edastada vastavatele osakondadele.

Kontrollküsimus:

- Kas eksisteerib arusaadav, dateeritud ja kõikide asjaosaliste poolt allakirjutatud vastuvõtuprotokoll?

M 5.143 Võrgu dokumentatsiooni pidev edasikirjutamine ja revisjon

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: IT-juht

Võrke muudetakse pidevalt täiendavate juhtmestike, ümberehituste ja laiendamismeetmetega kuni aktiivsete võrgukomponentide täiendite ja versioonide täiustamiseni välja. Seetõttu tuleb IT-juhtmestiku dokumentatsiooni täiendamist käsitleda iga võrku puudutava muudatuse elementaarse osana. Alles pärast dokumentatsiooni täiendamise lõpetamist on muudatusmeede täielikult lõpuni viidud.

Lisaks üldise tööohutuse ja kontrollivõimaluse tagamisele on IT-juhtmestiku dokumentatsioonil ka veel järgnevad eesmärgid:

- lühikesed ümberlülitusajad võrgu laiendamisel,
- lihtne vigade piiritlemine ja otsing,
- lühikesed taasteajad vigade korral,
- hooldusleping̃ute majanduslikkus.

Kõiki muudatusest puudutatud dokumentatsiooni osasid peab kindlasti olema lihtne leida ja muudatustega kohandada. Dokumentatsiooni koostamise reeglistik peaks lihtsustama sellega ümberkäimist. Reeglistik peaks kirjeldama protseduure, dokumentatsiooni hõlmatavaid valdkondi ja nõudeid, näiteks ka nimetus- ja nummerdamisskeeme. Lisaks tuleks kontrollida, kas võrgudokumentatsiooni jaoks oleks mõttekas kasutada dokumendihaldust.

Dokumendihaldus saab muuhulgas kergendada ka järgnevaid dokumentatsiooniga kaasnevaid aspekte:

- muudatuste dokumenteerimine juba alates planeerimisfaasist,
- kõikide osalevate isikute informeerimine planeerimise kohta,
- kasutuse aktsepteerimisega seatud protsesside integreerimine,
- vana dokumentatsiooni arhiveerimine.

Lisaks saab kaablite ja võrgukomponentide ning nende lülituste dokumentatsiooni jaoks kasutada erinevaid tarkvaratööriistu. Osad nendest tööriistadest võimaldavad ühendada ja integreerida ka võrguhalduse süsteeme. Ka passiivse infrastruktuuri ühendusteede aktiivse kontrolli tugi on olemas.

Kontrollküsimus:

- Kas dokumentatsiooni hetkeseis ja viimase muudatuse sisseviimise aeg on selgelt tuvastatavad?

M 5.144 IT-kaabelduse demonteerimine

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: tehnikajuht

Kui IT-juhtmestikku enam üldse ei vajata, tuleb see oskuslikult eemaldada. Sellal kui tertsiaarjuhtmestikku kasutatakse sama kaua kui hoonet ennast, asendatakse olemasolev sekundaarjuhtmestik ja serveri- ning tehnikaruumide sisemine juhtmestik sageli võimsamaga. Kahjuks jäetakse praktikas vanad kaablid uute kaablite vedamisel sageli eemaldamata ja uued kaablid pannakse lihtsalt vanade peale. Eriti kehtib see paigaldustrasside ja topeltpõrandate puhul.

Selline teguviis vähendab ülevaatlikkust ja suurendab tulekoormust. Lisaks võib õhu liikumise takistamine tekitada probleeme ruumi sisekliimas. Seega on soovitatav juba trasside planeerimisel arvestada võimalusega, et hiljem võib olla tarvis kaableid eemaldada ja lisatud kaableid kontrollida. Sellest tuleneva trasside laiendamisvajadusega tuleb arvestada õigeaegselt. Ebavajalike kaablite kohta tuleb koostada ülevaade, millega kaablite eemaldamisel ja paigaldamisel saaks arvestada. Seejärel tuleb IT-juhtmestiku komponentide kohta käivat dokumentatsiooni vastavalt täiendada.

Kontrollküsimused:

- Kas vanad kaablid, mida ei lähe enam tarvis, eemaldatakse?
- Kas pärast IT-kaablite eemaldamist/vahetamist täiendati vastavalt ka juhtmestiku dokumentatsiooni?

M 5.145 Turvaline CUPSi kasutamine

Algatamise eest vastutavad: administraator, IT-juht

Rakendamise eest vastutavad: administraator

Unix -süsteemides kasutatakse sageli võrgutoega printimissüsteemi Common Unix Printing System (CUPS). CUPS ühildub paljude teiste printimissüsteemidega, näiteks CIFS/SMB (Common Internet File System-i/ Server Message Blockiga), mis võimaldavad faile ja printereid Windowsi all ühiskasutusse anda. CUPSi turvalise kasutamise jaoks tuleb arvestada järgnevate aspektidega, mis tuleb kindlaks määrata planeerimisel (vt M 2.397 Printerite, koopiamasinate ja multifunktsionaalsete seadmete kasutamise planeerimine) või valimisel (vt M 4.304z Printerite haldamine)

Üldised aspektid

- Lokaalne kasutamine või keskne prindiserver - CUPSi saab kasutada jaotatud rakendusena (töökohaarvutis olev klient kasutab kaugemalasuvat serverit) või lokaalselt. Vastavalt tuleb ka konfigureerimisel eristada, kas CUPSi klient ja CUPSi server asuvad samas IT-süsteemis või erinevate IT-süsteemide all. Kui need asuvad erinevate IT-süsteemide all, tuleb CUPSi kliendi konfigureerimisfailis (client.conf) määrata IP-aadress või vastava serveri arvuti nimi. Lokaalse kasutamise korral tuleb seevastu sisestada Loopback -aadress (127.0.0.1) või arvutinimi „localhost“. CUPSi server tuleb lokaalse kasutamise puhul failis cupsd.conf konfiguratsiooni sissekandega „Listen“ siduda Loopback -aadressiga, et teenus poleks võrgu kaudu kättesaadav. Sõltumata sellest, kas printerit tohivad kasutada ainult kohalikud IT-süsteemid, saab CUPSi administreerida tsentraalselt. Teenused nagu SSH või CUPS-Webserver võimaldavad seadistusi teha võrgu kaudu.
- Haldus- ja seisundiinfo + Kliente tuleb regulaarselt informeerida saadaolevate printerite ja nende seisundi kohta. „Broadcasting“ funktsiooni korral saadab server regulaarselt teate kõikidele printimisklientidele ja „Polling“ funktsiooni kasutades esitab printimisklient serverile ise vastava infopäringu. Kui info jaotamine saadaoleva printeri kaudu ei toimu Polling- või Broadcasting-meetodil, vaid manuaalsete sissekannete abil, tuleb see cupsd.conf sissekande all „Browsing“ välja lülitada („off“). „Browsing“ -meetodi kasutamisel tuleb juurdepääs piirata ainult ilmtingimata vajamineva arvutitega, või kui vajalik, võrkudega.
- Krüpteering - Kui soovite printimisülesandeid või seisundipäringuid edastada krüpteeritult, tuleb rakendada krüpteerimist toetavat protokolli. CUPSi puhul eelseadistatud Internet Printing Protcol (IPP) võimaldab TLS/SSLi (Transport Layer Security / Secure Sockets Layer-i) valikulise kasutamise läbi kommunikatsiooni kasutada krüpteeritult. Krüpteeringu jaoks läheb CUPS-kliendi seadistusfailis (client.conf) tarvis sissekannet „Encryption“. Võimalusel peaks selle väärtuseks olema alati „Always“. Lisaks tuleb CUPS-server varustada TLS/SSL-i sertifikaatide ja krüptograafiliste võtmetega.
- Kõrge kättesaadavus - CUPSi saab rakendada suure kättesaadavusega printimissüsteemi osana. Selleks läheb tarvis organisatoorsete ja tehniliste aspektide põhjalikku planeerimist. Eriti oluline on kindlaks määrata, millise põhjapaneva funktsiooni abil soovitakse kõrget kättesaadavust tagada, näiteks kas „failover-switching“ või „load-balancing“ funktsiooni. „ failoverswitc-

hing“ funktsiooni jaoks tuleb konfiguratsioonifailis cupsd.conf defineerida nn täpsed printeriklassid (konfiguratsiooni sissekanne „ImplicitClasses On“). Täiendavat informatsiooni selle tehnika kohta leiate CUPSi dokumentatsioonist.

Juurdepääs printerile

- Kasutajate haldamine - Prindiserverile tohivad ligi pääseda ainult volitatud kasutajad. Selleks vajalik õiguste haldamissüsteem võib asuda prindiserveril endal, kuid selle võib siduda ka olemasoleva autentimisprotsessiga. Tavakasutajad peavad prindiserveril saama kasutada ainult printerirakendust, neil ei tohi olla juurdepääsu selle serveri failidele ega kataloogidele. Kuna prindiserveri kasutajad peaksid prindiserverit tavaliselt kasutama ainult printimiseks ja nad ei pea vahetult serverisse näiteks SSHga sisse logima, tuleks süsteemikasutajate rühm printerikasutajate rühmast eraldada. Printerikasutajad tuleks luua selliselt, et prindiserveril oleks nende ainukeseks õiguseks vaid printimine. Printeri kasutajaid saab näiteks luua programmikäsuga „lppasswd -a kasutajanimi “. Määratlust, milline kasutaja millist printerit kasutada võib, saab täpsustada failis cupsd.conf. Ka siin kehtib põhimõte, et kasutajatele tuleks anda tõesti ainult vajalikud pääsuõigused ja mitte rohkem. Vältida tuleks seadistust, mis võimaldab kõikidel kasutajatel kasutada kõiki printereid. Erandiks on selle puhul lokaalsete printerite kasutamine. Kui IT-süsteemis on vähe printerikasutajaid ja kui kõik printerikasutajad on nagunii samaaegselt süsteemikasutajad, ei ole eraldi printerikasutajaid tarvis määrata.
- Autentimismeetodid: CUPS toetab autentimiseks erinevaid meetodeid, näites „HTTP-Basic“, „HTTP-Digest“ või autentimine sertifikaatide alusel. Autentimismeetodi saab määrata sissekandega „AuthType“ seadistusfailis cupsd.conf. Kuna „HTTP-Basic“ puhul edastatakse kasutajanimed ja paroolid teksti kujul üle võrgu, ei tohiks seda meetodit rakendada ilma täiendavate turvameetmeteta. Selle asemel tuleks autentimiseks kasutada sertifikaate või „HTTP-Digest“ meetodit.

Haldamine

CUPSi haldamisega võivad tegeleda ainult selleks volitatud isikud. Neid saab määrata seadistusfaili cupsd.conf sektsioonis “/admin”. CUPSi puhul saab teha mitmed seadistusi ka kaasasoleva Webserveri kaudu. Võrkude kaudu Webserverile tagatavad juurdepääsud tuleb piirata vajaliku miinimumini. Seadistusfaili cupsd.conf sektsioonis “/admin” saab sisestada arvutid, mis tohivadWebserveriga ühendust võtta. Alternatiivina võib Webserveri pääsuõiguste piiramiseks kasutada ka lokaalset paketifiltrit.

Logimine

CUPS pakub mitmeid võimalusi sündmuste logimiseks. Mitmeid aspekte, mida kirjeldatakse meetmes M 4.302 Printerite, koopiamasinate ja multifunktsionaalsete seadmete logimine , saab rakendada vastavate sissekannetega seadistusfailis cupsd.conf. Logide täpsusastet saab näiteks määrata sissekandega „LogLevel“.

Arhiveerimine

CUPS pakub võimalust väljaprinditud dokumente elektroonilisel kujul prindiserveri failisüsteemis arhiveerida. Selleks läheb failis cupsd.conf tarvis seadistussissekannet „ PreserveJobs“. Valikuliselt saab seejuures määrata arhiveeritud dokumentide maksimaalse arvu. Sellisel juhul kirjutatakse vanemad sissekanded uuemate dokumentidega üle. Arhiivide loomisel tuleb arhiveeritud dokumente vastavate mehhanismidega kaitsta volitamata juurdepääsu ja andmekao eest. Lisainfot leiate moodulist B 1.12 Arhiveerimine .

Kontrollküsimused:

- Kas CUPSi konfiguratsioon vastab printimise kohta väljastatud reeglistikule?
- Kas administraatoriõigustega juurdepääs CUPSi serverile on piiratud?
- Millist informatsiooni logitakse?

M 5.146 Multifunktsionaalsete seadmete lahutamine võrgust

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator

Sageli pole majanduslikel või praktiliselt kaalutlustel otstarbekas kasutada eraldi seadmeid printimiseks, skaneerimiseks, kopeerimiseks ning fakside saatmiseks ja vastuvõtmiseks. Alternatiiviks on multifunktsionaalsed seadmed (kõik-ühes-seadmed), mis toetavad mitut või kõiki loetletud funktsioone. Osaliselt pakuvad need seadmed ka täiendavaid kommunikatsiooniliideseid, näiteks juurdepääsuks võrku. Enamasti on multifunktsionaalsete seadmete haldamine üksikseadmetega võrreldes lihtsam ja nende puhul läheb tarvis vähem ühenduskaableid (voolukaableid ja vastavalt olukorrale ka andmekaableid). Multifunktsionaalseid seadmeid saab töökoha arvutiga ühendada tavaliselt otse või LANi kaudu.

Füüsiline ühendus LANi ja telefonivõrgu vahel

Teatud seadmetel on olemas faksi ja andmete kaugedastuse funktsioon, mis eeldab ühendamist telefonivõrku. Nii saab teiste IT-süsteemide külge liidetult luua füüsilise ühenduse LANi ja telefonivõrgu vahel. Kui vastavat ühendust ei kontrolli turvalüüs, võib see võimaldada volitamata internetijuurdepääsu, tekitades seeläbi volitamata isikutele võimaluse väljastpoolt LANile ligi pääseda. Volitamata andmeühenduste loomist tuleb igal juhul takistada. Erandiks on faksifunktsiooniga multifunktsionaalsed seadmed, mida ei ole tarvis telefonivõrguga ühendada. Need seadmed skaneerivad dokumendid sisse ja edastavad need andmeühenduse kaudu kesksele faksiserverile, mis asub tavaliselt samuti LANis. Faksi saatmine selle määratud vastuvõtjale toimub alles faksiserveri poolt, mis on ühendatud telefonivõrku. Faksiserveri kasutamisel tuleb rakendada moodulis B 5.6 Faksiserver soovitatud meetmeid. Telefonivõrgu toega multifunktsionaalsete seadmete kasutamisel tuleb otsustada, kas see ühendus on vajalik, st, kas vastav faksi- või andmete kaugedastuse funktsioon on vajalik. Kui telefonivõrku ühendamisest võib loobuda, saab vastavalt vajadusele rakendada järgnevaid kaitsemeetmeid:

- Seadme faksi- või andmete kaugedastuse funktsiooni desaktiveerimine.
- Telefonivõrku ühendamise kaabli eemaldamine. Kaablit ei tohi mitte mingil juhul telefonipesasse pista.
- Kui seade asub vabalt ligipääsetavas kohas, tuleks võimalusel telefonipesad vastavas ruumis desaktiveerida või telefonivõrgu liides seadme küljest eemaldada. Kui see on võimatu, tuleks regulaarselt kontrollida, et keegi ei oleks loonud volitamata ühendust telefonivõrguga.
- Kui multifunktsionaalse seadme faksi- või andmete kaugedastuse funktsiooni soovitakse kasutada, tuleb tagada, et selleks vajalik ühendus telefonivõrguga ei saaks viia kontrollimatu andmeühenduseni LANi ja võõra võrgu vahel. Võimalikud on järgnevad lahendused:
- Multifunktsionaalne seade ühendatakse Stand-Alone -arvutiga, st arvutiga, mis ei ole LANiga ühendatud. Selle lahenduse puhul on probleemiks asjaolu, et andmete transportimiseks arvuti ja LANi vahel tuleb kasutada andmekandjaid.
- Alternatiiviks on multifunktsionaalse seadme või sellega ühendatud arvuti eraldamine LANist täiendava turvalüüsi abil. Arvestada tuleb mooduliga B 3.301 Turvalüüs (tulemüür) .
- Täiendavaks alternatiiviks on multifunktsionaalse seadme või sellega ühendatud arvuti paigaldamine olemasoleva turvalüüsi demilitariseeritud tsooni.

Ka sel juhul tuleb rakendada moodulit B 3.301 Turvalüüs (tulemüür) .

Kõikide nimetatud lahendustega tuleb süstemaatiliselt IT-turbe kontseptsioonis arvestada ning need vajavad täiendavaid IT-turvameetmeid, näiteks kaitseks kahjulike programmide nagu arvutiviiruste või trooja hobuste eest.

Täiendavad kontrollküsimused:

- Kas multifunktsionaalsete seadmete faksi ja andmete kaugedastuse funktsioone vajatakse?
- Kas kontrollimatud andmeühendused LANi ja võõraste võrkude vahel on tõhusalt takistatud?

M 5.147 Turvalise side tagamine kataloogiteenuste abil

Algatamise eest vastutavad: IT-juht, infoturbe eest vastutav töötaja

Rakendamise eest vastutavad: IT juht, administraator

Andmevahetus kliendi ja kataloogiteenuse serveri vahel toimub võrguühenduste kaudu. Olenevalt kataloogiteenuse süsteemist ja võrgustruktuurist toimub sidepakettide, mis võivad teatud juhtudel sisaldada lisaks kataloogisisule ka autentimisinformatsiooni, edastamine kaitsmata kujul. Seejuures on sõltuvalt installeeritud operatsioonisüsteemist võimalik kasutada erinevaid võrguprotokolle. Tavaliselt toimub juurdepääs kataloogiteenustele standardiseeritud LDAP-protokolli kaudu, aga see võib leida aset ka firmaomaste protokollide kaudu. Andmete edastamine toimub LDAP-protokolli puhul eranditult IP-võrkude kaudu.

Kasutaja autentimine võib seejuures toimuda protseduuride järgi, mis ei edasta autentimisandmeid otse üle võrgu. Kliendi ja serveri vahelist side siiski põhimõtteliselt ei krüpteerita. Ka side krüpteerimise eest on vastutav kasutatav klient. Kui juurdepääs kataloogiteenuse serverile on vajalik väljastpoolt, tuleb realiseerida kliendi ja serveri vahelise sideühenduse kaitse, mis tagaks edastavatele andmetele piisava konfidentsiaalsuse. Seda on näiteks võimalik saavutada virtuaalse privaatvõrgu (VPN) kasutamise teel.

Teenusele suunatud arhitektuuri (SOA) puhul tuleb teenusekirjete kaitseks teenuste registris kontrollida kõiki registrile tehtud päringuid kasutajate (teenusetarbijate) kehtivuse suhtes:

- Kas vastav teenusetarbija kasutab kehtivat sertifikaati?
- Kas nõutavad pääsuatribuudid on kooskõlas kohaliku WS-Policy'ga?
- Kas teenusetarbija päring on edastatavas SOAP-sõnumis allkirjastatud?

Administraatoritel on tihti võimalik kataloogiteenuste süsteemile juurde pääseda kaugpääsu kasutades. Näideteks on terminali- või veebiteenused, mis võimaldavad brauseri kaudu juurdepääsu süsteemi andmetele.

Administratiivse juurdepääsu kitsendused ja kaitse

Kuna kaugpöörduse kaudu kättesaadavad andmed annavad olulist informatsiooni kataloogiteenuse ülesehituse ja konfiguratsiooni kohta, peab ka kaugpääs kataloogiteenusele olema kaitstud. Protokolle, mis ei ole piisavalt kaitstud, tuleks kasutada vaid äärmisel juhul küllaldast kaitset omavates võrkudes. Kui kataloogiteenusele on võimalik juurde pääseda HTTP-protokolli kaudu, peab kohustuslikuks muutma kõikide kasutajate autentimise, anonüümset juurdepääsu sel teel ei tohiks lubada. Lisaks sellele tuleks autentimisandmete edastamist kaitsta TLS/SSL kaudu (vt M 4.310 Kataloogiteenuste LDAP-pöörduste seadmine)

Kontrollküsimused:

- Kas juurdepääs kataloogiteenuse andmetele välisühenduste kaudu on vajalikul määral kaitstud?

- Kas on defineeritud, millistele süsteemi andmetele millistest võrkudest ja milliste vahenditega on juurdepääs lubatud?
- SOA korral: kas on ellu viidud juurdepääsukaitse teenuste registrile?

M 5.148 Turvaline välisvõrguühendus OpenVPN-i abil

Algatamise eest vastutavad: IT-juht, infoturbe eest vastutav töötaja

Elluviimise eest vastutavad: administraator

Kui andmete edastamine toimub renditud liinide või avalike võrkude kaudu, mis ei allu asutuse kontrollile, tuleb nendele luua vajalik kaitse. Kui seda ei tehta, võidakse edastatavaid andmeid pealt kuulata või nendega manipuleerida. Teatud juhtudel on ründajal isegi võimalik esineda volitatud kommunikatsioonipartnerina või VPN-terminalidega manipuleerida. OpenVPN on GNU GPL litsentsiga (General Public Licence) vabavara, mis võimaldab virtuaalsete privaatvõrkude (VPN) loomist krüpteeritud TLS/SSL-ühenduste kaudu. Põhimõtteliselt sobib OpenVPN kahe võrgu vahelise (site-to-site-VPNs), otspunktide vahelise (end-to-end VPNs) ja kaugpääsu (Remote-Acsess-VPNs) VPN-ühenduse loomiseks. OpenVPN omab krüpteerimiseks juurdepääsu OpenSSL programmi arhiividele ning kasutab valikuliselt UDP või TCP transpordiprotokolli. Vastupidiselt IPSec -le ei võimalda TLS/SSL kasutamine tunneli protokollina informatsiooni kaitset andmepakettide IP päistes. Eeliseks on, et TLS/SSL puhul ei ole nii palju mõlemapoolselt kooskõlastatavaid konfiguratsiooniparameetreid kui IPSec puhul.

OpenVPN -i turvaline kasutamine

Kuna OpenVPN baseerub TLS/SSl-il, tuleb järgida meetmes M 5.66 TLS-i/SSL-i kasutamine antud soovitusi. OpenVPN -i turvaliseks kasutamiseks tuleks selle aluseks olevat operatsioonisüsteemi muuta kindlamaks ja vastupidavamaks (nt installeerida ainult tõeliselt vajalikud programmipaketid). OpenVPN -i tööks vajalikud krüptograafiliste võtmete loomine, kommunikatsioonipartnerite vahel jaotamine ja haldamine peab toimuma turvaliselt. Lisaks tuleb kasutada piisava võtmepikkusega turvalisi autentimis- ja krüpteerimisprotseduure. Täpsemat informatsiooni krüpteerimis- ja autentimisprotseduuride valiku kohta sisaldab meede M 2.164 Sobiva krüptoprotseduuri valimine . Sertifikaadipõhine autentimine on logimise kõige turvalisem vorm. Seejuures on VPN-komponentidel (nt server ja server või server ja klient) privaatsed ja avalikud võtmed. Sertifikaatide kasutamisel tuleb autentimisprotseduuri ajal kontrollida sertifikaadi staatust PKI –ga (Public Key Infrastructure). Seejuures tuleb tagada, et OpenVPN -i server lubaks luua vaid ühendusi, mille on signeerinud talle tuntud sertitseerimiskeskus. Turvalisuse tõstmiseks tuleks kaaluda VPN-kasutajate sertifikaatide paigutamist kiipkaardile või mõnele teisele turvalisele tokenile. VPN-serverite seisukohalt on eriti tähtis, et välimisel võrguliidesel oleks mitteusaldusväärsest võrgust juurdepääs vaid kõige vajalikumatele teenustele. Ühendusi tohib luua vaid kõige vajalikumate süsteemide ja teenustega ning peale vajalike teenuste ei tohi VPN-serveril olla teisi aktiveeritud teenuseid. VPN-serverite kaitseks rünnakute eest tuleb need integreerida turvainfrastruktuuri vastavalt meetmele M 4.224 Virtuaalsete privaatvõrkude integreerimine turvalüüsidesse .

Virtuaalse privaatvõrgu funktsioonitest

Enne iga virtuaalse privaatvõrgu kasutuselevõttu tuleb kontrollida selle korrektset funktsioneerimist (eelkõige turvamehhanisme) meetmes M 4.319 VPNi lõppseadmete turvaline installeerimine kirjeldatud viisil. See peaks toimuma eraldi testimiskeskkonnas, kuna teisiti pole võimalik välistada, et töökeskkonnast saadetakse Interneti kaudu kaitsmata andmeid. Juhul kui virtuaalne privaatvõrk ei funktsioneeri soovikohaselt, on suur abi OpenVPN -i dokumentatsioonist.

Täiendavad kontrollküsimused:

- Kas IT-süsteem, millel toimub OpenVNP käitamine, on kindel ja vastupidav?

- Kas OpenVPN -i rakendamisel kasutatakse piisava võtmepikkusega autentimis- ja krüpteerimisprotseduure?
- Kas OpenVPN -i kasutamiseks valitud võtmevahetuse protseduur vastab turvanõuetele?
- Kas on garanteeritud, et OpenVPN -i rakendamisel kasutatakse krüpteerimiseks ja autentimiseks vaid piisava turvalisusega krüptoprotseduure?
- Kas on tagatud, et VPN-ühendusi on *OpenVPN* -i kasutamisel võimalik rajada vaid selleks ettenähtud IT-süsteemide ja teenuste vahel?

M 5.149 Turvaline välisvõrguühendus IPSec-i abil

Algatamise eest vastutavad: IT-juht, infoturbe eest vastutav töötaja

Rakendamise eest vastutavad: administraator

Internet Protocol Security (IPSec) on standard, mis defineeritakse terve rea RFC-de IEEE Internet-draftide kaudu. IPSec koosneb tervest reast protokollidest, mis on ette nähtud IP-kommunikatsiooni krüpteerimiseks, tervikluse tagamiseks, autentimiseks ja võtmete haldamiseks. IPSec abil saab anda kasutajate käsutusse igakülgselt läbipaistvad ja turvalised arvutisüsteemide ühendused. IPSec -i kasutatakse majanduses ja halduses tihti virtuaalse privaatvõrgu juurutamiseks.

IPSec protokollid

IPSec -is kirjeldatakse mitmeid turvamehhanisme, näiteks

- autentimispäis (AH)
- sõnumi kapselturve (ESP).

iPSec töörežiimid

Autentimispäis võimaldab edastatud andmete autentimist ning peab sellega edukalt ära hoidma võimalikke IP aadressi võltsimise juhtusid või ründeid sessiooni ülevõtmiseks. Sõnumi kapselturve (Encapsulating Security Payload) võimaldab lisaks autentimisele ka edastavate andmete krüpteerimist. Kuna ESP-d on võimalik kasutada ka krüpteerimata, ühesõnaga ainult autentimiseks, ei ole AH kasutamine laialdaselt levinud. Et ühendusvariandid oleks võimalikult paindlikud, pakub IPSec kasutamiseks mõlemaid töörežiime:

- Transpordirežiim
- Tunnelrežiim

Transpordirežiimis võetakse esialgsete pakettide IP-päis üle ning see täidab marsruutimise funktsiooni. Transpordirežiimis krüpteeritakse vaid paketi sisu, mitte aga IP-päis. See režiim sobib vaid kommunikatsiooniühendusteks, mille puhul on tunneli lõpp-punktid samaaegselt kommunikatsiooni lõpp-punktideks, niisiis näiteks vahetu klient-server-kommunikatsiooni korral. Kuna edastamiseks vajalik info ei ole krüpteeritud, võivad selle vahel asuvad marsruuterid seda vahetult töödelda. Tunnelrežiimis krüpteeritakse kogu pakett, kaasa arvatud IP-päis, et kaitsta ka aadresse puudutavat siseinformatsiooni volitamata juurdepääsu eest. Ründaja saab seeläbi kindlaks määrata vaid tunneli lõpp-punktid, mitte aga kindlaks teha ühenduse kogu kulgemisteed. Kasutusala aluseks võttes tuleb virtuaalsele privaatvõrgule valida sobiv töörežiim. Erinevates kohtades asuvate võrguühenduste korral tuleks ESPd kasutada kombinatsioonis tunnelrežiimiga. Kahe arvuti vahelise kommunikatsiooni korral kohtvõrgus tuleks valida transpordirežiim.

IPSec võtmete haldus

Võtmete genereerimiseks ja jaotamiseks kasutab IPSec Internet Key Exchange (IKE) protokolli. IKE kirjeldab, kuidas toimub turvaparameetrite seadistamine ja ühisvõtmete väljavahetamine. IKE jaguneb kahte järgnevalt kirjeldatud faasi.

Faas 1

Esimeses faasis toimub ISAKMP Security Association' i seadistamine, kusjuures ISAKMP tähistab Interneti turvaühenduse sisseseadmist ja võtmehalduse protokolli. Turvaühendus (SA) kujutab endast autenditud, krüpteeritud kanalit ning koosneb reeglina turvaparameetri indeksist, siht-IP-aadressist ja turvaprotokolli identifikaatorist. SA võib sisse seada kas main mode 't või aggressive mode 'i kasutades.

Režiimid erinevad üksteisest vahetatavate sõnumite arvu ja vahetatud andmete krüpteerimise poolest. Main mode korral kaalutakse esimese sammuna mõlemate kommunikatsioonipartnerite poolt ühise salajase võtme kasutuselevõttu Diffi-Hellmanni võtmevahetusprotseduuri järgi. Tegelik autentimisandmete edastamine selle võtmega toimub kaitstult. Autentimine võib toimuda vaid mõlemale suhtluspartnerile tuntud märkide ahela (Pre Shared Key, PSK) või sertifikaatide abil. Selles faasis vajatakse seadistamiseks main modes kuut sõnumit. Aggressive mode vajab vaid kolme sõnumit, kuna autentimisandmete jaoks ei looda oma võtit. Selle asemel luuakse eeljagatud võtmest räsifunktsiooni abil kontrollsumma ja edastatakse see. Välisvõrgu turvaliseks ühendamiseks IPSec 'iga tuleb valida sobiv režiim. Aggressive mode on küll kiirem kui main mode , peaks aga kasutust leidma vaid erandjuhtudel, kuna see ei ole nii turvaline. Näiteks saab sõnastikuründe (dictionary attack) või jõhkra jõuga ründe (brute force attack) puhul tuletada eeljagatud võtme kontrollsummast. Et korrigeerida IKE aggressive modus 'e kitsaskohti eeljagatud võtmete kasutamisel, toetavad mõned tootjad XAUTH meetodit. Seejuures laiendatakse IKE-protokolli, et oleks võimalik rakendada mehhanisme nagu RADIUS ja teised.

Faas 2

Teises faasis luuakse turvaühendused ja võtmed, millega peab töötama IPSec turvaprotokoll või iga teine protokoll, mis vajab krüptograafilist võtmematerjali.

Turvaline konfigureerimine

IPSec 'i turvalisel konfigureerimisel tuleb arvestada järgmiste aspektidega:

- Võtmete vahetamisel tuleb kasutada piisava võtmepikkusega turvalist protseduuri. Diffie Hellmani võtmevahetusprotseduuri korral tuleks kasutada vähemalt ISAKMP/Oakley grupp 2 (1024 bitti) või grupp 5 (1536 bitti) protokolle.
- Krüpteerimiseks tuleb kasutada piisava võtmepikkusega turvalisi krüptoprotseduure (AES-128, Triple-DES).
- Kasutada tuleb piisava pikkusega räsialgoritme (RIPEMD-160, SHA-224, SHA-256, SH-384 või SHA-512).
- Autentimisprotseduurid peavad vastama tehnika tasemele. Vastava kasutusjuhuse jaoks ei tohi teada olla ühtki olulise tähtsusega turvaauku.
- IKE faaside 1 ja 2 vaheajad ei tohiks olla valitud liiga pikad, kõige rohkem näiteks 20 sekundit 1. faasile ja 15 sekundit 2. faasile.
- Kaugpääsu VPN-ide korral tuleks eeljagatud võtmetest (PSK) kui autentimismeetodist loobuda, kuna võtmete haldus sel juhul on väga kulukas.
- Kui kasutatakse eeljagatud võtmeid, tuleks valida turvalised võtmed, vastasel korral on võtmeid võimalik sõnastikurünnete abil tuletada.
- Autentima peab end nii VPN-klient VPN-serveri kui ka VPN-server VPN-kliendi suhtes.
- Sertifikaatide kasutamisel autentimiseks tuleb iga autentimisprotseduuri ajal kontrollida sertifikaadi staatust PKI –ga (Public Key Infrastructure).

Mitteusaldusväärsete võrkude kaudu turvalise VPN-andevahetuse pidamiseks peavad tsentraalsed serverid olema kättesaadavad ka mitteusaldusväärsest võrgust. Kaitseks rünnete eest LANile tuleb ründepind minimeerida. Seetõttu esitatakse osalevatele VPN-serveritele lisaks järgmised nõuded:

- Peale IPSec ühenduse ei peaks VPN-server pakkuma teisi võrguteenuseid.

- VPN-serveri ja LAN-i vahel tuleks luua vaid olulise tähtsusega ühendused.
- Kuna IPSec 'i puhul on tegemist väga keeruka protokolliperega, mis hõlmab mitmeid teenuseid, tuleks mittevajalikud teenused välja lülitada. Võimalusel tuleks lubada kasutada vaid teenuseid IKE, ESP ja vajadusel AH.

Pakutavad teenused ja antavad volitused tuleks arusaadavalt dokumenteerida. VPN-i turvalisuse pidevaks tõstmiseks tuleb lisaks järgida meetmes M 4.321 VPNi turvaline käitamine antud soovitusi.

Kontrollküsimused:

- Kas IPSec 'i kasutatakse sobivas töörežiimis? Kas on välja valitud sobiv SA-režiim?
- Kas IPSec -konfiguratsiooni juures on rakendatud virtuaalsele privaatvõrgule esitatavad turvanõuded?
- Kas IPSec- konfiguratsiooni juurde valitud võtmevahetusprotseduur vastab turvanõuetele?
- Kas on garanteeritud, et IPSec 'i rakendamisel kasutatakse krüpteerimiseks ja autentimiseks vaid piisava turvalisusega krüptoprotseduure?
- Kas VPN-terminalides on kättesaadavad vaid tõepoolest vajalikud teenused?

M 5.150 Penetratsioonitestide läbiviimine

Algatamise eest vastutavad: asutuse/ettevõtte juhatus, IT-juht, infoturbe eest vastutav töötaja

Rakendamise eest vastutavad: IT-juht, administraator

Penetratsioonitestid on äraproovitud ja sobiv protseduur IT-võrgu või üksiku IT-süsteemi turvalisuse kindlaksmääramisel. Nende läbiviimise eesmärk on anda eelnev hinnang IT-kooslusele või üksikule IT-süsteemile tehtava rünnaku õnnestumise võimalusele ja tuletada selle põhjal vajalikud täiendavad turvameetmed, näiteks juba rakendatud turvameetmete tõhususe kontroll.

Turvakriitiliste võrkude ja süsteemide turvalisuse kontrolliks tuleks penetratsioonitesti teha regulaarselt. Seejuures kontrollitakse põhjalikult installeeritud rakendusi (veebirakendus, meiliserver jne) või vastavalt aluseks olevaid kandesüsteeme (operatsioonisüsteem, andmebaas jne).

Tüüpilised rakenduspunktid penetratsioonitesti läbiviimiseks on järgmised:

- võrguühenduselemendid (marsruuterid, kommutaatorid, lüüsid);
- turvalüüs (paketifiltrid, sissetungi tuvastuse süsteem (intrusion detection system), viiruseskannerid jne);
- serverid (andmebaasiserver, veebiserver, failiserver, salvestussüsteemid jne);
- telekommunikatsiooniseadmed;
- veebirakendused (nt internetiühendus, protseduuride töötlemine, veebipood);
- veebiteenused (nt REST-liides, SOAP-API, SOA);
- kliendid;
- traadita võrgud (WLAN, Bluetooth);
- infrastruktuuri seadmed (juurdepääsukontrolli mehhanismid).

Üldiselt jagatakse penetratsioonitestid funktsionaaltestideks (black-box testing) ja strukturaaltestideks (white-box testing). Funktsionaaltestimisel on penetratsioonitesti läbiviijate käsutuses vaid sihtsüsteemi aadresse puudutav info, muud informatsiooni neile ei anta. Testimisel funktsionaalmeetodil simuleeritakse tüüpilist rünnet väljastpoolt, kusjuures ründajal puuduvad täielikud teadmised sihtsüsteemist. Strukturaalmeetodil penetratsioonitesti läbiviijatel seevastu on olemas laiaulatuslik, nende jaoks vajalik informatsioon testitava süsteemi kohta. Selle hulka kuulub näiteks info IP-aadresside, sisevõrgu, kasutatud tark- ja riistvara jne kohta. Nimetatud info saadakse eelnevalt tellijalt.

On vaieldav, kas funktsionaal- ja strukturaaltestimismeetodite eristamine on tänapäeval veel vajalik. Näiteks kätkeb funktsionaaltestimismeetod endas puuduliku informatsiooni tõttu suuremat, aga täiesti välditavat ohtu tekitada ettekavatsemata kahju. Lisaks sellele võivad puuduliku informatsiooni tõttu kahe silma vahele jääda ka turvaaugud. On ka oht, et funktsionaaltestimise käigus ei

avastata hästi informeeritud organisatsioonisisese pahategija rünnet. Seepärast tuleb penetratsioonitesti läbiviimiseks anda läbiviijate käsutusse kogu testitavat süsteemi puudutav vajalik info, et minimeerida testimisega kaasneda võivat riski ning tagada võimalikult täiuslik turvaaukude avastamine. Penetratsioonitestide klassifitseerimine võimalikult automatiseeritud turvaaukude otsinguks (ründeohu jälgimine) ning suurelt osalt manuaalseks turvarevisjoniks näib seega tänast teadmiste taset arvestades praktilisem ja edukam.

Penetratsioonitesti läbiviijale esitatavad isikuomadusi puudutavad ja erialased nõuded

Penetratsioonitestide läbiviimisele esitatakse kõrgeid nõudeid ning see äärmist täpsust nõudev ülesanne, mis võib avaldada mõju kogu IT-tööle.

Seetõttu tuleks selleks kasutada vaid küllaldase kvalifikatsiooniga ja usaldusväärset personali, kellel on põhjalikud teadmised järgmistel aladel:

- operatsioonisüsteemide ja rakenduste haldus;
- võrguprotokollid ja võrguliikluse analüüs;
- turvatooted (nt turvalüüsid, sissetungi tuvastuse süsteemid jne);
- programmeerimiskeeled;
- turvaaukude skannerid;
- auditi- ja haldustarkvara.

Kui penetratsioonitestide läbiviimine tellitakse väljast, tuleks jälgida, et valitaks kvalifitseeritud ja usaldusväärne teenuseosutaja (vt M 2.252 Väljasttellitava teenuse sobiva tarnija valimine), kelle käsutuses on vastava kvalifikatsiooniga usaldusväärsed töötajad. Lisaks peaksid penetratsioonitestide pakkujad suutma tellijale esitleda struktureeritud metoodikat penetratsioonitesti läbiviimiseks, mille põhjal oleks võimalik välja töötada vastav individuaalne protseduur.

Penetratsioonitesti struktureerimine ja protseduur

Ettevalmistusfaasis peavad tellija ja tellimuse täitja määrama kõigepealt võimalikult täpselt kindlaks penetratsioonitesti eesmärgid ja ulatuse. Testi teostaja peaks seejuures tutvustama tellijale struktureeritud protseduuri, milles pooled peavad kokku leppima. Kooskõlastamisprotsessi käigus tuleks silmas pidada, et teatud juhtudel peavad kolmandad isikud olema plaanitavast penetratsioonitestist informeeritud või selles osalema. Reeglina peavad protseduuri olema kaasatud personaliesindus ja andmekaitse eest vastutav töötaja, sageli ka veebimahutaja. Tellija ja teenuseosutaja peaksid juba eelnevalt teatud kindlates eeldustes kokku leppima.

Nende hulka kuuluvad näiteks:

- kokkulepped vaikimiskohustuses;

- kokkulepped riist- ja tarkvara kasutamises;
- kokkulepped testitavates IT-süsteemides ja IT-rakendustes;
- penetratsioonitestide teostajatele lubatud ja mittelubatud tegevuste kindlaksmääramine, et vältida maksimaalselt tekkida võivat kahju;
- kokkulepped, mis puudutavad andmekandjatega ümberkäimist enne ja pärast testimist ning selle ajal (andmekandjad võivad sisaldada tundlikku informatsiooni testi tulemuste kohta);
- penetratsioonitesti läbiviimise koha ning analüüsi ja raporti esitamise kindlaksmääramine;
- testi läbiviimise tähtaegade kindlaksmääramine koos hooldustähtaegadega;
- detailsed kokkulepped pääsuks internetti või testimissüsteemi ühendamiseks internetiga penetratsioonitestide läbiviimise ja analüüsimise ajal;
- kokkulepped vastutusalades ja kontaktisikute kättesaadavuses ning hädaolukorraks valmisolekus.

Järgnevas informatsioonifaasis koguvad testijad võimalikult palju informatsiooni testitava süsteemi kohta. Seejärel analüüsitakse testi ettevalmistamiseks kogutud informatsiooni, pidades silmas potentsiaalseid turvaauke. Penetratsioonitesti tegelikus testimisfaasis tuleks võimaluse korral vältida meetodeid, mille kasutamise tagajärg võib olla testitud IT-süsteemidele või IT-rakendustele destruktiivne tulemus. Nii näiteks on teenusetõkestusründed suunatud selle vastu, et ära hoida juurdepääsu üksikutele teenustele, süsteemidele või võrgusegmentidele. Selliste rünnete võimalikkust saab tihti juba eelnevalt süsteemianalüüsi kaudu kindlaks teha, nii et sellised ründed on penetratsioonitesti käigus üleliigsed. Kui aga penetratsioonitesti käigus otsustatakse siiski teenusetõkestusründeid või sarnaseid destruktiivseid ründeid läbi viia, peaks see toimuma väljaspool süsteemi produktiivset kasutusaega. Vajaduse korral võib sellist rünnet simuleerida ka testimissüsteemi abil. Protseduuride suhtes tuleks saavutada üksikasjalikud kokkulepped. Alles seejärel võetakse ette aktiivsed sissetungimiskatsed. Seejuures tuleb rangelt kinni pidada kokkulepitud hooldusaegadest ja terminitest. Kui ajakava on vaja muuta, tuleb see kindlasti tellijaga kooskõlastada. Vastasel juhul suureneb oht, et tellija kindlaksmääratud penetratsioonitesti toimingud aetakse segamini tegelike rünnetega. Soovitatav on kogu penetratsioonitest täielikult salvestada ja dokumenteerida.

Selleks, et saada võimalikult põhjalikud tulemused, tuleks pöörata tähelepanu sellele, et penetratsioonitestid tuleb läbi viia vahetult testitavatel IT-süsteemidel ja vältides vahelelülitatud aktiivseid võrguühenduselemente, nagu näiteks paketifiltrid. Kui on tegemist eriliste põhjustega viia test läbi aktiivsete vahelelülitatud turvakomponentidega, tuleb jälgida, et seejuures jäävad rakenduses esinevad turvaprobleemid avastamata, sest ees asuvad komponendid püüavad ründekatsed penetratsioonitestis kinni. Sellised avastamata jäänud nõrgad kohad on siiski piisavalt riskantsed, sest sageli võidakse muudetud ründega kahjustada kaitsesüsteeme ja kasutada ära nõrku kohti.

Tüüpilised ründetehnikad

- **Võrgu ja pordi skaneerimine** – kasutatakse selleks, et leida üles võrgu aktiivsed IT-süsteemid ja identifitseerida seal pakutavad teenused (pordid). IT-administratsioon teeb taolisi päringuid, et saada andmeid kasutatud IT-süsteemi hetkestaatuse kohta. Ründaja on teatud juhtudel võimeline selle informatsiooni abil identifitseerima üksikute IT-süsteemide nõrku kohti ja korraldama selle informatsiooni alusel ründe.
- **Puuduliku sisestuskontrolli ärakasutamine**. Sisestuskontrolliks nimetatakse protseduuri, mille käigus rakendusele täiendavaks töötlemiseks edastatavad kasutaja sisestused (andmed) esmalt filtreeritakse, puhastatakse või lükatakse tagasi. Filtreerimise eesmärk on takistada rakendusele ohtliku koodi edastamist, mille levimine kutsub esile vigu, näiteks konfidentsiaalse info avalikuks tulekut. Ründemeetodid, mille abil on võimalik taolisi vigu esile kutsuda, on näiteks murdskriptimine (cross-site scripting), SQL-süst, LDAP-süst, OS-süst ja hägustus.
- **Teenusetõkestusründed** – IT-süsteemidele või võrkudele suunatud ründed eesmärgiga kõrvaldada üks või mitmed käsutusse antud teenustest. Seda on võimalik teha suurenenud päringute tõttu tõusnud koormuse, massiliselt tõusnud andmete laekumise (nt e-kirjad), aga ka võimalike tarkvaravigade sihiliku ärakasutamise abil. Teenusetõkestusrünnete tuntud näide on surmasond (ping of death).
- **Informatsiooni kogumine**, mille all mõistetakse edaspidiseks ründeks vajaliku informatsiooni kogumist. Näide sellisest informatsioonist on kataloogide või serveri jaoks kasutatav numereerimisskeem.
- **Manipuleerimine (social engineering)**, mille all mõistetakse näiteks teeseldud kõnesid või muud kontaktivõttu isikutega, kes kasutavad vaadeldavat IT-süsteemi. Tavaliselt on selle eesmärk koguda konfidentsiaalset informatsiooni, selgitada näiteks välja paroole (vt G 5.42 Inimestega manipuleerimine (Social Engineering)).
- **Telefoniskanner (war dialer**), mille kasutamise all mõistetakse automaatseid ja süstemaatilisi katseid välja uurida telefoninumbreid, mis on ühenduses mingi modemiga. Sihtsüsteemi telefoninumbritele helistades püütakse vastavat modemit avastada.
- **Paroolide muukimine**, mille käigus testitakse paroolide turvalisust või tugevust niinimetatud sõnastikurünnete, jõhkra jõuga rünnete või dekrüpteerimiskatsete abil.
- **Tarkvara turvaaukude ärakasutamine**, millega kontrollitakse näiteks, kas installeeritud tarkvara on tundlik teatud eksploitide suhtes, või on see vigaselt konfigureeritud, kas selles on turvaaukusid või on see vananenud. Tihti uuritakse ka, kas äkki on võimalik ära kasutada vastava toote standardinstallatsiooni turvaaukusid.
- **Krüptograafilised ründed**, mille sisu seisneb näiteks kasutatud krüptograafiliste mehhanismide ning võtmete halduse tugevuse ja juurutamise väljaselgitamises.
- **Infrastruktuuri uuringud,** mille käigus selgitatakse muu hulgas välja ka ehituslikud turvameetmed, juurdepääsu- ja lukustusseadmed, aga ka materjalide jäätmekäitlus. Üks selliseid variante on niinimetatud prügisorimine (dumpster diving), st kasulike dokumentide või andmekandjate otsimine prügi hulgast (paberikorvid, prügikonteinerid).

Analüüsi ja aruandluse faasis kogutakse tulemused kokku, analüüsitakse neid ning koostatakse aruanne. Kogu penetratsioonitesti läbiviimise käigus saadud info tuleb säilitada turvaeeskirjade kohaselt. Tellija peaks tellimuse teostajat eelnevalt kohustama, kõik penetratsioonitesti puudutavad salvestused täies ulatuses tellijale üle andma või hävitama.

Aruanne peaks lisaks leitud turvaaukude loetelule sisaldama ka soovitusi, kuidas tuleks avastatud turvaaukudega ümber käia. Soovitatav on koostada ka plaan aruandes nimetatud meetmete rakendamiseks, kaasa arvatud prioriseerimine. Haldustegevuse jaoks peaks lõpparuanne sisaldama ka kokkuvõtet, milles on antud ülevaade olulise tähtsusega testimistulemustest ning edaspidiseks tegevuseks soovitatavatest toimingutest. Lõpparuanne tuleb esitada infoturbe eest vastutavale töötajale ning vastutavatele administraatorile. Soovitatavalt peaks penetratsioonitesti kõikides faasides tellija ja tellimuse teostaja koostöös valmima kokkuleppeid ja tulemusi kirjeldav ühine dokumentatsioon.

Kontrollküsimused:

- Kas penetratsioonitestide läbiviimiseks kasutatakse vaid usaldusväärset ja kvalifitseeritud personali?
- Kas on garanteeritud, et penetratsioonitestid tellitakse vaid usaldusväärsetelt ja kvalifitseeritud teenuseosutajatelt?
- Kas on garanteeritud, et penetratsioonitestide tulemused on piisavalt kaitstud ning nendega ümberkäimine usaldusväärne?
- Kas penetratsioonitestide lõpparuanded esitatakse infoturbe eest vastutavale töötajale ja vastutavale administraatorile?
- Kas kõikide penetratsioonitestide teostajatega on eelnevalt sõlmitud detailsed kokkulepped testide läbiviimiseks ja analüüsimiseks?
- Kas enne penetratsioonitestide läbiviimist on saadud nõusolek kõikidest vastutavatest keskustest?
- Kas penetratsioonitestide läbiviimise ajaks on kohustuslikus korras kindlaks määratud kontaktisikud ja nende kättesaadavus?
- Kas kontaktisikud ja nende kättesaadavus penetratsioonitesti läbiviimise ajal on siduvalt kindlaks määratud?

M 5.151 Samba veebiadministreerimistööriista turvaline konfigureerimine

Algatamise eest vastutavad: infoturvaspetsialist, IT-juht
Rakendamise eest vastutavad: administraator

Samba veebiadministreerimistööriista (SWAT) puhul on tegu veebipõhise konfigureerimisprogrammiga, mis on olnud kindel osa Sambast juba alates versioonist 2.0. Sõltuvalt distrost installeeritakse SWAT koos Samba serveripakettidega või siis pakutakse seda valikuliste pakettidena. SWAT käivitatakse internetideemoni kaudu (nt inetd või xinetd) ja seda ei saa käitada eraldi deemonina. SWATi kasutamisel tuleks arvestada, et muudatuste korral kirjutab SWAT faili smb.conf täielikult üle. Sellega kustutatakse ka kõik kommentaariread ning kõik parameetrid, mille väärtused vastavad standardväärtustele. Ka parameetrid „*include*" ja „*copy*" eemaldatakse. SWATi ei saa kasutada, kui mõni nendest parameetritest on vajalik. smb.conf failis leiduvad jutumärkides parameetriväärtused kustutab SWAT pärast esimest jutumärki (").

SWATi juurdepääsu desaktiveerimine või piiramine

Kui SWATi ei kasutata Samba-serveri administreerimiseks ja konfigureerimiseks, tuleks SWAT eemaldada. Kui see on võimatu, tuleb desaktiveerida SWATi käivitamine internetideemoni kaudu. Xinetdi puhul juhitakse SWAT-teenuse käivitamist tavaliselt failiga /etc/xinet.d/swat või /etc/xinet.d/samba. Parameetriga „*disable*" ei saa internetideemon siseneva pärigu korral SWATi käivitada. Kui SWATi kasutatakse ainult lokaalse Samba-serveri administreerimiseks ja konfigureerimiseks, tuleb SWATi käideldavust piirata nõnda, et see oleks kättesaadav ainult lokaalse arvuti päringutele. Selle tagab internetideemonis xinetd parameeter „*only_from = localhost*" vastavas konfiguratsioonifailis (tavaliselt /etc/xinetd.conf). Kui SWATi kasutatakse Samba-serveri administreerimiseks ja konfigureerimiseks kaugserverist, tuleks kaaluda vastavat juurdepääsupiirangut. Juurdepääs SWATile peaks piirduma ainult nende arvutitega, kus seda vajatakse. Kui kasutatakse internetideemonit xinetd, võib seda teha parameetriga „*only_from*" vastavas konfiguratsioonifailis (nt „*only_from*=128.138.193.0").

Sisselogimisandmete turvaline ülekandmine

SWATi tohib Samba-serveri administreerimiseks kasutada ainult usaldusväärsete võrkude kaudu. Kuna SWAT ei toeta *Hypertext Transfer Protocol Secure* (HTTPS) protokolli, edastatakse kogu info loetava teksti kujul. Kõrge turbevajaduse korral tuleks SWATi kasutamisest loobuda või side krüpteerida. Krüpteerimiseks võib kasutada virtuaalset privaatvõrku (VPN) või krüptograafilist tunnelit. Järgnevalt on selgitatud, kuidas programmi „stunnel" (versioon nr 4) kasutamise abil saab kommunikatsioon toimuda krüptograafilise tunneli kaudu. Esmalt tuleb openssl-iga luua stunnel-i jaoks sertifikaat. Selleks tuleb kasutada järgnevat käsklust:

```
root# /usr/bin/openssl req -new -x509 -days 365 -nodes \
config /usr/share/doc/packages/stunnel/stunnel.cnf \
out /etc/stunnel/stunnel.pem -keyout /etc/stunnel/stunnel.pem
```

On võimalik, et stunnel ootab sertifikaati ja võtit mõnes muus kohas. Et seda teada saada, võib kasutada käsku „*stunnel -Version*". Vajadusel tuleb muuta stunneli konfiguratsiooni või ülal näidatud openssl-i käsklust. Seejärel tuleb käsuga chmod 600 /etc/stunnel/stunnel.pem tagada, et privaatvõti ja sertifikaat oleksid volitamatu juurdepääsu eest piisavalt kaitstud. Vastasel korral stunnel ei käivitu.

Seejärel tuleb luua konfiguratsioonifail /etc/stunnel/swat.conf:

```
   exec = /usr/sbin/swat
execargs = swat


server swat
{
socket_type = stream
wait = no
user = root
port = 901
server = /usr/sbin/stunnnel
server_args = /etc/stunnnel/swat.conf
disable = no
}
```

Kui xinetd on uue konfiguratsioonifaili lugemise lõpetanud, saab SWATi DNSi nime abil kasutada aadressilt https:// või Samba-serveri:901.

SWATi autentimis- ja autoriseerimisskeem

SWATis kasutatakse väga lihtsat autentimis- ja autoriseerimisskeemi. Autentimine toimub SWATi käitava serveri lokaalsete mehhanismide kaudu. SWAT aktsepteerib iga kasutaja, kes suudab end serveris edukalt autentida. Iga kasutaja, kellel on failisüsteemis lugemisõigused Samba-serveri konfiguratsioonifailile smb.conf, võib seejärel lasta endale konfiguratsiooni väljastada. Kasutajad, kellel on ka konfiguratsioonifaili smb.conf kirjutamisõigus, tohivad konfiguratsiooni muuta.

Kõiki muid operatsioone, nt Samba-serveri taaskäivitamist või ühenduse katkestamist Samba-serveriga, saab teha ainult kasutaja, kelle kasutaja identifitseerimise (UID) numbriks on 0. Tavaliselt on selleks kasutaja tähistusega „root”.

Täiendavad kontrollküsimused:

- Kas administraatorid teavad, et SWAT kirjutab muudatuste korral faili smb.conf täielikult uuesti?
- Kas juhul, kui SWATi ei kasutata Samba administreerimiseks ega konfigureerimiseks, on SWAT eemaldatud või desaktiveeritud?
- Kas juhul, kui SWATi kasutatakse ainult lokaalse Samba-serveri administreerimiseks ja konfigureerimiseks, piirdub juurdepääs SWATile lokaalse arvuti päringutega?
- Kas juhul, kui SWATi kasutatakse ainult kaugarvutite administreerimiseks ja konfigureerimiseks, piirdub juurdepääs SWATile usaldusväärsete arvutite päringutega?
- Kas SWATi kasutatakse ainult usaldusväärsete võrkude kaudu, või kas kommunikatsioon krüpteeritakse? - Kas SWATi kasutatakse turvalise HTTPS-ühenduse kaudu?

M 5.152 Info ja ressursside vahetamine võrdõigusteenuste (p2p) kaudu

Algatamise eest vastutavad: IT-juht, infoturbespetsialist

Rakendamise eest vastutavad: administraator

Võrdõigusteenuseks (sageli kasutatakse lühendit „P2P") nimetatakse infovahetust, mis toimub samaõiguslike IT-süsteemide („ peers ") vahel. Iga IT-süsteem saab seejuures teenuseid pakkuda või kasutada. Selleks loodud sideühenduse kaudu saavad mitu IT-süsteemi ressursse omavahel hajusalt jagada. Nõnda koondatakse ühte IT-süsteemi kokku serveri ja kliendi tavapärased funktsioonid. Võrdõigusrakendusi kasutatakse sageli selleks, et pakkuda teistele partneritele järgmiseid teenuseid:

- teiste IT-süsteemide kasutajatele võimalus kasutada kohaliku IT-süsteemiga ühendatud printereid,
- juurdepääs IT-süsteemi paigaldatud salvestuskohtadele või kohapeal ühendatud kõvaketastele („File-Sharing"),
- otseside lühiteadete kaudu („Messaging") ja
- internetitelefon.

Võrdõigusteenuste eelised

Erinevalt serveri toega arhitektuurist on võrdõigusteenustel mitmeid eeliseid:

- Eriotstarbelise serveri soetamine ja käigushoidmine toob kaasa täiendavaid kulutusi.
- Keskserveri tõrke korral ei saa ressursse enam kasutada („Single Point of Failure"). Kui võrdõigusteenuse kliendis esineb tõrge, suudavad üldjuhul teised kliendid teda asendada.
- Geograafiliselt lähestikku asuvad kliendid saavad omavahel infot vahetada tõhusamalt kui näiteks olukorras, kus selleks tuleb kasutada kaugel asuvat serverit.
- Serverid vajavad klientidest rohkem ribalaiust, protsessori jõudlust ja suuremat kõvaketta- ja töömälu. Need nõuded saab võrdõigusvõrkudes klientide vahel laiali jaotada ja nõnda saab kasutada seal hetkel vabana seisvaid ressursse.
- Ühiskasutusse antud info on sageli olemas mitmel kliendil, st eksisteerib liiasusega.

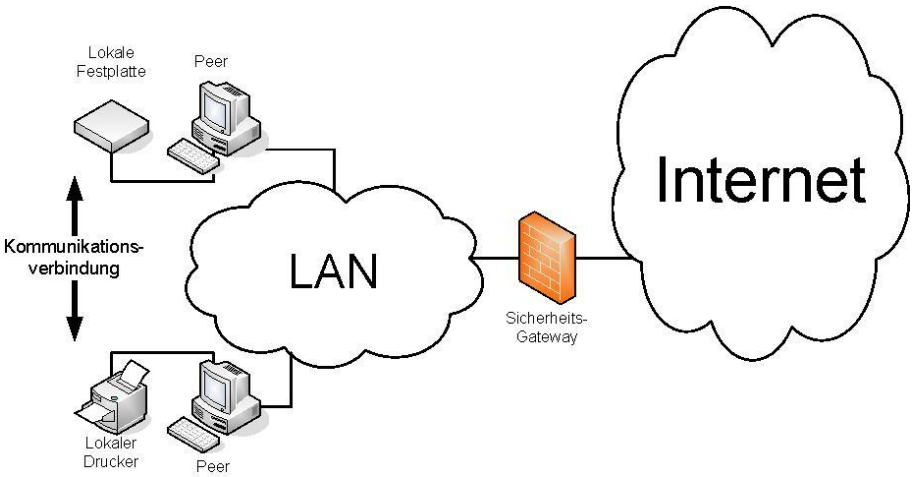
Samas on võrdõigusteenuste kasutamisel ka mitmeid puudujääke, mille juured on sageli puuduvas tsentraliseerimises (vt G 2.147 Võrdõigusteenustest tulenev puuduv tsentraliseerimine). Näiteks ei saa vahetatava info puhul kahjuliku tarkvara esinemist tsentraalselt kontrollida.

Arhitektuur

Sõltuvalt vajadusest saab võrdõigusteenuseid kasutada kohtvõrgus või kogu internetis. IT-süsteemid, mis saavad neid ressursse omavahel jagada, võivad piirduda ainult mõne väljavalitud partneriga või ulatuda süsteemini, mis koosneb määramatust hulgast tundmatutest partneritest. Üldiselt saab eristada kaht võrdõigusteenust.

Lokaalsed võrdõigusteenused

Lokaalsete võrdõigusteenuste puhul võivad üksikud kliendid teistele kohtvõrgu klientidele ressursse pakkuda. Sellist ühiskasutust saab sageli hallata operatsioonisüsteemi abil. Üheks näiteks on faili- ja printeri ühiskasutus Windowsi operatsioonisüsteemides. Juurdepääsu nendele teenustele saab sageli piirata paroolide või IP-aadresside abil. Tavaliselt ei kasutata neid teenuseid kohtvõrgu kaudu ja keelatakse turvalüüsi (tulemüüri) juures. Kuna need teenused ei vaja eraldi serverit, aitavad need säästa riist- ja tarkvara soetamiskulusid.



Joonis: kohalikud võrdõigusteenused kohtvõrgus

Lokale Festplatte – lokaalne kõvaketas ; Peer – partner ; Kommunikationsverbindung – sideühendus ; lokaler Drucker – lokaalne printer ; Sicherheitsgateway – turvalüüs

Avalikud võrdõigusteenused

Info vahetamiseks kasutajatega, kellel puudub juurdepääs kohtvõrgule, saab kasutada avalikke võrdõigusteenuseid. Tavaliselt tuleb selleks installeerida vastavatesse IT-süsteemidesse rakendused, tänu millele saaksid süsteemid kasutada teiste partnerite poolt pakutavaid teenuseid. Kuna võrdõigusteenuste puhul vahetatakse infot kahe või enama IT-süsteemi vahel otse, on ühenduse loomiseks vaja täiendavat infot nende IT-süsteemide kättesaadavuse kohta. Sel põhjusel peaks just suurte võrdõigusteenuste võrkude puhul olema ülevaade sellest, milline partner millist ressursse pakub. Peamiselt eristatakse järgmiseid tüüpe.

Kesksed võrdõigusteenused

Installeeritud rakendus loob ühenduse serveriga, mis haldab teistele partneritele liikuvat infot. Selleks peab partneri rakendus esmalt edastama serverile info, milliseid ressursse ta soovib teistele pakkuda. Enamasti saab IT-süsteem alles seejärel kasutada teiste, ühendatud partnerite infot. Selle alla kuuluvad näiteks IP-aadress, kasutaja ja pakutav sisu. Selle info baasil saab luua otseühenduse kaugemalasuva partneriga ja kasutada tema ressursse. Kui keskne server ei tööta, puudub ühendatud IT-süsteemide kontaktinfo ja partnerid ei saa enam omavahel andmeühendust luua. Selle tagajärjeks on kogu võrdõigusvõrgu tõrge.

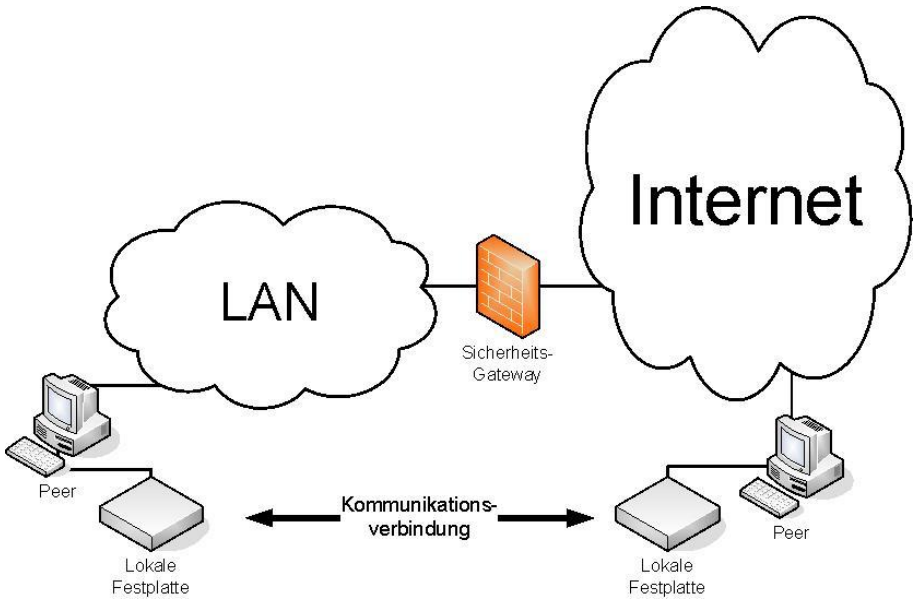
Hajusad võrdõigusteenused

Hajusate võrdõigusteenuste puhul ei vajata ühendatud kasutajaid haldavat keskset serverit. Nende teenuste kasutajate IT-süsteemid loovad pakutavate res-

sursside kohta info vahetamiseks andmeühenduse üksteise vahel. Lisaks ressursside infole, mida saadakse nende IT-süsteemi kohta, millega loodi otseühendus, saab infot ka teiste partnerite kohta, kes on selle süsteemiga omakorda ühenduse loonud. Kuna iga partner saab luua ühenduse mitme partneriga, tekib võrk, mille kaudu saab iga partner infot teiste partnerite pakutavate ressursside kohta. Hajusad võrdõigusteenused eeldavad, et selleks, et saada osaks võrgust, luuakse ühendus partneriga, kes juba on osa sellest võrgust. Selleks vajalik kontaktinfo peab eelnevalt teada olema. Kuna paljud võrgud saavad kasu suurest hulgast ühendatud IT-süsteemidest, avaldatakse sellist kontaktinfot sageli veebilehtedel.

Hübriidsed võrdõigusteenused

Hübriidsed võrdõigusteenused on võrreldavad kesksete võrdõigusteenustega, kuid erinev on see, et kasutada võidakse mitut üksteisest sõltumatut serverit. Nagu ka kesksete võrdõigusteenuste puhul, edastavad partnerid serverile pakutavate ressursside kohta infot ja kontaktinfot, mis võimaldab nendega ühendust saada. Serverid omakorda jagavad seda infot teiste serveritega. Vajadusel saavad partnerid kasutada teiste serverite ressursse, kuigi neid ei halda sama server.



Joonis: avalik võrdõigusteenus interneti kaudu („failijagamine")

Peer – partner ; Lokale Festplatte – lokaalne kõvaketas ; Kommunikationsverbindung – sideühendus ; Sicherheitsgateway – turvalüüs

Alternatiivid võrdõigusteenuste kasutamisele

Selliseid teenuseid, mille puhul peab IT-süsteemide vahel ilmtingimata kasutama Peer-to-Peer andmesidet, on küllaltki vähe. Näiteks saab ressursse pakkuda tsentraalselt, kasutades servereid. Näiteks selleks, et võimaldada juurdepääsu teatud infole ainult volitatud isikutele, saab tsentraalselt toimivaid ettekirjutusi hakata rakendama alates serverite kasutuselevõtmisest. Järgmiseid teenuseid, mida pakutakse tavaliselt läbi võrdõigusteenuse võrkude, saab pakkuda ka tsentraliseeritult.

Printerikasutus

Kui kohtvõrgus vajab printereid korraga mitu inimest, saab neid pakkuda tsentraalselt, läbi võrgu. Selleks võib kasutada võrgutoega printereid ja printimisserveril põhinevat haldamist (vt B 3.406 Printerid, koopiamasinad ja multifunktsionaalsed seadmed).

Failijagamine

Selle asemel, et anda korraga ühiskasutusse mitme kohtvõrgu kliendi („peer") salvestiruum, saab infot hoida ka keskses failiserveris. Kui kasutajad peavad serverile ligi pääsema ainult kohtvõrgu piires, saavad vajalikku infot pakkuda nt Samba-serverid (vt B 5.17 Samba) või NFS-serverid (vt B 3.102 Server Unixi all). Kui infole peavad ligi pääsema ka välised kasutajad, saab infot hoida väljastpoolt ligipääsetavas veebiserveris (vt B 5.4 Veebiserver).

Lühiteated

Kui on tarvis saata lühiteateid ilma meiliteenuseid kasutamata, tuleks kaaluda sõnumside (Instant Messaging) serveri, näiteks Jabberi kasutuselevõttu. Selle serveri abil saab sõnumeid võimaliku kahjuliku tarkvara osas keskselt kontrollida. Ka väliste vestluspartneritega suhtlemine võib toimuda institutsiooni poolt käitatava sõnumside serveri abil, mis on ligipääsetav nii institutsiooni siseselt kui ka väliselt.

IP-kõne (Voice over Internet Protocol) ja internetitelefon

IP-kõne lahendustes, nt sellistes, nagu kirjeldatud moodulis B 4.7 IP-kõne (VOIP) , eristatakse signaliseerimist ja meediatransporti. Signaliseerimine eeldab sageli osalejaid haldavat serverit. Pärast seda, kui signaliseerimise abil on loodud kõne kahe või enama kasutaja vahel, vahetatakse paljude lahenduste puhul kõneinfot kasutajate vahel otse. Kohtvõrgus on selline võrdõigusteenus mõistlik lahendus ja seda tuleks ka kasutada. Kohtvõrgu piiride ületamisel ei tohiks võrdõigusteenust helistamiseks kasutada, nt ei tohiks institutsioon lubada IP-kõnesid („internetitelefoni") väliste äripartneritega suhtlemiseks. Ka sel juhul tuleb nii signaliseerimine kui ka meediatransport omavahel sarnaselt proksile siduda kontsentraatoriga (vt M 4.289 Ligipääsu piiramine IP-kõne komponentidele). Sel moel on välistatud otsene ühenduse loomine üksikute partnerite ja väliste (nt internetis asuvate) kõnepartnerite vahel.

Soovitusi lokaalsete võrdõigusteenuste kasutamiseks

Võimalusel tuleks infovahetuse eesmärgil rakendada mitte võrdõigusteenusel põhinevaid ühiskasutusi, vaid hoopis eraldiseisvaid servereid. Erandjuhtudel, näiteks IP-kõne puhul, on siiski tarvis kasutada ka võrdõiguslahendusi. Seetõttu tuleb kindlaks määrata järgmised aspektid:

- milliseid võrdõigusteenuseid tohib kasutada,
- millist infot tohib vahetada ja
- milliseid teenuseid tohib kasutada.

Vajadusel tuleb kasutajaid võrdõigusteenuste rakendamise osas koolitada. Tuleb jälgida, et võrdõigusteenused piirduksid ainult kohtvõrguga.

Soovitused avalike võrdõigusteenuste kasutamiseks

Reeglina tuleb tagada see, et info kohtvõrgust kontrollimatult välja ei voolaks. Selle alla kuuluvad ka otsesed võrdõigusühendused lokaalsete partnerite ja kohtvõrguväliste IT-süsteemide vahel. Puuduva tsentraliseerimise tõttu pääseb info kontrollimatult kohtvõrgust välja (nt konfidentsiaalsed andmed) või sisse (nt kahjulik tarkvara). Järgmised meetodid takistavad avalike võrdõigusteenuste kasutamist.

Lokaalsed paketifiltrid

Lokaalseid paketifiltreid kasutades saavad kliendid suhelda ainult väljavalitud IT-süsteemidega. Näiteks saab filtreerimisreeglitega määrata seda, et ühendusi oleks võimalik luua ainult serveritega. Serveri IP-aadressile ja lubatud teenuse pordi numbrile toetudes on soovimatu sideühenduse loomine raskendatud. Lokaalsete paketifiltrite kasutamisega saab keelata nii lokaalsete kui ka avalike võrdõigusvõrkude kasutamist.

Tsentraliseeritud filtreerimine turvalüüsis (tulemüüris)

Reeglina peaks turvalüüs võimaldama ainult hädavajalikke sideühendusi, mis kohtvõrku sisenevad või sellest väljuvad. Kõiki teisi ühendusi peaks see keelama (vt B 3.301 Turvalüüs (tulemüür)). Kui turvalüüs ei lase kohtvõrgu klientidel internetis IT-süsteemidega suhelda, saab avalike võrdõigusvõrkude kasutamist takistada.

Poliitika

Lisaks tehnilistele soovitustele tuleb institutsiooni töötajaid eraldi informeerida ka sellest, et võrdõigusteenuste kasutamine on keelatud. Selle nõude võib kirja panna kasutajatele mõeldud turvapoliitikasse. Kui institutsioon soovib kasutada võrdõigusteenuseid, peab selle otsuse tegema institutsiooni juhtkond. Otsustusprotsessi tuleb kaasata IT-turbe eest vastutav töötaja, ning lisaks tuleb otsus koos jääkriskidega dokumenteerida.

Täiendavad kontrollküsimused

- Kas institutsiooni sees on otsustatud, kas võrdõigusteenuseid tohib kasutada või mitte?
- Juhul, kui võrdõigusteenused on lubatud: kas on määratletud, milliseid kohalikke võrdõigusteenuseid võib kasutada ja millist infot nende kaudu vahetada?

M 5.153 Võrgu planeerimine virtuaalsete taristute jaoks

Algatamise eest vastutavad: IT-juht, infoturbespetsialist

Rakendamise eest vastutavad: administraator

Virtualiseerimisserverid peavad tagama kõigile virtuaalsete IT-süsteemide jaoks juurdepääsu neile vajalikele taristukomponentidele nagu võrgud ja salvestusvõrgud, samuti taristuteenustele nagu DNS või DHCP.

Seejuures tuleb virtualiseerimisserveri võrguühenduse planeerimisel silmas pidada järgmisi aspekte:

- Virtualiseerimisserverite võrguühendus vajab tavaliselt juurdepääsu sellistele taristuteenustele nagu DNS ja salvestusvõrgud. Peale selle hallatakse neid sageli võrgu kaudu ja teatud virtualiseerimisfunktsioonid nagu Live Migration (virtuaalse IT-süsteemi liigutamine töö käigus ühest virtualiseerimisserverist teise) kasutavad samuti virtualiseerimisserverite vahelisi võrguühendusi. Seetõttu vajatakse ka virtualiseerimisserverite enda puhul vastavaid võrguliideseid. Kuna nende liideste kaudu võidakse hallata ka virtualiseerimisserveril käitatavaid virtuaalseid IT-süsteeme, tuleb neid eriliselt kaitsta ja käitada ühes haldusvõrgus. Juurdepääs sellele haldusvõrgule kujutab endast arvutuskeskusele või serveriruumile juurdepääsu virtuaalsete teisikut ja seda tuleks hallata samuti piirangutega nagu juurdepääsu serveriruumi (vt M 1.58 Tehnilised ja organisatsioonilised nõuded serveriruumidele). Haldusvõrku käitatakse eraldi, tagamaks, et virtualiseerimisserveri haldusfunktsioonid oleksid kättesaadavad ainult ettenähtud tööjaamadest ja ainult volitatud administraatoritele. Eeskätt tuleb haldusvõrk eraldada virtuaalsete IT-süsteemide võrkudest, peale selle tuleb kontrollida, kas virtualiseerimisfunktsiooni Live Migration jaoks on vaja luua eraldi võrk. Kuna Live Migration 'i puhul võidakse virtuaalse IT-süsteemi põhimälu sisu liigutada võrgus kodeerimata kujul, võib selline eraldamine vastavalt virtuaalsete IT-süsteemide kaitsevajadusele vajalikuks osutuda.
- **Virtuaalsete IT-süsteemide võrguühendus -** Virtuaalsete IT-süsteemide (virtuaalsed serverid, kliendid ja vajadusel virtuaalsed kommutaatorid) puhul tuleb rakendada mooduli B 3.101 Server ja B 3.302 Marsruuterid ja kommutaatorid meetmeid samuti kui füüsiliste serverite puhul. Virtuaalsete IT-süsteemide võrguühenduse puhul tuleb planeerimisel silmas pidada mõningaid eripärasid. Virtuaalsed IT-süsteemid kasutavad võrkudele juurdepääsuks virtualiseerimisserveri võrguliideseid. Seejuures ei allu liidesed tavaliselt otseselt ja ühemõtteliselt virtuaalsetele IT-süsteemidele, mis tähendab, et mõnede virtualiseerimistoodete puhul võivad mitmed virtuaalsed IT-süsteemid jagada sama füüsilist liidest. Kuna selle liidese tõrke puhul eraldatakse kohe mitmed virtuaalsed IT-süsteemid võrgust, soovitatakse selliste mitmekordselt kasutatavate võrguliideste käideldavust suurendada (kumulatsiooniprintsiip). See võib toimuda näiteks liiaste võrguliideste ja tehnoloogiate nagu IEEE 802.3ad (Link Aggregation Control Protocol - LACP) abil või teiste Load Balancing -meetodite abil. Seejuures tuleb eriti silmas pidada, et selliste protokollide kasutamine nõuab tavaliselt kohandatud konfiguratsiooni füüsilise kommutaatori jaoks, millega antud liidesed on ühendatud. Võimalusel tuleb füüsilised liidesed siduda erinevate kommutaatoritega.

Võrgusegmentide eraldamine

Virtualiseerimisserverid seotakse sageli paljude võrkudega. Mõnedel virtualiseerimistoodetel on funktsioonid mitme VLAN i kasutamiseks üle ühe füüsilise liidese (Port Trunking vastavalt IEEE 802.1q). Lisaks on võimalik kasutada ka virtuaalses taristus võrgu segmenteerimiseks VLAN e. Kui võrkude segmenteerimiseks piisab ainult loogilise jaotusega VLAN idest, võib see toimuda ka virtuaalse taristu raames. Vastavate virtuaalsete IT-süsteemide virtuaalsed võrgukaardid jaotatakse sel puhul füüsiliste võrguliideste vahel, nii et nad saaksid võrgupakette vahetada ainult omavahel. Kui võrgud eraldati enne virtualiseerimist erineva kaitsevajaduse alusel füüsiliselt, tuleb sellised võrgud üksteisest eraldada ka virtuaalselt. Seejuures tuleb kontrollida, kas võrgueraldusmehhanismid, samuti virtuaalsete IT-süsteemide kapseldus ja isolatsioon on rakendatud virtualiseerimislahenduse puhul piisavad kõrge ja madala kaitsevajadusega virtuaalsete IT-süsteemide ühes virtualiseerimisserveris koos käitamiseks. Kontroll võib seisneda näiteks selles, et antud virtualiseerimislahenduse tootja tunnistab nimetatud mehhanismid selle kasutusotstarbe (erineva kaitsevajadusega masinate eraldamine) jaoks sobivaks ja väljastab vastavasisulise sertifikaadi. Kõrgendatud kaitsevajaduse puhul võib selliste võrkude käitamine ühel eraldi virtualiseerimisserveril siiski problemaatiliseks osutuda, näiteks kui virtuaalse taristu administraatoritel ei tohi olla juurdepääsu väljaspool nende vastutusvaldkonda jäävatele virtuaalsetele IT-süsteemidele. Sel juhul tuleb need virtuaalmasinad, millel peab olema juurdepääs vastavatele võrkudele, paigutada isoleeritud ja vaid selleks ettenähtud virtualiseerimisserveritele. Vajadusel peaks vastav IT-süsteem töötama virtuaalse keskkonna asemel füüsilises IT-süsteemis.

Kõrgkäideldavad virtuaalsed taristud

Üksikute virtuaalsete IT-süsteemide kumuleeritud kaitsevajadus võib tuua kaasa selle virtualiseerimisserveri kõrge või väga kõrge kaitsevajaduse. Sel juhul soovitatakse ühendada mitu virtualiseerimisserverit näiteks klastriks. Seejuures käivitatakse ühe virtualiseerimisserveri klastrist väljalangemisel virtuaalsed IT-süsteemid ülejäänud virtualiseerimisserveritel uuesti. Kui mitme klastriühenduse vaheline suhtlus korraga katkeb, peab iga süsteem suutma otsustada, kas väljalangemine puudutab teda ennast või teisi süsteeme (isolatsiooniprobleem), et serveri väljalangemisest puudutatud virtuaalseid IT-süsteeme ei taaskäivitataks korduvalt. Selline isolatsiooniprobleem lahendatakse tavaliselt nii, et klastrisüsteem kontrollib, kas teatud ressursid nagu näiteks standardlüüs on kättesaadavad. Kui mitte, käsitleb ta ennast isoleerituna ja eemaldab ennast ise klastrist ning temal käitatavad virtuaalsed IT-süsteemid peatatakse vastavalt konfiguratsioonile. Seetõttu soovitatakse sellise virtualiseerimisklastri planeerimisel välja selgitada, milliseid ressursse isolatsiooni kontrollimiseks vajatakse ja anda neile siis arvutuskeskuse taristus piisav käideldavus. Võrguühendustele klastrisse kuuluvate virtualiseerimisserveritega tuleb samuti anda piisav käideldavus.

Kontrollküsimused:

- Kas virtuaalsete taristute haldamiseks on rajatud eraldi haldusvõrk?
- Kas on kontrollitud, kas virtualiseerimisfunktsioonide nagu Live Migration jaoks on vaja rajada oma võrk?
- Kas rakendatavate külalissüsteemide sidumiseks on rajatud eraldi võrk?

- Kas virtuaalsete IT-süsteemide jaoks kasutatavate võrguliideste käideldavus on piisavalt planeeritud?
- Kas võrgusegmentide eraldamine kasutatava virtualiseerimistoote abil on ühel virtualiseerimisserveril erineva kaitsevajadusega virtuaalsete IT-süsteemide käitlemisel piisavalt tagatud? Kas tootja on väljastanud vastava sertifikaadi?
- Kas virtualiseerimisserverite klastri võrguühendused on planeeritud piisava käideldavusega?

M 5.154 Virtuaalse taristu võrgu turvaline konfiguratsioon

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator

Virtualiseerimisserverid vajavad hulgaliselt sidesuhteid. Need on nii ühendused haldusvõrkudesse kui ka ühendused salvestusvõrku andmekeskuse vastavate teenuste kasutamiseks. Teisest küljest on virtuaalsete IT-süsteemide kasutada vastavad võrguühendused.

Virtuaalsete võrgukomponentide erinevad tehnikad

Siinjuures kasutatakse erinevate virtualiseerimistoodete korral erinevaid tehnikaid. Mõnede virtualiseerimistoodete korral jagatakse virtuaalsetele IT-süsteemidele eraldi võrgukaardid, mis on juba koheselt kasutatavate võrkudega ühenduses. Nendeks võivad olla nii virtuaalsed kui ka füüsilised võrgukaardid.

Teiste virtualiseerimistoodete korral kujutatakse virtualiseerimisserveri siseselt tervet võrgutaristut. Selleks luuakse virtuaalsed kommutaatorid, mis võimaldavad virtuaalsetele IT-süsteemidele vajaliku võrguühenduse ning juhivad virtuaalse võrgu üleminekut füüsilisse võrku. Seejuures on võimalik luua ka ainult virtuaalseid võrke millel üleminek füüsilisse võrku puudub.

Mõningad nendest virtualiseerimislahendustest toetavad füüsilise jaotuse kõrval ka loogilist jaotust, nagu näiteks VLAN-iga (Virtual Local Area Network). Virtuaalsete IT-süsteemide vahel loodava ühenduse viis on siiski väga erinev. Osaliselt juhitakse virtuaalsete IT-süsteemide vaheline kommunikatsioon ühel ja samal virtualiseerimisserveril erinevate võrkude kaudu läbi füüsilise võrgu (näiteks: Citrix XenServer, Sun VirtualBox oder VMware ESX). Osaliselt juhitakse see kommunikatsioon alati virtualiseerimiskihi siseselt, nii et kommunikatsiooniga ei oleks seotud mitte ükski marsruuter väljaspool virtualiseerimiskihti (Sun Solaris Containers).

Virtualiseerimisserverite võrkude konfigureerimisel tuleb jälgida mitmeid aspekte:

- Virtualiseerimisserveri haldusliidesed tuleks ühendada eraldi võrguga. See tuleb füüsiliselt või loogiliselt eraldada võrgust milles käitatakse virtuaalseid IT-süsteeme. Loogiline võrgueraldus ainult VLAN-iga ja ilma igasuguste lisameetmeteta jääb siinkohal puudulikuks, kuna virtualiseerimisserverid vahetavad haldusliidese kaudu konfidentsiaalset informatsiooni.
- Kõikidelt haldusliidese kasutajatelt tuleb nõuda autentimist, anonüümsed ligipääsud peavad olema keelatud. Autentimisandmete edastamine peaks toimuma krüpteeritult. Lisaks tuleks virtualiseerimisserveril endal kaitsta haldusliidest lokaalsete pakettfiltritega.

- Salvestusligipääsuks kasutatavate võrkude kaudu saab ligipääsu sihtidele (=kõvakettas) ja algatajatele (=server). Seeläbi saavad virtualiseerimisserveritele või virtuaalsetele IT-süsteemidele esitleda võltsitud algatajaid või sihte. Seetõttu tuleb ligipääs salvestusvõrgu ressurssidele turvata sobiva autentimismeetodi kaudu. Selleks kasutatavad võrgud tuleb samuti virtuaalsete IT-süsteemide võrkudest eraldada. Vaata ka M 5.130 Salvestisvõrgu (SAN-i) kaitse segmenteerimise abil .
- Kui virtuaalses taristus kasutatakse süsteemi töötamise ajal funktsioone nagu teisaldamine (VMotion, XENmotion, Live Migration), toimub virtuaalse IT-süsteemi jooksukeskkonna transport võrgu kaudu ühelt virtualiseerimisserverilt teisele. Siinjuures edastatakse kõik IT-süsteemis töödeldavad andmed võrgu kaudu. Need andmed võivad vajada veelgi suuremat turvet. Seetõttu tuleks selleks puhuks kasutatud võrk samuti eraldada.
- Virtuaalsete IT-süsteemide kommunikatsioon teiste virtuaalsete või füüsiliste IT-süsteemidega tuleks detailideni planeerida. Siinjuures tuleb kindlustada, et jälgitakse kehtivaid infoturbedirektiive. Võrgus paiknevaid turvalüüse või monitooringusüsteeme ei tohi olla võimalik virtualiseerimise vahenditega eirata. See kehtib eelkõige virtualiseerimistoodete kohta, mille juures ei toimu võrguühendus virtuaalsete IT-süsteemide vahel ilmtingimata füüsilise võrgu kaudu (vt üleval näiteid: SUN Solaris Containers ja VMware ESX Server).
- Kui virtuaalsed IT-süsteemid peavad mitme võrguga ühenduses olema, tuleb sobivalt kindlustada, et nende kaudu ei oleks võimalik luua ebasoovitavaid võrguühendusi. Selleks et ennetada, virtualiseerimisserveri kompromiteerimist kompromiteeritud virtuaalse IT-süsteemi kaudu, ei tohiks olla võimalik luua ühendusi haldusvõrgu ja virtualiseerimisserveri ning tootmises olevate virtuaalsete IT-süsteemide võrkude vahel.
- Virtuaalsetes taristutes saab käitada ka virtuaalseid turvalüüse (virtuaalseid tulemüüre). Selliste turvalüüside kasutamist sisevõrgus erinevate turbeastmega võrkude eraldamiseks tuleks eelnevalt hoolikalt kontrollida. Siseste, mitte väga erineva turbevajadusega võrkude eraldamiseks on turvalüüside kasutamine aga mõeldav. Selliste turvalüüside kasutamine tuleb hoolikalt planeerida. Seejuures tuleb arvestada, et sõltuvalt valitud virtualiseerimistootele ei pruugita võrguühendust niimoodi läbi virtualiseerimiskihi ootuspäraselt marsruutida. Peale selle ei ole kindlustatud, et virtuaalse turvalüüsi kaitsefunktsioon ka siis teiste virtuaalsete või füüsiliste IT-süsteemide jaoks olemas on, kui virtualiseerimisserverid ise on kompromiteeritud. Pärast virtualiseerimisserveri kompromiteerimist on sellest turvalüüsist väga lihtne mööda hiilida. Kuna turvalüüsid ise on samuti sageli rünnakute sihiks, tuleks loobuda ideest virtualiseerimiservereid kaitsta ainult virtuaalsete turvalüüsidega. Sellisel juhul on võrkude sobilik jaotus turvalüüside kaudu vajalik. Vaata B 3.301 Turvalüüs (tulemüür)).
- Kuna virtualiseerimisserverid ei paku virtuaalsetele IT-süsteemidele siinkohal mingisugust lisakaitset, tuleb neid lähtuvalt oma võrguintegratsioonist ja turvalüüside kaitsest kohelda samamoodi nagu füüsilisi IT-süsteeme.

Kontrollküsimused:

- Kas haldus- ja administratsioonivõrk on virtuaalse IT-süsteemi võrgust eraldatud ja kas see eraldatus on vastavalt virtuaalse IT-süsteemi turbavajadu-

sele piisav?

- Kas anonüümne ligipääs virtualiseerimisserveri haldusliidestele on välistatud?
- Kas on olemas sobiv autentimismeetod salvestusvõrgu ressurssidele ligipääsuks ning kas salvestusvõrgud on virtuaalsete IT-süsteemide võrkudest eraldatud?
- Kas Live Migration i võrgud on virtuaalsete IT-süsteemide võrkudest eraldatud?
- Kas virtuaalsete ja füüsiliste IT-süsteemide võrguühenduste korral arvestatakse kehtivate infoturbedirektiividega?
- Kas on kindlustatud, et võrgus paiknevaid turvalüüse või monitooringusüsteeme ei ole võimalik virtualiseerimisvahenditega eirata?
- Kas on välistatud, et virtuaalsete IT-süsteemide kaudu, mis on ühenduses mitme võrguga, ei ole võimalik luua soovimatuid võrguühendusi?
- Kui tahetakse kasutada virtuaalseid turvalüüse: Kas virtuaalsete turvalüüside kasutamine on kooskõlas IT-süsteemi turbenõuetega?

M 5.155z Interneti kasutamise andmekaitseaspektid

Algatamise eest vastutavad: andmekaitsespetsialist, infoturbespetsialist

Rakendamise eest vastutavad: kasutajad

Interneti kasutamisel kogutakse mitmel pool andmeid, mida on võimalik kasutada näiteks kliendiprofiilide koostamiseks. Paljud nendest andmetest kogutakse kasutajate teadmisel ja nõusolekul, teised aga märkamatult. Õige käitumisega saavad kasutajad soovimatuid andmejälgi vältida.

Küpsised (cookies)

HTTP-küpsised võimaldavad teatud veebilehtede infot interneti klientsüsteemi failikataloogis salvestada. Neid kasutatakse info ajaliselt piiratud arhiveerimiseks. Veebilehtede käitajad võivad küpsiseid kasutada näiteks veebilehtede isikupärastatud kasutajaseadistuste või veebipoodide ostukorvide loomiseks või sihtrühmaspetsiifilise reklaami paigaldamiseks. Tavaliselt ei ole info salvestatud küpsise sisse. Küpsis on pigem nagu seerianumber, mis võimaldab veebilehe käitajal siduda kasutajaga salvestatud infot.

Küpsis sisaldab tavaliselt järgmist infot:

- infot veebilehtede kohta, kuhu see tagasi saadetakse (nt kas ainult sellele serverile, mis selle küpsise koostas, või kõikidele serveritele, mis asuvad küpsise koostanud serveri domeenis);
- kehtivusaega (nt ainult pooleli olevaks brauseriseansiks või kuni määratud aegumiskuupäevani);
- teisi veebilehe käitaja vabalt pakutavaid andmeid, nt kasutajatunnust või seansi-ID-d.

Seevastu Flashi küpsiseid (ka Local Shared Objects, LSO) loovad Flashi animatsioonid. Neid kasutatakse Flashi failide kasutajaspetsiifiliste seadistuste, nt kasutaja seadistatud helitugevuse salvestamiseks kasutaja arvutis. Küpsised koostab Flash Player ja need on brauserist sõltumatud. Seetõttu pole neid võimalik ka brauseri seadistustega juhtida ega näiteks automaatselt kustutada. Olenemata kasutatavast operatsioonisüsteemist salvestatakse Flashi küpsised „application data" kataloogi. Brauseri seadistustes tuleks küpsiste vastuvõtt desaktiveerida. Flashi küpsiste vastuvõtt tuleb desaktiveerida Flash Playeris. Brauserid tuleks konfigureerida nii, et enne küpsise salvestamist küsitakse kasutajalt, kas ta on sellega nõus. Võimalik on ka küpsiste lubamine ainult ühe kindla seansi ajaks, keelates samas nende püsiva salvestamise. Mõned brauserid võimaldavad seadistada üksikasjalikke kriteeriume, mille alusel küpsised kas võetakse vastu või lükatakse tagasi.

Järgmised punktid aitavad otsustada, kas küpsisest peaks keelduma või on selle kasutamine probleemivaba.

- Üldjuhul tuleks keelduda küpsistest, mis saadetakse tagasi mõne nn võõra domeeni serveritele, mitte selle domeeni serverile, millelt hetkel külastatav veebileht pärineb (Third-Party-Cookies). Siia hulka kuuluvad eelkõige küpsised reklaamipakkujatelt, kelle ribareklaamid asuvad külastataval veebilehel.

- Tavaliselt tuleks keelduda küpsistest, mis saadetakse tagasi mõne domeeni kõikidele serveritele, mitte ainult serverile, kust hetkel külastatav veebileht pärineb.
- Keelduda tuleks küpsistest, millel on äärmiselt pikk eluiga.
- Lubada võib küpsiseid, mida kasutatakse isikustatud lehekülgede kasutajaseadistuste salvestamiseks. Selliste küpsiste tuvastamine eeldab siiski alati kasutaja otsust. Usaldusväärsed teenusepakkujad viitavad sageli lehekülgedel, kus kasutajad saavad seadistusi teha, ka sellele, et tehtud seadistused salvestatakse küpsises.
- Küpsiseid, mis kehtivad ainult käimasoleva veebiseansi jaoks (nimetatakse tihti ka seansiküpsisteks – session-cookies) ja saadetakse tagasi ainult kindlale serverile, võib üldjuhul lubada.

Kasutajad peavad seejuures arvestama, et interneti kasutamisel tekivad seetõttu mõned väiksemad piirangud, nt tuleb veebilehe korduval külastamisel teatud andmed uuesti sisestada. Kasutajad peaksid endale regulaarselt kuvama aktuaalselt salvestatud küpsiseid ning vajaduse korral neid valikuliselt kustutama. Parem on seadistada brauser nii, et selle sulgemisel kustutatakse kõik kogutud küpsised. Brauseri kustutussuvand ei arvesta aga Flashi küpsistega. Need tuleb kataloogist kustutada kas käsitsi või tarkvara abil. Andmekogud (ajalugu, Hotlists ja vahemälu) Brauserid koguvad erinevate kasutajate internetikasutuse kohta ka siseandmeid, kasutades selleks näiteks ajalugu (viimati külastatud veebilehtede loendit), vahemälu, allalaadimise ülevaateid, salvestatud otsingu- ja formulariandmeid ning paroole.

Brauserite kasutajaid tuleb teavitada sellest, kuhu nende lokaalses IT-süsteemis sellised andmed salvestatakse ja kuidas nad neid sealt kustutada saavad. Lisaks tuleb tagada, et ligipääs oleks ainult volitatud isikutel. Enamikus brauserites on võimalik isiklikku veebikasutust kajastavad failid ja andmed kustutada kas ühe hiirevajutusega või automaatselt brauseri sulgemisel. Eriti tundlikud on failid, mis paiknevad proksi-serverites, sest nendes logitakse kõikide töötajate interneti väliskasutus, kaasa arvatud klientsüsteemi IP-aadress, millelt päring esitati, ja päringus kajastunud URL. Klientsüsteemi IP-aadressi põhjal on enamasti võimalik välja jõuda mõne konkreetse kaastöötajani. Halvasti hallatud proksi-server võib seega põhjustada laiaulatusliku andmekaitsenõuete rikkumise. Enamik brausereid kogub kasutaja ja tema harjumuste kohta infot, mille edastamist kasutaja ei pruugi soovida.

Selle info hulka kuuluvad näiteks:

- lemmikud;
- külastatud veebilehed, vahemälus paiknev info;
- ajaloo andmebaas, URL-ide loetelu;
- küpsiste loetelu;
- kasutaja kohta käiv info, mis brauseris salvestatakse ja mida võidakse ka edastada.

Ajalookuva (ajaloo andmebaas)

Ajalookuvasse salvestatakse veebilehed, mida kasutaja külastab. Peaaegu kõik brauserid logivad URL-id, mida kasutaja on kindla aja jooksul külastanud (näiteks Chromes on selle nimeks History). Selline logi võib sisaldada kas ainult pooleliooleva seansi andmeid või ka eelnevate seansside infot. See andmebaas sisaldab infot külastatud veebilehtede kohta (URL-id ja pealkirjad). Andmebaasi märgitakse selle infoga üles ka kõik süsteemisisesed, kuid brauseris avatud dokumendid. See võib viia konfidentsiaalse info avalikustamiseni. Ajaloo andmebaasi tuleks kindla aja tagant korrastada. Enamik brausereid võimaldab konfiguratsioonis määrata, et ajaloo andmebaas kustutataks täielikult näiteks iga kord, kui brauser suletakse. Lisaks saab määrata, millist ajavahemikku ajaloo andmebaas kajastab, ning sellest vanem info kustutatakse automaatselt.

Info kasutajate kohta

Brauseris võib olla salvestatud suur hulk isiklikku infot kasutaja kohta, nt tema nimi, meiliaadress, tööandja, telefoninumber. Siinjuures tuleks hoolikalt mõelda, mis isikuandmed võivad selle kaudu avalikuks saada. Andmete esitamisega tuleks siinkohal olla võimalikult tagasihoidlik.

Paljud brauserid võimaldavad andmeblankettide sisestusväljades tehtud sisestusi salvestada, et järgmisel korral, kui leht avatakse, oleks võimalik väljad automaatselt täita. Seda funktsiooni tuleks kasutada ainult erandjuhtudel. Mitte mingil juhul ei tohiks sellisel viisil salvestada ligipääsuparoole. Kui esineb võimalus andmeid krüpteeritult salvestada, siis tuleks seda ka kasutada.

Info brauseri vahemälus

Brauseri vahemällu salvestatakse külastatud veebilehe kõik elemendid, nt tekstid, mallid, pildifailid ja helid. Kui vahemälu ei tühjendata, lüheneb veebilehe taasavamisel selle laadimisaeg, sest lehekülge ei laadita internetist, vaid brauseri vahemälust. Esmalt kontrollib brauser, kas vajalikud failid on vahemälus olemas või tuleb need internetist uuesti alla laadida. Nii nagu ajaloo andmebaasi puhul, võimaldavad ka brauseri vahemälu failid rekonstrueerida andmeid, millega kasutaja on kokku puutunud. Seda on võimalik ära kasutada kasutajaprofiilide loomiseks. Äärmuslikul juhul võib see viia isegi selleni, et konfidentsiaalne info jõuab avalikkuse ette, nt kui töökoha intraneti keskkonnas kasutatavat sülearvutit pruugitakse väljaspool asutust ja see ära varastatakse.

Seetõttu tuleks vahemälu, nagu ka ajaloo loendit, regulaarselt kustutada või vahemälu funktsioon juba brauseri konfigureerimisel täielikult välja lülitada. Vältimaks andmete salvestamist vahemällu, tuleks vahemälu suuruseks määrata 0 MB. SSL-i (Secure Sockets Layer) kaitsega veebilehti kasutatakse tihti konfidentsiaalsete andmete, nt krediitkaardinumbrite krüpteeritud edastamiseks läbi interneti. Selliste lehtede salvestamine vahemällu tuleks võimaluse korral keelata juba asjakohase konfiguratsiooniga. Selleks, et kasutajad ei jätaks endast maha soovimatuid andmejälgi, tuleks neid informeerida, kuidas seda õige käitumisega vältida.

Kontrollküsimus:

- Kas kasutajaid on informeeritud, kuidas vältida interneti kasutamisel tekkivaid soovimatuid andmejälgi?

M 5.156z Twitteri turvaline kasutamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht, ülemused

Rakendamise eest vastutavad: kasutajad

Mikroblogimisteenuses Twitter saavad registreeritud kasutajad omavahel uudiseid ja infot vahetada lühikeste, kuni 140-märgiliste teadetega. Kasutaja saab ennast teiste kasutajate juures registreerida jälgijaks (follower) ja seeläbi teiste tekstiteateid lugeda. Registreerimiseks tuleb sisestada ees- ja perekonnanimi, kasutajanimi ja parool ning meiliaadress. Kasutajanimest koostatakse kasutaja Twitteri lehekülje URL: https://twitter.com/kasutajanimi. Valitud parool peab olema vähemalt kuuekohaline, rohkem nõudeid ei ole. Kasutajate tähelepanu juhitakse aga sellele, et nad peaksid kasutama võimalikult keerulisi paroole (Be tricky!). Identiteedivarguse ennetamiseks tuleks jälgida üldiseid paroolireegleid (vt M 2.11 Paroolide kasutamise reeglid).

Kasutajatunnust saab registreerimisel vabalt valida. Seetõttu on võimalik kasutada valet identiteeti. Võimalik on valida tuttavate, kuulsuste või institutsioonide nimesid ning nende all teateid saata.

Twitteri teenusepakkujad võimaldavad kontrollitud identiteediga kasutajaid funktsiooniga „Kontrollitud konto" (Verified Accounts) markeerida, rakendades asjakohast sümbolit. Seda suvandit pakutakse aga siiani vähe.

Twitteri ja teiste veebiteenuste kasutamine peaks igas institutsioonis olema selgelt reguleeritud.

Selleks on mitmeid variante:

- Institutsioon võib Twitteri kasutamise täielikult ära keelata. Sellest tuleb loomulikult teavitada ka töötajaid. Keeldu saab toetada ka tehniliste lahendustega, rakendades teadaolevate veebilehtede filtreerimist, kuid siinjuures tuleb arvestada, et kasutajad leiavad sellistele teenustele ligipääsemiseks üha uusi võimalusi.
- Leidub ka asutusi, kus Twitter on ametitegevuses lubatud, nt kui Twitteri kaudu informeeritakse teisi oma teenustest ja toodetest.

Ametiasutus või ettevõtte peaks määrama kindlad reeglid, milles on kirjeldatud:

- kas Twitterit tohib tööl kasutada ning kui jah, siis millistel raamtingimustel (nt nõuded info edastamise, pseudonüümide kasutamise jms kohta); millele peaksid töötajad Twitteri ametialasel või isiklikul kasutamisel tähelepanu pöörama.

- Nagu kõigi veebiteenuste korral, peaks kasutaja enne registreerumist kontrollima, kas kasutustingimused on talle vastuvõetavad. Twitteri kasutustingimused lubavad kasutajainfot kasutada reklaamiks.

Twitter on tuntud kiire ja laialdase infoedastuse poolest. Twitteri kaudu levib tihti väga kiiresti ka selline info, mida isegi uudistetoimetused pole kas veel saanud või pole jõudnud selle õigsust kontrollida. Twitteri teateid edastatakse tihtipeale volitamata ja kontrollimata. Seepärast tuleks enne nende teadete kasutamist või edastamist nende õigsust kontrollida. Kuna sisestatav tekst on piiratud 140 märgiga, saadetakse Twitteri kaudu tihtipeale ainult lühi-URL-e. Lühi-URL-id on üldjuhul vormingus, mis näeb välja näiteks selline: tiny.url või t.co. Selle lingi taga peitub tegelik link, millele soovitakse viidata. See võib osutuda probleemiks, sest esmapilgul ei ole võimalik aru saada, kuhu lühi-URL viib, ning kasutaja võidakse suunata mõnele kahjurvara sisaldavale veebilehele. Lühi-URL-e võivad ära kasutada ka nn Spam-Followerid. Nende taga peituvad masinate loodud kasutajakontod, mis avaldavad aeg-ajalt teateid.

Need sisaldavad sama moodi nagu reaalsete isikute kasutajakontod uudiseid ja lingisoovitusi. Saabuvad teated sugereerivad, et tegu on erinevate ja huvitavate linkidega, kuid lõpuks viivad kõik ikkagi ühele kindlale veebilehele. Selleks, et kasutajad linkidele vajutaksid, luuakse palju kasutajakontosid, mis ühendatakse omavahel, st ülejäänud kontod märgitakse jälgijateks. Need kasutajakontod jälgivad veel ka ehtsaid kasutajakontosid ning loodavad seeläbi lingile võimalikult palju klõpse saada. Nii edastavad rämpsposti ka aktiivsete kasutajakontodega reaalsed Twitteri liikmed.

Kontrollküsimus:

- Kas Twitteri kasutamine on asutuses selgelt reguleeritud?

M 5.157z Sotsiaalvõrgustike turvaline kasutamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht, ülemused

Rakendamise eest vastutavad: kasutajad

Sotsiaalvõrgustikud on veebipõhised kasutajakeskkonnad (nt LinkedIn, Facebook ja Instagram), mis on sarnase ülesehituse, kuid erineva sisuga. Sisulise kujunduse loovad kasutajad ise. Sotsiaalvõrgustikke kasutatakse vanade sõprade või kolleegide ülesleidmiseks, aga ka selleks, et olla ise leitav, ja ametikontaktide loomiseks. Peale profiili loomise, millega isik end veebis nähtavaks muudab, on sellistes kasutajakeskkondades oluline ka kasutajate omavaheline kontaktiloomine.

Sidemed luuakse kasutajatevahelise sotsiaalse tegevuse tulemusena ning tegevus salvestatakse spetsiaalsete funktsioonidega tarkvara andmekogusse. Sotsiaalvõrgustikke kasutatakse suhtlemiseks ja andmete edastamiseks. Olenevalt kasutajakeskkonna suunitlusest on võimalik isiklike andmete kõrval lisada ka pilte ja teistsugust infot ning kasutada erinevaid rakendusi. Selleks, et saada sotsiaalvõrgustiku liikmeks, tuleb ennast selle kasutajakeskkonnas registreerida. Peale kasutajanime ja parooli tuleb sageli sisestada veel teisigi isiklikke andmeid. See, millist isiklikku või tööinfot avalikustatakse, sõltub kasutajast ja tema kasutuseesmärkidest.

Suur hulk isiklikku infot on vajalik selleks, et sotsiaalvõrgustikes nähtav olla ja nendes kaasa lüüa. Igale kasutajale peab olema selge, et kasutajate kohta kättesaadavat infot on võimalik kuritarvitada rünneteks, mille eesmärk on inimestega manipuleerimine (vt M 3.5 Turvameetmete koolitus).

Taustinfot võivad ründajad kuritarvitada selleks, et võita oma ohvrite usaldus ja veenda neid midagi tegema, nt avama mõnd kindlat faili. Seega tuleks hoolikalt mõelda, mis infot enda kohta internetis avalikustada. Infot, st ka fotosid, videoid ja tsitaate, saab kiiresti internetti üles laadida, kuid sama kiiresti saavad teised isikud seda infot edasi kasutada. Seepärast peaks sotsiaalvõrgustike kasutaja end kurssi viima teenusepakkuja tingimustega, st eelkõige teenuse kasutamiseks sõlmitava lepingu tingimustega.

Siinkohal tuleks kontrollida:

- millised isiklikud andmed tuleb sisestada registreerimiseks;
- kas ja kuidas kaitseb teenusepakkuja kasutajaandmeid volitamata ligipääsu eest, nt kas kasutaja virtuaalne identiteet on kolmandate isikute kuritarvitamise eest kaitstud;
- kuidas turvatakse andmesidet, nt kas kommunikatsioon krüpteeritakse täielikult või ainult osaliselt (tavaliselt SSL-iga), kas paroolid ja seansiküpsised edastatakse ainult krüpteeritud kujul;
- kas teenusepakkuja koostab kasutajaprofiile ja annab neid edasi kolmandatele isikutele, nt et sihipäraselt oma kasutajakeskkonda reklaamida;

- kas kasutajaandmeid on võimalik ükskõik millal iseseisvalt ja täielikult kustutada.

Enne sotsiaalvõrgustikuga liitumist peaks kasutaja kontrollima, kuidas järgitakse seal andmekaitseseadust. Kui kasutajatel on ise võimalik andmekaitse suvandeid konfigureerida, tuleks need seadistada võimalikult piiravalt. Andmeid tuleks teistele kasutajatele avalikustada nii vähe kui võimalik, nt tuleks nn avalikku profiili sisestada ainult kõige hädavajalikum info. Sotsiaalvõrgustike kasutajad peaksid hoolega järele mõtlema, millised kontaktipäringud nad vastu võtavad ja kellele nad millist infot avalikustavad. Kõikjal tuleks sisestada ainult hädapärane info, mida läheb tarvis kasutajakeskkonnas suhtlemiseks. Infot kolmandate isikute kohta tohiks edastada ainult pärast nendega kooskõlastamist. Sotsiaalvõrgustike kasutamine peaks ametiasutuses või ettevõttes olema kindlalt reguleeritud.

Selleks on mitmeid variante:

- Asutused võivad sotsiaalvõrgustike kasutamise täielikult ära keelata. Sellest tuleb loomulikult teavitada ka töötajaid. Keeldu saab toetada ka tehniliste lahendustega, rakendades teadaolevate teenusepakkujate filtreerimist, kuid siinjuures tuleb arvestada, et kasutajad leiavad sellistele teenustele ligipääsemiseks üha uusi võimalusi.
- Leidub ka institutsioone, kus sotsiaalvõrgustikud on tööülesannete täitmiseks lubatud, nt info saamiseks erinevatelt huvigruppidelt või enda teenuste ja toodete turustamiseks sotsiaalvõrgustikes.

Ametiasutus või ettevõte peaks määrama kindlad reeglid, milles on kirjeldatud:

- kas sotsiaalvõrgustikke tohib tööga seoses kasutada;
- millistel raamtingimustel tohib neid teenuseid kasutada (nt info edastamise nõuded, kaitse kahjurvara eest, pseudonüümide kasutamine);
- millele peaksid töötajad sotsiaalvõrgustike kasutamisel tähelepanu pöörama.

Kasutajad ei tohiks sotsiaalvõrgustike ametialast ja isiklikku kasutamist segamini ajada ning nad peaksid tundma institutsioonis kehtivaid reegleid.

Kontrollküsimused:

- Kas sotsiaalvõrgustike kasutamine on institutsioonis selgelt reguleeritud?
- Kas kasutajaid informeeritakse sotsiaalvõrgustike kasutamise ohtude kohta?

M 5.158z Veebimälu turvaline kasutamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht, ülemused

Rakendamise eest vastutavad: kasutajad

Veebimäluks (ka online -kõvakettaks) nimetatakse interneti teenusepakkujate pakutavat mälu. Kliendid saavad selle veebiteenuse pakkujalt ja kasutavad seda andmete pikaajaliseks talletamiseks ning selleks, et lihtsustada juurdepääsu andmetele läbi interneti. Sellist teenust hindavad eelkõige need töötajad, kes on pidevalt liikvel, sest nad pääsevad kõikjalt kiiresti ja ilma piiranguteta oma andmetele ligi. Veebimälu teenust kasutatakse meelsasti ka suuremahuliseks andmevahetuseks. Siin peitub aga ka suur risk, sest ligipääs välistele salvestusvõimalustele teeb andmevood raskemini kontrollitavaks. Andmete konfidentsiaalsuse säilimine ei sõltu ainult sellest, kas andmeside ja salvestamine on teenusepakkuja juures piisavalt turvatud, vaid ka sellest, millistest välistest IT-süsteemidest neid andmeid alla laaditakse, mis saab andmetest pärast allalaadimist ning kuhu need hiljem salvestatakse.

Tüüpilised probleemid on näiteks järgmised:

- Töötajad kasutavad väliseid veebimälusid firmasiseste andmete allalaadimiseks internetikohvikus või mõnes teises firmas. Andmeedastuse ebapiisava krüpteeringu tõttu (nii autentimis- kui ka tööandmed) saavad salvestatud firmasisestele andmetele ligipääsu ka volitamata isikud.
- Töötaja on kodus ja laadib töökohast oma koduarvutisse andmeid, et nendega nädalavahetusel töötada. Kuna töötaja koduarvuti on kahjurvaraga nakatunud, nakatab ta sellega ka töödeldavad failid.

Salvestatud andmete kättesaadavus sõltub mitmetest teguritest. Teenusepakkuja pakutava internetiühenduse ja süsteemide käideldavus. Kui andmeid soovitakse salvestada pikaks ajaks, tuleks esmalt kontrollida teenusepakkuja ärimudelit, et saada aimu, kas teenusepakkuja on suuteline tagama pikaajalise käitamise ja muutumatud raamtingimused. Ühenduse kiirus. Kui veebimälu soovitakse kasutada andmevarunduseks, ei ole tähtis mitte ainult aeg, mida vajatakse varundatavate andmete edastamiseks teenusepakkujale, vaid ka aeg, mis kulub varunduse installimiseks. Professionaalseks andmevarunduseks on enamik institutsioonisiseseid andmevarundussüsteeme paremad ja paremini kontrollitavad (võimalik, et ka soodsamad). Veebimälu kasutamine peaks olema igas institutsioonis selgelt reguleeritud.

Selleks on mitmeid variante:

- Asutused võivad veebimälu kasutamise täielikult ära keelata. Töötajaid tuleb sellest teavitada. Keeldu saab toetada ka tehniliste lahendustega, rakendades teadaolevate teenusepakkujate filtreerimist, kuid siinjuures tuleb arvestada, et kasutajad leiavad sellistele teenustele ligipääsemiseks üha uusi võimalusi.
- Asutus võib veebimälu kasutamise ametitegevuseks ametlikult heaks kiita ja töötada selle jaoks välja sobivad reeglid.

Ametiasutus või ettevõte peab selliste teenuste kasutamiseks alati välja töötama selged reeglid (vt M 2.460 Väliste teenuste reguleeritud kasutamine).

Need peaksid muu hulgas selgitama järgmist:

- Ametiga seotud ja isiklik kasutus tuleb hoida lahus.
- Asutus või ettevõte peab kindlaks määrama veebimälu ametikasutuse raamtingimused (nt info edastamine, kaitse kahjurvara eest).
- Enne veebimäluteenuste kasutamist tuleks hoolikalt kontrollida teenusepakkujate kasutustingimusi, et selgitada välja, kas need on vastuvõetavad.
- Selleks, et salvestatud andmetele saaksid ligi pääseda ainult volitatud isikud, tuleb veebimälu pääsuõigused täpselt kindlaks määrata ja neid regulaarselt värskendada.
- Andmevahetust tuleks alati kaitsta SSL-i/TLS-i krüpteeringuga.
- Kaitsmaks konfidentsiaalseid andmeid volitamata ligipääsu eest, tuleb need salvestada krüpteeritult.
- Tuleb kindlaks määrata, kust (millistest asukohtadest) ja millistesse IT-süsteemidesse tohib salvestatud andmeid alla laadida.

Kontrollküsimus:

- Kas veebimälu kasutamine on institutsioonis selgelt reguleeritud?

M 5.159w Veebiserveri protokollide ja sidestandardite ülevaade

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

(Kommunikatsiooni-)protokollidega reguleeritakse IT-s protsesside ja komponentide vahelist infovahetust (vt ka M 5.39 Protokollide ja teenuste ohutu kasutamine). Selleks, et ka erinevate arendajate loodud rakenduste protsessid omavahel suhelda saaksid, tuleb info edastamisel toetuda kindlaks määratud reeglitele. Neid reegleid nimetatakse protokollideks. Protsessideks võivad olla nii serveriteenused kui ka klientsüsteemide rakendused. Protokollidega on võimalik reguleerida ka lokaalsete protsesside infovahetust. Veebiserverites kasutatakse mitmeid protokolle, mida järgnevalt ka kirjeldame.

Hypertext Transfer Protocol (HTTP)

HTTP on kõige levinum veebis kasutatav andmeedastusprotokoll. Tegemist on TCP/IP-referentsmudeli rakenduskihi protokolliga. Versioon 1.1 on defineeritud dokumendis RFC 2616 ja see lähtub klient-server-põhimõttest. See tähendab, et klientsüsteem esitab alati päringu (request), millele veebiserver vastab (response). Protokoll töötab ilma olekuta, st pärast seda, kui andmed on edastatud (nt veebileht), ei jäeta ühendust serveriga aktiivseks, vaid katkestatakse. HTTP puhul on tegemist avatekstprotokolliga, mistõttu on ründajal võimalik kogu andmevahetust lugeda. Asjakohast täiendust pakub HTTPS, mis võimaldab veebiserveri ja brauseri vahelist ühendust krüpteerida TLS-i või SSL-i baasil.

HTTPS

HTTPS (HTTP üle SSL-i või HTTP üle TLS-i) on HTTP variant, mille korral saab autentimist ja andmeedastust kaitsta krüpteerimise ja sertifikaatidega. HTTPS-i definitsiooni leiab dokumendist RFC 2818. HTTPS-i toega veebiserverid kasutavad enamasti TCP-porti nr 443. HTTPS-i kasutamisel tuleb arvestada, et TLS toetab ka režiimi, kus andmeid ei krüpteerita. Vastavate turbenõuete korral tuleks HTTPS-proksis keelata selliste ühenduste loomise võimalus.

WebDAV

WebDAV (Web-based Distributed Authoring and Versioning) on avatud standard veebiserveril paiknevate andmete kasutusseandmiseks ja haldamiseks. WebDAV täiendab HTTP standardi versiooni 1.1, pakkudes lisafunktsioone.WebDAV-i kommunikatsioon klientsüsteemi ja serveri vahel põhineb ainult HTTP pordil nr 80. Võrreldes teiste protokollidega, millel on sarnased funktsioonid (nt FTP-ga), annab see märgatava eelise. FTP-sarnased protokollid kasutavad käskude ja andmete edastamiseks erinevaid ühendusi, mistõttu tekib tihti sideprobleeme paketifiltritega. Lihtsate failioperatsioonide, nt failide üleslaadimise, ümbernimetamise ja kustutamise kõrval võimaldab WebDAV ka versioonikontrolli, mis lubab faile töödelda mitmel kasutajal. Selleks, et kasutada kõiki olemasolevaid funktsioone, peavad kõik kasutajad ennast siiski kõigepealt HTTP pakutava autentimismeetodiga autentima. Igale kasutajale on võimalik väljastada erinevad õigused. Võimalik on lubada või keelata ka ainult kindlad failitüübid. Nõnda saab täitmisfaile (nt faile, mille laiend on.exe) blokeerida, et takistada kahjurvara soovimatut levikut.

XML-RPC

XML-RPC (Extensible Markup Language Remote Procedure Call) on protokoll, mida kasutatakse eemal asuvates süsteemides paiknevate funktsioonide käivitamiseks, seejuures kuvatakse edastatud andmeid XML-struktuurina. XML-RPC teateid edastatakse tegelikult HTTP-ga. RPC-d (Remote Procedure Calls), mida teostatakse näiteks XML-RPC kaudu, moodustavad jaotatud süsteemide põhialuse. See võimaldab võrgu kaudu käivitada funktsioone eemal olevates süsteemides. Kuna funktsiooni päringud ja tagastatavad väärtused kuvatakse XML-is, toimub aluseks oleva programmeerimiskeele ja operatsioonisüsteemi abstraktsioon. See tähendab, et päringud ei olene kasutatavast programmeerimiskeelest ega operatsioonisüsteemist.

Funktsiooni päring koosneb funktsiooni nimest ja sinna juurde kuuluvatest parameetritest. Funktsiooni poolt tagastatava väärtuse saadab server klientsüsteemile tagasi sarnase struktuuriga. XML-RPC-s ei ole ette nähtud ühtegi konkreetset turvameetodit. Seetõttu tuleb selle süsteemi programmiloogikasse, mis kasutab XML-RPC-d funktsioonide kaugpäringuks, paigaldada asjakohased turvameetmed.

SOAP

SOAP tähendas esialgu lihtsat objektipäringuprotokolli Simple Object Access Protocol. Alates versioonist 1.2 seda akronüümi aga enam ei kasutata, sest see ei kirjelda protokolli tegelikke funktsioone õigesti. Tegemist on raamistikuga, mis reguleerib andmete edastamist võrgu kaudu. SOAP võimaldab käivitada funktsioone eemal asuvates süsteemides. SOAP-i võib vaadelda kui XML-RPC järeltulijat. SOAP-teated põhinevad samuti XML-struktuuril ja neid on võimalik edastada erinevate protokollidega. Näideteks on siinkohal meiliedastusest tuntud SMTP ning ka juba varem mainitud HTTP. Krüpteeritud ühenduse loomiseks on võimalik võtta kasutusele ka HTTPS. SOAP-i üks olulisemaid kasutusalasid on veebiteenuste võimaldamine ja kasutamine.

Andmebaasikonnektorid

Konnektorid toimivad standardiseeritud liidesena andmebaasi ja andmebaasi haldussüsteemi (DBMS) vahel. Andmebaasikonnektorid võimaldavad olenemata DBMS-ist andmebaasis olevatele andmetele ligi pääseda või neid muuta. Lisaks loob, sulgeb ja haldab konnektor andmebaasiühendust. Sellega muutub tarkvara arenedes andmebaasidele ligipääsu võimaldamine tunduvalt lihtsamaks. Konnektorid tagavad kiire ligipääsu andmebaaside tabelitele või DBMS-i funktsioonidele. Andmebaaside ja nende sisu haldamiseks kasutavad andmebaasikonnektorid andmebaasikeelt, nt SQL-i. Tuntud andmebaasikonnektorid on muu hulgas avatud andmebaasipöördus ODBC (Open Database Connectivity) ja Java andmebaasipöördus JDBC (Java Database Connectivity).

SQL

SQL on lühend sõnaühendist Structured Query Language ja seda kasutatakse andmebaasikeelena. SQL-käskudega on võimalik olemasolevaid andmeid defineerida, esitada andmete kohta päringuid ja andmeid muuta. Sellega koondab SQL endasse andmetöötluskeele, andmekirjelduskeele ja andmete järelevalvekeele elemendid. Kuigi leidub veel teisigi andmebaasikeeli, on SQL kasutuses kõikides levinud andmebaasides ning sellele on olemas nii ANSI kui ka ISO standard. Rakenduste ja veebilehtede jaoks, mis kasutavad andmebaasipäringuteks SQL-käske, tuleb võtta mõningaid turvameetmeid. Näiteks tuleb vältida vastuvõtlikkust SQL-süstidele. SQL-süstide korral on tegemist veebilehtede nõrkade kohtadega, mis võimaldavad andmebaasi infole volitamata ligi pääseda.

Nõrgad kohad tekivad juhul, kui veebilehed ei filtreeri piisavalt kasutajate sisestusi ja kui ründajatel on võimalik mõjutada SQL-päringuid. Kui SQL-päringuid õnnestub manipuleerida, tekib võimalus andmebaasis hoitavat infot lugeda, muuta või kustutada. Levinud meetod SQL-süstide vastaseks kaitseks on talletatud protseduuride (stored procedures) kasutamine. See on DBMS-i funktsioon, mis salvestab kokkukuuluvad käsud ja jadad ühtseks valmis protsessiks. Seeläbi ei ole ründajal enam võimalik SQL-päringut SQL-süstiga muuta. Samasugust kaitset SQL-süsti eest pakuvad ka raamistikud (frameworks). Raamistikud (nt Hibernate) moodustavad andmebaasi ja andmebaasile ligipääsu võimaldava rakenduse vahel veel ühe abstraktsioonikihi.

Raamistik on programmeerimisliides, mis ei sõltu reaalselt kasutatavast andmebaasist, ja see sobib mis tahes objektide salvestamiseks. Kui talletatud protseduure või raamistikke ei kasutata, peavad kõik andmed, mida kasutajad on andmebaasi sisestanud ja mida saab kasutada andmebaasi sissekannetena, läbima sisestuse õigsuse kontrolli. Seejuures filtreeritakse kõiki märke, mis võiksid mõjutada SQL-käske ja sellega ka andmebaasipäringute toimimist. Rakendused, mis kasutavad andmebaasipäringuteks SQLkäske, langevad ikka ja jälle SQL-süsti tüüpi rünnete ohvriks.

Eemal asuvate protseduuride käivitamise tehnikad

Üks tuntud ja sageli kasutatav kaugpäringutehnika on CORBA (Common Object Request Broker Architecture). Tegemist on jaotatud süsteemide standardiga, mis võimaldab luua sideühendusi erinevates süsteemides jooksvate protsesside vahel ning teostada andmevahetust.

Programmeerimiskeelest sõltumatult defineeritud liides IDL (Interface Definition Language) teeb võimalikuks side erineva programmeerimiskeelega programmide vahel. Kahe protsessi vahelise side loomiseks on mõlemal pool vaja kasutada nn objektipäringu maaklerit (Object Request Broker, ORB). ORB-d toimivad mõlema poole programmeerimiskeeles ning nende ülesanne on andmete vastuvõtmine ja saatmine. Erinevate ORB-de andmeside toimub kas mõne kindla tootja protokolli või tootjast sõltumatu IIOP (Internet Inter-ORB Protocol) kaudu. CORBA-sarnaseid kontsepte leiab ka erinevatest programmeerimiskeeltest. Kaks kõige levinumat võimalust on meetodi kaugkäivitus (Remote Method Invocation, RMI) ja

hajus-komponentobjektimudel (Distributed Component Object Model, DCOM).

Java keskkonnast pärinev RMI võimaldab käivitada eemal asuvaid Javameetodeid. DCOM võimaldab kasutada DCE standardil põhinevat objektile suunatud RPC-süsteemi. Andmetöötluse hajuskeskkonna (Distributed Computing Environment, DCE) korral on tegemist jaotatud rakenduste tööstusstandardiga, mis põhineb klient-server-mudelil. Kuna süsteemiüleste funktsioonipäringutega avatud arhitektuurid võimaldavad kasutada paljusid liideseid, tuleb tähelepanu suunata sellele, kes on need isikud, kes liidestele juurde pääsevad, ja milliseid andmeid nende liideste kaudu edastatakse. Turvaaspektid, eelkõige kasutajate autentimine, kaetakse CORBA turvaspetsifikatsiooniga.

M 5.160w Autentimine veebiserveril

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

Kasutajate isikute kindlakstegemiseks ja neile vastavate õiguste jagamiseks on olemas erinevaid mehhanisme, mida järgmistes lõikudes lähemalt tutvustatakse. Pärast seda, kui kasutaja on ennast edukalt veebiserveri suhtes autentinud (näiteks kasutajanime ja parooli sisestamisega), määratakse talle nn seanss (session). Session 'i korral on tegemist seansiga, mis on määratud kindlale kasutajale ja mis kujutab endast aktiivse ühenduse loomist serveriga. Seansid on hädavajalikud, sest veebirakendustes kasutataval protokollil (HTTP-l) puudub olekurežiim. Igat uut veebiserverile laekuvat päringut töödeldakse sõltumata teistest, juba varem laekunud päringutest. Selleks, et veebilehtedes kasutajatest tingitud olekuid ikkagi kuvada (nt kasutaja sisselogimise olekut või ostukorvi sisu), kasutatakse seansse. Seanss identifitseeritakse seansi ID-ga. Pärast edukat autentimist kantakse see üle klientsüsteemile ning edastatakse edaspidi iga uue serverile suunatud päringuga. Selle abil tuvastab veebiserver, et päring on seotud kindla kontekstiga ja seeläbi kindla kasutajaga.

Veebivormil põhinev autentimine

Veebivormil põhinev autentimine on laialt levinud autentimismeetod, mida kasutatakse enamikus veebirakendustes. Sisselogimisandmed edastatakse veebirakendusele blanketiga. Kasutaja autenditakse seejärel veebirakenduses, mis kontrollib, kas kasutaja kohta edastatud sisselogimisandmed on korrektsed. Sellise autentimise eelis on sisselogimisfunktsiooni otsene liitmine veebirakendusega, sest sisselogimisandmed sisestatakse veebirakenduse andmesisestusväljadele. Kuna autentimise viib läbi veebirakendus, on võimalik sisselogimiskatseid käsitleda väga paindlikult (nt reageerida ebaõnnestunud sisselogimiskatsetele, väljastada veateateid). Suur paindlikkus toob endaga aga kaasa nõrgad kohad teostuses. Näiteks tuleb jälgida, et sisselogimisandmed edastataks turvalise kanali kaudu.

Basic Access Authentication

HTTP Basic Access Authentication määratleti seoses HTTP/1.0-ga dokumendis RFC 1945 ja see võimaldab kasutada lihtsat autentimismehhanismi. Sisselogimisprotsess ei leia selle puhul aset mitte veebirakenduses, vaid veebiserveris. Sisselogimisandmeid ei edastata seejuures krüpteeritult, vaid ainult Base64 kodeeringuga, mistõttu tohib sellist autentimist kasutada üksnes turvatud kommunikatsiooni korral. Kui ründaja on võimeline kommunikatsiooni pealt kuulama, saab ta kodeerimisest mööda hiilida ning kasutajanime ja parooli avatekstina lugeda. Basic Access Authentication pakub kaitset kataloogi tasandil, sest sellega on võimalik defineerida ligipääsufunktsioone erinevate kasutajate ja kataloogide kaupa. Seda liiki autentimist toetavad eelkõige levinumad veebiserverid ja brauserid, kuid see on juba vananenud ning seda kasutatakse tänapäeval vähe.

Digest Access Authentication

Digest Access Authentication põhineb Basic Access Authentication'il, kuid sellele on lisatud mõned turbefunktsioonid. Näiteks edastatakse sisselogimisinfo asemel ainult vastav MD5 kontrollsumma. MD5 ei ole enam kõigi kasutusvaldkondade jaoks turvaline. Kuna MD5 korral kasutatakse juhuarve, siis kokkupõrgete leidmise võimalus autentimist ei mõjuta. MD5 kontrollsumma kasutab iga autentimiskatse korral serverilt saadud uut juhuarvu. Nii saab turvaliselt autentida ka ebaturvaliste kanalite kaudu. Digest Access Authentication on spetsifitseeritud dokumendiga RFC 2617.

Hostil põhinev autentimine

Hostil põhineva autentimise korral jagatakse ligipääsuõigusi IP-aadressi alusel. Selline autentimisliik on aga jällegi vastuvõtlik IP-võltsimisele. IP-võltsimise korral võltsib ründaja tema saadetavate võrgupakettide IP-aadresse, mistõttu tehakse nendes sisalduvad päringud valede pääsuõigustega.

Sertifikaadid

Sertifikaadist lähtuv autentimine põhineb avaliku võtme (public key) taristul. Identiteet tuvastatakse sertifikaadi alusel, mis peab sisaldama teatud olemi (nt kasutaja) avalikku võtit ja olema sertifitseerimiskeskuse poolt allkirjastatud. Sertifitseerimiskeskus vastutab seega enne sertifikaadi allkirjastamist identiteedi kontrollimise eest. Üldjuhul täidab seda ülesannet oma registreerimiskeskus. Enamasti kasutatakse sertifikaadil põhineva autentimise korral nn kahefaktorilist meetodit. See tähendab, et identiteedi tuvastamiseks ei piisa ainult sertifikaadi olemasolust, vaid vaja on veel ühte faktorit, milleks enamikul juhtudel on parool. Olenevalt kasutusalast võib sertifikaat olla salvestatud erinevatele andmekandjatele. Näideteks on tokenid, kiipkaardid ja tarkvara sertifikaadisalvestid.

Küpsised (cookies)

Tavaliselt on küpsised klientsüsteemides asuvad väikesed tekstifailid, kuhu salvestatakse lokaalselt andmeid HTTP-seansi kohta. Kui HTTP-päises saadetakse veebiserverile uus päring, saadetakse küpsistesse salvestatud info päringuga kaasa ning see võimaldab serveril kliendi uuesti ära tunda. Küpsiste põhjal saab server näiteks tuvastada, milline kasutaja päringut saadab. Küpsised võivad peale kindla ID sisaldada ka teist laadi informatsiooni. Näitena võib nimetada infot selle kohta, milliste domeenide ja andmeteede jaoks küpsis kehtib. Kuna küpsiste kaasasaatmist reguleerib brauser, vastutab brauser ka selle eest, et neid suudaks lugeda ainult serveri poolt kindlaks määratud domeen. Küpsised võivad lisaks sisaldada ka lippe (flags). Kui lisatakse lipp nimega httponly, ei ole JavaSkriptil enam võimalik küpsist lugeda ega muuta. Murdskriptimise (Cross-Site Scripting, XSS) abiga on võimalik nõrkadelt domeenidelt röövida küpsiseid ning näidata end veebiserverile mõne teise kasutajana. Selleks smugeldab ründaja veebilehele koodi, mis käivitatakse kasutaja klientsüsteemis, ning see saadab ründajale kasutaja teadmata soovitud küpsise.

M 5.161w Dünaamiliste veebilehtede koostamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

Dünaamiliste veebilehtede genereerimiseks läheb tarvis serveripoolset programmiloogikat. Paljudel juhtudel võib selle funktsiooni jätta veebiserveri hooleks, nt lihtsate skriptide või SSI (Server Side Includes) abil. Keerukate veebilehtede jaoks kasutatakse siiski sageli veebirakenduste serverit koos vastava raamistikuga (framework). Veebirakenduste server ei pea ilmtingimata olema veebiserverist lahutatud, sest paljude levinud veebiserveritega on veebirakenduste server juba integreeritud (nt Tomcat Apache). Veebirakenduste server ja juurdekuuluvad raamistikud võimaldavad luua mahukaid veebilehti. Lisaks lihtsustavad need olulisel määral juurdepääsu taust- ja Alt -süsteemidele. Järgmistes lõikudes kirjeldatakse dünaamiliste veebilehtede koostamiseks sagedamini kasutatavaid programmeerimiskeeli ja raamistikke.

CGI

CGI on akronüüm sõnadest Common Gateway Interface ning selle puhul on tegu meetodiga, mis võimaldab kujundada dünaamilisi ja interaktiivseid veebilehti. Dünaamilist sisu genereeritakse väliste rakendustega, mille käivitab veebiserver. Selle jaoks on CGI-l veebiserveri ja süsteemirakenduse vaheline liides. Seega ei ole CGI programmeerimiskeel, vaid funktsioon, mis võimaldab veebiserveril käivitada programme. Seetõttu saab CGI-programme luua mis tahes programmeerimiskeelega, eelduseks on vaid see, et veebiserverid peavad oskama neid käivitada. Olenevalt kasutatud tehnoloogiast on CGI-rakendus kas binaarfaili või skripti kujul. CGI-keelte tüüpilisteks näideteks on C, Perl, TCL, Unix-Shell jms. Kuna CGI-programmid teostavad dünaamilisi funktsioone, peavad nad tagama ka vajaliku turbeastme järgimise. See tähendab näiteks seda, et iga CGI-programm peab iseseisvalt kontrollima ka parameetreid.

SSI

CGI-sarnane meetod, millega saab genereerida dünaamilisi lehekülgi, on SSI (Server Side Includes). SSI võimaldab veebilehega siduda mis tahes faile või süsteemikäskude tagastusväärtuseid. Kuna aga SSI dünaamiliste veebilehtede kujundamise võimalused on üsna piiratud, siis seda enam palju ei kasutata. Sama moodi nagu CGI puhul, saab ka SSI-ga kitsaskohti integreeritud süsteemikäskudega ära kasutada. Näiteks kui integreeritud faili asukohta õnnestub muuta, on võimalik lugeda serveris asuvaid faile või käivitada süsteemis käske.

PHP

PHP (akronüüm sõnadest Hypertext Preprocessor) on skriptikeel, mis võimaldab luua dünaamilisi veebilehti. Alates 4. versioonist täiendati PHP-d objektipõhise programmeerimisvõimalusega. PHP olulised omadused on kiire õpitavus ja andmebaasidega integreerimise laialdane tugi. Lisaks pakub PHP mitmeid turvafunktsioone. Näiteks võimaldab nn Magic Quote potentsiaalselt ohtlike märkide automaatset tuvastamist ja maskeerimist. See muudab mitmed levinud ründed raskemaks. Lisaturvet pakub ka funktsioon Open Base Dir, mis tõkestab juurdepääsu failidele, mis asuvad väljaspool defineeritud kataloogi, piirates nõnda ründaja võimalusi. Lisaks saab PHP abil piirata potentsiaalselt ohtlikke funktsioone. Nn Safe-Mode võimaldab paljusid õiguseid piirata. See on eriti mõistlik just Multi-Domain-keskkonnas, kus mitut veebilehte käitatakse samal serveril. Vaatamata nendele turvafunktsioonidele on erinevate funktsioonide tõttu (nt register_globals) ka PHP-ga siiski mõningaid probleeme. See funktsioon võimaldab näiteks PHP-

skripti avamisel sisestada suvalisi muutujaid, muutes veebilehe kompromiteerimise ründaja jaoks niimoodi palju lihtsamaks. Vanemates PHP-des esines mitmeid kitsaskohti. PHP kõrval suutsid dünaamiliste veebilehtede loomisel end tõestada ka mitmed teised skriptikeeled. Tuntuimad neist on Ruby, Python ja Perl. Üldjoontes pakuvad kõik need skriptikeeled sarnaseid funktsioone ja seetõttu on neil ka sarnased turvaprobleemid. Kogemused on näidanud, et suur osa veebirakenduste tuntud kitsaskohtadest ei sõltu kasutatud programmeerimiskeelest.

JSP (Java Server Pages)

Java Server Pages leiab esmajoones rakendust Java veebirakenduste presentatsioonikihis. Kuvatavad andmed salvestatakse tavaliselt nn JavaBeansi (andmeedastuse ümbrisrakendusse), mis võimaldab lihtsat juurdepääsu. JSP-lehekülgedel saab siiski kasutada ka protsessiloogikat. Sellega kaasneb aga andmete funktsiooni ja kuva kohmakas lahutamine ning see on vastuolus Model-View-Controlleri põhimõttega. Viimane nõuab andmete, funktsiooni ja esitluse selget eraldamist.

J2EE

Java Enterprise Edition, lühendatult J2EE, määrab kindlaks tehingupõhiste Java-rakenduste tarkvaraarhitektuuri. See võimaldab luua dünaamilist sisu, integreerides Java-koodi HTML- ja XML-dokumentidega. Java pakub mitmeid turvafunktsioone. Näiteks on Java tüübikindel, mis viitab sellele, et kasutamise käigus kontrollitakse muutujate ja parameetrite andmetüüpi. Java väldib juba oma disainiga selliseid salvestihalduse kitsaskohti nagu rakenduse puhvri ületäitumine (buffer overflow) ja kuhja ületäitumine (heap overflow). Seeläbi ei suuda ründaja enam programmi oma kontrolli alla saada sellega, et täidab programmi mälusektsiooni manipuleeritud sisestustega. Mõned teist tüüpi kitsaskohad on siiski ka Javas ohtlikud. Nn liivakasti näol pakub Java võimalust käivitada kood turvalises ja eraldatud keskkonnas, ilma et see ohustaks operatsioonisüsteemi. J2EE Security abil on lisaks võimalik süsteemiressursside piirav haldamine.

ASP/ASP.NET/Mono

Active Server Pages (ASP) leiab peamiselt kasutust Microsofti keskkondades, sest see tehnoloogia töötab esmajoones Microsoft Internet Informationi serveril. ASP pole eraldi programmeerimiskeel, vaid raamistik, mis võimaldab koostada programmiloogikat, kasutades erinevaid programmeerimiskeeli. ASP-d siiski enam edasi ei arendata ja seda asendab ASP.NET. Mono näol on peale Microsofti kasutusvaldkonna olemas ka Unixis töötav variant. ASP.NET-i jaoks on olemas mitmeid turvafunktsioone. Üheks näiteks on gatekeeper -mehhanism, mis koosneb erinevatest moodulitest ja pakub mitmesuguseid turvafunktsioone (nt filtreerimine, autentimine). Lisaks saab kasutada eraldi Anti-Cross-Site-Scriptingu raamistikku. Lisaraamistikuga on võimalik rakendada rollipõhist juurdepääsukontrolli.

Veebiteenus

Veebiteenust võib võrrelda veebirakendusega. Erinevus on selles, et tulemuste väljundit ei seata brauseri jaoks sobivasse vormi, vaid kasutatakse teistsugust struktuuri (nt SOAP-i). Veebiteenuste ühendamisega saab luua serverile orienteeritud arhitektuuri (SOA). Selleks võetakse rakenduse üksikud osad kasutusse veebiteenusena. Nii saavad neid korraga kasutada mitu rakendust. Sel moel suureneb funktsioonide taaskasutatavus ja rakenduse üksikute osade hooldamine muutub kergemaks. Kuna veebiteenused kasutavad samu protokolle mis veebirakendused, on nad turvanõuete poolest veebirakendustega võrdsed. Web-Service Security (WS-Security) jaoks on olemas eraldi standard. Teenusele orienteeritud arhitektuuri avatuse tõttu muutub erinevalt suletud arhitektuuridest ülimalt oluli-

seks just juurdepääsu kaitse. Seetõttu on veebiserveriga suhtlemisel kehtivad autentsuse, tervikluse ja konfidentsiaalsusega seotud nõuded väga ranged. Päringute ja avateksti kujul vastuste pealtkuulamine ja teadete võltsimine ning muutmine peab olema takistatud. Turvanõuete täitmiseks võib kasutada krüptograafilisi meetodeid. Teenusele orienteeritud arhitektuuri puhul on turvameetmeid võimalik juurutada ka eraldi teenustena. Oluline veebiteenustega seotud mõiste on WSDL (Web Service Description Language). WSDL võimaldab veebiteenusele esitada funktsionaalseid andmeid, mis on vajalikud selle teenuse kasutamiseks. WSDL-fail kujutab endast veebiserveri liidese kirjeldust. Fail määrab, milliseid funktsioone veebiteenus osutab, kuidas neid avada ja milliseid parameetreid läheb tarvis nende avamiseks. Seega sisaldab WSDL-fail veebiteenuse kasutamise põhiinfot (nt pääsupunkti ja -protokolli), mis võimaldab veebiteenust kasutada.

WSDL-iga seotud turbeaspektid puudutavad esmajoones vajalikke XML-parsereid. Need on vajalikud veebiteenusele edastatud andmete töötlemiseks. Kuna parserid on sageli ise välja töötatud, ohustavad neid mitmed erinevat tüüpi ründed. Rünneteks kasutatakse peamiselt meelega valesti kujundatud XML-teateid, mis võivad põhjustada parseri või kogu veebiteenuse kokkuvarisemise. Selle näiteks on XML-pomm. See on XML-dokument, mille osad viitavad korduvalt iseendale, mistõttu võib parseril tekkida probleeme dokumendi sisselugemisega. Veel üks veebiteenuste oht on ebapiisavalt kaitstud SOAP-teadete pealtkuulamine ja taasesitamine (nn Replay-rünne). Seejuures edastatakse juba saadetud ja ründaja salvestatud SOAP-teateid suvaline arv kordi uuesti, millega kaasneb volitatud kasutajalt serverile esitatud korralduste korduvtäitmine. See võimaldab teenusepakkuja andmekogumeid volitusteta muuta ja kustutada.

AJAX/Atlas

Atlas on veebiteenusena töötava AJAX-i (Asynchronous JavaScript and XML) raamistik. Selle tehnoloogia eesmärk on seni ainult arvutites kasutatavate programmide imiteerimine veebirakendustena. See tähendab, et on võimalik laadida veebilehe osasid, ilma et oleks tarvis uuesti laadida tervet lehte. Tavaliste rakendustega võrreldes saavutatakse seeläbi märksa parem jõudlus. AJAX-it ei saa siiski soovitada, sest selleks peavad kasutajad oma klientsüsteemides lubama aktiivsisu kasutamist. Aktiivsisu kasutamisega kaasnevad peamised ohud on Session-Riding-ründed ja Cross-Site-Scripting-ründed.

Voogteenused

Voogteenustega edastatakse klientsüsteemidele esmajoones heli- ja videoandmeid. See eeldab aga kliendipoolsete eriprogrammide või brauseri pluginate kasutamist. Kuvatava sisu volitustekontseptsioonide ellurakendamiseks kasutatakse sageli nn DRMS-süsteeme (Digital-Rights-Managemen-System). Need tagavad näiteks selle, et klient saab andmeid näha või kopeerida ainult siis, kui tal on vastavad õigused olemas litsentsina. Andmete saatmiseks klientsüsteemile kasutavad voogteenused mitmeid protokolle. Levinuimad on RTSP (Real Time Streaming Protocol) ja RSVP (Resource Reservation Protocol).

M 5.162 Ribalaiuse planeerimine terminaliserverite kasutamisel

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator

Klassikalises klient-server võrgus on kliendi ja serveri vaheline võrgukoormus allutatud tugevale perioodilisele kõikumisele, näiteks failide edastamisel. Kui rakendus ei vaja hetkel uut informatsiooni, siis ei vajata ka ribalaiust. Terminaliserveri keskkonnas tuleb aga tihti andmeid võrgu kaudu edastada, aga isegi siis, kui tehakse minimaalsete muudatusi kasutajakihis. Seevastu on selle kaudu lihtsam andmevoolu kontrollida. Ühest küljest on võimalik sisendeid ja väljundeid efektiivsemalt kokku pakkida ja seeläbi ribalaiuse haldust piirata, teisest küljest tekib terminali ja terminaliserveri vahel igale kasutajale seanssi kohta ainult üks andmevoog. Terminaliserverist väljuvad siis ühendused näiteks andmebaaside ja meiliteenuste suunas. Failid ise ei lahku hetkekski terminaliserverilt, vaid need ainult kuvatakse kliendil.

Terminaliserveri kontsepti teostamiseks vajalikud ribalaiused varieeruvad suurel määral. Seansside jaoks RDP kaudu tuleb keskmiselt arvestada 250 kbit/s, Citrix soovitab ICA protokolli jaoks arvestada 160 kbit/s, X11 kasutab ilma lisameetmeteta isegi 4 kuni 5 Mbit/s. Tavaline 100 Mbit võrk on sedasi juba 15 aktiivse X-Windowsi terminaliga täiel määral koormatud, sest sisse tuleb arvestada selle all asuv TCP/IP protokoll, mis vajab omakorda veel 30%. Kokkupakkimise ja proksisüsteemide puhvermehhanismide abiga, näiteks NX või Free NX, on andmemahtu võimalik vähendada keskmiselt 40 kbit/s peale. Siin nimetatud väärtusi tuleb planeerimisel vaadelda kui ligikaudseid piirväärtusi. Praktikas on seetõttu ilmtingimata vajalik analüüsida konkreetset kasutussituatsiooni. Rakendused, mis nõuavad ekraanisisu suurte alade aktualiseerimist, koormavad võrku tugevamini kui need rakendused, mille korral ainult harva mõningad märgid kasutajadialoogides muutuvad. Graafiliselt nõudlikud kasutajaliidesed vähendavad samuti piiratud jõudlusega kasutajate arvu nagu kasutajate käitumine mõjutab võrgu koormusprofiili. Kui planeeritud stsenaariumile eelnevad kogemused puuduvad, tuleks suuremate installatsioonide juures läbi viia reaalsed testid konkreetse konfiguratsiooniga, et oleks olemas põhjendatud andmed oodatavatest andmemahtudest ja oleks võimalik teha ettevalmistusi vajalike võrguressursside kasutusele võtmiseks. See võib toimuda nii katsete kaudu reaalsetes kasutajagruppides kui ka sünteetiliste testide abil, mis on läbi viidud skriptide poolt juhitud ligipääsusimulatsioonides. Mõlemal juhul tuleb enne analüüsi kindlaks määrata reaktsiooniajad, mida ei tohi ületada. Lisaks tuleks luua reserve, et tulevikus tekkiva kõrgema nõudlusega, näiteks kasutajatearvu suurenemisel või rakenduste uuendamisel, oleks võimalik olukorda teatud määral leevendada.

Kui vajaduste välja selgitamisel ilmneb, et erinevate terminaliserverite jõudlusmahud ei ole piisavalt suured, kuna nad konkureerivad teiste võrgus kasutusele antud teenustega, võimaldab ribalaiusehaldurite kasutamine andmevoolu prioriseerida ja seeläbi kitsaid kohti vältida. Selle kõrval on terminaliserverid sobilikud andma kiiresti ja suhteliselt väikese vaevaga kasutaja kasutusse salvestusvõrke. Allavooluteenuste ühendamine võib seega toimuda teise võrgu kaudu, näiteks iSCSI või Fiber Chanell tehnikate kaudu, otse terminaliserveril ja sellega terminali ja terminaliserveri vahelise võrgu koormust jäädavalt vähendada. Terminaliserveri teenuste võimaldamisel laivõru kaudu (Wide Area Network - WAN) peale võrgu ribalaiuse olulise tähtsusega ka ühenduse latentsus. Kuna rakenduse ekraanil kuvatav väljund toimub peaaegu sünkroonselt töötlemisega terminaliserveril, on vii-

vitusteta töötamiseks olulise tähtsusega pakettide liikumisaeg eemal asuvale süsteemile. Suurem andmemaht lisa protokollikihi, näiteks krüpteeritud kaugligipääsu VPN-süsteemides tuleb arvestada samamoodi nagu sidepakkujate peakorrektuure, mis võivad signaali kandumise aega samuti negatiivselt mõjutada.

Täiendavad kontrollküsimused:

- Kas selgitati välja terminaliserverile ligipääsuks vajalik ribalaius, mis tuleneb oodatavast kasutajate arvust ja maksimaalselt lubatud paralleelselt jooksvatest seanssidest?
- Kas sama võrgu kaudu võimaldatakse ligipääsu ka teistele teenustele, mis ribalaiust või latentsust vähendavad? Kas sellisel juhul kontrolliti, kas need mõjutavad terminaliserveri kasutamist?
- Kas juhuks kui teine võrguliiklus hakkab terminaliserveri kasutamist üle teatud piirmäära segama, võeti kasutusele meetmed, et mõju sobivate vahenditega kompenseerida?

M 5.163 Piirav õiguste jaotus terminaliserveritel

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator

Mitme kasutajaga keskkonnas nagu terminaliserveri süsteem on olulise tähtsusega klientide eraldamine üksteisest ja riskantsetest süsteemifunktsioonidest. Tõrgetevaba käitust kindlustamiseks ja seansisiseste andmete konfidentsiaalsuse tagamiseks tuleb laiali jagada piiravad õigused.

Turvaline baasinstallatsioon on alati lähtepunktiks järgnevatele turbemeetmetele. See valitakse suvandiga Full-Security ja mitte Relaxed-Security. Relaxed-Security t tuleb selles kontekstis vaadelda ühilduvusrežiimina, mis võimaldab käitada rakendusi, mis ei ole välja töötatud aktuaalsete terminaliserveri keskkondade jaoks. Selle režiimi kasutamine toob endaga kaas turbekriitilised failiõigused süsteemikataloogides ja laialdased ligipääsuvõimalused registreerimisandmebaasile (Windows Registry). Relaxed-Security režiimi tohib kasutada ainult põhjendatud erandjuhtudel ja pärast individuaalse ohutaseme määramist. Igal juhul tuleb rakenduste ja kasutajate õigusi vähendada ainult hädavajalikuni. Selle tarvis võib kasutusele võtta näiteks tööriistad, mis teostavad tarkvara failioperatsioonide järelvalvet ja protokollivad ligipääsu registreerimisandmebaasile. Lisaks ei tohiks peale vastava rakenduse, mis vajab seda ebaturvalist režiimi, terminaliserveril võimaldada mitte ühegi teise rakenduse kasutamist.

Terminaliserveril paiknevaid rakendusi on võimalik kasutada erinevatel viisidel. Täieliku kasutajaliidese (Desktop) ligipääsu kõrval terminaltarkvara kaudu on võimalik edastada autoriseeritud rakenduste nimekiri. Ainult need on siis kasutajatele terminaliserveri kliendi või veebiserveri siseselt kätte saadavad. See avalikustamismehhanism ennetab väärkasutust ja lihtsustab kasutajate töö teostamist, kuid ei keelusta ligipääsu programmidele, mis asuvad väljaspool lubatud programmide nimekirja. Nii on teatud juhtudel võimalik ilma erilise ettevalmistuseta kasutajadialoogide kaudu teostada lubatud rakendustes autoriseerimata rakendusi. Terminaliserveri süsteemide edukaks kindlustamiseks tuleb järgida veel teisigi punkte.

Teenustele ligipääsuvõimaluste keerukuse vähendamiseks, tuleks terminaliserveri süsteemid installeerida eraldi, võimalusel virtualiseeritud süsteemidele. Terminaliserveri samaaegsel kasutamisel domeenikontrollerina viib see kasutajate õiguste laiendamiseni kõikidele haldusserveritele, ka sellistele masinatele, mis ei ole terminaliserverid. Standardkonfiguratsioonis installeeritud ning mittevajalikud teenused tuleks seetõttu desaktiveerida. See võib hõlmata ka olemasolevaid marsruutimisfunktsioone. Uuesti paigaldatud rakendusserverid tuleb enne kasutuselevõttu varustada uusima tarkvaraga ja soovitatav on see eelnevalt võrgust eraldada. Peale selle tuleb mittevajalikud kasutajakontod eemaldada või desaktiveerida.

Kõigil terminaliserveritel peaks olema installeeritud viirusetõrjeprogrammid. Erineva kaitse- ja turbeastmega rakendused tuleks kasutusse anda erinevatelt terminaliserveritelt. Kui see ei ole organisatoorsetel põhjustel võimalik või mõttekas, tuleb kõiki rakendusi nagu installeeritud tarkvara käsitleda suurima turbevajadusega.

Kasutada tuleb failisüsteemi, mis eristab ligipääsuõiguseid kasutajatasandil, näiteks:

- Kirjutamis- ja lugemisligipääsud mittevajalikele failidele tuleb keelustada (näiteks kustutamise või vastavate õiguste kaudu).
- Võimalusel tuleks loobuda failisüsteemi sisestest viidetest (näiteks sümbolitega lingid, NTFS-Joins jne).
- Haldustööriistad võivad olla teostatavad ainult volitatud administraatorite poolt.
- Hilisem õigus tarkvara installeerimiseks võib olla ainult administraatoril.
- Terminaliserveri keskkonnas tuleks desaktiveerida võimalus teostada tarkvara võõras kasutajakontekstis (näiteks käskluste „ runas ” või „ sudo ”).
- Kõrge infoturbevajadusega süsteemides tuleks autoriseeritud programme hoida Whitelist is. Operatsioonisüsteem teostab siis ainult selles loendis oleva tarkvara. Windowsi operatsioonisüsteemi korral saab seda realiseerida näiteks Appsec i kaudu. Linuxi jaoks võib kasutata laiendeid SELinux ja AppArmor ning Solaris süsteemide jaoks RBAC-d (Role based access control) ja Privilegs i. Peale nende on veel olemas mõned lahendused kolmandatelt tootjatelt, mille funktsioonimaht on operatsioonisüsteemi vahenditest osaliselt suurem.

Seansi dubleerimise (Shadowing) all peetakse silmas võõra seanssi jälgimist. Kasutaja ekraaniväljund kuvatakse ühele või mitmele kliendile, teatud juhtudel on võimalik üle võtta ka sisestusseadmete juhtimine. Seda meetodit kasutatakse eelkõige koolitustel või haldustegevuses. Ilma kasutajat teavitamata või ilma tema loata ei tohi seanssi dubleerida. See tuleb konfiguratsioonis administraatori õigustega läbi suruda. Allavoolusüsteemide, näiteks andmesalvestus või edasitöötlevate süsteemide, kaitseks tuleb kasutusele võtta meetmed, mille põhirõhk asetseb rakenduste kommunikatsiooni realiseerimisel oma Backends idega. Seda peaksid näitlikustama rakendusstsenaariumid spetsialiseeritud rakendused ja üldised rakendused.

Spetsiaalsed rakendused

Spetsialiseeritud rakendused on siinkohal defineeritud kui tarkvara, millel puudub vabalt konfigureeritav tagapõhi. Programmi ei saa kasutada mitte ettenähtud allavoolusüsteemiga suhtlemiseks ja kasutajal ei ole autoriseeritud teenuse kaudu võimalik ligi pääseda teistele mitte lubatud Backendsidele. Sellisel juhul on keskkonna turbeks sobilik kasutada juba eelnevalt tutvustatud meetodit. Sellekohane näide oleks rakendus, millel on ligipääs kindlalt defineeritud andmebaasile. Lisaks ei ole kasutajal võimalik sisestada ligipääsuparameetreid, peale sisselogimisandmete ja eessüsteemi (frontend).

Üldised rakendused

Üldised rakendused, näiteks SQL-konsool või brauser on siinkohal palju turbekriitilisemad. See käib just seetõttu terminaliserveri keskkonna kohta, kuna terminaliserveritel peab olema ligipääs kõigile Backend itele, mis kasutajate nõudlustest lähtuvalt vajalikud on. Üks võimalus selle probleemi vältimiseks on nende programmide käitamine eraldi terminaliserveril ja need individuaalsete DMZ-idega keelatud taustasüsteemidest eraldada. Suure hulga rakenduste korral muutub selline lähenemisviis aga väga ruttu keerukaks, segaseks ja ebamajanduslikuks. Lisaks kaovad väga ruttu keskse arhitektuuri eelised klassikalise klientserverühenduse ees. Alternatiivse variandina saab terminaliserveri ja allavoolu teenuste vahele asetada turvalüüsi, võimaldab reeglitepõhise suhtluse, mis ühendab omavahel kasutaja sisselogimise, rakendused ja Backendi. Seda tegevust illustreerib joonis „allavoolu teenuste eraldamine“. Kasutajale lubatakse Prog-A kaudu ligipääs ainult Backend A-le ja ligipääs Backend B-le keelatakse.

Kontrollküsimused:

- Kas kasutajate ligipääsuõigused terminaliserveri ressurssidele jagatakse piiravalt?
- Kas terminaliserveri kasutajate ligipääsuõigused Backend teenustele jagatakse piiravalt?
- Kas terminaliserveritel, mida käitatakse Relaxed-Security režiimis, on ühel terminaliserveril installeeritud ainult üks rakendus?
- Kas terminaliserveri teenused installeeritakse ainult spetsiaalsetel, teatud juhtudel virtuaalsel süsteemil?
- Kas kõik standardkonfiguratsioonis installeeritud ja mittevajalikud teenused, kasutajakontod ja grupid on terminaliserverilt kustutatud või deaktiveeritud?
- Kas kõigil terminaliserveri süsteemidel installeeriti viirusetõrjeprogrammid?
- Kas õiguste jagamisel arvestati, et kõige suurema turbevajadusega rakendus määrab kõigi teiste sellel terminaliserveril käitatavate rakenduste turbeastme?

M 5.164 Terminaliserveri turvaline kasutamine kaugvõrgust

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator

Kui terminalserver ja selle kliendid on ühenduses ebaturvalise võrgu kaudu, tuleb esmalt luua turvalüüside abil tõhus kaitse andmete edastamise turvalisuse tagamiseks. Peale selle tuleb kasutusele võtta vastavad abinõud, et sidet ei oleks võimalik pealt kuulata, muuta või segada. Edasine tegevus sõltub järgnevatest erinevatest ühendustüüpidest. Mõned terminaliserveri süsteemid võivaldavad protokollisisest krüpteerimist. Standardkonfiguratsioonis on see tavaliselt seadistatud lokaalse võrgu vajadustele. Seetõttu on tavaliselt eelseadistatud lühikesed võtmed, mis kontrollitavas võrgus on täiesti piisavad. Tihti loobutakse siinjuures kahesuunalisest krüpteeringust terminali ja terminaliserveri vahel, et kasutada mõnda vähem ressursse nõudvat ühendust. Sel juhul krüpteeritakse ainult kasutaja sisestus, aga mitte serveri poolt tagasi saadetud väljund kuvaril. Lisaks on protokolli siseselt võimalik sinna paigutada veel teisigi kliendi krüpteerimata andmevoogusid (Virtual Channels), näiteks lokaalsete andmekandjate, liideste või printerite ühendamiseks. Et sidet ebaturvalise võrgu kaudu kaitsta, tuleb eelnevalt kontrollida, milliseid krüptograafilisi meetmeid ja võtmepikkusi käitatavas konfiguratsioonis kasutatakse ja millistel kommunikatsiooni elementidele krüpteerimist kasutatakse. Turvaline kommunikatsioon saab olla tagatud ainult siis, kui kogu andmevoog, kaasa arvatud saatmis- ja vastuvõtmissuuna autentimine on kaitstud. Sobivad protokollisisesed lahendused kasutavad hetkel SSL-i (Secure Socket Layer) või TLS-i (Transport Layer Security), vähemalt 128 bittise võtmepikkusega. Vaatlusesse tuleb kaasata nii serveri kui ka kliendi seaded. Turvalise ühenduse administratiivseks läbisurumiseks peavad serveri ja kliendi seaded ühilduma.

Kui X-Window süsteem ei toeta protokollisiseseid krüpteerimismehhanisme, saab ühenduse realiseerida ka krüptograafiliselt turvatud tunneli kaudu. X-Window süsteemide jaoks on ennast kinnistanud X11-Forwarding meetod koos SSH-ga (vt M 5.64 Secure Shell (SSH)). NX-iga on olemas alternatiiv X11-protokollile, mis võimaldab turvalise autentimise ja terminaliserveri seansside krüpteeritud transpordi X-Windowsiga, RDP-ga ja VNC-ga. Terminaliserveri seanssi turbeks võib kasutada ka virtuaalset privaatvõrku (VPN) (vt B 4.4 Virtuaalne privaatvõrk (VPN)). Selle lähenemisviisi eeliseks on andmevoolu elementide automaatne eraldamine VPN-i poolt. Kuna VPN kindlustab turvalise sisselogimise ja krüpteerimise, võib edasisest terminaliserveri turvalisuse analüüsist siinkohal loobuda. VPN-i kasutamisel tuleb aga jälgida, et eemal asuva kliendi ligipääs võib laieneda peale terminaliserveri ka teistele teenustele. Lisaks on protokollisisesed meetodid optimeeritud terminaliserveri keskkonna tehniliste iseärasustega ja saavad reeglina saadaolevat ribalaiust kiiremini kasutada kui virtuaalsed privaatvõrgud.

Peale perimeeterala ja edastustee turbe tuleb arvestada vastavate klientsüsteemidega. Eriti ligipääs arvutite kaudu, mis paiknevad avalikes kohtades, nagu internetikohvikud, kujutab endast suurt turberiski, kuna informatsioon, nagu sisselogimisnimi ja parool on teatud juhtudel kolmandate isikute poolt loetav. Ka mobiilsed IT-süsteemid ja statsionaarsed kaugtöökohad on raskesti kontrollitavad ning võivad oma algsest autoriseeritud tarkvaratasemest kõrvale kalduda. Kui tahetakse lubada ligipääs ebaturvaliste klientide kaudu, tuleb esitada eriti suured nõudmised sisselogimisprotsessile. Selles stsenaariumis võiks kasutada vähemalt kahe-faktorilist autentimist. Siinjuures küsitakse autentimisel lisaks kasutajanimele ja paroolile veel ühekordset tunnust (One-Time Pasword - OTP). See tunnus

võidakse luua mobiilse seadme (tokeni) abil. Seadme omamine ja kasutajanime ning parooli teadmine on siinkohal üksteist täiendavad turvameetmed, mis takistavad ühekordselt pealtnähtud sisselogimise kuritarvitamise võimaluse. Kahefaktorilist autentimist peaks kasutama eriti juhul, kui terminaliserveri teenustele on võimalik ligi pääseda portaallahenduse kaudu, näiteks veebiliidese kaudu. Lisaks sellele on ligipääsuks erinevatele informatsioonikanalitele sõltuvalt kliendi turvalisusest mõttekas teostada astmeline õiguskontseptsioon. Avalikult ligipääsetavatel IT-süsteemidel tuleks andmevahetus terminaliserveri ja terminali vahel ning ligipääs liidestele keelustada. Lisaks ei tohiks kasutajatel olla lubatud kliendile üle kanda serveri lõikelaua (Clipboard) sisu.

Erinevad terminaliserveri lahendused võimaldavad sisselogimise ajal läbi viia kliendi analüüsi. Seejuures kontrollitakse riistvara ja tarkvara ning viirusetõrjeprogrammi aktuaalsust ja võrreldakse seda salvestatud direktiividega. Sel moel on tehniliste meetmetega võimalik eristada turvalisi ja ebaturvalisi kliente.

Täiendavad kontrollküsimused:

- Kas terminaliserveri keskkond on turvalüüsiga kaitstud?
- Kas kõik terminaliserverilt tulev või sinna suunatud informatsioon edastatakse krüpteeritud andmevoos?
- Kas on administratiivsel tasandil läbi surutud, et terminaliserver võib terminaliserveri seanssiga siduda ainult lubatud enda liideseid, seadmeid ja ajameid?
- Kui ligipääs terminaliserverile toimub ebaturvaliste klientide kaudu, siis kas informatsiooni edastamisel serverilt kliendile keelustatakse selle transport üle lõikelaua?
- Kas takistatakse ebaturvaliste terminaliserverite kliente ühendavad enda liideseid, ajameid või muid seadmeid?
- Kui ligipääs terminaliserverile toimub ebaturvalise kliendi kaudu, kas sellisel juhul nõutakse kahe-faktorilist autentimist või lisameetmena ühekordseid paroole?

M 5.165 Mac OS X mittevajalike võrguteenuste desaktiveerimine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

Mittevajalikud võrguteenused tuleb desaktiveerida, sest need kasutavad süsteemi ressursse ja võivad olla ründe sihtmärgiks. Selleks on vaja administraatoriõigusi. Kui süsteemiteenuseid muudetakse, tuleb see dokumenteerida. Lisaks tuleb korrapäraselt kontrollida, kas sisse lülitatud ja võrgus kättesaadavad on ainult turbepoliitikas lubatud teenused. Kättesaadavad teenused on loetletud süsteemiseadistustes menüüpunkti „Kasutusload" all. Üldjuhul peaks klientoperatsioonisüsteem võrgus ainult väheseid teenuseid või üldse mitte teenuseid pakkuma. Vastavalt kasutusvaldkonnale tuleb teha individuaalsed valikud, kas ja mis teenused peaksid sisselülitatuks jääma.

Haldamiseks kasutatavad teenused, nt Apple Remote Desktop (TCP-port 5900), kauglogimine (SSH-juurdepääs, TCP-port 22) või viirusetõrjetarkvara võrguteenused, peavad jääma sisselülitatuks. Kui võrgus ei kasutata teenust Bonjour, siis tuleb ka see välja lülitada, sest see tarvitab süsteemiressursse ja kujutab endast ründesihtmärki. Võrguteenus Bonjour lülitatakse välja järgmiste käskudega:

sudo launchctl unload -w /System/Library/LaunchDaemons/com.apple.mDNSResponder.plist

sudo launchctl unload -w /System/Library/LaunchDaemons/com.apple.mDNSResponderHelper.plist

Kui internetiprotokolli versiooni 6 (IPv6) ei kasutata, tuleb ka see välja lülitada. IPv6 väljalülitamise vahendid leiate süsteemiseadistustest „Võrgu" alt vastava võrgukaardi täpsemate valikute juurest. Operatsioonisüsteemi värskendamisel võivad teenused soovimatult taas sisse lülituda. Seepärast tuleb pärast iga värskendamist kontrollida, kas teenused on ikka välja lülitatud.

Täiendavad kontrollküsimused:

- Kas kõik Mac OS X mittevajalikud võrguteenused on välja lülitatud?
- Kas Mac OS X süsteemiteenuste muudatused on dokumenteeritud?
- Kas Mac OS X haldamiseks vajalikud teenused on ikka sisse lülitatud?
- Kas kontrollitakse regulaarselt, eriti pärast süsteemivärskendusi, et endiselt oleksid võrgus kättesaadavad üksnes Mac OS X lubatud teenused?

M 5.166z Mac OS X isikliku tulemüüri konfiguratsioon

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

Mac OS X-ga kaasnevate turbemehhanismide hulka kuulub isiklik tulemüür. Isiklik tulemüür pakub mitmesuguseid turbefunktsioone, nagu näiteks paketifiltri funktsioon kohaliku süsteemi sisenevate ja väljuvate ühenduste võrgusuhtluse tõkestamiseks. Enne Mac OS X-s isikliku tulemüüri kasutamist tuleb kontrollida kahte fakti. Isikliku tulemüüriga saab sisenevaid ja väljuva /Path/to id ühendusi filtreerida või programmide ja teenuste ligipääsu internetile piirata. Enne üksikute programmide võrgusuhtluse väljalülitamist tuleb kontrollida, kas võrgusuhtlust saab programmi sees välja lülitada. Peale selle tuleb kontrollida, ega vastaval programmil või teenusel ei teki pärast võrgusuhtluse tõkestamist soovimatuid kõrvalnähte. Kui isikliku tulemüüriga püütakse programmi võrgusuhtlust otse tõkestada, võivad tekkida probleemid, sest programm võib tööks vajada võrgusuhtlust ning ootab enne jätkamist vastust võrgust. Otse kaitstavas klientarvutis töötavat isiklikku tulemüüri ei saa mingil juhul asendada iseseisva turvalüüsiga (tulemüüriga), mis kaitseb kogu institutsiooni sisevõrku. Isiklikku tulemüüri on mõttekas kasutada ka suurema turbevajadusega Mac OS X arvutite kaitsmiseks kohtvõrgu rünnete eest. Isiklikku tulemüüri on alati soovitatav kasutada Mac OS X arvutite mobiilse kasutuse korral, et kaitsta arvutit internetist tulevate rünnete eest.

Enne isikliku tulemüüri kasutamist tuleb kindlaks teha, millistel programmidel peab säilima ligipääs võrgule ja millistel mitte. Üldiselt tuleb kõigepealt tõkestada igasugune võrgusuhtlus ning seejärel lülitada tööle ainult soovitud pordid või rakendused. Isikliku tulemüüri seadistamisel tuleb järgida meetmes M 4.238 Lokaalse paketifiltri rakendamine esitatud soovitusi. Mac OS X pakub kahte tulemüüri, mis toimivad alltoodud erinevatel tasanditel.

Rakenduskihi tulemüür

Rakenduskihi tulemüür võimaldab tõkestada ja lubada konkreetsete rakendusprogrammide suhtlust. Selle puhul ei pea kasutaja teadma, millist porti kasutatakse. Rakenduskihi tulemüür kontrollib ka programmi allkirja. Võrgusuhtluseks lubatud programmi ei ole võimalik programmeerida tulemüüri reeglite definitsiooni uut päringut tegemata. Mac OS X-s on rakenduskihi tulemüür tarneseisundis välja lülitatud. See tuleb süsteemiseadistustes „ Süsteemiseadistused I Turvalisus I Tulemüür” sisse lülitada . Menüüpunktis „Täpsemad valikud” on võimalik seadistust kohandada. Valikuga „Keela kõik sisenevad ühendused” lubatakse ainult järgmised Mac OS X andmeside- ja suhtlusteenused:

- configd: DHCP ja teiste võrgukonfiguratsiooni teenuste jaoks;
- mDNSResponder: Bonjouri jaoks;
- racoon: IPSeci jaoks.

Kui valikut „Keela kõik sisenevad ühendused” ei kasutata , siis defineeritakse rakenduskihi tulemüüri nimekirjas, mis teenustel ja programmidel on õigus tulemüüris porte avada. Sellesse nimekirja saab programme lisada, klõpsates hiirega sümbolil „+”. Pärast programmi lisamist tuleb määrata, kas selle programmi sisenevad ühendused peavad olema lubatud või keelatud. Sellesse nimekirja võib lisada ka käsureaprogramme. Rakendustarkvara lisamisel nimekirja täiendab Mac OS X programmi digisignatuuri, kui seda pole varem tehtud. Kui hiljem muudetakse nimekirjas asuvat programmi, küsitakse kasutajalt uuesti, kas programmi sisenevad võrguühendused lubada või keelata. Ka digisignatuurita programmide

puhul, mida ei ole selles nimekirjas, kuvatakse kasutajale dialoogiaken valikutega ühendused lubada või keelata. Kui kasutaja lubab või keelab ühendused, varustab Mac OS X programmi digisignatuuriga ja lisab selle automaatselt koos antud õigustega rakenduskihi tulemüüri nimekirja.

Valiku „Luba signeeritud tarkvaral sisenevaid ühendusi automaatselt vastu võtta” aktiveerimisel võivad kõik digisignatuuriga varustatud programmid sisenevaid ühendusi vastu võtta, seda ka siis, kui programmi ei kuvata nimekirjas. Selle digisignatuuri peab olema väljastanud sertifitseerimisasutus (CA), mida Apple usaldab. Alates versioonist Leopard varustati kõik Apple'is kasutatavad operatsioonisüsteemi komponendid digisignatuuriga ja need võivad sisenevaid ühendusi vastu võtta. Sellesse rühma võivad kuuluda ka teised digisignatuuriga programmid, mida avavad automaatselt teised programmid. Kui on vaja digisignatuuriga programmi võrgule ligipääs tulemüüriga keelata, siis tuleb programm kõigepealt tulemüüri rakenduse nimekirja lisada ja seejärel ühendused selgelt keelata. Kui keelata tulemüüris ühe programmi ligipääs, võib see põhjustada programmi tõrkeid või teiste, sellel põhinevate programmide tõrkeid või mõjutada teiste kasutatavate programmide või teenuste töövõimet. Kuna see valik ei ole läbipaistev, tuleks selle kasutamisest loobuda. Valikut „Lülita maskeerimisrežiim sisse” ei tuleks kasutada, sest see on vastuolus internetistandardiga RFC 1122. Kui maskeerimisrežiim on sisse lülitatud, siis ei saadeta vastuseid päringutele, mis tulevad keelatud rakendusest. Näiteks on ping üks ICMP-teadetest, mis maskeerimisrežiimiga enam ei funktsioneeri. Pealegi ei paku maskeerimisrežiim kaitset: kui arvutit ei oleks tegelikult olemas, teataks viimane jaam enne arvutit saatjale, et sihtkoht ei ole kättesaadav, kuid maskeerimisrežiimis ei tule mingit teadet tagasi. Sellest võib saatja järeldada, et arvuti on olemas, kuid ei vasta.

Paketifilter ehk IP-tulemüür (ipfw)

Teine Mac OS-iga tarnitav isiklik tulemüür on IP-tulemüür (ipfw) ehk paketifilter. Paketifilter toimib OSI madalamas kihis ja sel on rakenduskihi tulemüüri ees eelis. IP-tulemüür (ipfw) sobib ainult internetiprotokolli versioonile 4. Kui on vaja kontrollida IPv6 andmevahetust, võib kasutada käsurearakendust IP6FW. Mõlema internetiprotokolli versiooni kasutamisel on tulemüüri konfiguratsiooni jaoks paratamatult rohkem faile vaja, kusjuures erinevus piirdub suuremas osas IPv4 ja IPv6 aadressivormingutega. IP-tulemüüri ja rakenduskihi tulemüüri saab kasutada paralleelselt ning koos võimaldavad nad võrgusuhtlust mitmeti reguleerida. Rakenduskihi tulemüüri saab sisse lülitada ja konfigureerida süsteemiseadistustes turvalisuse menüüsakis „Tulemüür”. IP-tulemüür (ipfw) võimaldab rakenduskihi tulemüüriga võrreldes reegleid täpsemalt defineerida. Selle käsitsemine on veidi keerulisem, sest konfigureerimisel kasutatakse käsurida. IP-tulemüüriga TCP-ühenduse keelamiseks eri serveritega pordi 80 kaudu võib kasutada järgmist käsku:

```
ipfw add 500 deny tcp from any to any dst-port 80
```

Igal tulemüüri reeglil on number ja süsteem töötab need läbi suurimast väikseimani. Seega saab reeglit teisega muuta või tühistada. Kuna IP-tulemüür toimib väga tähtsas osas, on käskude rakendamiseks vaja administraatoriõigusi. Tulemüüri laiaulatusliku reeglistiku loomisel tuleb konfiguratsioonifaili sisu ümber tõsta. Reeglite automaatseks laadimiseks sellest konfiguratsioonifailist on vaja shellscripti, mis võib välja näha selline:

```
#!/bin/sh
# eemalda senised tulemüüri reeglid
/sbin/ipfw -q flush
```

rakenda IPFW ja laadi reeglid failist
/sbin/ipfw -q /ABLAGEORT/Firewall-Regelwerk.conf
lülita sisse logimine faili /var/log/system.log
/usr/sbin/sysctl -w net.inet.ip.fw.verbose=1
Seejärel tuleb anda shellscript 'ile käskude täitmiseks vastavad õigused:
sudo chown root:admin Shellscript.sh
sudo chmod 544 Shellscript.sh

Pärast seda etappi tuleb shellscript käivitada iga kord, kui arvuti käivitatakse. Mac OS X puhul soovitab Apple selle ülesande täitmiseks kasutada süsteemiteenust launchd . Süsteemiteenus launchd vajab programmide käivitamiseks erivorminguga faili (Plist) kataloogis „/Library/ LaunchDaemons". Selle faili sisu näeb välja selline:

www.apple.com/DTDs/PropertyList-1.0.dtd ">
Label
com.apple.firewall
ProgramArguments
/usr/local/bin/Shellscript.sh
RunAtLoad

Viimase etapina peab see Plist-fail saama vastavad õigused, nt järgmise käsuga:
sudo chown root:admin NameDer.plist
Muudatused saab salvestada ja aktiveerida kohe, ilma eelneva taaskäivituseta, kasutades selleks järgmist käsku:
sudo launchctl load /Library/LaunchDaemons/NameDer.plist
Isikliku tulemüüri logifaili (asukoht /private/var/ log/ipfw.log) tuleb korrapäraselt kontrollida, et selles ei oleks midagi silmatorkavat, nt palju ebaõnnestunud kaugpöördusi või sisselogimiskatseid. Tulemüüri logifailid võivad väga kiiresti suureneda ja võtta enda alla märkimisväärselt palju mäluruumi. Seepärast on mõttekas kindlaks määrata, millistel reeglitel on kõrgem prioriteet ning mida on vaja logida ja mida mitte. Vastav käsk võib välja näha selline:
ipfw allow log tcp from any to any dst-port 6112-6119
Selle käsuga logitakse kõik ühenduskatsed TCP baasil serverisse portide 6112 kuni 6119 kaudu.
Täiendavad kontrollküsimused:

- Kas on kindlaks määratud, millistel Mac OS X programmidel on võrgule ligipääs?
- Kas Mac OS X isiklik tulemüür on sisse lülitatud ja vastavad käsud seadistatud?
- Kas Mac OS X isikliku tulemüüri logifaili uuritakse regulaarselt?

M 5.167 Mac OS X kaugpöörduste turvalisus

Algatamise eest vastutavad: infoturbespetsialist, IT-juht
Rakendamise eest vastutab: administraator

Alates versioonist Panther (10.3) sisaldab Mac OS X kaughoolduse võrguteenust Apple Remote Desktop. Serverikomponent põhineb protokollil Virtual Network Computing (VNC) ja suudab suhelda iga VNC-kliendiga, olenemata operatsioonisüsteemist ja tootjast. Kliendikomponent integreeriti operatsioonisüsteemi ekraaniloana aga alles alates Mac OS X versioonist Leopard (10.5). Kui süsteemiseadistustes on menüüpunktis „Kasutusload" ekraaniluba sisse lülitatud, siis saab igaüks, kel on pääsuõigused, Mac OS X IT-süsteemile ligi. Turvalisuse suurendamiseks tuleb sisse lülitada valik „VNC-kasutajad võivad ekraani juhtida järgmise parooliga" ja vältida liiga lihtsaid paroole (vt M 1.1 Vastavus normidele ja eeskirjadele). Lisaks võivad ekraaniloale pääseda ligi ainult valitud kasutajarühmad.

Alates Mac OS X versioonist Leopard (10.5) on toetatud kaugjuhtimisandmete krüpteeritud edastamine VNC kaudu ning see peab olema sisse lülitatud. Klientarvuti ekraaniloa seadistustes tuleb siis märkida valik „Krüpteeri kõik võrguandmed (turvalisem)" , et mitte krüpteerida üksnes paroole ja klaviatuurivajutusi, vaid kogu andmeedastust. Kui VNC-tarkvara ei toeta krüpteeritud andmeedastust või kui kasutatakse vanemat Mac OS X operatsioonisüsteemi, on soovitatav andmeedastuse turvalisuse huvides kasutada SSH-tunnelit või VPN-i.

Täiendavad kontrollküsimused:

- Kas Mac OS X ekraaniloa jaoks on alati parooli vaja?
- Kas juurdepääs Mac OS X ekraaniloale anti ainult teatud kasutajarühmadele?

M 5.168 Taustsüsteemide turvaline sidumine veebirakenduste ja veebiteenustega

Algatamise eest vastutavad: IT-juht, üksikute IT-rakenduste eest vastutavad töötajad

Rakendamise eest vastutab: administraator

Veebirakendused ja veebiteenused kasutavad sageli taustsüsteeme, näiteks andmetalletuseks andmebaasis või autentimiseks identiteedi mälu kaudu. Andmeid tuleb piisavalt kaitsta ka edastamisel ja salvestamisel taustsüsteemidesse. Selleks peavad taustsüsteemid olema kindlalt ühendatud veebirakenduse või veebiteenusega.

Tüüpilised veebirakenduste ja veebiteenuste taustsüsteemid on järgmised:

- andmebaasid,
- kataloogiteenused,
- vahevara,
- veebiteenused ja
- Legacy-süsteemid.

Taustsüsteemide kindlaks ühendamiseks tuleks järgida alljärgnevaid punkte.

Taustsüsteemide asukoht ja juurdepääs taustsüsteemidele

Veebirakenduse kasutajad või veebiteenuste käivitajad ei peaks otse taustsüsteemidele ligi pääsema, sest sel moel välditakse kaitsemeetmeid. Selle asemel peaks juurdepääs olema võimalik ainult eeldefineeritud liideste ja veebirakenduse või veeniteenuse funktsioonide kaudu.

Seetõttu peaks ühendus taustsüsteemidega olema suure kaitsevajaduse korral täiendavalt kaitstud. Selleks peaksid süsteemid end enne andmete edastamist autentima ja edastatavad andmed krüpteerima, nii et neid ei saaks märkamatult lugeda või muuta (nt SSL/TLS; vt ka M 5.66 SSL-i/TLS-i kasutamine kliendis ja M 5.177 SSL-i/TLS-i kasutamine serveris).

Kui osalevad IT-süsteemid ühendatakse ebaturvaliste kanalite kaudu, tuleks igal juhul kasutada krüptograafiliselt kaitstud tunnelit koos vastava krüpteeringu ja autentimisega.

Juurdepääsud taustsüsteemidele peaksid toimuma minimaalsete õigustega. Selleks peaksid olema kõikidel taustsüsteemidel seadistatud teenusekontod.

Kui juurdepääsuks taustsüsteemile kasutatakse ühtainsat teenusekontot, töödeldakse kõiki selle teenusekonto päringuid turbekontekstis. See kehtib nii selliste kasutajate juurdepääsudele, kellel on piiratud juurdepääsuvolitused, kui ka administratiivsete õigustega kasutajate juurdepääsudele. Selle vältimiseks tuleks kasutada mitmeid teenusekontosid erinevate juurdepääsuõigustega taustsüsteemide jaoks.

Nõuetekohase süsteemikeskkonna korral (nt kataloogiteenuse kasutamisel, mida kasutab veebirakendus ja mida kasutatakse ka taustsüsteemi jaoks kasutajate haldamiseks) võib kasutajakontod edasi suunata taustsüsteemile. Sel moel võidakse limiteerida veebirakendusse sisseloginud mis tahes kasutaja privileege vajalikele õigustele.

Tähelepanu tuleb pöörata sellele, et autentimata juurdepääsude jaoks veebirakendusele kasutatakse oma teenustekontot kataloogiteenuses piiratud volitustega.

Enterprise Service Bus

Nn teenusele suunatud arhitektuuride (SOA) kontekstis seotakse veebirakendused ja veebiteenused sageli Enterprise Service Bus'i (ESB) kui tsentraalse sidetaristu kaudu taustsüsteemidega. Seeläbi saavutatakse, et iga rakenduse jaoks peab ESB-le alati määratlema ja realiseerima ainult liidese ja mitte palju erinevaid liideseid muudele rakendustele ja teenustele. ESB salvestab oma kataloogis (Repository) metaandmeid ühendatud teenuste kohta.

Lisaks võib ESB realiseerida ka keskseid turbefunktsioone, et kaitsta täiendavalt ühendatud rakendusi. Sellised turbefunktsioonid võivad tuvastada näiteks Replay-ründeid ja neid tõrjuda või kontrollida XML-andmeid võimalike kahjulike sisude suhtes ning logida keskselt ja revisjonikindlalt ka sõnumivahetust.

ESB rakendamisel tuleb kindlaks teha, et kõik teenused end ESB suhtes autendiksid, enne kui neile võimaldatakse juurdepääs. See kehtib ka juurdepääsul ESB-Repository'le. ESB peab olema võrguarhitektuuri integreeritud nii, et juurdepääs on võimalik ainult ühendatud rakenduste ja teenuste serveritest ja välistatud on juurdepääs ESB-le väljastpoolt. Selleks peaks ESB saama oma loogilise võrgusegmendi.

ESB peab läbi viima oma isikliku volituste kontrollimise, et kontrollida kas juurdepääs päritud teenusele päringu teinud teenuse või rakenduse kaudu on lubatud. Seejuures tuleb kindlalt välistada, et väliskontaktiga rakendused või teenused pääseksid ligi sisemistele teenustele, mis ei ole selleks ette nähtud.

Sellised rakendused ei tohi ka ESB-Repository kaudu saada teavet sisemistest teenustes ja nende liidestes.

Kui teenusele suunatud arhitektuur hõlmab paljusid turvadomeene, näiteks DMZ-i, millel on väliselt käivitatavad teenused, ja Backend-süsteemidega sisevõrku, tuleb ka ESB jagada vastavatesse kontrollitud üleminekutega turvadomeenidesse või tuleb üksikute turvatsoonide jaoks realiseerida rohkem ESB-sid.

Kui ESB ei suhtle lokaalselt ainult kaitstud RZ-võrgus, tuleb suhtlust ESB ja ühendatud rakenduse vahel kaitsta nõuetekohaselt (autentimine ja krüpteerimine).

Paljude rakenduste ja teenuste suhtluse koondamisega muutub ESB kättesaadavus eriti oluliseks. Seda tuleb ESB realiseerimisel ja käitamisel vastavalt liiasustele ja teenuse nõuetekohasele järelevalvele arvesse võtta.

Kontrollküsimused

- Kas veebirakendused ja veebiteenused pääsevad taustsüsteemidele ligi ainult defineeritud liideste kaudu ja defineeritud süsteemidest?
- Kas andmeliiklus kasutajate ja veebirakenduse või rakenduste, veebiteenuste ja muude teenuste ning taustsüsteemide vahel on reguleeritud turvalüüsidega (tulemüürid)?
- Kas ühendusi veebirakenduste või veebiteenuste ja taustsüsteemide vahel kaitstakse suure kaitsevajaduse korral edastuskrüpteeringuga?
- Kas on tagatud, et veebirakenduse või veebiteenuse päringuid taustsüsteemidele teostatakse ainult minimaalsete õigustega nendele?
- Kas ESB rakendamisel on ESB-le ette nähtud oma loogiline võrgusegment? Kas juurdepääs ESB-le on võimalik ainult ühendatud rakenduste ja teenuste kaudu?
- Kas on jäädud kindlaks segmenteerimisele tsoonide järgi vastavalt ESB-s olemasolevatele domeenidele, minnes vajaduse korral kuni ESB eraldamiseni?
- Kas kõik juurdepääsud ESB-le autenditakse ja kas need on suhtlemisel asukohast ja võrgupiiridest väljapoole piisavat turvatud/krüpteeritud?
- Kas ESB realiseerimisel ja rakendamisel on rakendatud nõuetekohaseid meetmeid asjakohase kättesaadavuse tagamiseks?

M 5.169 Veebirakenduse süsteemiarhitektuur

Algatamise eest vastutavad: üksikute rakenduste eest vastutavad isikud

Rakendamise eest vastutab: administraator

Veebirakendused kasutavad üldiselt mitut IT-süsteemi komponenti, nt veebiserverit, veebi rakendusserverit ja taustsüsteeme. Veebirakenduse turvaliseks käitamiseks on tarvis sobivat süsteemiarhitektuuri. Veebirakenduse süsteemiarhitektuuri ja sellesse kaasatud IT-süsteemide võrgustiku kavandamisel tuleb silmas pidada järgmisi punkte.

Eraldamine serveri rollide põhjal

Veebirakenduse serveriteenuseid (nt veebiserverit, rakendusserverit, andmebaasiserverit) tuleb käitada vastavates eraldi IT-süsteemides. Kui selle käsitluse kohaselt kasutatakse ära süsteemis (nt veebiserveris) eksponeeritud komponendi turvaauku, siis ei mõjuta see teistele süsteemikomponentidele (nt andmebaasi) salvestatud andmeid. Serveri rollide eraldamist võib rakendada ka serveri virtualiseerimise abil. Kui serveri virtualiseerimist kasutatakse ära, siis tuleb rakendamisel järgida moodulit B 3.304 Virtualiseerimine .

Süsteemikomponentide serveri protsesside piiratud kontod

Süsteemikomponentide erinevate serveri protsesside jaoks tuleb kasutada eraldi kontosid (nt eraldi süsteemikasutaja veebiserveri protsessi jaoks). Seejuures tuleb nende teenusekontode õigusi operatsioonisüsteemi tasandil nii palju piirata, et säilib ligipääs üksnes operatsioonisüsteemi vajalikele ressurssidele ja failidele. Sel moel saab ründaja ka serveri protsessi õnnestunud kompromiteerimise korral ainult piiratud õigused, nii et operatsioonisüsteemi tasandil on ligipääs raskendatud.

Mitmekihiline võrguarhitektuur

Veebirakenduse IT-süsteemi komponendid peavad turvalüüsi demilitariseeritud tsoonides (DMZ) olema turbevajaduse põhjal eraldatud (vt M 1.1 Vastavus normidele ja eeskirjadele). Võrguarhitektuur peab olema mitmekihiline (Multi-Tier). Seejuures tuleb arvestada vähemalt järgmiste turbetsoonidega:

- Veebikiht - See kiht piirneb mitteusaldusväärse võrguga (nt internet) ja kujutab endast kasutaja otsese ligipääsuga eksponeeritud kihti. Piirnevate võrkude (nt rakenduskihi ja interneti) vahel paiknevad paketifiltrid peavad andmevahetust filtreerima, nii et üle veebikihi võrgupiiride ei ole mitteusaldusväärsest võrgust otsene ligipääs võimalik. Selles kihis peavad asuma niisugused süsteemid nagu veebiserver, mis võtavad endale eksponeeritud koha ja nõuavad näiteks kasutaja otsest ligipääsu.
- Rakenduskiht - Rakenduskiht peab piirnema ühest küljest veebikihiga ja teisest küljest andmekihiga. Võrguliiklus piirnevate võrkude vahel peab olema paketifiltriga filtreeritud, nii et piirnevate võrkude puhul ei oleks otsene ligipääs võimalik. Selles võrgusegmendis peavad asuma süsteemid ja server rakendusloogikaga (nt veebirakendusega rakendusserver). Süsteemid pääsevad ligi piirneva andmekihi andmetele (nt andmebaasidele), töötavad need läbi ja annavad need veebikihis olevate süsteemide (nt veebiserveri) käsutusse.
- Andmekiht - Andmekiht on mitmekihilise arhitektuuri usaldusväärseim tsoon. Piirnevate võrkude vahel asuv paketifilter reguleerib andmevahetust. Selles kihis peaksid asuma veebirakenduste taustsüsteemid, nt andmebaasid, kataloogiteenus ja pärandsüsteemid. Neisse süsteemidesse pää-

seb üksnes piirnevatest võrkudest (nt rakenduskihist). Andmekihti tuleb rakendada eraldi tsoonina ja seda ei tohi teistesse tsoonidesse (nt intranetti) integreerida.

Tuleb tagada, et eelmainitud tsoonidest ei pääsetaks intraneti süsteemidesse. Kui näiteks veebirakenduse autentimisel kasutatakse kataloogiteenust, tuleb võimaluse korral kasutada eraldi domeeni eraldatud riistvaral. Andmevahetuse filtreerimine peab toimuma eraldatud filtrikomponentide (nt paketifiltri) kaudu. Suure turbevajaduse korral tuleb filtrikomponendid asendada kõrgema protokollitasandi filtrifunktsioonidega (nt Application Level Gateway) või neid nendega täiendada. Application Level Gateway tuleb seejuures integreerida oma turbetsooni, mis võtab kasutaja päringud vastu enne veebikihi süsteeme.

Veebirakenduse tulemüüride kasutamine

Kõrgema protokollitasandi filtreerimiseks võib kasutada veebirakenduse tulemüüre (Web Application Firewalls – WAF). Kuna WAF analüüsib HTTP-protokolli ja selle kaudu edastatavaid andmeid, filtreeritakse rakendustasandi ründemustrid juba WAF-is. Sel moel tuvastatakse ründekatsed varakult ja neid ei saadeta enam veebirakendusele edasi. WAF-is toimuvaks filtreerimiseks on üldjoontes kaks võimalust:

- Veebirakendusele saadetud andmetest otsitakse tuttavaid ründemustreid. Ründemustrid pärinevad WAF-i tootjalt ja hõlmavad nii tüüpilisi märgiridasid, mida kasutatakse üldistes rünnetes veebirakenduste vastu (nt SQL-injektsioonis), kui ka spetsiifilisi ründemustreid, mis puudutavad standardseid tarkvaratooteid. Et tuntud ründeid usaldusväärselt tuvastada, tuleb ründesignatuure (nagu ka viirusetõrjetarkvara) regulaarselt värskendada.
- Kui standardtarkvara ei kasutata või on vaja lisakaitset, võib WAF-i jaoks koostada ka oma filtreerimisreeglid. Seejuures defineeritakse näiteks see, millised sisestatavad andmed on veebirakenduse jaoks lubatud. See meetod nõuab suuremaid konfiguratsioonikulusid ja täpset ülevaadet veebirakenduse töödeldavatest andmetest.

Täiendavad kontrollküsimused:

- Kas veebirakenduste puhul on serveriteenuste eraldamine vastavatesse eraldi IT-süsteemidesse ette nähtud (eraldamine serveri rollide põhjal)? {E: C/ I/A}
- Kas veebirakenduste süsteemikomponentide serveri protsesside jaoks kasutatakse piiratud kontosid?
- Kas veebirakenduse jaoks kasutatakse mitmekihilist võrguarhitektuuri (Multi-Tier)?
- Kas veebirakenduse tulemüüride kasutamisel on WAF-i konfiguratsioon kaitstava veebirakenduse jaoks kohandatud?
- Kas veebirakenduse tulemüüride kasutamisel värskendatakse WAF-i ründesignatuure regulaarselt?

M 5.170 OpenLDAP-d kasutavate sideühenduste turve

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

Side slapd-serveri ja tema sidepartneri vahel peab olema krüpteeritud, et vahetatav teave ei satuks volitamata isikute kätte või nad ei saaks seda muuta. Seejuures võivad sidepartnerid olla kliendid ja teised serverid, nt partitsioonide või replikatsioonide loomise raames.

StartTLS ja ldaps://

OpenLDAP turvalisuse tagamiseks TLS-i/SSL-i abil tuleb eelisjärjekorras kasutusele võtta StartTLS ja ldaps:// (vt M 1.1 Vastavus normidele ja eeskirjadele).

- StartTLS on dokumendis RFC 2830 defineeritud LDAP extended operation , mida LDAPv3 kasutab edastusturvalisuse tagamise standardmehhanismina. TLS-iga turvatud edastus põhineb juba olemasoleval LDAP-ühendusel, kogu suhtlus toimub pordi 389 kaudu.
- Seevastu ldaps:// puhul luuakse juba ühendus krüpteeritult. Selleks peab slapd-server ootama lisapordi ühendumist, tavaliselt kasutatakse porti 636.

Kuigi OpenLDAP toetab mõlemat ühendusvarianti, on soovitatav kasutada StartTLS-i. StartTLS-i eelised on standardühilduvus ja keskse võrgukomponendi täiendava avatud pordi/teenuse vältimine. Kuid on võimalik, et sidepartner ei toeta StartTLS-i. Veel on teada juhtumeid, kus LDAP-kliendid on LDAP-ühenduse kaudu autentimiseks vahetanud konfidentsiaalset teavet enne, kui StartTLS-i töötlus on lõpetatud. Teabeedastus toimus osaliselt ilma kaitseta. Sellistel juhtudel on mõistlik võtta kasutusele ldaps://. SSLv2-t ei tohiks kasutada ei StartTLS-i ega ldaps:// korral.

Sertifikaatidega konfiguratsioon

Krüpteeritud suhtluse jaoks läheb tarvis serveri sertifikaati, mis sisaldab sertifikaadi eraldusnimena (Distinguished Name – DN) serveri täielikku arvutinime. Kui suhtlus peab hõlmama ka kasutaja sertifikaadil põhinevat identiteedi tuvastamist, on kasutajal vaja ka X.509 sertifikaati. Kui DN-sissekanded kasutaja sertifikaadis ja tema kataloogi sissekandes ei lange kokku, tuleb kasutada vastendamist (mapping). Krüpteeritud ühendused tuleb konfigureerida nii serveris kui ka klientarvutis. slapd-serveri seadistused tuleb teha konfiguratsioonifaili slapd.conf globaaldirektiivides, OpenLDAP ldap*-tööriistade puhul kohalikus ldap.conf'is. ldap.conf'i seadistused võib kasutajaspetsiifilise konfiguratsioonifailiga .ldaprc üle kirjutada, seejuures tuleb kasutaja sertifikaadid sinna igal juhul sisse kanda. Teiste tööriistade ja klientide puhul tuleb uurida vastavaid dokumentatsioone. Muu hulgas tuleb seada järgmised parameetrid:

TLSCACertificateFile (server) või TLS_CACERT (klient või kasutaja)

Sissekanne viitab failile, mis sisaldab avalikku võtit või usaldusväärse sertifitseerimisasutuse juursertifikaati. Nimetada võib mitu faili.

TLSCACertificatePath (server) või TLS_CACERTDIR (klient või kasutaja)

Eelmainitud parameetritega failide asemel võib kirjeldada üht või mitut asukohta, kus failid asuvad.

TLSCertificateFile (server) või TLS_CERT (kasutaja, mitte klient)

Parameeter tähistab faili, mis sisaldab eraldi sertifikaati või avalikku võtit.

TLSCertificateKeyFile (server) või TLS_KEY (kasutaja, mitte klient)

See parameeter viitab salajasele võtmele, mida tuleb igal juhul kaitsta. Faili pääsuõigused tuleb seada ettevaatlikult, et failile pääseks ligi ainult vastav kasutaja (või kasutaja, kelle õigustega slapd-serverit käitatakse).

TLSCipherSuite (ainult server)

Sissekanne loetleb usaldusväärsed krüpteerimismeetodid soovitud järjekorras ning sõltub kasutatava SSL-i/TLS-i teostusest. Mida vähem ja mida tugevamaid krüpteerimismeetodeid nimetatakse, seda parem, sest nii peaks saama vältida SSLv2-t. Mingil juhul ei tohi siin olla sissekanne „NULL" (krüpteeringud puuduvad).

TLSRandFile (server) või TLS_RANDFILE (klient või kasutaja)

Sisestus tähistab juhuslike väärtuste allikat. Fail annab lähteväärtuse (seed), mille põhjal luuakse matemaatiliste funktsioonidega piisavalt juhuslikke arvväärtusi seansivõtmeteks. Enamiku Linuxi ja Unixi süsteemide puhul ei ole sisestust vaja, sest selle otstarvet täidab da /dev/urandom.

TLSVerifyClient (server) või TLS_REQCERT (klient või kasutaja)

See parameeter määrab, kui palju iga vastaspoole sertifikaate kontrollitakse. Võimalikud väärtused on järgmised.

- never: vastaspoole sertifikaati ei kontrollita kunagi (serverite eelseadistus, need ei identifitseeri kliente). Seda väärtust ei tohi valida, kui kasutatakse SASL-i ning TLS-i/SSL-i autentimisel kasutatakse omakorda SASL-i. Sel juhul tuleb kliendi või kasutaja sertifikaati kontrollida, sest teda autenditakse selle kaudu.
- allow: esitatakse sertifikaadi päring, aga kui sertifikaati ei esitata või kontrollimine ebaõnnestub, pole sel mõju.
- try: esitatakse sertifikaadi päring. Kui seda ei esitata, pole sel mingit mõju. Kui sertifikaat esitatakse ja selle kontrollimine ebaõnnestub, siis seanss katkestatakse.
- demand: sertifikaat tuleb esitada ja selle kontrollimine peab õnnestuma, sest muidu seanss katkestatakse (eelseadistus klientidel, need peavad serveri identiteedis veenduma).

Turvalise ühenduse loomine

StartTLS-i puhul toetavad kõik OpenLDAP ldap*-tööriistad lippe „-Z" ja „-ZZ". „Z" tähendab, et tuleb proovida luua krüpteeritud ühendus ja õnnestumise korral seda kasutada. Seevastu „ZZ" tähendab, et krüpteering peab olema õnnestunult toestatud, enne kui võib käsu täita. Teiste slapd-serveriga ühendust võtvate klientide puhul tuleb järgida asjakohast dokumentatsiooni.

ldaps:// käivitatakse tavaliselt vastava sihtaadressi kaudu ldaps://... ldap://... asemel, teine võimalus on üldine sissekanne kliendispetsiifilise konfiguratsioonifaili ldap.conf URI direktiivis.

Ülekatete kasutamisel tuleb arvestada, et need pakuvad osaliselt TLS-i/SSL-i jaoks oma alamdirektiive, kui tegemist on serveritevahelise andmevahetusega. See kehtib muu hulgas ülekatete „syncprov" ja „chain" korral.

Võrguliikluse piiramine

Suhtluse suurema turvalisuse tagamiseks pakub OpenLDAP funktsiooni „ selective listening " ja süsteemirakenduse TCP Wrapper ühendamist. „ Selective listening" piirab operatsioonide vastuvõtmist teatavatelt saatja IP-aadressidelt. TCP Wrappers kujutab endast TCP/IP-suhtluse reeglitel põhinevat seiret. Soovitatav on jätta „selective listening" ja TCP Wrapper ära. Suuremat tähelepanu tuleb pöörata sellele, et server oleks juba operatsioonisüsteemi tasandil adekvaatselt kaitstud

(vt M 4.238 Lokaalse paketifiltri rakendamine). Võrguliikluse lisaseire OpenLDAP abil toob kaasa tarbetu administratiivtöö ja kokkuvõttes ka selle, et OpenLDAP võtab üle funktsiooni, mille jaoks rakendus ei ole mõeldud.

Teistsugused pordid

Vahel soovitatakse kataloogiteenused konfigureerida nii, et need kasutavad muid porte kui 389-t ja 636-t. See peaks raskendama LDAP-versiooni tuntud turvaaukudele suunatud otseseid ründeid. Seda soovitust ei ole soovitatav järgida, sest mahuka ja seetõttu ka potentsiaalseid vigu tekitava administratiivkulu tulemusena saadakse turvalisuses minimaalne kasu. Võib ka juhtuda, et ebapiisavalt konfigureeritavate klientide puhul tekivad funktsioonipiirangud.

Täiendavad kontrollküsimused:

- Kas suhtlus slapd-serveri ja tema sidepartneri vahel on krüpteeritud?
- Ega SSLv2 ei kasutata ei StartTLS-i ega ldaps:// korral?

M 5.171 Turvaline andmeside keskse logiserveriga

Algatamise eest vastutavad: IT-juht, infoturbespetsialist

Rakendamise eest vastutavad: administraator

Keskse logimise korral edastatakse seiratavate IT-süsteemide ja rakenduste teave võrgu kaudu kesksesse logiserverisse, kus see kogutakse kokku, analüüsitakse ja salvestatakse. Kuna logiandmed võivad sisaldada ka isikutega seotud teavet, peavad need olema volitamata ligipääsu (vaatamise, muutmise, kustutamise) eest kindlasti kaitstud. Et vältida logiandmete nägemist või manipuleerimist nende edastamisel kesksesse logiserverisse, tuleb need andmed edastada krüpteeritult või eraldi haldusvõrgu (Out-of-Band) kaudu. Niiviisi suureneb ka logiteadete terviklus ja konfidentsiaalsus.

Tundliku teabe konfidentsiaalsus

Mõned andmeallikad genereerivad logiteateid, mis võimaldavad neid seostada konkreetse isikuga. Seepärast tuleb logiandmete konfidentsiaalsus tagada ka edastamise ajal, nt ühenduse turvamisega SSL-i abil (vt M 5.66 TLS-i/SSL-i kasutamine) või andmete krüpteerimisega. Andmete kaitsmisel edastamise ajal võib abi olla ka eraldi haldusvõrgust (Out-of-Band).

Logiandmete terviklus ja täielikkus

Kui logiteavet on vaja kasutada seoses IT-eelhoiatusega ja IT-kohtuekspertiisi valdkonnas, siis on tähtis, et turvaintsidentide tõendid ei läheks kaduma ja säiliks kogutud teabe tõendusjõud. Pealegi peab logiserveri ja logiandmeid edastava IT-süsteemi vahel toimuma autentimine. See raskendab Man-in-the-Middle -ründeid ja väldib andmete tahtmatut saatmist volitamata kohtadesse. Seepärast peavad olemas olema mehhanismid, mis kaitsevad edastatava ja salvestatava teabe terviklust ja autentsust. Logiandmed peavad olema õiged ja täielikud. See on vajalik nii tõendusjõu kui ka tehnilisest seisukohast. Kuna suuremates teabekooslustes tekib sageli palju logiandmeid, tuleb hoolitseda selle eest, et ribalaiusest piisaks logiinfo edastamiseks ja logiinfo ei läheks ribalaiuse ajutiste kitsaskohtade tõttu kaotsi. Samuti tuleb veenduda, et logiandmete edastamine ei takistaks tööandmete edastamist. Logiteateid võib edastada tegeliku andmevõrgu (In-Band) asemel eraldi haldusvõrgu (Out-of-Band) kaudu. Olenevalt turbevajadusest tuleb kaaluda, kas logi- ja tööandmete loogiline või füüsikaline eraldamine on mõistlik ja tehniliselt võimalik.

Turvalise suhtluse näited

Järgmised meetmed näitavad, kuidas saab logiandmete edastamise ajal tagada kättesaadavust, terviklust ja konfidentsiaalsust. Soovitusi võib kasutada nii üksikult kui ka kombineeritult.

Tarkvara agendid

Sellega installitakse tarkvara seiratavasse süsteemi. Tarkvara edastab kogutud logiandmed kesksele logiserverile krüpteeritult. Selle oluline eelis on see, et kõik need seiratavad süsteemid töötavad samasuguse logimisstandardiga ja seega saab osa standardiseerimisest teha detsentraalselt. See eeldab, et IT-süsteemi saab installida agenttarkvara, kuid see ei ole selliste võrguelementide nagu marsruutrite või turvalüüside puhul sageli võimalik.

Layer 2 eraldamine

Kommutaatori kasutamisel tuleb arvesse võtta, et VLAN-e (virtuaalkohtvõrke) ei töötatud välja selleks, et täita turvanõudeid võrkude eraldamisel. VLAN-idel on palju ründekohti, nii et eriti suurt kaitset vajavate võrkude eraldamisel tuleb alati

võtta lisameetmeid. Lisateavet VLAN-ide kohta leiate punktist M 2.277 Kommutaatori funktsionaalne kirjeldus .

Layer 3 eraldamine

Marsruutimisvõimelised komponendid otsustavad OSI-kihimudeli tasandil 3 logi alusel, mistõttu on need ideaalsed ühenduselemendid. Lisaks on marsruutritega võimalik tagada IP-võrguühenduse struktureeritud eraldamine. Puuduseks on see, et marsruuter jagab tavaliselt mälu protsesside, liideste halduse ja pääsunimekirjadega, mistõttu võib ressurssides tekkida kitsaskohti. Üksikasjalik marsruutimine, nt alamvõrgu eraldamine, süsteemi autonoomne marsruutimine jms võib osutuda ka haldamise seisukohast väga keeruliseks.

VPN-ühendus

See variant tagab konfidentsiaalsuse ja tervikluse suurema turbevajadusega komponentidele, mis on näiteks avaliku võrgu kaudu ühendatud. VPN-ide kasutamiseks peavad IT-süsteemidel olema üksteisega ühilduvad mehhanismid. Teine võimalus on lasta ka IT-süsteemidel ühenduda VPN-masinatega, mis loovad krüpteeritud ühenduse.

Ribaväline haldus (haldusvõrk)

Ribavälise halduse korral kasutatakse logiandmete edastamiseks eraldi LAN-i. Kuna see LAN on üksnes logimise ja võib-olla ka haldamise jaoks, siis on võrgu järjepideva eraldamise korral ründaja ligipääs raskendatud. Ribaväline haldus on tavaliselt teistest meetoditest kulukam, sest logivas IT-süsteemis on vaja täiendavat võrguliidest ja infokoosluses sõltumatut võrgu infrastruktuuri. Haldusvõrgu eelis on see, et saab kasutada logisid (eriti SNMP versiooni 1), mis on küll ebaturvalised, kuid mida tuleb alternatiivsete lahenduste puudumisel käituse jälgimiseks (nt IT-eelhoiatussüsteemide kaudu) kasutada.

Täiendavad kontrollküsimused:

- Kas logiandmed on volitamata ligipääsu eest kaitstud?
- Kas logiteabe jaoks on olemas turvatud edastusmoodus?
- Kas logiserveri ja IT-süsteemi vahel toimub autentimine?
- Kas teabe tervikluse ja autentsuse kaitsmiseks kasutatakse mehhanisme?

M 5.172 Turvaline aja sünkroniseerimine keskse logimise korral

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

Hilisema analüüsi võimaldamiseks tuleb logimisel esinevad sündmused seostada hetke kellaajaga. Tuleb hoolitseda selle eest, et kõik IT-süsteemid kasutaksid sama ajabaasi. Selleks et suuremas infokoosluses oleks kõikide süsteemide aeg sünkroonis, kasutatakse tavaliselt keskset võrguaja serverit. See annab keskse ajatakti näiteks võrguaja protokolli (Network Time Protocol – NTP) kaudu (vt M 4.227 Lokaalse NTP -serveri kasutamine aja sünkroniseerimiseks). Kõik ülejäänud süsteemid infokoosluses sünkroniseerivad end selle välise ajatakti abil.

Aja sünkroniseerimise tõrked

Aja sünkroniseerimise tõrge võib tekitada probleeme keskses logimises. Näiteks ei saa enam viga selgelt konkreetse hetkega seostada. Võib juhtuda, et vigase ajabaasi tõttu muutub ka teadete järjestus, nii et analüüsimisel kuvatakse logiandmete vale järjekord. Probleeme tekitab ka see, kui infokoosluses võetakse lepinguliste kokkulepete (Service Level Agreements – SLA-d) järgimise kontrollimisel aluseks aeg. IT-süsteemide või keskse logisüsteemi vigane aja sünkroniseerimine või selle puudumine võib kaasa tuua selle, et logimist ei saa enam pidada kindlaks tõendusmaterjaliks. Seepärast peab tagama, et kõik logifailid oleksid varustatud aktuaalse kuupäeva ja kellaajaga. Siinjuures tuleb silmas pidada ka kuupäeva ja aja seadistuse ühtset kuvamist logifailis. Kui logiandmeid analüüsitakse automaatselt, peab kõikidel logiandmetel olema ühtne kuupäeva ja kellaaja vorming, et analüüsimisel ei tekiks arusaamatusi.

Selleks et suurema turbevajadusega infokoosluses keskse logimise korral oleks alati tagatud kõikide osalevate IT-süsteemide korrektne kellaaeg, võib kasutada mitmeastmelist ajatakti kontseptsiooni. Sel juhul määratakse süsteemiaeg peale NTP-teenuse ka DCF-raadiomooduli kaudu.

Täiendavad kontrollküsimused

- Kas kõikide infokoosluse IT-süsteemide süsteemiaeg on sünkroniseeritud, et oleks võimalik tuvastada IT-süsteemide ja rakenduste vastu suunatud ründeid ning nende IT-süsteemide ja rakenduste vigu?
- Kas hoolitsetakse selle eest, et logifailide kuupäeva ja kellaaja vorming oleks ühtne?

M 5.173z Lühi-URL-ide või QR-koodide kasutamine

Algatamise eest vastutavad: infoturbeametnik, asutuse/ettevõtte juhtkond

Rakendamise eest vastutab: vastutav spetsialist, IT-juht

Veebilehti juhitakse tavaliselt URL-i kaudu (Uniform Resource Locator), mida seetõttu nimetatakse ka veebiaadressiks. Paljude veebilehtede keerukus toob sageli kaasa suhteliselt pikad veebiaadressid, mida on raske meelde jätta, ja eriti kaasaskantavate lõppseadmete nagu mobiiltelefonide korral ei ole neid võimalik esitada ühes reas. Seetõttu on arendatud välja erinevaid meetodeid, et teha kasutajatele veebiaadresside kasutamine lihtsamaks. Kuulsamad esindajad on lühi-URL-id ja QR-koodid.

Lühi-URL-id

Lühi-URL-id tähistavad ülemaailmset teenust internetis, mille korral asendatakse pikad URL-id lühemate URL-idega. Lühi-URL-id on võrreldavad Link-tekstiga HTML-is, mille võib samuti meelepäraselt lühikese valida. Teisiti kui nende linkide puhul internetilehtedel on lühikeste ja pikkade URL-ide jaotus salvestatud andmebaasi ja ei ole seetõttu nii lihtsalt tuvastatav.

Lühi-URL-ide laia leviku põhjused on muu hulgas järgmised:

- tänu lühi-URL-idele saab e-kirjades vältida URL-ide reapoolitusi. Kui URLis on reapoolitus, tähendab see lingi avaja jaoks tavaliselt suuremat vaeva. Lühi-URL-id on tavaliselt nii lühikesed, et neid ei ole vaja poolitada;
- selleks, et sisestada linke mikro-blogi-kirjetesse nagu näiteks Twitteri säutsud, ei saa kasutada pikki URL-e. Mikroblogidel on tugev märgipiirang, mille reegel on 140 märki kirje kohta, sest mikroblogisid jälgivad kasutajad tavaliselt mobiiltelefonides, mitte arvutites. Seetõttu on lühi-URL-id kui linkide tavapärane vorm mikro-blogi-kirjetes läbi löönud;
- lühi-URL-id lihtsustavad ajakirjaartiklite viidete jälgimist. Paljud artiklid paberajakirjades viitavad allikatele internetist või sisaldavad juhiseid internetilehekülgedele.

Teisiti kui veebiartiklites tuleb need trükkida käsitsi. Lühi-URL-id vähendavad seda vaeva oluliselt.

Kõikide nende eeliste kõrval võivad aga lühi-URL-id kaasa tuua ka ohte (vt G 5.177 Lühi-URL-ide või QR-koodide kuritarvitamine). Asutuse töötajaid tuleks nendest probleemidest teavitada. Kõik töötajad peavad teadma, et lühi-URL-e tuleb kasutada ettevaatusega.

Selleks, et mitte sattuda muudele kui soovitud veebilehtedele, saab kasutada lühi-URL-teenuseosutajate eelvaateteenuseid. Seal kuvatakse ühelt poolt lingi taha peidetud aadress ja teiselt poolt lehekülje pilt. See funktsioon on saadaval

laiendusena ka tavalistele internetikasutajatele. Lühi-URL-ide eelvaatefunktsiooni tuleks võimaluse korral alati kasutada. Lühi-URL-ide pakkujaid, kellel ei ole eelvaatefunktsiooni, ei tohiks kasutada. Siiski saab korduvate lühi-URL-ide eelvaatefunktsiooni vältida. Lühi-URL on korduv, kui see viitab ise teisele lühi-URL-ile (ehtsa lehekülje asemel). Seetõttu tuleks kasutada ainult selliseid lühi-URL-ide pakkujaid, kes korduvad lühi-URL-id keelavad. Raskem on tõrjuda korduvaid lühi-URL-e mitmete pakkujate kaudu. Kuna korduvad lühi-URL-id on praktilises mõttes kasulikud ainult ründe toimepanijatele, ei tohiks kasutajad korduvaid lühi-URL-e üldiselt klikkida.

Risk sattuda lühi-URL-ide kaudu soovimatutele või ohtlikele lehekülgedele, on nüüd vähenenud, kuid seda ei saa välistada. Selleks, et vältida kahjulikke tagajärgi, tuleb veebilehitsejale ja operatsioonisüsteemile paigaldada tingimata ajakohased turvavärskendused ning samuti peab olema aktiveeritud viiruseskanner.

Lisaks nendele meetmetele võib asutus otsustada, et lühi-URL-id kujutavad endast liiga suurt riski ja seetõttu nende kasutamise keelata. Sellisel juhul on juurdepääs lühi-URL-ide teenuseosutajatele lukustatud, nt vastavate filtreerimisreeglitega.

QR-Code'i kasutamine

Selleks, et päästa kasutajad lühi-URL-ide, WLAN-juurdepääsuandmete, telefoninumbrite ja muude andmete trükkimisest, kasutatakse aina enam QR-koode (Quick Response Codes). Siin kodeeritakse andmed kujutisel, enamasti ruudukujulise pikslimustrina nii, et neid võib usaldusväärselt IT-süsteemidest lugeda. Selleks tuleb lõppseadmete nagu nutitelefonidega, millel on vastav varustus, QRCode'i pildistada või sisse skaneerida, et oleks võimalik lugeda sinna kodeeritud andmeid.

QR-Code'i standard on avalik ja QR-Code'e võib kasutada litsentsivabalt ja tasuta, sest need on nüüdseks juba üsna levinud. Klassikalised QR-Code'id võivad sisaldada kuni 2,953 baiti andmeid. QR-Code'idel on kõrge veatolerants. Olenevalt veakorrektuuri tasemest on võimalik taastada 7–30% QR-Code'ide kahjustatud andmetest. Levinud QR-Code'ide kõrval on edasiarendusi, milles andmed salvestatakse (osaliselt) krüpteeritult, millel on suhteliselt väikesed mõõtmed või milles on tuvastatavad pildid, tekstid või logod.

QR-Code'ides salvestatud andmeid ei saa kasutajad lihtsalt niisama lugeda. Sellest tulenevad, nii nagu ka lühi-URL-ide puhul mõned ohud (vt G 5.177

Lühi-URL-ide või QR-koodide kuritarvitamine). Kasutaja võiks näiteks oma lõppseadmel sisse lugeda QR-Code'i, mis viitab sellesse kodeeritud URL-i kaudu kahjurvaraga nakatunud veebilehele. Seetõttu tuleb tähelepanu pöörata sellele, et lõppseadmel ei teostataks pärast QR-Code'i sisselugemist automaatselt järgmisi tegevusi. URL-i korral tuleks seega kuvada kõigepealt selle taha peidetud aadressi, enne kui vastavat veebilehekülge avada. Üldiselt ei tohiks pärast sisselugemist ka ühelegi telefoninumbrile automaatselt helistada või SMS-i saata. Kasutajad peaksid väljuvad kõned enne valimist kinnitama.

Turbehaldus peaks seetõttu selgitama töötajatele QR-Code'ide kasutamist. Lisaks tuleks lõppseadmetel kasutada ainult QR-rakendusi, mille korral ei teostata pärast QR-Code'ide sisselugemist automaatselt tegevusi, vaid kasutaja peab need eelnevalt kinnitama.

Kui andmed avaldatakse ainult väiksema kasutajate ringi jaoks, tuleb kaaluda seal salvestatud andmete krüpteerimist. Selleks võib kasutada näiteks Secure-QR-Code'e (SQRC). Selle jaoks peavad kasutatavad lugemisseadmed või IT-süsteemid oskama loomulikult neid ka dekodeerida.

Kontrollküsimused:

- Kas töötajaid on teavitatud lühi-URL-ide probleemidest?
- Kas lühi-URL-ide ja QR-koodide sisusid kuvatakse enne nende avamist?

M 5.175z XML-lüüsi kasutamine

Algatamise eest vastutavad: IT-juht, üksikute IT-rakenduste eest vastutavad töötajad

Rakendamise eest vastutab: administraator, IT-juht

Klassikalise turvalüüsi kaudu saab tagada, et suletud keskkondades pääsevad veebiteenusele ligi ainult need lõppseadmed, millel on volitatud IP-aadressid (Whitelisting) või et internetis saadaolevate veebiteenuste IP-aadressid, millest väljuvad ründed, näiteks robotvõrkudest, lukustatakse (Blacklisting). Üksikasju vt M 4.454 Veebiteenuste kaitsmine keelatud kasutuse eest . Sellised turvalüüsid ei ole siiski tavaliselt võimelised analüüsima SOAP-sõnumeid ja tuvastama ründeid rakenduskihile (SOAP/HTTP). Seetõttu tuleks eriti suurenenud kaitsevajaduse korral veebiteenuste kaitsmiseks kaaluda XML-lüüside kasutamist, mis teostab selle filtreerimise XML-tasemel.

XML-lüüs on taristukomponent, mis lülitatakse veebiteenuse ja tarbija vahele ja see toimib seal kui turvalüüs veebiteenuse taristu sõnumite jaoks. See pakub veebiteenustele sama, mis Web Application Firewall (WAF) veebirakendustele.

Mõlemad kujutavad endast Application Level Gateways'i (ALG) teostusi erinevate rakendusprotokollide jaoks. XML-lüüs püüab XML-sõnumid kinni, et neid määratud nõuete kohaselt analüüsida, enne kui see need veebiteenusele edasi suunab. Selleks kasutatakse tavaliselt võimast ja tugevdatud parserit, mis kasutab defineeritud turbesuunist ja omab osaliselt ka heuristikat, mis võimaldab tüüpiliste suhtluste õppimist. Nii saab näiteks tuvastada hüppeliselt kasvanud sõnumisuurusi ja käivitada määratletud tegevusi ja alarme.

XML-lüüs (tähistatud ka kui XML-Firewall, Web-Service-Firewall, Web-Service-Security-Gateway või XML-SOAP-Proxy) on komponent, mis on mõeldud teenuste kaitseks rünnete vastu üle XML-il põhinevate liideste, kontrollides XML-andmeid, mis asutusse saabuvad või sealt väljuvad. XML-lüüse võib realiseerida kui iseseisvaid süsteeme või ka kui Enterprise Service Bus'i (ESB) komponente.

Kasutada saab tavaliselt järgmisi funktsioone:

- autentimise ja volitamise käitamine lüüsil,
- juurdepääsukontrollid sertifikaatide, SAML-i, LDAP, RADIUS-i ja muude meetodite kaudu,
- andmeedastuskiiruse piiramine kui meede Denial-of-Service-tüüpi rünnete vastu,
- krüpteerimine ja dekrüpteerimine edastus- või sõnumitasandil,

- XML-allkirjade lisamine ja kontrollimine,
- andmevoogude kontrollimine,
- XML-sõnumite valideerimine skeemide ja poliitikate abil,
- kaitse XML-i smugeldatud rünnete eest nagu Cross-Site Scripting, SQLInjection või Command-Injection,
- kaitse teatud SOAP-/XML-spetsiifiliste rünnete eest nagu liiga suured sõnumid, liiga tugevalt krüpteeritud elemendid, rekursiivne analüüs, pahatahtlikult manipuleeritud skeemid või WSDL-failid ning ründed marsruutimisel,
- SOAP-Body ja SOAP-manuste skaneerimine kahjurvara suhtes,
- erinevate veebiteenuse turbestandardite nagu WS-Security, WSSecureConversation, WS-Trust või WS-Federation toetus,
- alarmide käivitamine, osaliselt tänu anomaaliate tuvastamisele suhtluses,
- ka osaline teenuste virtualiseerimine URL-Rewriting'i, XSLtransformatsioonide ja SOAP-I põhineva marsruutimise kaudu.

Erinevate tootjate mudelid erinevad üksteisest eelkõige andmete läbilaskevõime ja ühenduse latentsusaja, kättesaadavuse tagamise funktsioonide läbi liiasusega süsteemide, olemasolevate sertifitseerimiste (nt Common Criteria järgi), identiteedi ja juurdepääsuhalduse toetuse (nt SAML, QAuth või SSOlahendused), konfigureerimisvõimaluste ja laiendatavuse poolest.

XML-lüüsi kasutuselevõtmiseks peaks seetõttu esimese sammuna toimuma nõuete analüüs, milles tehakse kindlaks vajalikud ja soovitavad funktsioonid. Kui XML-lüüse kasutatakse suurema kaitsevajaduse korral, tuleb lisaks kindlaks määrata saavutatavad turbe eesmärgid. XML-lüüsid on võimelised kontrollima sissetulevat andmeliiklust pahatahtlike sisude suhtes ja neid välja filtreerima, mille tõttu töötlemine lõppsüsteemis ei saa toimuda kohe. Nii saab näiteks ründe toimepanija poolt loodud valed XMLsõnumid juba lüüsil välja filtreerida (vt G 5.183 XML-i vastu suunatud ründed).

Lüüsid pakuvad sageli ka väljuva andmevoo kontrolli, mis püüab takistada, et tundlikud sisud sisevõrgust välja ei imbuks. Sellega võib XML-lüüs üle võtta suurema osa ülesandeid, mis on esitatud meetmetes M 4.393 Sisestuste- ja väljastuste põhjalik valideerimine veebirakendustes ja veebiteenustes ja M 4.454 Veebiteenuste kaitsmine keelatud kasutuse eest . Skeemi valideerimine võib toimuda näiteks (vt M 4.454 Veebiteenuste kaitsmine keelatud kasutuse eest) kas juba XML-lüüsil või otse süsteemis, mis veebiteenust pakub. Otsus, kus valideerimine peab toimuma, tuleb dokumenteerida juba planeerimisfaasis, sest sellel võivad olla mõjud ka üldstruktuuri jaoks.

XML-lüüsi kasutamisest tulenevad järgmised eelised:

- XML-lüüsid on optimeeritud oma kasutamise eesmärgi jaoks. See tähendab tavaliselt, et neid on spetsiaalselt tugevdatud ja need on seetõttu vastupidavad;

- kuna arendusse on imbunud palju teavet XML-il põhinevate rünnete ja vastavate turvameetmete kohta, võimaldavad XML-lüüsid veebiteenuste turvalist kasutamist, kui need on õigesti konfigureeritud;
- üks XML-lüüsi suuri eeliseid on veebiteenuse turbesuunise erinevate aspektide haldus tsentraalses kohas (tavaliselt Web-Interface'il), mitte iga teenuse jaoks eraldi. See võib aidata vältida kontseptsiooni- ja konfigureerimisvigu.

Managementinterface'i tuleb kaitsta nõuetekohaselt.
Puudused, mis XML-lüüsi kasutamisest tekkida võivad, on järgmised:

- nagu ka muude ALG-de korral ei ole XML-lüüsi konfiguratsioon triviaalne, vaid vajab hoolikat planeerimist ja põhjalikke teste. See ei kehti ainuüksi kasutuselevõtmise, vaid ka kõikide muudatuste kohta seotud veebiteenuste suhtluskäitumises;
- XML-lüüsi hoolduskulud on küll väikesed, aga see ei ole hooldusvaba. Ka siin tuleb teostada regulaarseid tarkvara- ja allkirjavärskendusi, kui tootja neid pakub. Tähelepanu tuleb pöörata ka lüüsi kitsaskohtade tundmaõppimisele ja nendele reageerimisele.
- järgmise süsteemi paigaldamisel töötlusahelasse tõuseb kättesaadavuse kaotuse risk konfiguratsiooni-, tarkvara- või riistvaravigade tõttu. Kõrge kättesaadavuse vajaduse korral peaks toimuma liiasusega väljaehitamine;
- eriti siis, kui lüüs võtab üle ka kahjurvara kontrollimise, võivad valehäired kaasa tuua funktsioonide ja kättesaadavuse kahjustamise. Seepärast tuleb lisaks põhjalikele testidele läbi viia ka riskide hindamine üksteise suhtes ning vajaduse korral tuleb koostada hädaolukorra kontseptsioon;
- teatud ründetüübid on keerulised ja arenevad jooksvalt edasi, nii et ei tohi lähtuda sellest, et XML-lüüs tunneb ära kõik rünnete variandid. Näited on XML Signature Wrapping-ründed (XSW) või uuemad ründed TLS-ile/SSLile nagu näiteks CRIME;
- just paljude krüptograafiliste operatsioonidega ressursikriitilised teenused võivad vajada lüüsi rakendamist, et oleks võimalik hallata arvutuskoormust.

Samaaegselt võib lüüs endast kujutada pudelikaela, mille sisemisele funktsioonile ja jõudlusele on käitajal vähem mõju kui veebiteenusele endale. See teeb vajalikuks ettevaatliku planeerimise ja testid.

Sarnaselt Web-Application Firewall'ile (WAF) võib ka XML-Firewall luua vale tunde turvalisusest ja see võib kaasa tuua selle, et ei pöörata piisavalt tähelepanu turvameetmetele veebiteenuse tarkvaraarenduses ja kasutamisel. See on sageli fataalne, sest enamiku lüüside jaoks saavad aja jooksul tuntuks meetodid, kuidas nende filtreerimisfunktsioone vältida. Tugeva koodi ja turvakontrollide vajadus teenuses endas ei muutu seega üleliigseks.

Tavaliselt võib XML-lüüs nagu ka muud ALG-d asuda ka neutraalses piirivõrgus (DMZ). Siinjuures soovitatakse ka P-A-P-ülesehitust ette ja vahele lülitatud

paketifiltritega ja XML-lüüsiga keskel, mis pakub tunduvalt paremaid kontrollimisja logimisvõimalusi (vt M 2.73 Sobiva turvalüüsi (tulemüüri) põhistruktuuri väljavalimine). Lisaks võivad mõlemad paketifiltrid kaitsta XML-lüüsi ennast lihtsate rünnakute eest ja kompenseerida osaliselt keerulisusest tingitud valekonfiguratsioone. Tänu sellele võivad nad filtreerimisega kaitsta lüüsi soovimatu andmeliikluse (nt internetiusside kaudu) eest ja hoida ära ülekoormust.

Kuna XML-lüüs kujutab endast keerulist süsteemi, tuleb kõikidele kasutusaja etappidele alates kontseptsioonist kuni hädaolukorra ettevalmistamiseni seada üksikasjalikud nõuded. Seetõttu tuleb XML-lüüsi ennast käsitleda turbekontseptsioonis mooduli B 3.301 Turvalüüs (tulemüür) abil.

Kontrollküsimused:

- Kas nõuete analüüsis määrati kindlaks, milliseid XML-lüüsi funktsioone vajatakse?
- Kas võeti vastu otsus ja dokumenteeriti, kus tuleb läbi viia sõnumite valideerimine?
- Kas on kindlaks tehtud, et rakenduste arendus võtab edaspidi arvesse tugeva koodi ja sisestusandmete kontrollimise nõudeid?
- Kas on planeeritud XML-lüüsi asukoht ja seda põhjendatud, nt DMZ-s ja kahe paketifiltri vahel (P-A-P)?
- Kas XML-lüüs ise on lisatud turbekontseptsiooni ja kirjeldatud mooduli B 3.301 Turvalüüs (tulemüür) abil?

M 5.176 Nutitelefonide, tahvel- ja pihuarvutite turvaline ühendamine asutuse võrguga

Algatamise eest vastutab: infoturbeametnik

Rakendamise eest vastutab: IT-juht

Nutitelefonid, tahvel- ja pihuarvutid ühendatakse asutuse võrguga tavaliselt ilma juhtmeta, nt WLAN-i või mobiilse telekommunikatsioonivõrgu kaudu. Põhimõtteliselt peaks ühendus lõppseadme ja asutuse võrgu vahel olema järjekindlalt krüpteeritud. Seda saab teostada krüpteeritud VPN-tunneliga (vt moodulit B 4.4 Virtuaalne privaatvõrk (VPN)), mis rajatakse lõppseadme ja asutuse VPN-serveri vahele. Nii välditakse, et mobiilsete telekommunikatsioonivõrkude või krüpteerimata WLAN-ühenduse nõrkused ohustaksid usaldusväärsust. Kui lõppseade pääseb asutuse krüpteeritud WLAN-i kaudu ligi asutuse võrgule, tuleks kaaluda, kas VPN-tunnel ei ole järsku vajalik.

Nutitelefonid, tahvel- ja pihuarvutid peaksid asutuse sees olema paigutatud oma võrgusegmenti (vt meedet M 5.7 Võrguhaldus). Kui neid või võrreldavaid lõppseadmeid kasutatakse infokoosluses, tuleks segmenteerimist täiendada võrgule juurdepääsu kontrolliga. See peaks täiendavalt kontrollima, kas:

- kaasaskantavatel lõppseadmetel on olemas kõik ajakohased süsteemipaigad,
- kõikidel rakendustel on uusimad värskendused,
- viirusesignatuuri andmebaas on ajakohane ja
- kõik muud seadistused lõppseadmel, nt parooli loomine ja aeg kuni automaatse lukustamiseni, vastavad nõuetele.

Kui võrgule juurdepääsu kontroll peaks kindlaks tegema, et nutitelefon, tahvel- või pihuarvuti ei vasta ühele nendest punktidest, tuleb see tõsta karantiinivõrgusegmenti. Seal saab võrgule juurdepääsu kontrolli agent seadet vastavalt turvanõuetele värskendada või juhendada kasutajat lähtestama lõppseadmel muudetud seadistused. Seejärel võib lõppseadme jälle karantiinialalt eemaldada.

Kui nutitelefon, tahvel- või pihuarvuti varastatakse või kaotatakse ja selle kohta on tehtud teade, tuleb selle lõppseadme juurdepääs asutuse võrgule lukustada (vt meede M 6.159 Nutitelefonide ning tahvel- ja pihuarvutite kaotuste ja varguste ennetamine). Suurema kaitsevajaduse korral tuleb lisaks kontrollida, kas lõppseadmega ei ole vahepeal volitamata ligi pääsetud asutuse andmetele ja kas vastavalt suunistele turvaintsidentide käsitlemiseks kasutatakse täiendavaid meetmeid (vt moodul B 1.8 Turvaintsidentide käsitlus). Selleks tuleb eelnevalt kasutada võrgule juurdepääsu kontrolli vastavaid logimisfunktsioone.

Kordamisküsimused:

- Kas nutitelefonid, tahvel- ja pihuarvutid on asutuse sees paigutatud oma võrgusegmenti?
- Kas silmatorkavad nutitelefonid, tahvel- või pihuarvutid tõstetakse karantiini-võrgusegmenti?

M 5.177 SSL-i/TLS-i kasutamine serveris

Algatamise eest vastutavad: infoturbeametnik, IT-juht

Rakendamise eest vastutab: administraator

Transport Layer Security (TLS) on Secure Sockets Layer'i (SSL) edasiarendus ja seda kasutatakse, et kaitsta andmeid võrkudes edastamisel krüptograafiliselt, tavaliselt serveriteenuste ja klientide või serveriteenuste vahel. Konfigureerimisjuhiseid, kuidas SSL-i/TLS-i klientides kasutada ja üldist teavet SSL-i/TLSI-i tööpõhimõtte kohta leiate meetmes M 5.66 TLS-i/SSL-i kasutamine kliendis. Kliendid saavad krüpteerimist SSL-i/TLS-i kaudu kasutada ainult siis, kui serveriteenused seda toetavad. SSL-i/TLS-i saab kasutada selleks, et kanda andmeid krüpteeritult TCP/IP kaudu rakenduskihist (nt HTTP, LDAP, POP3, IMAP ja SMTP) üle. Ühtlasi saab SSL-i/TLS-i abil üles ehitada turvalisi VPN-e (virtuaalsed privaatsed võrgud). OpenVPN'iga, mis on GNU GPL-i (General Public Licence) alla kuuluv vabalt saadaolev tarkvara, võivad VPN-id SSL-i/TLS-i abil realiseerida krüpteeritud ühendusi. Täpsemat teavet VPN-ide kohta leiate moodulist B 4.4 Virtuaalne privaatvõrk (VPN) .

Tavaliselt on see suurema osa serveriteenuste jaoks üksnes vähene lisakoormus, et konfigureerida nii, et toetatakse SSL-i/TLS-i, või nii, et andmevahetuseks kasutatakse ainult neid. Seepärast tuleb kõikide serveriteenuste puhul kontrollida, kas on võimalik mõistliku hinnaga saada krüpteerimist SSL-i/TLS-i kaudu ja kas see on ka elluviidav. Kui see on mõistliku hinnaga võimalik, tuleks SSL/TLS-krüpteering aktiveerida. Üldiselt peaks nii sisene kui ka väline sõnumite voog LDAP-st ja LDAP-sse, e-posti- ja veebiserveritesse ning sealt välja olema SSL-i/TLS-iga krüpteeritud.

Usaldusväärse sertifitseerimisasutuse valimine

Uue, SSL-i/TLS-iga kaitstud sideühenduse rajamise alguses toimub nn Handshake kliendi ja serveri vahel. Siinjuures lepivad klient ja server kokku krüptograafiliste algoritmide suhtes, mida rakendatakse võtmete vahetuseks, krüpteerimiseks ja tervikluse kaitsmiseks. Lisaks sellele lepivad klient ja server kokku, millist SSL-versiooni kasutama hakatakse. Sellele lisaks saadab server kliendile oma X.509-sertifikaadi. Valikuliselt võib server olla konfigureeritud ka nii, et ka kliendilt nõutakse oma X.509-sertifikaadi saatmist serverile.

Suhtluspartnerite identiteeti kontrollitakse seejuures nende sertifikaatide abil. X.509-sertifikaadid sisaldavad avalikku võtit ja täiendava instantsi, sertifitseerimisasutuse või ka Trustcenter'i või Certificate Authority (CA) kinnitust avaliku võtme õige määramise kohta selle „omanikule". Sertifikaadi väärtus sõltub sellest, milliseid X.509-sertifikaadi välju sertifitseerimisasutus kontrollib, enne kui sertifikaat väljastatakse, ja kui usaldusväärne on sertifitseerimisasutus ise. Seetõttu mängib usaldusväärse sertifitseerimisasutuse valik olulist rolli.

Sertifitseerimisasutuste suure hulga tõttu turul peaks asutus sertifitseerimisasutust hoolega valima. Mõistlik oleks eelnevalt kindlaks teha hilisema töö jaoks olulised valikukriteeriumid. Nende hulka võivad kuuluda näiteks järgmised:

- kas Root-sertifikaat on juba klientide CA-nimekirjades, näiteks veebilehitsejal olemas,
- kus on sertifitseerimisasutuse asukoht ja milline on tema õiguslik seisund, ja kus on ka tehnilise käituse asukoht,
- mis on sertifitseerimisasutuse ärialane suunitlus (kas CA-osakond on tsentraalne ärivaldkond?), mida hõlmavad pakutavad CA-teenused (nt OSCP, CRL),
- millist turbeastet võib sertifitseerimisasutus tõendada,
- milline on tehnilise toe ulatus ja kvaliteet,
- kui suured on sertifikaadi kulud.

Põhimõtteliselt ei tohiks sertifikaadi kulud olla mingil juhul otsustav kriteerium. Kui pakutavat serveriteenust kasutab piiratud kasutajate ring, nt LAN-i sees, võib sertifikaadi koostada ka ise, ilma sertifitseerimisasutuse osavõtuta, selle allkirjastada ning paigaldada kõikidele klientidele, millel serveriteenust kasutama hakatakse.

Extended-Validation-sertifikaadid

Selleks, et raskendada ründeid võltsitud veebilehtedega ja seista vastu probleemidele olukorras, kus erinevad sertifitseerimisasutused ei kontrolli SSL-i/TLS-i taotlusi alati usaldusväärselt, võeti kasutusele Extended-Validation-sertifikaadid, et käsitleda kõrgemate turbenõuetega sertifikaate. Need peavad ära hoidma, et CA kontrollib sertifikaadi väljastamisel üksnes domeeni nime. Seepärast peab CA lisaks veel täpselt järele uurima, kes nimetatud domeeni registreeris. Erinevalt tavapärastest X-509 SSL/TLS-sertifikaatidest kontrollitakse nende laiendatud sertifikaatide (Extended Validation SSL-sertifikaadid, EV-SSL) taotluse esitaja identsust põhjalikult. Seejuures kohustuvad osalev sertifitseerimisasutus ja veebilehitseja tootja pidama kinni CA/Browser Forums'i juhendist Guidelines for the Issuance and Management of Extended Validation Certificates. Selle kohaselt peavad taotluse esitajad täitma muu hulgas järgmisi kriteeriume:

- taotluse esitaja identiteedi tõestamine ja aadress,
- tõestus selle kohta, et taotluse esitaja on domeeni ainuke omanik,
- kinnitus, et taotlust esitaval isikul on volitus taotluse esitamiseks ja
- peamine kontaktisik.

Lisaks ei tohi taotluse esitaja või taotlust esitav isik olla kirjas üheski keelatud organisatsioonide või isikute nimekirjas. Riik, kus on taotluse esitaja asukoht

või õiguspädevus, ei tohi olla välja andnud kauplemisembargosid või muid sanktsioone, mis nimetatud riik on kehtestanud, kelle jurisdiktsiooni alla sertifitseerimisasutus kuulub.

Kasutajad tunnevad EV-SSL-sertifikaadid ära selle järgi, et kaitstud brauseritel on teatud alad nagu aadressivälja URL või paljude brauserite poolt kasutatav tabaluku sümbol, mis tähistab krüpteeritud lehekülge, märgitud rohelisega. Vastavalt turvalüüside (tulemüür) konfiguratsioonile, mille tagant kasutajad EV-SSL-sertifikaatidega veebilehtedele ligi pääsevad, võib ette tulla, et neid veebilehitsejates olevaid tähistusi klientidele ei kuvata. Kui näiteks sõnumivoog kliendi ja veebiserveri vahel proksi poolt dekrüpteeritakse või uuesti krüpteeritakse, kuvab veebilehitseja turvalüüsi SSL/TLS-sertifikaati.

Lisaks suurematele finantskuludele, mis EV-SSL-sertifikaadi väljastamisega tekivad, kestab ka taotlemine tavaliselt kauem, sest sertifitseerimisasutus kontrollib täiendavaid andmeid. Võimaluse korral soovitatakse see täiendav kulu vastu võtta. Eriti alad, kus edastatakse suurema kaitsevajadusega andmeid, mis puudutab konfidentsiaalsust ja terviklust, tuleks eelistatult kasutada EV-SSL-sertifikaate.

Üldnime (Common Name) sissekanne

Brauserid kuvavad alati turvahoiatust, kui veebilehe sertifikaadis sissekantud Common Name (üldnimi) ei vasta täielikule DNS-nimele (Fully Qualified Domain Name), mille kaudu on server veebis kättesaadav. Seetõttu tuleb kindlaks teha, kas üldnimi sobib URL-ile, mida tegelikult kasutatakse, et serveriga suhelda. Kui see on võimalik, tuleks vältida Wildcard-sertifikaate (nt *.example.de). Neid kasutatakse tihti, et kaitsta ühe sertifikaadiga paljusid alamdomeene.

Täielik sertifikaadiahel

Seoses sellega, et hierarhilise sertifikaadiahela kontrollimiseks veebilehitseja poolt on vaja vahesertifikaate, ei piisa ainuüksi serveri SSL-sertifikaadist. Seepärast peaks server olema konfigureeritud nii, et ühenduse loomisel saadetakse kliendile kõik vajalikud sertifikaadid. Selleks tuleb luua veebiserveris vastav sertifikaadiahel.

Lisaks tuleb tähele panna, et puuduvate sertifikaatide kõrval katkestavad sertifikaadiahela kontrollimise ka tähtaja ületanud või suletud sertifikaadid. Ainult juhul, kui kõik sertifikaadid on kehtivad ja ühenduse loomisel üle kantakse, saab sertifikaadiahelat edukalt kontrollida.

SSL-i/TLS-i protokolliversiooni valik

Praegu kehtib viis SSL-i/TLS-i protokolliversiooni: SSL v2, SSL v3, TLS v1.0, TLS v1.1 ja TLS v1.2. SSL v1 ei avalikustatud. Turvalise ühenduse tagamiseks kliendi ja serveri vahel tuleks kasutada versiooni TLS 1.2. TLS 1.1 pakub piisavat turvalisust, aga võrreldes versiooniga TLS 1.2 on sellel siiski mõned nõrgad

kohad, nt on versioonis TLS 1.1 veel alles Cipher-Suites, mis põhinevad IDEA-l ja DES-il, versioonil TLS 1.2 enam mitte. TLS 1.0 võib olemasolevates rakendustes üleminekuna edasi kasutada, kui kohene üleviimine versioonile TLS 1.1 või eelistatult versioonile TLS 1.2 ei ole võimalik ning rakendada tuleb sobivaid meetmeid Chosen-Plaintext-tüüpi rünnete vastu (nt BEAST) CBC-rakendusele. Üldiselt peaks siiski üleviimine versioonile TLS 1.2 toimuma nii kiiresti kui võimalik. SSL v2 ja SSL v3 ei tohi enam kasutada.

Turvalised Cipher-Suites

SSL/TLS kasutab Cipher-Suite'e mis määravad, kui turvaline on HTTPS-ühendus. Iga Suite koosneb spetsiifilistest moodulitest. Kui mõnda moodulit peetakse ebaturvaliseks või nõrgaks, saab Cipher Suite'i muutmisega vahetada selle mooduli turvalisema vastu.

Kuna klient võib peale suruda nõrgemate Cipher Suite'ide kasutamist, on nõutav pakkuda serveri poolt ainult selliseid, mis rakendavad autentimist ja krüpteerimist piisava tugevusega. Seetõttu peaksid kasutatavad Cipher Suite'id toetama Perfect Forward Secrecy't (PFS) (vt TR-02102-2).

Täiendavad suunised krüptograafiliste algoritmide ja võtmepikkuste kohta sisalduvad BSI tehnilises suunises Krüptograafilised meetodid. Soovitused ja võtmepikkused – sisalduvad 2. osas, TLS-i kasutamine (TR-02102-2) ja meetmes M 2.164 Sobiva krüptoprotseduuri valimine

Seansi uuendamine / TLS-tihendus

Niinimetatud seansi uuendamisega (Session Renegotiation) saavad nii klient kui ka server olemasoleva HTTPS-seansi parameetrid uuesti kokku leppida. Vea tõttu TLS-protokolli (RFC 5246) standardis on võimalik, et man-in-the-middle-tüüpi rünnete toimepanijad kasutavad ära seansi uuendamist, et sisestada mis tahes sisusid olemasolevasse HTTPS-seanssi. Vahepeal täiendati TLS-protokolli (RFC 5746) ja need projektivead kõrvaldati. Üldiselt tuleks kaaluda, kas seansi uuendamine serveri poolt on vajalik. Kui see on nii, tuleks see konfigureerida turvaliselt RFC 5746 alusel. Kliendipoolse seansi uuendamise peaks server tagasi lükkama.

Seetõttu tuleks TLS-tihendus välja lülitada.

Veebiserveriga seotud aspektid

Üldiselt soovitatakse veebiserveritel kasutusse antud sisusid ülekandel serverilt kliendile ja vastupidi kaitsta SSL-i/TLS-iga.

Võimaluse korral tuleks vältida segatud sisudega veebilehti. Segatud sisuga veebileheks nimetatakse lehte, mis kasutab küll krüpteeringut, sisaldab aga

sealjuures ka krüpteerimata sisu (nt JavaScript-, CSS-failid või pildid). Man-in-the-middle-tüüpi ründe toimepanija saab üksiku krüpteerimata faili ülekannet ära kasutada, et üle võtta HTTPS-seanssi. Kuna segatud sisudega veebilehed genereerivad tavaliselt ka veebilehitseja hoiatusi, halvendatakse sellega kasutajasõbralikkust.

HTTP Strict Transport Security (HSTS) on teine meetod, mis kaitseb SSL-i tuntud nõrkuste vastu. Sellega tehakse raskemaks, et külastaja ründe või serveripoolse konfiguratsiooniprobleemi tõttu turvaliselt lehelt ebaturvalisele ümber suunatakse. Kui ründe toimepanija asub näiteks samas WLAN-is kus ohver, saab ta lugeda seansi küpsiseid ja HTTPS-seansi üle võtta. HSTS-i aktiveerimiseks peab serveril olema konfigureeritud HSTS-Header.

Privaatsete serverivõtmete kaitse

Üks SSL-i/TLS-i kasutamise oluline turvalisusega seotud aspekt on privaatse serverivõtme kaitse. Seepärast on mõistlik konfigureerida server nii, et privaatne serverivõti väljastatakse serveri käivitamisel parooli sisestamise kaudu. Kui on olemas kahtlus, et privaatset võtit on kahjustatud, tuleb aluseks olev sertifikaat tühistada. Täiendavaid juhiseid krüptograafiliste võtmete kasutamiseks leiate meetmes M 2.46 Krüpteerimise õige korraldus .

Valideerimine

Serveril teostatavate konfiguratsioonimuudatuste tagajärgi ei või kunagi täie kindlusega ennustada. Ka tarkvara uuendused võivad mõnikord kaasa tuua üllatavaid muudatusi. Seetõttu soovitatakse SSL-i/TLS-i konfiguratsiooni enne kasutusloa väljastamist kontrollida vigade suhtes ja valideerida olekut perioodliste intervallidega (regulaarselt).

Kontrollküsimused

- Kas kõik serveriteenused, mille puhul see on kasulik ja võimalik, pakuvad andmeid krüpteeritult SSL-i/TLS-i kaudu?
- Kas sertifitseerimisasutus valiti välja hoolikalt?
- Kas üldnimi (Common Name) valiti välja hoolikalt?
- Kas veebiserveris loodi täielik sertifikaadiahel?
- Kas kasutatavad serveritooted toetavad SSL-i/TLS-i turvalist versiooni?
- Kas on tagatud, et kasutatavad serverid kasutavad krüptograafilisi algoritme ja võtmepikkusi, mis vastavad tänapäeva tehnika tasemele ja asutuse turvanõuetele?
- Kas seansi uuendamine inaktiveeriti või toimub see RFC 5746 alusel? Kas kliendipoolne uuendamine inaktiveeriti?
- Kas veebilehed loobuvad segatud sisudest?

- Kas TLS-tihendus inaktiveeriti?
- Kas privaatset serverivõtit kaitstakse parooliga?
- Kas SSL-i/TLS-i konfiguratsiooni kontrolliti enne kasutusloa andmist vigade osas ja kas olekut valideeritakse korrapäraste ajavahemike järel?

M 5.178 Infosüsteemis autentimislahendustele kehtivad nõuded ehk autentimisnormatiiv

Füüsilise isiku elektroonsel tuvastamisel ehk autentimisel peab lähtuma autentimisnormatiivi (https://www.ria.ee/public/PKI/Autentimislahendustele-kehtivad-nouded.pdf) nõuetest.

Juhul, kui autentimisega antakse ligipääs vaid infosüsteemi piiratud osale, siis antud nõuete täitmisel tuleb lähtuda Infosüsteemile või selle osale määratud ISKE turbetasemest.

Näiteks kõrge turbetaseme puhul ei tohi aktsepteerida muid lahendusi kui Eesti riigi ja ka teiste EL liikmesriikide poolt tunnustatud kõrge turbetasemega autentimislahendusi.

Andmetele ligipääsu juures on määrav lisaks ISKE turbetasemele ka asjaolu – kas peab nõudma täiendavat tugevamat autentimislahendust kui ISKE turbetase seda nõuab (sellisteks andmeteks võivad olla näiteks delikaatsed isikuandmed, nagu tervise andmed, finantsandmed jms).

Autentimislahendust saab luua lokaalselt, juurutades sobivate vahendite liidesed infosüsteemi või tsentraalselt läbi RIA autentimisteenuse.

eIDAS-e nõuded ja autentimisnormatiiv on kehtivad ainult avaliku teenuse pakkumisel kodanikule.

Rakendamiseks vajalik dokumentatsioon on leitav siit: https://www.ria.ee/ee/eid-info-ja-juhendid.html#eIDAS.

Kontrollküsimused:

- Kas portaalis on vajalik kasutajate autentimine?
- Kas portaalis on eri teenuseid, mille minimaalne isikutuvastuse tagatistase on erinev?
- Kui avate portaali teenuse isikule, kas kontrollite enne kolmanda osapoole autentimisteenuse kasutuselevõtmist autentimise taset?

M 5.E1 Sertifikaatide õigeaegne peatamine

Algatamise eest vastutavad: turvajuht
Rakendamise eest vastutavad: kasutaja

Kui omaniku (kasutaja) ainuvaldusest on väljunud nii pöördkonstrueerimatu seade (ID-kaart, digi-ID, mobiil-ID) kui ka selles sisalduvate võtmepaaride privaatvõtmeid kasutada võimaldavad PIN-koodid, on seadme ebaseaduslikul valdajal (ründajal) võimalik nii kasutaja nimel end volitamata autentida kui ka kasutaja nimel volitamata digiallkirju anda. Nimetatud tegevused saab blokeerida sertifikaadi peatamisega – selleks tuleb helistada Sertifitseerimiskeskuse ASi lühinumbril 1777 või talitada teistel veebilehel Sertifitseerimiskeskus - Sertifikaatide peatamine kirjeldatud viisidel. Sertifikaadi peatamise osas peavad kõik ID-kaardi, digi-ID ja/või mobiil-ID kasutajad lähtuma järgmistest reeglitest.

Sertifikaat tuleb koheselt peatada esimese tõsise kahtluse tekkimisel, et varastatud on nii seade kui ka seda aktiveerivad PIN-koodid (vt G 5.E4 PIN-koodide vargus ja/või volitamata kasutamine ja G 5.E5 ID-kaardi või sarnase seadme vargus või röövimine).

Kui nii seadet kui ka PIN-koode hoitakse piisavalt hoolsalt (vt M 2.E14 Digitempli turvaline evitamine asutuses , M 2.E18 ID-kaardi või digi-ID edasiandmiskeeld teisele isikule (tavakasutaja) ja M 2.E19w ID-kaardi või digi-ID kaasavõtmiskohustus arvuti juurest lahkumisel), siis sertifikaatide peatamise vajadust praktikas ei teki.

- Kasutajad peavad endale teadvustama, et seadme ja selle PIN-koodide lohakas hoidmine koos sellejärgse sertifikaadi peatamata jätmisega võib kaasa tuua ülimalt tõsiseid tagajärgi – mitmeid kohustusi võtvate dokumentide (laenu-, liisingu- ja järelmaksulepingud) volitamata allkirjastamist ründaja poolt, ründaja poolset väärautentimist veebipõhistes keskkondades (nii eraasjus kui ka tööasjades) jms.
- Kasutajad peavad endale teadvustama, et ekslikult peatatud sertifikaadi toimimise saab hiljem taastada (nt juhtumil, kui seade välja tuleb ja seega vargusevariant ära langeb), kuid see eeldab füüsilist kohaleminemist teeninduspunkti. Seega on võimalike käideldavuskadude ning täiendavate sekelduste vältimiseks siiski alati mõistlik nii seadet kui ka PIN-koode hoida hoolsalt.
- Kui ID-kaarti, digi-ID-d ja/või mobiil-ID-d kasutatakse töökohustuste täitmiseks, tuleb sertifikaadi peatamisest koheselt teavitada ka asutuse turvajuhti, kellega koos töötatakse välja edasine tegevusplaan, mis edasisi turvariske võimalikult valutult maandab ja haldab.

Lisaks tuleb asutuse tasemel (turvajuht, infosüsteemide arhitektid) teadvustada, et asutuse töötajate ID-kaardid on töötajate omand ning asutuses kehtestatud

juhised (sh ka sertifikaatide peatamiseks-tühistamiseks) saavad olla vaid soovitusliku, mitte kohustusliku iseloomuga. Teisiti on olukord digi-ID korral. ID-kaardi ja PIN-koodide hoolsa hoidmise teemat koos sertifikaatide tühistamise teemaga tuleb kindlasti käsitleda ka töötajate koolitamisel (vt M 3.E2 Töötajate koolitus ID-kaardi/PKI lahenduste kasutamise osas).

Kontrollküsimused:

- Kas ja kui tihti on asutuses ette tulnud juhtumeid, kus kasutajate sertifikaate on tulnud lohaka tegevuse tagajärjel peatada?
- Kas kõik lõppkasutajad on teadlikud, millal ja kuidas on sertifikaate võimalik peatada?

M 5.E2 Varem antud digiallkirjade õigeaegne ülesigneerimine

Algatamise eest vastutavad: turvajuht
Rakendamise eest vastutavad: IT juht või tema määratud isik

Praktilistelt kõikidele kaasajal kasutatavatele krüptoalgoritmidele on omane nende nõrgemaks jäämine aja jooksul (vt G 4.35 Ebaturvaline krüptoalgoritm). Seetõttu on praktiliselt kõikide krüptoalgoritmide turvaline ajahorisont lõplik, st kunagi tulevikus osutub võimalikuks nende praktiline murdmine. Mainitud põhjusel vahetati alates 2002. aastast digiallkirjades kasutatud DigiDOCi standard (mis põhines SHA-1 räsil ning 1024-bitisel RSA-l) 2011. aastal DigiDOC3 vastu. DigiDOC3 kasutab varasemast turvalisemat, 2048-bitist RSAd. Eeltoodu ei tähenda, et varasemad, enne 2012. aastat ja/või vana ID-kaardi põhjal antud digiallkirjad on juba muutunud ebaturvaliseks. Samas on prognoositav, et uue, DigiDOC3 standardi põhjal antud digiallkirjad muutuvad ebaturvaliseks tõenäoliselt palju hiljem kui vana standardi põhjal antud.

Ebaturvaliseks muutuvate algoritmide põhjal antud digiallkirjadega digidokumentide tõestusväärtuse säilitab dokumentide ülesigneerimine. Sel korral varustab digidokumenti säilitav instants (digiarhiiv) dokumendi endapoolse täiendava digiallkirjaga, mis põhineb varemkasutatutest turvalisematel krüptoalgoritmidel ning mille turvahorisont on seetõttu varemkasutatutest pikem. Niiviisi ülesigneeritud digidokumendi tõestusväärtus säilib jälle teatud perioodi. Hetkel on raske prognoosida, millal muutuvad ebaturvaliseks (praktikas murtavaks) nii vana DigiDOCi kui ka uue, DigiDOC3 standardi põhjal antud digiallkirjad. Kriitilisimal juhul võivad vana DigiDOCi põhjal antud digiallkirjad vajada ülesigneerimist juba mõne aasta pärast.

Kui asutuses on vaja digiallkirjaga digidokumente tõestusväärtuslikult säilitada, siis on asutuse turvajuhi kohuseks jälgida muuhulgas ka krüptomaastikul toimivat, et anda õigeaegselt signaal digidokumentide ülesigneerimiseks. Turvajuht peab sellise vajaduse kättejõudmisest informeerima asutuse IT-juhti, kes korraldab seejärel praktilise ülesigneerimise, sh vastavate süsteemide väljatöötamise ja toimimise (vt M 2.264 Krüpteeritud andmete regulaarne regenereerimine arhiveerimisel ja HT.49 Lisanõuded arhiveeritud andmete krüptoatribuutide regenereerimisele).

Kontrollküsimus:

- Kas ja kui sügavuti on asutuse turvajuht IT-juhti ja teisi võtmeisikuid tulevikus ees seisvast digiallkirjade (massilise) ülesigneerimise vajadusest informeerinud?

M6: Hädaolukorraks valmisolek

Meetmete nimekiri

M 6.1 Käideldavusnõuete inventuur

Algatamise eest vastutavad: IT-juht, IT turvaosakond
Rakendamise eest vastutavad: üksikute IT-rakenduste eest vastutavad töötajad

IT-süsteemides kasutatavate IT-rakenduste ja nende andmete kohta tuleb välja selgitada käideldavusnõuded. Kuna IT-rakendused ei vaja oma tööks ilmtingimata kõiki IT-süsteemi koostisosi, tuleks IT-rakenduste käideldavusnõuete väljaselgitamisel lähtuda IT-süsteemi peamistest komponentidest.

Töö tulemuse võib vormistada tabelina, mis sisaldab nt järgmist infot:

IT-süsteem	IT-komponent	IT-rakendus	Avariiaja talutav kestus
Kesksüsteem	Host	reisikulude arvestus	5 tööpäeva
		raamatupidamine	3 tundi
	Andmete kaugedastus	e-mail	3 tööpäeva
		raamatupidamine	1 tööpäev
	Printer	reisikulude arvestus	10 tööpäeva
		raamatupidamine	2 tööpäeva
		kasutamise planeerimine	1 tööpäev
LAN	Server	andmesisestus	1 tööpäev
		juhtimiskeskus	4 tundi
	PC	andmesisestus	10 tööpäeva
	PC	juhtimiskeskus	4 tundi

(Selgitus: kuna IT-komponenti nimega Host, mis asub IT-süsteemis nimega Kesksüsteem, kasutatakse raamatupidamise IT-rakenduse tarbeks, on komponendi Host maksimaalse talutava avariiaja kestus 3 tundi).

Erinevate IT-komponentide talutavate avariiaegade väljaselgitamiseks on mõistlik küsida seda vastavate protseduuride eest vastutavate töötajate käest ja kanda küsitluse tulemused IT-süsteemide alusel süstemaatiliselt tabelisse. Selline ülevaade kergendab IT-süsteemi ajaliselt eriti kriitiliste komponentide leidmist, millega tuleb avariiplaanis ilmtingimata arvestada. Teatud komponendi avarii puhul aitab niisugune ülevaade lisaks muule hankida infot puudutatud IT-rakenduste ja nende käideldavusnõuete kohta. Käideldavusele esitatavaid nõudeid peavad kasutajad või vastavad osakonnad ka põhjendama, välja arvatud juhul, kui põhjendused on juba mõne teise allüksuse poolt ette antud. Ettevõtte või ametiasutuse juhtkond peab

käideldavusnõuded kinnitama.

IT-süsteemi komponendi avarii puhul võimaldab selline ülevaade saada kiirelt infot selle kohta, millest alates liigitub konkreetne sündmus avariiolukorraks. Seda, kas eriti ajakriitilise komponendi avarii puhul on kindlasti tegemist avariiolukorraga või mitte, aitavad selgitada asendushankeplaan ning võimalik uuring sisemiste ja välimiste alternatiivlahenduste kohta.

Kontrollküsimused:

- Kas iga IT-rakenduse kohta on olemas põhjendatud käideldavusnõuded?
- Kas käideldavusnõuded on kooskõlas kõige uuemate kasutusprotseduuridega?
- Millal tabelit viimati värskendati?

M 6.16z Kindlustus

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond
Rakendamise eest vastutavad: ametiasutuse/ettevõtte juhtkond

Jääkohtude likvideerimiseks, mis võivad esineda ka vaatamata hoolikale avariiolukordadeks valmisoleku planeerimisele, on võimalik sõlmida erinevaid kindlustuslepinguid.

Kindlustusi võib liigitada alljärgnevalt:

- varakindlustused,
- tulekindlustus,
- veekindlustus,
- murdvarguskindlustus,
- montaaži-/demonteerimiskindlustus,
- transpordikindlustus,
- andmekandjakindlustus,
- elektroonikakindlustus,
- järelkulude kindlustus,
- tulevastane tööseisakukindlustus,
- masinate tööseisakukindlustus,
- lisakulude kindlustus,
- elektroonika tööseisakukindlustus,
- isikutega seotud kindlustused,
- kindlustus kohustuse täitmatajätmise puhuks,
- arvuti väärkasutuskindlustus,
- andmekaitsekindlustus.

Kontrollküsimus:

- Kas jääkohud on asjakohaste kindlustuslepingutega piisavalt kaetud?

M 6.17 Avariiolukorrast teavitamise plaan ja tuleohutuse alased õppused

Algatamise eest vastutavad: ametiasutuse või ettevõtte juhtkond, tuleohutusspetsialist

Rakendamise eest vastutavad: tuleohutusspetsialist

Ohutuse tagamiseks tuleb koostada meetmed, mida rakendatakse tulekahju korral. Avariiolukorrast teavitamise plaaniga tuleb kindlaks määrata järgnev:

- Erinevate sündmuste puhul rakendatavad abimeetmed
- Tingimused, millal ja kuidas toimub evakueerimine (inimesed ja seadmed)
- Loetelu isikutest, keda on tarvis informeerida
- Loetelu abijõududest, keda on tarvis informeerida.

Avariiolukorrast teavitamise plaani võib täiendada tulekahjude puhuks väljatöötatud käitumisreeglitega, millest tuleb kõiki töötajaid ka ilmtingimata teavitada. Täiendavat infot leiate moodulist B 1.3 Hädaplaanimine . Tuleb arvestada, et ka kõige paremini väljatöötatud avariiolukorrast teavitamise plaanist pole üldse kasu, kui ei suudeta tagada, et need meetmed on õiged ja toimivad. Seetõttu on tarvis teavitamisplaani regulaarselt kontrollida ja värskendada. Üheks võimaluseks teavitamisplaani kontrollida on korraldada tuleohutusalaseid õppuseid.

Näide

- 1993. a sügisel ühes Bonni 21-korruselises büroohoones korraldatud tuleohusalane õppus näitas, et paljud töötajad ei teadnud tulekustutite asukohta ega ka seda, kus asuvad väljapääsutrepid. Ohu puhul võib selliste teadmiste puudumine viia katastroofini. Osade töötajad aga ignoreerisid vastavat õppust sootuks ning ei suvatsetud mugavusest isegi mitte ruumist lahkuda.

Inimelude kaitsmiseks ja kahjude, muuhulgas ka IT-kahjude minimeerimiseks tuleks tuleohusalaste õppuste käigus õppida ja harjutada seda, kuidas tulekahju korral õigesti käituda. Enne vastavate õppuste läbiviimist tuleb see ettevõtte või ametiasutuse juhtkonnaga kokku leppida.

Täiendav kontrollküsimus:

- Millised olid viimase tuleohutusalase õppuse tulemused?

M 6.18z Varuliinid

Algatamise eest vastutavad: IT-juht, üksikute IT-rakenduste eest vastutavad töötajad

Rakendamise eest vastutavad: tehnikaosakond, administraator

Varuliinide paigaldamisega luuakse sobivate võrgupunktide vahele tavatöös kasutavate liinide kõrvale täiendavad varuliinid. Need tuleks suunata läbi mõne teise liinitrassi. Sellega luuakse võimalus rikete korral varuliinidele ümber kolida. Ümberlülitamine võib toimuda nii käsitsi kui ka automaatselt. Automaatne ümberlülitus tuleks siduda sellise instantsiga, kellel on õigus algatada tavaliinides tekkinud rikete kõrvaldamine. Varuliinide funktsioneerimist tuleb mõistlike ajavahemike tagant reaalse kasutamise abil kontrollida. Varuliinide dimensioneerimine, kontrollimisintervallid ja üldine vajadus varuliinide järele sõltub otseselt võrgule kehtivatest käideldavusnõuetest. Muuhulgas tuleb arvestada ka sellega, kui palju aega kulub varuliinide kasutuselevõtmiseks võrreldes tavaliinide taastamiseks kuluva ajaga. Siinkohal sõltub paljugi sellest, kas tegemist on avaliku sektori (nt sideoperaatori) või eraomanduses olevate liinidega.

- Avaliku sektori liinide puhul pole kasutajal mitte mingisugust võimalust nende kaitset mõjutada. Avalikud võrgud on aga reeglina varustatud piisava arvu varuliinidega. Enamasti piisab nii püsiühenduse kui ka sissevalimisega ühenduse katkemise puhul ühenduse taastamiseks lihtsalt ühenduse loomisest valitava liini kaudu. Püsiühenduste ümberlülitamine varuliinidele on enamasti liiga kallis ning paljudel juhtudel ebaotstarbekas.
- Eraomandis oleva võrgu puhul on selle käitajal seevastu küllaltki suur võimalus selle turvalisust mõjutada. Hinnakalkulatsioonid viivad aga tihti selleni, et varuliinide paigaldamisest loobutakse. Eraomandis olevate võrkude puhul ei kaasne varuliinide käitamisel siiski mitte mingisuguseid täiendavaid kulusid peale nende väljaehitamiskulude.

M 6.20 Varukoopia andmekandjate õige ladustus

Algatamise eest vastutavad: IT-juht, IT turvaosakond
Rakendamise eest vastutavad: administraator, kasutaja
Varukoopiate andmekandjate ladustamisele kehtivad järgmised erinõuded:

- Andmekandjatele tohib olla juurdepääs ainult volitatud isikutel, mis peab tagama, et neid poleks võimalik varastada.
- Vajaduse korral peab olema tagatud võimalikult kiire juurdepääs.
- Ladustuskoha kliimatingimused peavad vastama andmekandjate pikaajaliseks ladustamiseks ette nähtud hoiutingimustele.
- Õnnetusjuhtumite puhuks tuleb andmete varukoopiaid sisaldavaid andmekandjaid hoida arvutist eraldi ruumis, võimaluse korral mõnes teises tuletõkketsoonis.

Lisaks tuleb arvestada ka meetmest M 2.3 Andmekandjate haldus tulenevate nõuetega.

Kontrollküsimused:

- Kus hoitakse erinevate arvutite andmetest tehtud varukoopiaid?
- Kas lisaks nõutud juurdepääsutingimustele vastavad ladustuskoha kliimatingimused ka andmekandjate pikaajaliseks ladustamiseks ette nähtud hoiutingimustele?

M 6.21 Kasutatava tarkvara varukoopia

Algatamise eest vastutavad: IT-juht, IT turvaosakond
Rakendamise eest vastutavad: administraator, kasutaja

IT-süsteemides esinevate probleemide korral on tihti tarvis nii operatsioonisüsteemi kui ka rakendusi kiiresti uuesti installida. Selleks peavad kõik installimiseks vajalikud failid olema alati käepärast. Seetõttu on oluline luua tarkvarast varukoopiad ja need sobivas kohas arhiveerida.

Kui algne tarkvara on tarnitud mõnel andmekandjal (nt DVD, CD, USB mälupulk), tuleks originaaltarkvarast ja selle põhjal loodud enda tarkvaraarendustest teha varukoopiad, mis muudavad uuesti installimise võimalikult lihtsaks. Originaalandmekandjaid ja nendest loodud varukoopiaid tuleb hoida eri kohtades.

Rakenduste puhul on üldjuhul tavaks, et neid ei müüda koos andmekandjatega, vaid eraldi installimisfailide, mõne paketi- või tarkvarahalduse osa või lähteteksti paketina. Ka selliseid installimisallikaid tuleks hoida mõnes sobivas kohas.

Tasuliste operatsioonisüsteemide ja rakenduste puhul nõutakse installimisprotseduuri käigus sageli ka litsentsinumbri sisestamist. Seetõttu on tähtis, et installimiseks vajaliku tarkvara kõrval arhiveeritaks sobivalt ka litsentsinumbrid. Volitamata juurdepääs installimiseks kasutatavale tarkvarale ja litsentsinumbritele, nt piraatkoopia tegemiseks, peab olema välistatud.

Kui tarkvara transleeriti lähtetekstist, peab asjakohane dokumentatsioon sisaldama kõiki transleerimiseks kasutatud suvandeid ja eelkõige selliseid suvandeid, mida kasutati võimaliku konfigureerimisskripti käivitamiseks. Binaarpaketist installitud tarkvara puhul tuleks dokumenteerida kõik installimisprotsessi etapid selliselt, et nende põhjal oleks võimalik hiljem installimise käigust aru saada.

Kõik konfiguratsioonifaili muudatused tuleb alati dokumenteerida. Soovitatav on kasutada versioonihaldust. Samuti tuleks konfiguratsioonifailidest teha regulaarselt varukoopiad.

Kontrollküsimused:

- Kas hädaolukorras on kogu vajalik tarkvara ja teave kohe käepärast, kui midagi on tarvis kiiresti uuesti installida?

- Kas rakendatavast tarkvarast on loodud varukoopiad?
- Kas installimistarkvara ja võimalikke litsentsinumbreid hoitakse sobivas kohas?
- Kas lähteteksti transleerimisel kasutatud suvandid ja konfiguratsioonifailides tehtavad muudatused dokumenteeritakse?

M 6.23 Käitumisreeglid arvutiviiruste esinemisel

Algatamise eest vastutavad: IT-juht, IT turvaosakond
Rakendamise eest vastutavad: administraator, kasutaja

Arvuti nakatumisest arvutiviirusesse peaks teada andma viirusetõrjetarkvara. Selleks peab tarkvara olema ajakohane. Viirustesse nakatumise tunnused võivad hõlmata ka nt süsteemi seletamatut käitumist, seletamatut ressursikasutust või ootamatut võrgukasutust. Viirusetõrjetarkvara on suuteline tuvastatud viirusi automaatselt kõrvaldama. Selle käigus toimub nakatunud failide (peremeesfailide) puhastamine, st taastatakse failide algseisund. Viirusetõrjetarkvara suudab kustutada ka eraldiseisvat kahjurvara. Alternatiivne lahendus on nakatunud failide karantiin.

Kasutajad peaksid ennekõike täitma järgmisi punkte:

1. Säilitage rahu!
2. Kui võimalik, kutsuge appi mõni pädev arvutitehnik.
3. Sulgege töötavad programmid.

Järgmiste meetmete võtmine tuleks, kui vähegi võimalik, jätta administraatoritele:

- käivitage (buutige) arvuti mõne viirusevaba, kirjutuskaitsega varustatud andmekandja abil. Selleks võib kasutada süsteemi- või buutimisdisketti (avariidiskett, vt M 6.24 Rikkejärgse buutimismeedia olemasolu). Alternatiivina võib buutimiseks kasutada ka värskelt loodud viirusevaba buutimisvõimelist CD-ROMi või USB mälupulka. Selleks on võimalik kasutada nt Knoppixit ehk täielikku CD-ROMina kasutatavat GNU/Linux-tarkvarakogumit (vt www.knoppix.org).
- Vajaduse korral tuleb selleks eelnevalt CMOS-häälestuses buutimisjärjekorda muuta (vt M 4.84 BIOSi turvamehhanismide kasutamine).
- Kontrollige arvutit värske viirusetõrjetarkvaraga, et veenduda, kas tegu on tõepoolselt arvutiviirusega ning millist tüüpi viirusega on tegemist. Selle käigus tuleb koostada logi.
- Tehke andmetest varukoopiad, kuid ärge kirjutage selle käigus ühtki värskemat andmevarundust üle.
- Kõrvaldage arvutiviirus ja kontrollige kõvaketast uuesti viirusetõrjetarkvaraga.
- Kontrollige ka kõiki ülejäänud andmekandjaid (diskette, vahetatavaid kettaid) ja eemaldage ka nendelt võimalikud arvutiviirused.
- Juhul kui nakatunud arvutis leidis aset andmevahetus, hoiatage viiruse suhtes ka teisi IT kasutajaid.

Windowsi operatsioonisüsteemidel on kaitsemehhanismid, mis võivad takistada arvutite puhastamist arvutiviirustest. Viiruste kõrvaldamiseks tuleb need funktsioonid esmalt välja lülitada.

Seetõttu on tähtis, et läbitaks järgmised etapid:

- Desaktiveerige Windowsi süsteemitaaste funktsioon.
- Käivitage arvuti uuesti turvalises režiimis (koos administraatorivolitustega), et eelnevalt sisselülitatud viirusetõrjetarkvaral oleks võimalik pääseda ligi ka sellistele failidele ja süsteemiosadele, mis on tavaolukorras kaitstud.
- Rakendage viiruse kõrvaldamiseks viirusetõrjetarkvara.
- Käivitage süsteem uuesti täisfunktsioonideks.
- Kontrollige veel kord, ega arvutisse ei ole jäänud arvutiviirusi.
- Lülitage Windowsi süsteemitaaste funktsioon uuesti sisse.

Teadmiseks: võimaliku väärkasutuse vältimiseks tuleks pärast kahjurvara arvutist kõrvaldamist ära muuta ka vastavas arvutis rakendatud kasutajatunnused ja paroolid. Juhul kui arvutiviirusel õnnestus faile kustutada või muuta, proovige andmete seisu taastada varukoopiate abil (vt M 6.32 Regulaarne andmevarundus) ja programme programmidest loodud varukoopiate abil (vt M 6.21 Kasutatava tarkvara varukoopia).

Kontrollküsimused:

- Kas kõiki töötajaid on teavitatud õigetest käitumisreeglitest?
- Kas on olemas pädevad isikud, kes suudavad vajaduse korral eespool loetletud etappe läbi viia?

M 6.24 Rikkejärgse buutimismeedia olemasolu

Algatamise eest vastutavad: IT-juht, IT turvaosakond

Rakendamise eest vastutavad: administraator, kasutaja

Avariikäivitust võimaldav andmekandja tuleks arvutile luua juba selle kasutuselevõtul, et tagada kontrollitav süsteemiseisund nt kõvaketta avarii või viirusesse nakatumise puhul. Sellised andmekandjad võivad olla nn avariidisketid või CDd, mille loomisvõimalusi võivad pakkuda isegi erinevad operatsioonisüsteemid, enda koostatud CDd või välised andmekandjad (nt USB mälupulgad või välised kõvakettad, millel on USB- või FireWire-liidesed).

Avariikäivituse andmekandja liik ja andmete maht sõltub arvuti kasutusotstarbest ja selle olemasolevatest liidestest. Avariikäivituse andmekandja peaks ideaalis sisaldama kõiki hädavajalikke programme ja andmeid, mida rakendatakse erinevate probleemide korral, nagu nt

- väärkasutusest tingitud andmekadu,
- kasutus- ja administreerimisvead, mis takistavad kasutamist ja taaskäivitamist (rebuutimist),
- süsteemi nakatumine kahjurvaraga (nt arvutiviirustega),
- süsteemi kompromiteerimine ründaja läbi,
- riistvaraprobleemid.

Avariikäivituse andmekandja baasvarustus

Avariikäivituse andmekandja peaks võimaldama süsteemi kontrollida ja probleeme võimalikult suures osas kõrvaldada. Vajaduse korral tuleks luua erinevate probleemide kõrvaldamiseks erinevad avariikäivituse andmekandjad, mis on mõeldud ainult teatud konkreetseks otstarbeks.

Nn baasvarustusse on soovitatav kaasata järgmised programmid:

- värskete signatuuridega varustatud viirusetõrjetarkvara,
- süsteemikonfiguratsioonide töötlemist võimaldavad programmid või andmebaasid (File Editor, Registry Editor vms),
- süsteemiketta buutimissektori taastamist võimaldav programm,
- varundus-/taasteprogrammid,
- diagnoosimisprogrammid riistvaradefektide analüüsimiseks.

Samuti erinevad programmid süvaanalüüsiks, nt juurkrattide avastamiseks või kompromiteeritud süsteemi kohtuanalüüsiks. Ka kõik draiverid peavad olemas olema!

Siinjuures on oluline, et kõik programmid ja raamatukogud käivitataks eranditult avariikäivituse andmekandjalt. Selleks ei tohi kasutada mitte ühtegi installeeritud

süsteemi komponenti.

Avariikäivituse andmekandja loomisel on muu hulgas oluline silmas pidada, et lisaks hädavajalikele programmidele peaks seal olema ka kõik vajalikud draiverid, mis võimaldavad juurdepääsu arvutisse paigaldatud ketastele. Siia alla kuluvad nt kõvaketta kontrollerite draiverid (eriti RAID-kontrollerite draiverid) ja kõvaketta krüpteerimise ning kõvaketta kokkupakkimise draiverid. Juhul kui avariikäivituse andmekandja on piisavalt suure salvestusmahuga, võib sinna salvestada veel ka täiendavaid programme ja dokumentatsiooni. Vigade tuvastamise efektiivsust võib nt tõsta see, kui avariikäivituse andmekandja sisaldab alati kõige ajakohasemaid andmeid süsteemikonfiguratsiooni dokumentatsiooni kohta. Avariikäivituse andmekandja peab olema alati vaba igasugustest viirustest ja muust kahjurvarast. Seetõttu peavad rakendatavad programmid olema hangitud usaldusväärsetest allikatest (nt otse tootja CDlt) või siis tuleks neid kasutada alles pärast digitaalsete allkirjade kontrollimist.

Avariikäivituse andmekandja värskendamine

Iga süsteemi puhul ei ole alati ilmtingimata hädavajalik, et välja töötataks eraldi avariikäivituse andmekandja. Paindlikult koostatud andmekandjaga on võimalik lahendada küllaltki paljude erinevate süsteemide vajadused. Samuti pole sugugi hädavajalik, et avariikäivituse andmekandjal tuleks kasutada sama operatsioonisüsteemi nagu sihtsüsteemis. Ühilduvusnõuete tõttu on see aga siiski soovitatav.

Selle vaatamata on ilmtingimata tarvis testide abil kindlaks teha, kas loodud avariikäivituse andmekandjat saab kõikides arvutites, mille jaoks see koostati, ka reaalselt kasutada. Lisaks tuleb olenevalt operatsioonisüsteemist arvestada veel ka täiendavate süsteemi eripäradega, mille kohta leiate infot asjakohastest moodulitest.

Pärast sihtsüsteemis tehtud muudatusi, nt pärast operatsioonisüsteemi värskenduste paigaldamist või pärast konfiguratsiooni muutmist, tuleb vajaduse korral värskendada ka avariikäivituse andmekandjat ja sinna salvestud dokumentatsiooni.

Avariikäivituse andmekandjas tehtud muudatused tuleb dokumenteerida. Avariikäivituse andkandjat tuleb testida! Avariikäivituse andmekandja peab olema süsteemi hooldajatele kättesaadav, et tõrgete korral ei läheks palju väärtuslikku aega kaotsi. Teiselt poolt jällegi tuleb seda hoida võimalikult turvalises kohas, et volitamata isikud ei pääseks sellele ligi.

Avariikäivituse andmekandja töökorda tuleks regulaarselt testida, samuti tuleks harjutada sinna salvestatud programmide kasutamist, et avariiolukorras oleks tagatud selle töötamine ja administraatorid oskaksid sellega ümber käia. Andmekandja kohta on soovitatav koostada ja välja trükkida lühiülevaade, mida tuleks hoida käepärast ning mis peaks sisaldama selle tüüpilisi kasutusvaldkondi ja tähtsamaid rakendusmeetmeid.

Kontrollküsimused:

- Kas iga arvutitüübi ja operatsioonisüsteemi versiooni kohta on koostatud avariikäivituse andmekandja?
- Kus hoitakse vastavat andmekandjat? Kas administraatorid pääsevad sellele kiirelt ligi?
- Kas avariikäivituse andmekandjate töökorda kontrollitakse regulaarselt?

M 6.26 Kodukeskjaama (PBX) konfiguratsiooniandmete regulaarne varundus

Algatamise eest vastutavad: kodukeskjaama eest vastutav töötaja

Rakendamise eest vastutavad: administraator

Kodukeskjaama konfiguratsiooni- ja kasutusandmeid tuleb regulaarsete ajavahemike tagant varundada, eriti pärast nende muutmist. Selleks tuleb välja töötada vastav kontseptsioon ja ühitada see andmevarunduse üldpoliitikaga (vt B 1.4 Andmevarunduspoliitika).

Kuna kodukeskjaama konfiguratsiooniandmete varundamine sarnaneb võrgu aktiivkomponentide varundamisega, võib kontseptsiooni koostamisel sellest lähtuda (vt M 6.52 Võrgu aktiivkomponentide konfiguratsiooniandmete regulaarne varundamine). Hübriid- või VoIP-keskjaama puhul võib süsteemi paigaldada ja seda konfigureerida süsteemikujutise , hetktõmmise, tarkvara- ja konfiguratsioonivarunduse kaudu (vt M 6.101 IP-kõne (VOIP) andmevarundus).

Varundada tuleks ka kasutusandmeid nagu kontaktinfo või arvelduskuupäevad. Varundusaja ja viisi valikul tuleks lähtuda maksimaalse lubatava andmekao nõuetest. Vastavad punktid tuleb sätestada IT-valdkonna keskses andmevarundusplaanis. Oluline on, et igal juhul oleks rakendatavate meetmete abil võimalik taastada enne rikke või hädaolukorda toimumist kehtinud andmete seis. Regulaarsete ajavahemike tagant tuleks kontrollida, kas praktikas on võimalik varundatud andmete abil süsteemi funktsioneerimisvõimelisust taastada. Sel juhul tuleks kontrollida:

- kas varundatud andmed on andmekandjal loetavad ja
- kas varundatud andmeid saab süsteemi või asendusriistvarale tagasi paigaldada.

Läbiviidud testid ja nende tulemused tuleks dokumenteerida.
Täiendavad kontrollküsimused:

- Kas keskjaama konfiguratsiooniandmete varundus viidi läbi pärast jaama kasutuselevõttu, aga ka pärast igat muudatust, ning kas seda tehakse regulaarsete ajavahemike järel?
- Kas on koostatud keskjaama kontseptsioon ja kas see on ühitatud serveri ja võrgukomponentide üldise andmevarunduskontseptsiooniga?
- Kas testitakse, et keskjaama varundatud andmeid saab ka tõepoolest kasutada süsteemi taastamiseks?

M 6.27 BIOS-süsteemi turvaline värskendamine

Algatamise eest vastutavad: IT turvaosakond, IT-juht
Rakendamise eest vastutavad: administraator, kasutaja

Basic Input-Output System

Paljud IT-süsteemid, nt PCd, vajavad käivitamiseks ja töötamiseks põhimist sisend-väljundsüsteemi (Basic Input-Output System, BIOS). BIOS koosneb programmikoodist ja andmetest, mille otstarve on teha süsteemis olulisi konfiguratsiooniseadistusi ning võimaldada elementaarsete sisend-/väljundfunktsioonide kasutamist. Paljudel juhtudel käivitatakse selle funktsiooniga IT-süsteemi operatsioonisüsteem, mis võtab seejärel kontrolli riistvara üle enda peale või suhtleb sellega jätkuvalt BIOS-funktsioonide vahendusel. BIOS salvestatakse tavaliselt spetsiaalsetesse mälukiipidesse (nt EEPROMi või Flash-EPROMi), mille sisu jääb alles ka pärast elektritoite väljalülitamist.

BIOS võib sisaldada vigu

Eriti just PCde puhul on konfigureerimisvõimaluste rohkus viinud selleni, et BIOS on muutunud väga keeruliseks ning seetõttu ka vastuvõtlikumaks erinevatele vigadele. Paljud tootjad on seetõttu võtnud kasutusele BIOSi uuendusmehhanismi ning väljastavad regulaarselt BIOSi versioone, mis on vigadest puhastatud. BIOS-värskenduste sisseviimiseks on tootjad loonud sageli ka spetsiaalsed programmid, millega on võimalik vastavate mälukiipide sisu üle kirjutada.

Vana BIOSi varundamine

BIOSi värskendusmehhanismi tasub enamasti kasutada, et varustada IT-süsteeme võimalikult veavabade BIOSi versioonidega.

Siinkohal tuleks aga arvestada järgmiste aspektidega:

- Esimese sammuna tuleks hetkel installeeritud BIOSist teha varukoopia. Tavaliselt pakub tootjatarkvara selleks võimalust BIOSi väljalugemiseks ja faili kujul salvestamiseks. Juhul kui pärast BIOSi värskendamist peaks esinema probleeme, on võimalik vana BIOSi versiooni taastada.
- Tsentraasete süsteemide BIOSi arhiveerimine – tsentraalsete IT-süsteemide, nagu nt serverite võrguühenduselementide ja kodukeskjaamade puhul tuleks süsteemides kasutatavad BIOSi versioonid ja kasutatavale versioonile eelnenud töövõimeline BIOSi versioon arhiveerida. Siinkohal tuleb jälgida, et faile oleks võimalik siduda üheselt vastava IT-süsteemiga, mille juurde see kuulub.
- Tähtsamate seadistuste dokumenteerimine – BIOSi värskendamine mõjutab paljudel juhtudel salvestatud konfiguratsiooniandmeid. Olenevalt olukorrast võidakse värskenduse käigus eelnevad seadistused asendada standardsete väärtustega ja seetõttu lähevad seadistused kaotsi. Tänapäevane PCdele mõeldud BIOS on küll võimeline paljusid konfiguratsiooniandmeid ka iseseisvalt tuvastama (auto detect), kuid eriti just spetsiaalsete seadmete

puhul võib olla siiski vajalik kasutuses olnud seadistused enne BIOSi värskendamist dokumenteerida. Siinkohal tuleks järgida tootjafirma soovitusi.

- BIOS-värskenduse hankimine usaldusväärsest allikast – tootjad panevad oma BIOS-värskendused ja nende paigaldamist võimaldava tarkvara tihti üles internetikeskkonda. Siinkohal tuleks jälgida, et mõlemat hangitaks kas otse tootjate endi käest või siis ametlikest peegelserveritest. Kahtluse korral tuleks tootja käest järele küsida, kas teatud internetikeskkonnas saadaolev versioon on ka tegelikult vastava tootja heakskiiduga.
- Võimalike varuvariantide käepärast hoidmine – ühilduvusprobleemid ja kahjustada saanud failid võivad olla põhjusteks, miks IT-süsteem ei pruugi enam pärast BIOSi värskendamist korralikult tööle hakata. Tihti pole sellistel juhtudel BIOSi võimalik taastada ka eelnevas, toiminud versioonis. Tavaliselt suudavad IT-seadet seejärel töökorda seada ainult kas edasimüüja või seadme tootja ning võib juhtuda, et sellest tingituna pole vastavat seadet võimalik pikka aega kasutada. Seetõttu peab olema enne BIOSi värskendamist tagatud, et juhul, kui seadme rivist väljalangemist pole võimalik pikka aega taluda, saaks vajaduse korral kasutada mõnda avariilahendust (nt asendusseadet).
- Uued BIOSi versioonid tuleb võimalikult põhjalikult läbi testida – enne kasutuselevõttu tuleks uued BIOSi versioonid võimalikult korralikult läbi testida. See on võimalik ainult sellisel juhul, kui eksisteerib mitu IT-süsteemi, mis töötavad ühe ja sama BIOSiga. Sellise võimaluse korral tuleks BIOSi uus versioon installeerida korraga ainult ühele nendest süsteemidest ja selle süsteemi tööd teatud aja jooksul jälgida. Kui jälgimise ajal ei tuvastata probleeme, võib kaasata ka kõik ülejäänud süsteemid. Mõned tootjad ei soovita oma seadmetes kasutada mitte lihtsalt kõige uuemat BIOSi versiooni. Selle asemel on välja töötatud tabelid, kus loetletakse erinevaid BIOSi versioone kas kasutusvaldkonna või mudeli numbri alusel. Peamiselt on sellest puudutatud võrguühenduselemendid. Tootjafirmade soovi tuleks järgida.

Kontrollküsimused:

- Kas enne BIOSi värskendamist leiab aset olemasoleva BIOSi versiooni varundamine?
- Kas BIOSi värskendused hangitakse eranditult usaldusväärsetest allikatest?
- Kas BIOSi värskendamise puhul järgitakse tootjafirmade soovitusi?

M 6.29z Hädaabikõnede avariiliin

Algatamise eest vastutavad: kodukeskjaama eest vastutav töötaja

Rakendamise eest vastutavad: administraator

Kodukeskjaama täieliku või osalise avarii puhul võib juhtuda, et läbi selle seadme ühendatud ametiliinide kaudu ei ole võimalik luua enam mitte ühtegi ühendust. Et abi oleks võimalik kutsuda ka avariiolukorras, oleks mõistlik sisse seada täiesti eraldi baasühendus ehk analoogne kaugkõneühendus.

Täiendavad kontrollküsimused:

- Kuidas võimaldatakse hädaabikõnede tegemist kodukeskjaama avarii puhul?

M 6.31 Protseduurid süsteemi tervikluse kao puhuks

Algatamise eest vastutavad: IT-turvaosakond, IT-juht

Rakendamise eest vastutavad: administraator, kasutaja

Väärkasutusesarnane kasutus

Juhul, kui Unix-süsteem ei käitu nii nagu peaks, nt süsteem käitub arusaamatult, süsteemist pole võimalik leida vajalikke andmeid, failide sisu on muudetud, salvestusmaht väheneb pidevalt, ilma et midagi salvestataks, võib olla tegemist süsteemi tervikluse kaoga. See võib olla põhjustatud süsteemi väärast kasutamisest, nt süsteemiseadistuste muutmisest, Trooja hobusest või mõnest arvutiviirusest. Neil juhtudel peaksid kasutajad arvestama järgnevate punktidega:

- Ärge sattuge paanikasse!
- Säilitage rahu!
- Teavitage olukorrast administraatorit.
- Sulgege töötavad programmid.

Administraator peaks teostama järgnevad sammud:

- Süsteemi väljalülitamine - Süsteemi sisselülitamine tuleb läbi viia selliselt, et juurdepääs oleks võimalik ainult konsooli kaudu (nt Single-User -režiimis)
- Andmete täielik varundamine - Andmete täieliku varukoopia loomine (sellest on kasu nt siis, kui järgneva analüüsi käigus peaksid mõned andmed või jäljed kahjustatud saama)
- Käitusfailide kontrollimine - Käitusfailide kontrollimine silmnähtavate muudatuste suhtes, nt loomiskuupäeva ja failisuuruse muudatused (kuna ründaja võib neid taastada oma algsetele väärtustele, tuleks failide terviklust kontrollida kontrollsumma protseduuriga nagu nt tripwire)
- Originaalfailide taaspaigaldamine - Käitusfailide kustutamise ja originaalfailide taaspaigaldamise kohta kirjutuskaitsega varustatud andmekandjatelt (vt M 6.21 Kasutatava tarkvara varukoopia) tuleb meeles pidada, et äsja loodud varukoopiale ei tohi uuesti paigaldada mitte ühtki programmi.
- Süsteemikaustade, süsteemifailide ja nende atribuutide kontrollimine ja vajadusel uuestipaigaldamine (nt. /etc/inetd.conf , /etc/hosts.equiv , cron- ja at-jobs, jne)
- Atribuutide kontrollimine - Kõikide kasutajakataloogide ja kasutajafailide atribuutide kontrollimine nt kontrollsummaprotseduuriga nagu tripwire ning vajadusel nende taastamine minimaalsetele seadistustele (volitused ainult omanikele, root -failide keelamine kasutajakeskkondades, .rhost - ja .forward -failid, ka tõkestatud kontod)
- Kõikide paroolide muutmine
- Kõikide kasutajate teavitamine sooviga, et nad kontrolliksid ebareeglipärasuste ilmnemist oma kasutusvaldkonnas
- Uute paroolide juhuslik genereerimine - Pärast kõikide paroolide muutmist tuleb sellest puudutatud kasutajatele ka teada anda. Siinkohal ei tohi kasutada mitte ühtegi parooli, mis on kõikidele kasutajatele teada, või nende

ühtset tuletamisskeemi. Parem on paroolid genereerida juhuslikkuse põhimõttest lähtuvalt ja need kasutajatele turvaliselt üle anda, nt suletud ümbrikus. Vastavad paroolid tuleb kohe pärast esimest sisselogimist ära muuta.

- Teavitamisplaani kasutamine - Kui peaks ilmnema, et Unix-süsteemi suhtes pannakse toime ettekavatsetud rünne, on kahjude minimeerimiseks ja võimalike täiendavate kahjude ärahoidmiseks tarvis kiiresti tegutseda. Selleks on vaja teavitamisplaani, mis sisaldab loetelu kõikidest vajalikest sammudest ja määratleb, milliseid isikuid tuleb vastavast intsidendist informeerida (vt M 6.60 Turvaintsidentide käsitlusprotseduurid ja teavitamiskanalid). Teavitamisplaan võiks sisaldada vajadusel infot ka selle kohta, kas ning mil moel tuleks protsessi kaasata ka andmekaitsespetsialist ja organisatsiooni juristid.

Juhul, kui andmeid on kustutatud või soovimatul moel muudetud, on neid võimalik varukoopiate abil taastada.

Täiendavad kontrollküsimused:

- Kas kasutajaid informeeritakse regulaarselt selle kohta, et ebakorrapärasuste ilmnemisel on kohustuslik sellest kohe informeerida administraatorit?
- Kas seda ettekirjutust järgitakse?
- Kas on olemas vastavate teadmistega administraatorid?
- Kas paroolide kiireks väljajagamiseks on kasutusele võetud asjakohane protseduur ning kas seda on piisavalt testitud?

M 6.32 Regulaarne andmevarundus

Algatamise eest vastutavad: IT-juht, IT turvaosakond
Rakendamise eest vastutavad: administraator, kasutaja

Andmekadude vältimiseks tuleb andmeid regulaarselt varundada. Enamikes arvutisüsteemides on võimalik rakendada selleks automaatselt toimivaid varundamisprotsesse.

Kindlaks tuleb määrata reeglid, milliseid andmeid tuleb erinevatel ajahetkedel varundada. Varukoopiad tuleb luua regulaarselt vähemalt nendest andmetest, mida ei ole võimalik muu info põhjal tuletada. Dokumentatsioone, programmikirjeldusi ja programmi töökirjeldusi tuleb meetme M 2.111 Juhendite käepärast hoidmine kohaselt käepärast hoida. Soovitatav on koostada andmevarunduskontseptsioon.

Olenevalt sellest, kui suures koguses erineva tähtsusega andmeid jooksvalt salvestatakse ja sellest, kui suurt kahju nende kaotsiminek endast kujutab, tuleb kindlaks määrata järgnevad aspektid:

- Ajaline intervall – näited: iga päev, iga nädal, iga kuu
- Ajahetk – näited: öösiti, reede õhtul
- Säilitatavate andmegeneratsioonide arv – näide: kui täielik varundus tehakse iga päev, hoitakse alles viimased seitse varundust ja lisaks nendele ka kahe viimase kuu reede õhtuti tehtud andmevarundused.
- Varundamisele kuuluvate andmete hulk – kõige lihtsam on kindlaks määrata regulaarsesse andmevarundusse kaasatavad partitsioonid või kataloogid. Sobiva eristamise abil on võimalik suurendada ülevaatlikkust ning töövaeva ja kulusid kokku hoida. Näide: enda loodud failid ja individuaalsed konfiguratsioonifailid
- Salvestusvahendid (sõltuvad andmete hulgast) – näited: lindid, kassetid, CDd või DVDd, kõvakettad
- Andmekandjate kustutamise kord enne nende uuesti kasutamist (nt lintide ja kassettide puhul)
- Teostuse eest vastutavad isikud (administraator, kasutaja)
- Vastutusalad seoses varunduse seirega, eriti automaatse andmevarunduse puhul (veateated, salvestusvahendite olemasolev salvestiruum)
- Loodud andmevarunduste dokumentatsioon (kuupäev, läbiviidud varunduse liik ja selleks valitud parameetrid, andmekandjate märgistamine).

Astmeline varundamine

Kuna täieliku andmevarunduse loomine on küllaltki töömahukas, suudetakse seda läbi viia maksimaalselt kord päevas. Andmeid, mis on tekkinud pärast andmete viimase varukoopia loomist, ei ole võimalik taastada. Sel põhjusel ning ka kulude kokkuhoiu otstarbel tuleks täielike andmevarunduste vahel läbi viia astmelisi andmevarundusi, mis tähendab, et varukoopiad luuakse vaid nendest

andmetest, mis on tekkinud pärast viimase täieliku andmevarunduse loomist (kui kahe täieliku andmevarunduse vahel viiakse läbi mitu astmelist andmevarundust, võib varundamisse kaasata ainult pärast viimast astmelist varundust tekkinud uued andmed). Astmelist andmevarundust võib läbi viia tihedamini, nt kohe pärast oluliste failide koostamist või ka mitu korda päevas.

Siinkohal tuleb tagada, et see ei häiriks igapäevaseid tööprotsesse. Eraldi otsus tuleb langetada kasutatava tarkvara kohta, kas kaasata see regulaarsesse varundusse või mitte. Otsus sõltub nt sellest, kui töömahukas on tarkvara reinstalleerimine originaalandmekandjatelt ning paikade ja värskenduste paigaldamine. Mõningatel juhtudel võib olla täiesti piisav, kui luua varukoopiad ainult originaalandmekandjatest.

Andmevarundusi tuleb regulaarselt testida, et välja selgitada, kas need töötavad soovitud kujul, ning ennekõike, kas varundatud andmeid on võimalik ilma probleemideta taastada.

Kasutajate informeerimine
Kõik kasutajad peaksid olema teadlikud andmevarunduses kehtivatest põhimõtetest, et nad suudaksid muu hulgas anda nt tagasisidet võimalike puudujääkide kohta (nt vajadusest pikema intervalli järele) ja võtta individuaalseid meetmeid (nt oma kõvaketta andmeid vahepeal peegeldada). Kasutajaid on oluline informeerida ka sellest, kui pikast varundusperioodist on võimalik andmeid taastada. Juhul kui täielik varundamine toimub ainult kord kuus ning säilitatakse ainult kaks viimast andmegeneratsiooni, jääb olenevalt andmekao tekkimise ajahetkest vajalike andmete taastamiseks aega ainult umbes kaks kuni kolm nädalat.

Konfidentsiaalsete andmete krüpteerimine
Kui võrguarvutite puhul varundatakse ainult serverikettaid, tuleb tagada, et varundamisele kuuluvad andmed salvestataks ka reaalselt vastavatele serveritele kas kasutajate endi poolt või automaatselt. IT-süsteemide või IT-koosluse suurema muutuse korral tuleb vastavalt muuta ja kohandada ka andmete varukoopiate loomise protsessi. Konfidentsiaalsed andmed tuleks enne varundamist krüpteerida, kusjuures tuleb arvestada, et andmeid peab olema võimalik dekrüpteerida pikema aja möödumisel (vt M 6.56 Andmevarundus krüptoprotseduuride kasutamisel). Andmete väljatrükk ei ole andmete varundamiseks sobiv viis.

Kontrollküsimused:

- Kas iga arvuti kõik andmed on varundatud?
- Kas andmevarundusi on kontrollitud?
- Kas andmevarundusprotseduur on dokumenteeritud?
- Kas andmevarunduseks kasutatav protseduur on kooskõlas olemasoleva andmevarunduskontseptsiooniga?
- Kas kõikide IT-süsteemide või IT-koosluse suuremate muutustega kaasneb vajaduse korral andmevarundusprotsessi kontroll ja kohandamine?

M 6.33 Andmevarunduskontseptsiooni loomine

Algatamise eest vastutavad: IT turvaosakond

Rakendamise eest vastutavad: IT turvaosakond, IT-juht, üksikute IT-rakenduste eest vastutavad töötajad

Andmete varundamiseks kasutatavat protseduuri mõjutab suur hulk erinevaid tegureid. IT-süsteem, andmete hulk, andmete muutumise sagedus ja käideldavusnõuded on mõned nendest. Andmevarunduskontseptsiooni eesmärk on leida lahendus, kuidas arvestada piisavalt kõigi mõjufaktoritega ja jääda samas majanduslikult talutavatesse kulupiiridesse. Andmevarunduse läbiviimise tehniliste võimaluste valik on väga lai. Valik sõltub aga alati eespool loetletud tegureist. Seetõttu tuleb esmalt kindlaks teha, millised on erinevate IT-süsteemide ja nende abil töötle pandud IT-rakenduste osatähtsused ning need kõigile arusaadavalt dokumenteerida. Seejärel tuleb välja töötada ja dokumenteerida neile sobivad protseduurid. Lõpetuseks peab ametiasutuse või ettevõtte juhtkond vastu võtma otsuse nende rakendamise kohta. Toimiva andmevarundusprotsessi tagamiseks peab andmevarunduskontseptsioon kehtestama kohustuse harjutada andmete taastamist ka praktikas. Tulemused peaksid leidma oma koha andmevarunduskontseptsioonis selliselt, et neid oleks võimalik värskendada ja täiendada.

Järgnev andmevarunduskontseptsiooni sisukord on toodud näitena kontseptsiooni ühe võimaliku ülesehituse kohta:

Andmevarunduskontseptsiooni sisukord:

1 – Definitsioonid

- Rakendusandmed, süsteemiandmed, tarkvara, logiandmed
- Täielik andmevarundus, astmeline andmevarundus

2 – Vastuvõtlikkus ohtudele ja motivatsioon

- Institutsiooni sõltuvus andmete kättesaadavusest
- Tüüpilised ohud, nagu ebapiisavalt koolitatud kasutajad, ühiselt kasutatavad andmehulgad, arvutiviirused, häkkerid, elektrikatkestus, kõvaketta rikked
- Institutsiooni puudutavate kahjude põhjused
- Seni esinenud kahjud

3 – Mõjurid IT-süsteemide lõikes

- Varundamisele kuuluvate andmete spetsifikatsioon
- IT-rakenduste nõuded andmete kättesaadavusele
- Andmete taastamisega seotud vaev, kui andmeid ei varundataks
- Andmemahud
- Muudatuste mahud
- Andmete muutmise ajahetked
- Tähtajad
- Andmete konfidentsiaalsusnõuded
- Andmete terviklusnõuded
- IT-kasutajate teadmised ja andmetöötlusega seotud võimed

4 – Andmevarundusplaan IT-süsteemide lõikes

- Määratlus andmeliigi põhjal
- Andmevarunduse liik
- Andmevarunduse sagedus ja aeg
- Andmegeneratsioonide arv
- Andmevarunduseks kasutatav andmekandja
- Andmevarundusega seotud vastutusalad
- Varukoopiaid sisaldavate andmekandjate hoiukoht
- Andmevarundusarhiivile esitatavad nõuded
- Transporditingimused
- Taastamisele kuluv aeg, kui andmed on varundatud
- Varundatud andmete taastamisprotseduuri määratlemine
- Andmevarundusarhiivile esitatavad raamtingimused
- Lepingutingimused (väliste arhiividega)
- Varundatud andmete värskendamistsüklid
- Inventari loetelu
- Varundatud andmete kustutamine
- Defektsete andmekandjate hävitamine
- Funktsioneerivate lugemisseadmete varu hoidmine

5 – Minimaalse andmevarunduse kontseptsioon
6 – Töötajate kaasamine andmevarundusse
7 – Pistelised taastamisharjutused

Andmevarunduskontseptsiooni erinevaid punkte kajastatakse lähemalt meetmetes M 2.41 Töötajate kaasamine andmevarundusse , M 6.34 Andmevarunduse mõjutegurite määratlemine , M 6.35 Andmevarunduseks vajalike protseduuride määratlemine ja M 6.37 Andmevarunduse dokumenteerimine . Loetletud meetmete läbitöötamisega on võimalik koostada iga olulisema IT-süsteemi kohta oma kasutajapõhine andmevarunduskontseptsioon.

Kontrollküsimused:

- Kas institutsioonil on olemas dokumenteeritud värske andmevarunduskontseptsioon?
- Kas kontseptsioonis esitatakse kõik selle valdkonna alla kuuluvad IT-süsteemid?
- Kuidas toimub töötajate teavitamine seoses neid puudutava kontseptsiooni osaga?
- Kas kontseptsiooni järgimist kontrollitakse?
- Kuidas arvestatakse mõjufaktorite võimalikku muutumist?

M 6.34 Andmevarunduse mõjutegurite määratlemine

Algatamise eest vastutavad: IT turvaosakond

Rakendamise eest vastutavad: administraator, üksikute IT-rakenduste eest vastutavad töötajad

Iga tähtsama IT-süsteemi ja mõningatel juhtudel ka iga IT-rakenduse kohta tuleb tuvastada alljärgnevalt kirjeldatud mõjutegurid. Nende väljaselgitamiseks võib küsitleda süsteemiadministraatoreid ja IT-rakenduste eest vastutavaid töötajaid. Küsitluse tulemused tuleb kõigile arusaadaval kujul kirja panna. Alljärgnevalt on püütud fiktiivse näite põhjal selgitada, kuidas võiks mõjurite tuvastamine praktikas välja näha. Näites on vaatluse alla võetud serveri toega LAN, mille külge on ühendatud 10 PCd, mis töötavad tööjaamadena. IT-süsteemi ülesanne on tellimuste töötlemine, kasutades selleks klientide andmebaasi. Rakendusandmed salvestatakse tsentraalselt võrguserverile. Üksikasjadesse laskudes tuleks välja selgitada järgmised aspektid:

Varundamisele kuuluvate andmete spetsifikatsioon

Välja tuleks selgitada IT-süsteemi (IT-rakenduse) andmete hulk, mida läheb tarvis ettenähtud ülesannete täitmiseks. Siia alla kuuluvad rakendus- ja käitustarkvara, süsteemifailid (nt lähtestusfailid, makrodefinitsioonid, konfiguratsiooniandmed, tekstimoodulid, paroolifailid, juurdepääsuõiguste failid), rakendusandmed ise ja logiandmed (sisselogimisprotseduuri logi, turvaintsidentide logid, andmeedastuse logid).

Näidistulemus nr 1: varundamisele kuuluvate andmete spetsifikatsioon

IT-süsteem: serveritoega LAN, mille külge on ühendatud 10 PCd

Varundamisele kuuluvad andmed:

- tarkvara: võrgukäitustarkvara, PCde operatsioonisüsteemid, tekstitöötlustarkvara, andmebaasitarkvara jms tüüptarkvara;
- süsteemiandmed;
- võrguserver: süsteemi puudutavad seadistused (nt volituste struktuur, paroolid);
- PCd: tekstitöötlustarkvara ja andmebaasitarkvara lähtestusfailid, makrodefinitsioonid ja tekstimoodulid;
- võrguserveri rakendusandmed: kirjavahetusega seotud failid ja klientide andmebaas;
- võrguserveri logiandmed: võrgusündmuste logimine.

IT-rakenduste nõuded andmete kättesaadavusele

Seejärel tuleb kindlaks teha esimeses etapis tuvastatud andmete käideldavusnõuded. Üks läbiproovitud mõõdupuid on siinkohal maksimaalselt talutav seisakuaeg (MTS). Nimetatud väärtus annab infot selle kohta, millise aja jooksul on võimalik jätkata vajaliku tööülesande täitmisega, ilma et oleks tarvis hakata kasutama andmetest loodud varukoopiaid. Siinkohal tuleks arvestada ka sellega, kas

lühiajaliselt on võimalik edasi töötada ka ilma IT-toeta, kasutades selleks paberit ja kirjutusvahendit.

Näidistulemus nr 2: nõuded käideldavusele

- tarkvara: MTS 1 päev;
- süsteemiandmed: võrguserver: MTS 1 päev, PC: MTS 1 nädal (ühest PCst on võimalik loobuda kuni üks nädal);
- rakendusandmed: kirjavahetusega seotud failid: MTS 1 nädal, klientide andmebaas: MTS 1 päev;
- logiandmed: MTS 3 päeva.

Andmete taastamisega seotud vaev, kui andmeid ei varundataks

Majanduslikest vaatepunktidest talutava andmevarunduskontseptsiooni väljatöötamiseks on vaja tingimata teada, kas ja millise vaevaga on võimalik rikutud andmehulki taastada juhul, kui selleks ei saa kasutada varundatud andmeid. Tuleks välja selgitada, millistest allikatest oleks võimalik andmeid taastada. Sellekohaste näidetena võib välja tuua dokumentatsiooni seisu, väljatrükid, mikrofiššid, küsitlused ja järelepärimised. Mõõta tuleks rahalist väljaminekut või kulutusi, mis kaasnevad andmesisestusega tegelevate töötajatega tööpäevades (TP).

Näidistulemus nr 3: rekonstrueerimise keerukus

- tarkvara: uue tarkvara hankimine, st ostmine ja sellele järgnev installeerimine ühe päeva jooksul (juhul kui originaaltarkvara enam pole);
- süsteemiandmed: võrguserver: käsitsi taastamine: 1 TP, PC: 1 TP;
- rakendusandmed: kirjavahetusega seotud failid: sihipärane andmesisestus värskete paberdokumentide alusel: 10 TP (kirjavahetuse täies mahus taastamine ei ole vajalik), klientide andmebaas: täies mahus uuesti koostamine paberdokumentide alusel: 10 TP;
- logiandmed: pole taastatavad, kuna väljatrükid puuduvad.

Andmemahud

Andmekandjate valikul on üks otsustavaid tegureid salvestatavate ja varundatavate andmete hulk. Kogutav informatsioon puudutab ainult varundamisele kuuluvaid andmeid ning selle kajastamiseks tuleks mõõtühikuna kasutada megabaite (MB).

Näidistulemus nr 4: andmemahud

- tarkvara: 100 MB;
- Süsteemiandmed: võrguserver: 2 MB, PC: 0,3 MB;
- rakendusandmed: kirjavahetusega seotud failid: 100 MB, klientide andmebaas: 10 MB;
- logiandmed: 10 MB (iganädalane kontroll ja kustutamine).

Muudatuste mahud

Andmevarunduse vajaliku sageduse ja adekvaatse varundamisprotseduuri kindlakstegemiseks peab olema teada, kui paljud andmed/failid võivad teatud kindla aja jooksul muutuda. Võrreldava suurusena oleks siinkohal mõeldav kasutada näitajat MB/nädal. Ilmtingimata on tarvis teada, kas olemasolevate andmete sisu on muutunud või kas uusi andmeid on juurde tekkinud.

Näidistulemus nr 5: muudatuste mahud

- tarkvara: keskmiselt 50 MB versioonivahetuse korral, maksimaalselt kord aastas;
- süsteemiandmed: võrguserver: 0,1 MB/nädal, PC: 0,1 MB/nädal;
- rakendusandmed: kirjavahetusega seotud failid: 1 MB/nädal, uued, juurde tekkivad failid; klientide andmebaas: 10 MB/nädal, andmebaasi muudatuste arvelt (andmebaasi on võimalik varundada ainult täies mahus);
- logiandmed: 10 MB/nädal.

Andmete muutmise ajahetked

IT-rakenduste hulgas leidub ka selliseid, mille muudatused leiavad aset ainult teatud kindlatel tähtaegadel, nagu nt palgaarvestuse arvutuskäigud kalendrikuu lõpus. Sellistel juhtudel on andmeid kõige mõistlikum varundada vahetult pärast asjakohaste protsesside lõppemist. Seetõttu tuleks varundatavate andmete puhul ära märkida, kas need muutuvad iga päev, iga kuu või hoopis mõnedel muudel kindlatel tähtaegadel.

Näidistulemus nr 6: muudatuste ajahetked

- tarkvara: muudatused leiavad aset ainult versiooni vahetumisel;
- süsteemiandmed: sagedased muutused;
- rakendusandmed: kirjavahetusega seotud failid: igapäevane muutus; klientide andmebaas: igapäevane muutus;
- logiandmed: pidev muutus.

Tähtajad

Andmete puhul tuleb selgeks teha, kas nendega ümberkäimisele on kehtestatud kindlad tähtajad. Siinkohal võib olla tegu nt säilitamis- või kustutamiskohustustega, mis tulenevad isikuandmeid kajastavate andmete käitlemisest. Andmevarunduspõhimõtete kehtestamisel tuleb vastavate tähtaegadega arvestada.

Näidistulemus nr 7: tähtajad

- tarkvara: varundatud andmemahtude hoidmine ei ole vajalik;
- süsteemiandmed: varundatud andmemahtude hoidmine ei ole vajalik;
- rakendusandmed: kirjavahetusega seotud failid: raamatupidamisdokumentide säilitamiskohustus kuus aastat; selle aja jooksul tuleb säilitada üks (aasta) andmevarundus; klientide andmebaas: andmete säilitamine pole vajalik, kustutamise tähtajad riikliku andmekaitseseaduse alusel;
- logiandmed: pärast iganädalast logiandmete analüüsimist tuleb andmeid säilitada reeglina 2 MB ulatuses kas terve aasta või seni, kuni andmekaitsespetsialist need läbi kontrollib.

Andmete konfidentsiaalsusnõuded

Iga faili konfidentsiaalsusnõue kandub andmevarundusel üle andmete varukoopiale. Sama konfidentsiaalsusastmega andmetest loodud varukoopiate kokkukogumisel võib salvestatud andmete konfidentsiaalsusnõue suureneda. Seega tuleb ära märkida, kui suur on üksikute varundamisele kuuluvate andmete konfidentsiaalsusnõue ja lisaks, milliste andmekombinatsioonide puhul kasvab konfidentsiaalsusnõue suuremaks kui andmete enda konfidentsiaalsusnõue eraldi vaadelduna.

Näidistulemus nr 8: konfidentsiaalsusnõuded

- tarkvara: madal konfidentsiaalsusnõue, kuna tegemist on valikuliselt ligipääsetavate andmetega, arvestada tuleb ainult autoriõigusi puudutavaid kokkuleppeid;
- süsteemiandmed: võrguserver: keskmine konfidentsiaalsusnõue (paroolid on salvestatud krüpteeritult), PC: konfidentsiaalsusnõue puudub;
- rakendusandmed: kirjavahetusega seotud failid: üksikutele failidele kehtib keskmine konfidentsiaalsusnõue, kõikidele failidele kokku kehtib kõrge konfidentsiaalsusnõue; klientide andmebaas: kõrge konfidentsiaalsusnõue;
- logiandmed: kõrge konfidentsiaalsusnõue (isikuandmetega seotud andmed, mis võimaldavad luua kasutajaprofiili).

Andmete terviklusnõuded

Andmevarunduse otstarbel peab olema tagatud, et andmed on salvestatud terviklikult ja et neid ei muudetaks säilitusaja jooksul. Mida kõrgemad on kasutajaandmete terviklusvajadused, seda tähtsamad on need nõuded. Seetõttu tuleb andmevarunduse jaoks ära märkida, kui kõrgete terviklusnõuetega on tegemist.

Näidistulemus nr 9: terviklusnõuded

- tarkvara: tarkvara peab vastama kõrgetele terviklusnõuetele;
- süsteemiandmed: võrguserver: kõrged terviklusnõuded (õiguste haldamise tõttu), PC: kõrged terviklusnõuded;
- rakendusandmed: kirjavahetusega seotud failid: üksikute failide suhtes kehtib keskmine terviklusnõue; klientide andmebaas: kõrged terviklusnõuded;
- logiandmed: kuni analüüsimiseni kehtib andmetele kõrge terviklusnõue, pärast analüüsimist kehtivad keskmised terviklusnõuded ainult nendele andmetele, mis kuuluvad säilitamisele.

IT kasutajate teadmised ja andmetöötlusega seotud võimed

Otsustamaks, kes on piisavalt pädevad andmevarundusi tegema, kas nt IT kasutajad ise või spetsiaalselt selleks kohustatud töötajad või süsteemiadministraatorid, on määrava tähtsusega, millised on töötajate teadmised ja andmetöötlusalased kogemused ning milliseid tööriistu on võimalik nende käsutusse anda. Juhul kui andmevarunduste tegemine on IT kasutajate jaoks ajaliselt liiga koormav, tuleks see ära märkida.

Näidistulemus nr 10: teadmised

- võrguserveri andmete varundamiseks on piisavad teadmised võrguadministraatoril. PCde kasutajatel on piisavad teadmised ja oskused PC süsteemiandmete iseseisvaks varundamiseks.

Kontrollküsimused:

- Kas mõjutegurite väljaselgitamisel pöörati piisavalt tähelepanu nii süsteemiadministraatoritele kui ka IT kasutajatele?
- Kuidas toimub vastavate andmete värskendamine?
- Kas vastavas värskendatud andmevarunduskontseptsioonis arvestatakse asjakohaste nõuetega õigel ajal?

M 6.35 Andmevarunduseks vajalike protseduuride määratlemine

Algatamise eest vastutavad: IT turvaosakond

Rakendamise eest vastutavad: IT turvaosakond, spetsialist

Andmevarunduse jaoks vajalike protseduuride määratlemist mõjutavad meetme M 6.34 Andmevarunduse mõjutegurite määratlemine baasil tuvastatud mõjurid. Igale IT-süsteemile ja igale andmeliigile tuleb kehtestada sobivad andmevarundusprotseduurid. Vajaduse korral tuleb siinkohal rakendada koguni erinevat lähenemist IT-süsteemi erinevatele IT-rakendustele, kui peaks selguma, et tarvis on erinevaid andmevarundusstrateegiaid, mis võib olla eriti mõttekas nt suurarvutite puhul.

Andmevarunduseks vajalike protseduuride määratlemisel tuleb arvestada järgmiste tingimustega:

- andmevarunduse liik,
- andmevarunduse sagedus ja aeg,
- andmegeneratsioonide arv,
- protseduurid ja andmekandja,
- andmevarundusega seotud vastutusalad,
- ladustuskoht,
- andmevarundusarhiivile esitatavad nõuded,
- transporditingimused,
- säilitustingimused.

Järgnev tabel on toodud näitena andmevarundusele kehtivate tingimuste ja mõjurite omavahelisest seosest, millele järgneb ka selgitus:

	Andmevara liik	Andmevara sagedus ja aeg	Andmegen arv	Protseduu ja andmekan	Andmevara seotud vastutusa	Ladustusko	Andmev. arhiivile esitatavad nõuded	Transporditingimused	Säilitustingimused
Käidelda	X	(X)	X	X	X	X	X	X	
Taastamisega seotud vaev, kui andmev. puudub		(X)	X						

Andmemahud	X		X	X		X	X	X	
Muudatuste mahud	X	X	X	X					
Andmete muutmise ajahetked	(X)	X						(X)	
Tähtajad				X			X		X
Andmete konfidentsiaalsusnõuded				(X)	X		X	X	X
Andmete terviklusnõuded			(X)	(X)	X		X	X	X
IT-kasutajate teadmised	X			X	X				

Tabel. Andmevarundus

Selgitused:

Andmevarunduse liik
Välja võib tuua järgmised andmevarunduse alaliigid:

- Täielik andmevarundus: täieliku andmevarunduse puhul luuakse teatud ajahetkel varukoopiad kõigist varundamisele kuuluvatest andmetest, mis salvestatakse mõnele lisaandmekandjale. Selle käigus ei oma tähtsust, kas pärast viimati toimunud andmevarundust on vastavad andmed muutunud

või mitte. Seetõttu vajab täielik andmevarundus palju salvestusruumi. Eeliseks on täielike andmemahtude olemasolu teatud kindla hetkeseisuga, mis muudab andmete taastamise lihtsaks ja kiireks, kuna puudutatud failid tuleb taastamiseks välja otsida ainult viimasest andmevarundusest. Juhul kui täielikku andmevarundust tehakse harva, võib juhtuda, et failides vahepeal asetleidnud laialdaste muudatuste tõttu tuleb hiljem näha palju vaeva vajaliku info uuesti kokku kogumisega.

- Astmeline andmevarundus: astmelise andmevarunduse puhul tehakse varukoopiad vastupidiselt täielikule andmevarundusele ainult sellistest failidest, mis on võrreldes viimase andmevarundusega (täieliku või astmelisega) muutunud. See hoiab kokku salvestusruumi ja andmevarundusele kuluvat aega. Andmete rekonstrueerimisele kulub reeglina rohkem aega, kuna taastamiseks tuleb kasutada mitut erineval ajahetkel loodud varundust. Astmeline andmevarundus põhineb alati täielikul andmevarundusel. Teatud ajaperioodide möödumisel luuakse täielik andmevarundus ja nende vahepeal omakorda astmelised andmevarundused. Andmete taastamisel võetakse aluseks viimane täielik andmevarundus, mida täiendavad vahepealsetel aegadel loodud astmelised andmevarundused.
- Diferentseeritud andmevarundus: diferentseeritud andmevarunduse puhul tehakse varukoopiad ainult sellistest failidest, mis on võrreldes viimase täieliku andmevarundusega muutunud. Diferentseeritud andmevarundus vajab rohkem salvestusruumi kui astmeline andmevarundus, kuid failide taastamine on seevastu lihtsam ja kiirem. Andmete taastamiseks piisab viimasest täielikust andmevarundusest ning värskest direfentsiaalvarundusest, mitte nagu astmelise andmevarunduse puhul, kus tuleb olenevalt olukorrast võibolla isegi mitu andmevarundust üksteise järel uuesti sisse lugeda.
- Teadmiseks: andmevarundusmeetodite alla liigitatakse tihti ka andmete peegeldamine. Andmete peegeldamise puhul salvestatakse andmed liiasusega ühekorraga mitmele erinevale andmekandjale. Kuna niimoodi on võimalik ühe andmekandja avarii korral ilma aega kaotamata andmeid edasi kasutada, tõstab andmete peegeldamine nende käideldavust. Siiski tuleb arvestada, et see ei asenda andmete varundamist, kuna see ei kaitse ohtude vastu, nagu vargus, tulekahju või andmete tahtmatu kustutamine.

Nimetatud andmevarundusstrateegia üks alaliike on kettapilt-andmevarundus. Kettapilt-andmevarunduse puhul ei looda varukoopiaid mitte kõvaketta üksikutest failidest, vaid kõvaketta füüsilistest sektoritest. Tegu on täieliku varundusega, mida on võimalik sarnasele kõvakettale väga kiiresti taastada.

Üks täiendavaid alaliike on veel hierarhiline salvestihaldus (HSH). Siinkohal on esiplaanil kallite salvestite võimalikult majanduslik rakendamine. Faile hoitakse olenevalt nende kasutussagedusest kas kiiretel online-salvestitel (kõvaketastel), nearline-salvestitel (automaatsetel andmekandja vahetussüsteemidel) või arhiveeritakse offline-salvestitele (magnetlintidele). Lisaks pakuvad HSH-süsteemid ka automatiseeritud andmevarundusrutiinide kasutamist, mis kujutavad endast astmelise ja täieliku andmevarunduse kombinatsiooni.

Liisasusega andmevarundust pakuvad ka RAID-süsteemid (ingl redundant array

of independent disks, sõltumatute ketaste liiasmassiiv). RAID-kontseptsioon kirjeldab mitme kõvaketta koondamist ühe nn array controller'i alla. Eristatakse erinevaid RAID tasemeid, millest RAID tase 1 tegeleb andmete peegeldamisega. RAID-süsteemid ei asenda andmetest varukoopiate tegemist! RAID-süsteemidest pole kasu ka varguse või tulekahju korral, mistõttu tuleb RAID-süsteemidele salvestatud andmeid varundada ikkagi täiendavatele andmekandjatele ja toimetada vastavad andmekandjad teistesse tuletõkketsoonidesse.

Andmevarundusstrateegia valimisel tuleks vajadusi toetava ja ühtlasi majanduslikult vastuvõetava lahenduse leidmiseks arvestada järgmiste mõjuritega:

- Käideldavusnõuded: kui käideldavusele esitatavad nõuded on väga kõrged, tuleks kaaluda andmete peegeldamist, kui käideldavusele esitatavad nõuded on kõrged, tuleks kaaluda astmelise andmevarunduse asemel hoopis täieliku andmevarunduse rakendamist.
- Andmemaht ja muudatuste maht: kui muudatuste maht vastab enam-vähem andmete enda mahule (nt andmebaasi kasutamise puhul), on astmelise varunduse pealt säästetav salvestiruum nii väike, et võiks kaaluda täieliku andmevarunduse juurutamist. Kui aga muudatuste maht on tunduvalt väiksem kui andmemaht, saab astmelise varundusega kokku hoida salvestiruumi ja seeläbi on võimalik märkimisväärselt kokku hoida ka kulusid.
- Andmete muutmise ajahetked: teatud vähesel määral võivad andmevarundusstrateegia valikut mõjutada ka andmete muutumise ajahetked. Kui on olemas kindlad ajahetkel, mille puhul on tarvis varundada terve rakenduse andmed (nt raamatupidamise otstarbel nädala, kuu või aasta lõpuseis), tuleb vastavate ajahetkede varundamiseks kõne alla vaid täieliku andmevarunduse loomine.
- IT kasutajate teadmised: andmete peegeldamise juurutamine nõuab süsteemiadministraatorilt vastavaid teadmisi, IT kasutajate puhul ei eelda see seevastu mitte mingisuguseid lisateadmisi. Täieliku andmevarunduse loomisega saab hakkama ka väheste süsteemiteadmistega IT kasutaja. Astmeline varundamine nõuab aga seevastu juba suuremaid süsteemiteadmisi ja kogemusi seoses andmevarundustega.

Andmevarunduse sagedus ja ajahetked

Andmekao tekkimisel (nt kõvaketta headcrash), tuleb andmete taastamiseks veel kord sisse viia kõik muudatused, mis on aset leidnud pärast viimase andmevarunduse loomist. Mida lühema ajavahemiku tagant andmevarundusi luuakse, seda vähem kulub reeglina aega andmete taastamiseks ja tagantjärele uuesti sisestamiseks. Samas tuleb ka arvestada, et andmevarunduse loomise ajahetke valikul ei piirdutaks ilmtingimata ainult teatud kindla perioodiga (iga päev, iga nädal, tööpäeviti), kuna varunduse loomine võib olla hädavajalik ka teatud sündmuste järel (nt pärast x arv tehinguid, pärast teatud programmi kasutamist, pärast süsteemis tehtud muudatusi).

Andmevarunduse ajahetkede sageduse valikul tuleb arvestada järgmiste mõjuritega:

- käideldavusnõuded,
- andmete taastamisega seotud vaev, kui andmevarundus puudub,
- andmemuudatuste maht.

Andmevarunduste vahele jääv ajavahemik tuleks valida selline, et taastamisele ja järelsisestamisele kuluv aeg (muutunud, andmevarunduses mittesisalduvate andmete rekonstrueerimiseks kuluv aeg) oleks väiksem kui vastavas ajavahemikus muutunud andmete (andmemahu) puhul maksimaalselt talutav seisakuaeg.

- Andmete muutmise ajahetked: kui on teada kindlad ajahetked, mil andmed võivad suures ulatuses muutuda (nt pärast palga maksmist kajastavate programmide kasutamist või pärast tarkvara versiooni vahetamist) või ajahetked, mil andmed peaksid olema täies mahus varundatud, tuleks täielik andmevarundus läbi viia vahetult pärast selliseid ajahetki. Selleks tuleb lisaks perioodiliselt läbiviidavatele andmevarundustele kindlaks määrata ka sündmustepõhiste andmevarunduste toimumisajad.

Andmegeneratsioonide arv

Ühelt poolt korratakse andmete varundamist lühikeste vaheaegade tagant selle pärast, et omada andmetest võimalikult värsket koopiat, teisalt aga peab andmevarundus suutma tagada, et varundatud andmeid säilitataks võimalikult kaua. Nimetades täielikku andmevarundust generatsiooniks, on tarvis kindlaks määrata, mitut andmegeneratsiooni tuleb säilitada ning ajavahemik, mis peab jääma kahe generatsiooni vahele.

Vastavaid nõudeid võib selgitada järgnevate näidete põhjal:

- Mõne faili kas meelega või kogemata kustutamisel ei sisalda vastavat faili enam ükski hilisem andmevarundus. Kui aga peaks selguma, et vastavat faili on siiski jätkuvalt tarvis, tuleb selle taastamiseks kasutada mõnda vanemat andmevarundust, mis oleks loodud ajaliselt enne vastava faili kustutamist. Vajamineva andmegeneratsiooni puudumisel tuleb vastava faili andmed uuesti sisestada.
- Faili tervikluse kao puhul (nt tehnilise defekti, faili tahtmatu muutmise või arvutiviiruse mõju tõttu) on tõenäoline, et tervikluse kadu ei avastata mitte kohe, vaid alles mõne aja möödudes. Faili tervikluse taastamiseks tuleb kasutada mõnda andmegeneratsiooni, mis on loodud enne vastavat tervikluse kadu.
- Andmete varukoopiate loomisel ei saa vigu ja protsessi poolikuks jäämist täielikult välistada. Sellistel juhtudel on tihti abi täiendavate andmegeneratsioonide kasutamisest.

Nimetatud generatsioonipõhimõtte eeliste ärakasutamiseks peavad siiski olema täidetud teatud raamtingimused: andmegeneratsioonide vahele jääv ajavahemik ei tohi olla väiksem kui etteantud miinimum. Näide: automaatselt toimiva andmevarundusprotsessi käigus leiab aset mitu katkestust. Selle tagajärjel toimuks üksteise järel kõikide andmegeneratsioonide ülekirjutamine. Selle vältimiseks on

võimalik kehtestada nõue, et enne andmegeneratsiooni ülekirjutamist tuleb kontrollida selle minimaalset vanust ning alustada selle ülekirjutamist alles siis, kui etteantud vanus on ületatud.

Generatsioonipõhimõtet saab kirjeldada kahe suuruse läbi: vanima andmegeneratsiooni minimaalne vanus ja saadaolevate andmegeneratsioonide arv.

Siinkohal kehtib alljärgnev:

- mida suurem on vanimale andmegeneratsioonile kehtestud minimaalne vanus, seda suurem on tõenäosus, et failist, mille kohta avastatakse, et selle terviklus on kaduma läinud (siia alla kuuluvad muu hulgas ka sellised kustutatud failid, mille puhul hiljem selgub, et seda oleks siiski tarvis), võib veel alles olla mõni vanem failiversioon,
- mida suurem arv erinevaid andmegeneratsioone eksisteerib, seda värskem on saadaolev vajalik eelmine failiversioon.

Andmegeneratsioonide arv on aga otseses seoses andmevarunduseks tehtavate kulutustega, kuna selleks peab olema piisaval hulgal andmekandjaid. Kulud tekivad vajadusest kasutada iga andmegeneratsiooni jaoks eraldi andmekandjat. Seetõttu on tarvis andmegeneratsioonide arvu piirata majanduslikult vastuvõetavale tasemele. Generatsioonipõhimõtte rakendamisel mõjutavad selle jaoks valitavaid parameetreid järgmised tegurid:

- Andmete käideldavusnõuded ja terviklusnõuded: mida kõrgemad on andmetele kehtivad käideldavus- või terviklusnõuded, seda rohkem peab olema erinevaid andmegeneratsioone, et muuta andmete taastamiseks kuluv aeg tervikluse kao puhul võimalikult lühikeseks. Juhtudeks, kus faili kaotsiminek või faili tervikluse kadu võidakse avastada alles väga hilja, on soovitatav luua kas kvartalite või aastate lõikes täiendavad andmevarundused.
- Taastamisega seotud vaev, kui andmevarundus puudub: kui andmeid on palju, aga need on ilma andmevarunduseta siiski taastatavad, võib kaaluda täiendava „pseudogeneratsiooni” loomist.
- Andmemahud: mida suuremad on andmemahud, seda suuremaid kulutusi tuleb vastavate andmemahtude tõttu teha ka vajaminevate andmegeneratsioonide loomiseks. Seetõttu võib suur andmemaht piirata loodavate andmegeneratsioonide arvu majanduslikel põhjustel.
- Muudatuste mahud: mida suurem on muudatuste maht, seda lühemad peaksid olema generatsioonide vahele jäävad ajavahemikud, tagamaks, et andmetest on olemas alati võimalikult värske versioon, mis aitaks hoida andmete taastamisele ja järeltöötlemisele kuluvat aega võimalikult lühikesena.

Protseduurid ja andmekandja

Pärast andmevarunduse liigi, sageduse ja andmegeneratsiooni põhimõtte kehtestamist tuleb välja valida andmevarundusprotseduur koos selleks vajalike, majanduslikult mõistlike andmekandjatega. Mõningad näited levinud andmevarundusprotseduuride kohta:

Näide nr 1

- Andmete detsentraliseeritud käsitsi varundamine PCdel. Ilma võrguühenduseta PCde puhul teeb IT kasutaja andmetest varukoopiad tavaliselt käsitsi, luues täieliku andmevarunduse rakendusandmetest. Andmekandjatena kasutakse kas CDsid või DVDsid.

Näide nr 2

- Käsitsi, tsentraalselt toimiv andmevarundus Unix-süsteemis. Unix-süsteemides, kus on tegu külgeühendatud terminalide või PCdega, on tsentraalselt hoitava andmemahu tõttu kõige mugavam andmevarundusprotseduur tsentraliseeritult toimiv andmevarundus. Tihti kombineeritakse sel otstarbel iganädalasi täielikke andmevarundusi igapäevaste astmeliste andmevarundustega, mille UNIX-administraator loob käsitsi vastavatele striimeri lintidele.

Näide nr 3

- Käsitsi, tsentraalselt toimiv andmevarundus kohtvõrgus. Kohtvõrgu puhul, kuhu on ühendatud PCd, viiakse andmevarundus tihti läbi selliselt, et PC kasutaja salvestab oma varundamisele kuuluvad andmed võrgus olevale tsentraalsele serverile ja seejärel varundab võrguadministraator vastavad andmed tsentraalselt, luues selleks täieliku andmevarunduse igal nädalal ja astmelise andmevarunduse iga päev.

Näide nr 4

- Automaatne, tsentraalselt toimiv andmevarundus suurarvutite puhul. Sarnaselt näitele nr 2 luuakse ka suurarvutite andmevarundused nii, et iganädalast täielikku andmevarundust kombineeritakse igapäevase astmelise andmevarundusega. Enamasti luuakse see automaatselt vastavate hierarhilise salvestihalduse (HSH) tööriistade toel. Mõningate IT-rakenduste puhul on laialt levinud ka täiendav sündmustepõhine andmevarundus.

Näide nr 5

- Automaatne, tsentraalselt toimiv andmevarundus jagatud süsteemis. Üks variant on ka näidete nr 3 ja nr 4 kombinatsioon. Jagatud süsteemide kohapeal olevad andmed edastatakse tsentraalsele suurarvutile, st tsentraalsele serverile, kus andmed varundatakse täieliku ja astmelise andmevarunduse kombinatsioonina.

Näide nr 6

- Täisautomaatne, detsentraalselt salvestatud andmete tsentraalselt toimiv andmevarundus jagatud süsteemis. Vastupidiselt eelnevale näitele edastatakse selle variandi puhul andmed detsentraalselt toimivast süsteemist tsentraalsesse süsteemi automaatselt. Tänapäeval pakutakse juba ka tarkvaratööriistu, mis võimaldavad tsentraalse andmevarundusserveri kaudu juurdepääsu detsentraalselt hoitavatele andmehulkadele. Niimoodi on võimalik andmevarundust läbi viia piisavalt läbipaistvalt ka detsentraalse kasutaja jaoks.

Andmekandjale salvestatava andmemahu minimeerimiseks on võimalik rakendada täiendavaid andmetihendusalgoritme. Mõningatel juhtudel võib andmemahtu seeläbi kuni 80 protsendi võrra vähendada. Andmetihenduse rakendamisel tuleb tagada, et valitud parameetrid ja algoritmid oleksid andmevarunduse raames dokumenteeritud ja andmete taastamiseks (dekompressiooniks) olemas.

Protseduuri jaoks tuleb kindlaks määrata kaks parameetrit: automatiseerituse aste ja tsentraliseerimine (salvestuskoht). Automatiseerituse astme puhul tuleb teha vahet käsitsi ja automaatsete protseduuride vahel:

- Käsitsi andmevarundus tähendab, et andmevarundus algatatakse käsitsi. Käsitsi variandi eeliseks on asjaolu, et töötajal on võimalik andmevarunduse ajahetke määrata ise nii, et see sobiks kõige paremini kõikvõimalike tööprotsessidega. Puuduseks on tõsiasi, et andmevarunduse toimimine ja kvaliteet sõltuvad sellisel juhul vastutava töötaja motivatsioonist ja distsiplineeritusest. Haigestumiste ja muudest põhjustest tingitud eemalviibimiste tõttu võivad andmevarundused jääda tegemata.
- Automaatsed andmevarundused algatab programm teatud kindlatel ajahetkedel. Eeliseks on sõltumatus vastutava töötaja distsipliinist ja usaldusväärsusest juhul, kui programmi tööplaan on täielik ja ajakohane. Puuduseks võivad olla juhtimisprogrammidega seotud kulud, tööplaani kohandamine värskete muudatustega või tõsiasi, et süsteem ei varunda olulisi muudatusi mitte kohe pärast nende toimumist, vaid hoopis hiljem.

Tsentraliseerituse seisukohast tuleb vahet teha tsentraalselt ja detsentraalselt läbiviidavate andmevarunduste vahel.

- Tsentraalselt toimivate andmevarunduste puhul asub salvestuskoht tsentraalses IT-süsteemis, kus andmevarunduse viib läbi vastutav töötaja. Sellise protseduuri eeliseks on vajadus koolitada intensiivselt ainult ühte töötajat, mistõttu ei pea IT-süsteemi ülejäänud IT kasutajad vastava ülesandega enam eraldi tegelema. Lisaks on suuremal hulgal tsentraalses kohas tekkivate andmemahtude eeliseks veel ka kulude kokkuhoid, kuna selle variandi puhul on võimalik kasutada varundamiseks soodsamaid andmekandjaid. Puuduseks on võimalus, et edastada võidakse ka konfidentsiaalseid andmeid ning volitamata isikutel võib tekkida võimalus nendega tutvuda.
- Detsentraalsed andmevarundused viivad läbi IT kasutajad ise, ilma et andmeid oleks tarvis mõnda tsentraalsesse süsteemi edastada. Eeliseks on kasutajatele säiliv kontroll oma andmete ja varukoopiate andmekandjate üle, eriti juhul, kui on tegemist konfidentsiaalsete andmetega. Puuduseks on järjekindla andmevarunduse sõltuvus IT kasutaja vastutustundest ning tõsiasi, et detsentraalsed andmevarunduslahendused nõuavad IT kasutajatelt tööaega.

Pärast otsuse langetamist, kas valida käsitsi või automaatne andmevarundus, tsentraalselt või detsentraalselt toimiv lahendus, tuleb leida andmevarunduse jaoks sobivad andmekandjad. Selleks võib vaadelda

järgnevaid parameetreid:

- Andmekandja töövalmis seadmisele kuluv aeg: andmete taastamisega seotud ajakulu sõltub ajast, mis kulub alates vajamineva andmekandja identifitseerimisest selle süsteemis kättesaadavaks tegemiseni. Robotsüsteemi kassetid võivad olla andmevarunduseks valmis mõne minuti jooksul, mujale hoiule viidud linte tuleb olenevalt olukorrast võib-olla esmalt transportida ja töövalmis seada, mis on küllaltki töö- ja ajamahukas.
- Juurdepääsuaeg, edastusjõudlus: andmete loomisele ja taastamisele kuluv aeg sõltub andmekandja keskmisest juurdepääsuajast ja andmeedastuse jõudlusest. Kõvakettad võimaldavad juurdepääsu teatud liiki failidele millisekundite jooksul, kuid magnetlinti tuleb esmalt vajamineva kohani edasi või tagasi kerida. Andmekandja valimisel on oluline silmas pidada, et kõrgetel andmeedastuskiirustel ei tekiks edastuskanalites ülekoormust.
- Kasutusmugavus/salvestiruum: mida keerulisem on andmeid varundada, seda suurem on oht, et protsessi käigus tekib vigu või et vastutav töötaja jätab selle töö sootuks tegemata. Liiga väikese salvestusruumiga andekandjad pärsivad efektiivse andmevarunduse toimimist, kuna pidev vajadus andmekandjaid vahetada kulutab palju aega ja annab palju võimalusi vigade tekkeks.
- Kulutused: andmevarundusega seotud kulud, st lugemis- ja kirjutusseadmete ning andmekandjate soetamiskulud, arvutustehnika ja töötajate tööaeg peavad olema omavahel vastuvõetavas seoses. Siinkohal tuleb arvestada ka andekandjate kasutusea ja nende töökindlusega. Andmevarundusele tehtavad jooksvad kulutused ei tohi mingil juhul ületada kulutusi, mis on seotud andmete taastamisega juhul, kui andmevarundust ei loodaks või sellega seotud hilisemaid kahjusid. Erilist tähelepanu tuleb pöörata järgmistele teguritele:
- Käideldavusnõuded: mida kõrgemaid nõudeid käideldavusele seatakse, seda kiiremini peab olema võimalik andmekandjale kui andmevarunduse salvestusvahendile juurde pääseda ja seda kiiremini peavad ka vajaminevad andmed olema uuesti sisseloetavad. Käideldavusnõuete täitmiseks peab olema tagatud, et salvestusvahendeid oleks võimalik kasutada andmete taastamiseks ka juhul, kui lugemisseade peaks rivist välja langema. Tuleb tagada, et asendusseade töötaks ja ühilduks kasutatud andmekandjatega.
- Andmemaht ja muudatuste maht: andmemahtude suurenedes võetakse reeglina kasutusele soodsama hinnaga lintsalvestusvahendid, nagu magnetlindid või lindikassetid (data cartridge).
- Tähtajad: juhul kui andmete puhul tuleb kinni pidada teatud kindlatest kustutustähtaegadest (nt isikuandmete puhul), peab väljavalitud andmekandja seda ka võimaldama. Andmekandjaid, mida pole võimalik kustutada, või mida saab kustutada ainult suure vaevaga (nt WORM-andmekandjad), tuleks sellistel juhtudel vältida.
- Andmete konfidentsiaalsus- ja terviklusnõuded: kui varundamisele kuuluvate andmete konfidentsiaalsus- ja terviklusnõuded on kõrged, kandub andmete kaitsevajadus üle ka andmevarunduseks kasutatud andmekandjatele. Kui andmevarunduse krüpteerimine ei osutu võimalikuks, võiks kaaluda selliste andmekandjate valimist, mida saab oma kompaktse konstruktsiooni ja kerge transporditavuse tõttu hoida nt andmevarunduskappides või seifides.

- IT kasutajate teadmised: IT kasutajate teadmised ja andmetöötlusega seotud oskused on andmevarundusprotseduuri valikul määrava tähtsusega ning võimaldavad valida, kas võtta kasutusele protseduur, mille käigus peavad IT kasutajad ise käsitsi andmevarunduse läbi viima, protseduur, mille käigus loovad andmevarunduse koolitatud kaastöötajad tsentraalselt, või hoopis protseduur, mis toimib automatiseeritult.

Andmevarundusega seotud vastutusalad
Otsuse langetamisel, keda andmevarunduse sooritamiseks kohustada, tuleb kõne alla kolm töötajate gruppi. Esiteks võivad need olla IT kasutajad ise (reeglina detsentraalsete ja ilma võrguühenduseta IT-süsteemide puhul), süsteemi haldaja või keegi spetsiaalselt andmevarunduse jaoks väljakoolitatud administraator. Juhtudel, kus andmevarundust ei vii läbi kasutajad ise, tuleb vastutavatele töötajatele panna andmete sisu suhtes vaikimiskohustus ja kaaluda vajaduse korral ka andmete krüpteerimist. Lisaks tuleb määrata pädevad isikud, kes peavad vastavas olukorras otsustama, kas alustada andmete taastamist või mitte. Samuti tuleb kindlaks määrata, kellel on õigus varukoopiad sisaldavatele andmekandjatele juurde pääseda, eriti juhul, kui andmekandjaid hoitakse väljaspool mõnes andmevarundusarhiivis. Tuleb tagada, et juurdepääs oleks võimalik ainult volitatud isikutele. Lõpetuseks tuleb määratleda, millistel töötajatel on õigus hakata kogu andmemahtu või väljavalitud üksikuid faile operatiivselt taastama.

Vastutusalade kindlaksmääramisel tuleb hoolikalt vaadelda andmetele kehtivaid konfidentsiaalsus- ja terviklusnõudeid ning vastutavate töötajate usaldusväärsust. Tuleb tagada, et vastutavad töötajad oleksid kättesaadavad ja et igale töötajale määrataks ka asendaja, kes tuleb samuti ülesannetega kurssi viia.

Arvesse tuleks võtta järgmist mõjutegurit:
IT kasutajate teadmised: IT kasutajate teadmised ja andmetöötlusega seotud kogemused määravad, kas iga töötaja peaks andmevarunduse läbi viima ise omal vastutusel või mitte. Kui IT kasutajate teadmised ei ole piisavad, tuleks vastutus anda süsteemiadministraatorile või spetsiaalselt selleks ülesandeks väljakoolitatud isikule.

Ladustuskoht
Andmevarundusi sisaldavaid andmekandjaid ja originaalandmekandjaid tuleks reeglina hoida teineteisest lahus ja erinevates tuletõkketsoonides. Andmevarunduse andmekandjate hoidmine mõnes teises hoones või väljaspool tootmisasukohta vähendab nende hävimise tõenäosust katastroofjuhtumite korral. Kuid mida kaugemal andmekandjaid vastavast taastamiseks vajaminevast lõppseadmest (nt lindiajamist) hoitakse, seda pikemaks muutuvad nende transporditeekonnad ja transportimisajad ning seda rohkem aega kulub andmetaastuse tervikprotsessile.

Seetõttu tuleks arvestada järgmiste mõjuritega:

- Käideldavusnõuded: mida kõrgemad on käideldavusele esitatavad nõuded,

seda kiiremini peavad olema andmevarundusi sisaldavad andmekandjad kättesaadavad. Juhul kui turvalisuse põhjustel hoiustatakse andmekandjaid väljaspool ettevõtet, tuleks väga kõrgete käideldavusnõuete puhul kaaluda täiendavate andmevarunduskoopiate hoidmist IT-süsteemi vahetus läheduses.
- Andmete konfidentsiaalsusnõuded ja terviklusnõuded: mida kõrgemate nõuetega on tegu, seda paremini peab olema takistatud andmekandjate manipuleerimisvõimalus. Vajaminevat juurdepääsukontrolli saab reeglina rakendada vaid sobivate infrastruktuuriliste ja organisatoorsete meetmetega, vt B 2.5 Andmekandjate arhiiv .
- Andmemahud: mida suuremaks kasvavad andmemahud, seda tähtsamaks muutub hoiukoha turvalisus.

Andmevarundusarhiivile esitatavad nõuded

Kuna andmevarunduse andmekandjatele on talletatud suures koguses erinevaid andmeid, on andmekandjate endi konfidentsiaalsus- ja terviklusnõuded vähemalt sama kõrged kui sinna salvestatud andmete omad. Andmekandjate hoiustamisel mõnes tsentraalses andmevarundusarhiivis tuleb seetõttu kindlasti võtta tõhusaid IT-turvameetmeid, nagu nt juurdepääskontroll. Lisaks tuleb organisatoorsete ja personalialaste meetmetega (andmekandjate haldamisega) tagada, et vajalikele andmetele oleks olemas kiire ja sihipärane juurdepääs. Selleks tuleb järgida meedet M 2.3 Andmekandjate haldus ja moodulit B 2.5 Andmekandjate arhiiv .

Arvestada tuleb järgmiste mõjuteguritega:

- Käideldavusnõuded: mida kõrgemad on käideldavusele esitatavad nõuded, seda kiiremini peab olema võimalik vajalikele andmekandjatele sihipäraselt juurde pääseda. Kui käsitsi koostatud loeteludest käideldavusnõuete täitmiseks ei piisa, on võimalik võtta kasutusele automatiseeritud juurdepääsuprotseduurid (nt robotkassettarhiivid).
- Andmemahud: andmemaht määrab hoiustatavate andmekandjate hulga. Suurte andmemahtude puhul tuleb piisava ladustusruumi võimaldamiseks ette näha andmekandjaarhiivi kasutamine.
- Tähtajad: kustutustähtaegade järgimiskohustuse puhul tuleb andmekandjaarhiivi töökorraldus viia tähtaegadega kooskõlla ja vajaduse korral muretseda ka vajaminevad kustutusseadmed. Etteantud tähtaegade saabumisel tuleb andmekandjaarhiivis algatada ja läbi viia andmete kustutamine ning see kindlasti ka dokumenteerida. Kui andmete kustutamine ei ole tehniliselt võimalik, tuleb organisatoorsete meetmete abil tagada, et kustutamisele määratud andmeid ei oleks võimalik uuesti kasutusele võtta.
- Andmete konfidentsiaalsus- ja terviklusnõuded: mida kõrgemate nõuetega on tegu, seda paremini peab olema takistatud andmekandjate manipuleerimisvõimalus. Vajaminevat juurdepääsukontrolli saab reeglina rakendada vaid sobivate infrastruktuuriliste ja organisatoorsete meetmetega sarnaselt moodulile B 2.5 Andmekandjate arhiiv .

Transporditingimused

Andmevarunduse loomise käigus leiab aset andmete transportimine. Andmeid transporditakse läbi võrgu või sideliini ja andmekandjaid toimetatakse andmekandjaarhiivi.

Arvestada tuleks järgmiste aspektidega:

- Käideldavusnõuded: mida kõrgemad on käideldavusele esitatavad nõuded, seda kiiremini peab olema võimalik muuta andmeid taastamise eesmärgil kättesaadavaks. Sellega tuleb arvestada andmete edastusvahendi ja andmekandjate transporditeekonna valikul.
- Andmemahud: kui andmed edastatakse taastamise eesmärgil läbi võrgu, tuleb arvestada andmemahtude ja võrgu edastusjõudlusega. Tuleb tagada, et andmemahud jõuaksid sihtkohta ettenähtud aja jooksul (käideldavusnõudeid täites).
- Andmete muutmise ajahetked: kui andmeid varundatakse läbi võrgu (eriti kindlaksmääratud ajahetkedel), võib suuremate andemahtude korral võimsusest puudu tulla. Seetõttu tuleb andmevarunduse läbiviimise ajal tagada piisav andmeedastusvõimsus.
- Andmete konfidentsiaalsus- ja terviklusnõuded: mida kõrgemate nõuetega on tegu, seda paremini peab olema transpordi ajal takistatud andmete pealtkuulamine, nende volitamata kopeerimine ning manipuleerimine. Andmete edastamisel tuleks kaaluda krüpteerimise või krüptograafilise manipuleerimise rakendamist, füüsilise transpordi puhul tuleb kasutada turvalisi transportimispakendeid ja turvalisi teekondi ning vajaduse korral hinnata ka krüpteerimisega seotud kasuteguri ja kulude omavahelist suhet.

Säilitustingimused

Andmevarunduskontseptsiooni raames tuleks arvestada, kas teatud andmeliikidele kehtivad mõned säilitus- või kustutuskohustused.

- Tähtajad: juhul kui tuleb järgida teatud säilituskohustusi, saab seda tagada vastavate andmegeneratsioonide arhiveerimisega. Pikkade säilitustähtaegade puhul tuleb lisaks veel tagada vajalike lugemisseadmete varu ning et vajaduse korral tehtaks magnetandmekandjatele värskendus (magnetiliselt salvestatud andmete läbimängimine), kuna aja jooksul kaotavad need andmekandjad oma magnetilisuse ning andmed võivad kaduma minna. Kustutustähtaegade järgimiskohustuse puhul tuleb andmekandjaarhiivis kehtestada kindel töökorraldus ja muretseda ka vajaminevad kustutusseadmed. Etteantud kustutustähtaegade saabumisel tuleb andmekandjaarhiivis algatada ja viia läbi andmete kustutamine.

Kontrollküsimused:

- Kas IT-varustuses asetleidvate muudatuste korral täiendatakse vastavalt ka andmevarundusprotseduuri?
- Kas andmete taastamist harjutatakse pisteliselt?
- Kas andmevarunduskontseptsiooniga kehtestatud tingimuste täitmist kontrollitakse?
- Kas andmevarundusega seotud ülesandeid täitvaid isikuid koolitatakse piisavalt?

M 6.36 Minimaalse andmevarunduse kontseptsiooni määratlemine

Algatamise eest vastutavad: IT turvaosakond
Rakendamise eest vastutavad: IT turvaosakond

Igas ettevõttes ja ametiasutuses tuleb kindlaks määrata andmevarundusega seotud kohustuslikud miinimumnõuded. Sellega on võimalik paljusid juhtusid, kus üksikasjalikumad uuringud ja andmevarunduskontseptsiooni väljatöötamine võivad osutuda liiga töömahukaks, käsitleda üldistavalt, ilma liigsetesse detailidesse laskumata. Lisaks luuakse sellega alus, mis kehtib üldjuhul kõikidele vanadele IT-süsteemidele ja ka uutele, mille kohta ei ole andmevarunduskontseptsiooni veel välja töötatud.

Näide:

Minimaalse andmevarunduse kontseptsioon

- Tarkvara: kogu tarkvara, nii ostetud kui ka enda loodud, tuleb varundada ühekordselt, tehes täieliku andmevarunduse.
- Süsteemiandmed: süsteemiandmetest tuleb luua vähemalt kord kuus üks andmegeneratsioon.
- Rakendusandmed: kõikidest rakendusandmetest tuleb luua vähemalt kord kuus täielik andmevarundus, rakendades seejuures kolme andmegeneratsiooni põhimõtet.
- Logiandmed: kõikidest logiandmetest tuleb luua vähemalt kord kuus täielik andmevarundus, rakendades seejuures kolme andmegeneratsiooni põhimõtet.

Kontrollküsimused:

- Kas kõikidele töötajatele, muu hulgas ka äsja tööle võetud töötajatele edastatakse kehtivat andmevarunduskontseptsiooni või minimaalset andmevarunduse kontseptsiooni puudutav info ning kas töötajaid kohustatakse seda järgima?
- Kas minimaalset andmevarunduse kontseptsiooni uuendatakse?
- Kas töötajad on varustatud vajaminevate töövahenditega, mida on tarvis minimaalse andmevarunduse kontseptsiooni täitmiseks?

M 6.37 Andmevarunduse dokumenteerimine

Algatamise eest vastutavad: IT turvaosakond

Rakendamise eest vastutavad: andmevarunduse eest vastutav töötaja

Andmevarunduskontseptsioonis peab olema kindlaks määratud, kuidas tuleb andmevarundust dokumenteerida. Korrakohase ja toimiva andmevarunduse jaoks on dokumentatsioon hädavajalik.

Seetõttu tuleb andmetest varukoopiate tegemisel dokumenteerida iga IT-süsteemi kohta järgnev info:

- andmevarunduse tegemise kuupäev,
- andmevarunduse maht (milliseid faile/kaustu varundati),
- andmekandja, kuhu vastavad andmeid operatiivse töö käigus salvestatakse,
- andmekandja, mille peale andmed varundati,
- andmevarunduse käigus kasutatud riist- ja tarkvara (koos versiooni numbriga),
- andmevarunduse jaoks valitud parameetrid (andmevarunduse liik jms).

Lisaks tuleb kirjeldada ka protseduuri, mida tuleks rakendada varundatud andmemahtudest andmete taastamiseks. Ka siin tuleb üles loetleda vajaminev riist- ja tarkvara, vajalikud parameetrid ja protseduur, mille abil andmeid rekonstrueerida.

Kontrollküsimused:

- Kas andmevarundusi dokumenteeritakse eespool kirjeldatud põhjalikkusega?
- Kas loodud dokumentatsioonist piisab andmete taastamiseks ka juhul, kui konkreetsel töötajal, kes varukoopiad tegi, pole teatud põhjustel võimalik taastamisega tegeleda?

M 6.38 Edastatud andmete varukoopiad

Algatamise eest vastutavad: IT-turbespetsialisti

Rakendamise eest vastutavad: kasutajad

Juhul, kui edastavad andmed on koostatud ainult edasisaatmiseks ning neid ei ole kuhugi mujale andmekandjale salvestatud, tuleks nendest andmetest luua varukoopia. Edastatud andmekandja kaotsimineku või kahjustuse korral on niimoodi võimalik andmeid kerge vaevaga uuesti saata.

Täiendav kontrollküsimus:

- Kas edasiantavate andmekandjate puhul on ette nähtud, et nendest tuleks luua varukoopia?

M 6.39 Faksitoodete tarnijate loend asendushangeteks

Algatamise eest vastutavad: IT-turvaosakond
Rakendamise eest vastutavad: faksi kasutamise eest vastutav töötaja, hankija

Avarii- ja katastroofiplaanis peaks olema nimekiri faksiseadmete edasimüüjatest, kelle käest on võimalik vajadusel hankida viivitamata uued seadmed, kui seadmete remont ei peaks ajalistel põhjustel enam kõne alla tulema.

Kontrollküsimus:

- Kas avariiplaanis on olemas nimekiri faksiseadmete edasimüüjate kohta?

M 6.41 Andmete taastamise harjutamine

Algatamise eest vastutavad: IT turvaosakond

Rakendamise eest vastutavad: andmevarunduse eest vastutav töötaja

Andmete taastamist andmevarunduslintide abil tuleb pisteliselt, kuid vähemalt pärast igat andmevarundusprotseduuri sisseviidud muudatust katsetada. Selle käigus on tarvis esmalt saada kinnitus, et andmeid on võimalik täies mahus taastada (nt ühe serveri kogu andmemahtu).

Sellisel moel on võimalik usaldusväärselt välja selgitada, kas

- andmete taastamine on üleüldse võimalik;
- andmevarunduseks valitud protseduur on mõistlik;
- andmevarunduse kohta on olemas piisavas mahus dokumentatsioon, mis võimaldab vajaduse korral ka mõnel asendustöötajal andmeid taastada;
- andmete taastamiseks kuluv ajaline ressurss on kooskõlas käideldavusnõuetega (vt M 6.1 Käideldavusnõuete inventuur).

Andmete taastamise harjutamise käigus tuleks muu hulgas arvestada ka alljärgnevaga:

- Andmed tuleb vajaduse korral installeerida mõnele varuks hoitavale IT-süsteemile.
- Andmete varunduseks ja andmete taastamiseks tuleb kasutada erinevaid lugemis- ja kirjutusseadmeid.

Kontrollküsimus:

- Kas valdkonnas pädev kolmas isik on suuteline andmeid taastama, tuginedes ainult olemasolevale dokumentatsioonile?

M 6.42 Andmete taastamise harjutamine

Algatamise eest vastutavad: IT-turvaosakond

Rakendamise eest vastutavad: andmevarunduse eest vastutav töötaja

Andmete taastamist andmevarunduslintide abil tuleb pisteliselt, kuid vähemalt pärast igat andmevarundusprotseduuri sisseviidud muudatust katsetada. Selle käigus on tarvis esmalt saada kinnitus, et andmeid on võimalik täies mahus taastada (nt ühe serveri kogu andmemahtu). Sellisel moel on võimalik usaldusväärselt välja selgitada, kas:

- andmete taastamine on üleüldse võimalik
- andmevarunduseks valitud protseduur on mõistlik
- andmevarunduse kohta on olemas piisavas mahus dokumentatsioon, mis võimaldab vajadusel ka mõnel asendustöötajal andmeid taastada
- andmete taastamiseks kuluv ajaline ressurss on kooskõlas käideldavusnõuetega (vt M 6.1 Käideldavusnõuete inventuur).

Andmete taastamise harjutamise käigus tuleks muuhulgas arvestada ka järgnevaga:

- Andmeid tuleb võib-olla installeerida mõnele varuks hoitavale IT-süsteemile.
- Andmete varunduseks ja andmete taastamiseks tuleb kasutada erinevaid lugemis- ja kirjutusseadmeid.

Täiendav kontrollküsimus:

- Kas antud valdkonnas pädev kolmas isik on suuteline andmeid taastama, toetudes ainult olemasolevale dokumentatsioonile?

M 6.43z Liiasusega Windowsi serverid

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator

Sõltuvalt andmetele ja rakendustele kehtivatest käideldavusnõuetest tuleb luua liiasus, mis peab aitama vastuvõetavate kulutustega ennetada täielikku andmekadu. Vastavalt kehtivatele nõuetele tuleb kas osa andmemahust või kogu andmemahtu hoida paralleelselt mitmel kettasalvestil, et kettasalvesti avarii ei tooks endaga kaasa vastavate andmete kaotsiminekut ning töötajad saaksid oma tööga jätkata, ilma et nad peaksid ootama, kuni andmeid andmevarundustest taastama hakatakse. Sõltuvalt kehtivatest käideldavusnõuetest võib süsteemi üles ehitada selliselt, et serveri avarii korral saaks selle funktsiooni üle võtta mõni teine või koguni mitu erinevat serverit. Siinkohal tuleb siiski hoolitseda ka selle eest, et laialijagatult hoitavad andmemahud jääksid ühesuguseks ning seda tuleb suuta tagada ka üksikute seadmete avariide korral.

Selles valdkonnas on erinevate liiasust võimaldavate kontseptsioonide jõudluses lausa mäekõrgused erinevused:

- RAID-kettasüsteemid - Otsesest füüsikalist liiasust on võimalik saavutada RAID-kettasüsteemidega (RAID: Redundant Array of Independent Disks). Selle meetodi kasuks otsustamisel tuleb arvestada, et RAID-süsteemi üksikute ketaste ruumilisele vahekaugusele kehtivad suured piirangud, mis tähendab, et tulekahju või muu sarnase kahju puhul hävivad ühtmoodi kõik paralleelselt hoitavad andmekoopiad. Seetõttu ei asenda RAID-süsteemid andmete varundamist.
- Üksikute kaustade replikeerimine võimaldab andmeid samamoodi laiali jaotada, kuid siin pole võimalik kasutada sünkroniseerimismehhanisme, mis lubaksid lisaks muule hoida ühtmoodi paralleelselt ka hetkel töödeldavaid faile. Peamise kettaajami avarii toob endaga kaasa seetõttu suurema või väiksema andmekao.

Eraldi arvutid

Serveri võimaliku avarii ennetamiseks tuleks need vajadusel üles ehitada liiasusega.

Selleks on mitmeid võimalusi, mille hulgast tuleb valida endale vastuvõetava seisakuaja põhjal sobiv alternatiiv:

- juhul kui pooletunnised seisakuajad on vastuvõetavad, tuleks valmis hoida lisaarvuti, mis suudaks serveri avarii korral selle ülesanded üle võtta. Juurdepääsu võimaldamiseks avariilise serveri andmetele tuleb selle kettaajamid ümber lülitada asendusarvutile.
- täieliku liiasusega, avariikindel süsteem

Cluster -süsteemid

- Juhtudel, kus seisakuajana on vastuvõetav ainult mõni minut, tuleks kasutada klastrisüsteemi, mis võimaldab juurdepääsu kõikide arvutite kõikidele ketastele. Vastav süsteem tuleb konfigureerida selliselt, et ühe serveri avarii korral toimuks automaatselt ümberlülitus mõne süsteemi kuuluva lisaarvuti peale.
- Juhtudel, kus seisakuaegadena on talutavad vaid mõned sekundid, tuleb kasutada täieliku liiasusega avariikindlat süsteemi, mis koosneb paralleelselt töötavatest mitmetest CPUdest. Selliste süsteemide puhul jääb üksiku CPU või põhisalvestusmooduli avarii kasutaja jaoks märkamatuks. Antud lahendus pakub kõige suuremat avariikindlust, kuid on samal ajal ka märgatavalt keerulisem ning kulukam ülal pidada kui teised lahendused, mistõttu rakendatakse seda ainult ekstreemsete käideldavusnõuete puhul.

Kõikidel juhtudel tuleb siiski põhjaliku analüüsi abil välja selgitada, millised on kehtivad käideldavusnõuded ning seejärel leida detailse süsteemi- ja võrguarhitektuuri planeerimise abil sobiv kombinatsioon liiasusega varustatud arvutitest ja/või kettaajamitest, mis suudaks vastavaid nõudeid ka reaalselt täita.

Kontrollküsimus:

- Kas hetkel rakendustele kehtivad käideldavusnõuded ja nende omavahelised sõltuvussuhted on teada?

M 6.47 Kaugtöö andmevarundus

Algatamise eest vastutavad: IT-juht, IT-turbespetsialist

Rakendamise eest vastutavad: kaugtöö tegijad

Kaugtöö raames võidakse andmeid salvestada erinevatesse IT-süsteemidesse ja erinevatesse kohtadesse, nt konkreetse institutsiooni serveritele ja klientidesse, kuid ka kaugtöökoha klientidesse. Kaugtöökoha puhul tuleb tagada kõikide oluliste andmete varundamine. Institutsiooni andmevarunduskontseptsioon ei tohi piirduda mitte ainult serveritega, vaid peab hõlmama ka kaugtöökohti. Enamatel juhtudel saab kaugtöökoha andmevarunduse tarbeks rakendada järgmisi protseduure:

- Andmete varundamine välistele andmekandjatele - Selleks peavad kaugtöökohad olema varustatud vajaliku tehnikaga. Siia alla kuuluvad vajaminevad välised andmekandjad ning arvutis vajalik riistvara ja tarkvara. Lisaks peab kaugtöö tegija olema piisavalt koolitatud, et ta suudaks andmevarundusi iseseisvalt läbi viia.
- Andmete varundamine üle võrgu - Lokaalsete randmeta varundamine võib aset leida ka institutsiooni võrguga loodava ühenduse kaudu. Siinkohal on eeliseks, et andmevarundusi ei pea läbi viima kaugtöö tegijad iseseisvalt ning neil pole tarvis tegeleda ka andmekandjate haldamisega. Võrguühenduse kaudu toimiva andmevarunduse puhul on määravaks, et varundatava andmemahu jaoks oleks olemas piisav ribalaius. Andmeedastus ei tohi võtta liiga palju aega ning eemalasuvate ressursside samaaegne kasutamine koos andmevarundusega ei tohi tekitada liigseid viivitusi. Enamlevinud juurdepääsutehnoloogiad (nt ISDN ja modem) suudavad iga varundusprotsessi jaoks transportida ainult väikseid andmekoguseid. Sõltuvalt andmevarundustarkvarast on ka võimalik edastada ainult pärast viimast andmevarundust tekkinud muudatusi (inkrementaalne andmevarundus). Paljudel juhtudel on seeläbi võimalik transporditavaid andmemahte tugevalt vähendada. Üheks tähtsaks nõudeks andmevarunduseks kasutatavale tarkvarale on selle võime ühenduse ootamatuid katkemisi tuvastada ja nendega korrektselt ümber käia.

Mõlema andmevarundusprotseduuri puhul on soovitatav varundamisele kuuluvat andmehulka minimeerida. Lisaks kaovabade tihendusprotseduuride rakendamisele, mis on paljudesse andmevarundustarkvaradesse juba integreeritud, võib rakendada ka inkrementaalset või diferentseeritud andmevarundust (vt M 6.35 Andmevarunduseks vajalike protseduuride määratlemine). Andmete taastamine võib aga selle tagajärjel sõltuvalt konkreetsetst asjaoludest muutuda keerukamaks. Andmete varundamine peaks toimima võimalikult automaatselt, et kaugtöö tegijate enda tööoperatsioonide hulk jääks selle puhul nii väikeseks kui võimalik. Kui andmete varundamisprotsessi on tarvis kaasata ka töötajad, tuleb töötajatele kehtestada kohustus viia regulaarselt läbi andmevarundusi (vt M 2.41 Töötajate kaasamine andmevarundusse). Lisaks tuleks pisteliselt kontrollida, kas loodud andmevarundustest on võimalik andmeid ka taastada.

Varukoopiaid sisaldavate andmekandjate hoidmine

Kui andmevarunduse andmekandjaid hoitakse kodus, tuleb neid hoida luku taga. Tuleb tagada, et neile on võimalik juurde pääseda ainult kaugtöötajal endal ja tema asendajal. Igast andmevarunduse andmekandjate generatsioonist tuleks hoida siiski ka ühte koopiat institutsiooni enda ruumides, et katastroofi korral säiliks asendajal juurdepääs vastavatele andmetele.

Täiendavad kontrollküsimused:

- Kas kõiki andmeid, mida kaugtöö raames töödeldakse, varundatakse regulaarselt?
- Kas andmevarunduseks väljavalitud protseduur on tekkiva andmemahu jaoks sobiv ning katab kõik vajadused?
- Kas andmevarunduse läbiviimisel on kaugtöö tegija sekkumine varundusprotsessi minimaalne?
- Kas igast andmevarunduse andmekandja generatsioonist hoitakse ühte varukoopiat ka institutsiooni ruumides?
- Kas loodud andmevarunduste puhul kontrollitakse pisteliselt nende taastamisvõimet?

M 6.48 Protseduurid andmebaasi tervikluse kao puhuks

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator, kasutaja

Juhul, kui andmebaasisüsteem ei käitu ootuspäraselt (nt süsteem käitub arusaamatult, süsteemist pole võimalik leida vajalikke tabeleid või andmeid, tabelite sisu on muudetud, seletamatult pikk reaktsiooniaeg), võib olla tegemist andmebaasi tervikluse kaoga. See võib olla põhjustatud süsteemi väärast kasutamisest, nt süsteemiseadistuste muutmisest. Selliste probleemsete juhtude jaoks tuleks koostada kontseptsioon (taastekontseptsioon), mis kirjeldaks kontrolliprotseduuri, otsuste langetamist ja tegevusi, mis on vajalikud andmebaasi taastamiseks võimalikult kiirel ja turvalisel moel (vt M 6.51 Andmebaasi taastamine).

Täiendavaks oluliseks aspektiks on andmebaasi kasutajate teavitamine. Kasutajaid tuleks teavitada võimalikult kohe pärast seda, kui on ilmnenud esimesed märgid tervikluse kadumise kohta ning enne taastamistööde alustamist. Sellisteks juhtudeks ning ka juhtudeks, kus kasutajad avastavad ebareeglipärasusi andmebaasi kasutuses, tuleks kasutajatele koostada ja laiali jagada käitumisreegleid tutvustav infoleht, mis peab sisaldama vähemalt järgnevat infot:

- Säilitage rahu!
- Teavitage olukorrast andmebaasi administraatorit!
- Lõpetage andmebaasi kasutamine!
- Järgige andmebaasi administraatori juhiseid!

Andmebaasi administraator peaks täpselt järgima taastekontseptsiooni, mis peaks sõltuvalt vea põhjusest muuhulgas ette nägema järgmisi samme:

- Informatsioon - Kõikide puudutatud kasutajate viivitamatu teavitamine tekkinud olukorrast koos palvega lõpetada andmebaasi kasutamine ja oodata uute juhiste saabumist. Kasutajate informeerimine kindlate ajavahemike tagant, millises staadiumis on vea kõrvaldamise protseduur.
- Hetkeseisundi varundamine - Andmebaasisüsteemi väljalülitamine. Andmebaasisüsteemi käivitamine *exclusive* -režiimis (juhul, kui andmebaasisüsteem seda toetab). Kõikide failide varundamine, mis võiks anda infot tekkinud probleemi liigi ja põhjuse kohta (nt kas tegu oli reaalse ründega ning millisel viisil õnnestus ründajal süsteemi sisse tungida), st eriti oluline on varundada kõik olulised logifailid.
- Analüüs ja hinnang - Logifailides silma hakanud kõrvalekallete analüüsimine ja lahtiseletamine (koostöös revidendi ja/või IT-turbespetsialistiga). Süsteemitabelite pääsuõiguste kontrollimine. Andmebaasitarkvara kontrollimine silmnähtavate muutuste suhtes, nt vastavate failide loomise kuupäev ja suurus. (Kuna ründajal on võimalik neid ka oma algses väärtuses taastada, tuleks kontrolliks rakendada kontrollsumma protseduuri).
- Situatsioonipõhine reageerimine - Andmebaasitarkvara kustutamine ja originaalfailide taaspaigaldamine kirjutuskaitsega varustatud andmekandjatelt (vt M 6.21 Kasutatava tarkvara varukoopia). Olemasolevatest andmevarundustest tuleks programme taaspaigaldada ainult juhul, kui on piisavalt kindel,

et taaspaigaldatav tarkvara ei sisalda vastavaid vigu. Paroolide taastamine algväärusele. Süsteemitabelite pääsuõiguste taastamine algväärtustele. Kõikide kasutajate teavitamine sooviga, et nad kontrolliksid ebareeglipärasuste ilmnemist oma kasutusvaldkonnas.

Paroolipoliitika ettekirjutuste järgimiseks tuleb pärast paroolide taastamist *default* -paroolivääruse kasutajatel kohe paluda oma paroolid järgmise sisselogimise käigus ära muuta. Juhul, kui paroolide taastamine *default* -väärtusele ei ole võimalik või kui paroolipoliitika seda keelab, tuleks luua juhuslikkuse põhimõttel uued paroolid ning need kasutajatele turvaliselt edasi anda, nt suletud ümbrikutes. Vastavad paroolid tuleb kohe pärast esimest sisselogimist ära muuta. Administraator peab ka kontrollima, kas kõik *default* -paroolid on kiirkorras ära muudetud. Juhul, kui andmeid on kustutatud või soovimatul moel muudetud, on neid võimalik varukoopiate abil taastada (vt M 6.51 Andmebaasi taastamine). Kui peaks ilmnema, et andmebaasi suhtes pannakse toime ettekavatsetud rünne, on kahjude minimeerimiseks ja võimalike täiendavate kahjude ärahoidmiseks tarvis kiiresti tegutseda. Selleks on vaja teavitamisplaani, mis sisaldaks loetelu kõikidest vajalikest sammudest ja määratleks, milliseid isikuid tuleb vastavast intsidendist informeerida (vt lisaks M 6.60 Turvaintsidentide käsitlusprotseduurid ja teavitamiskanalid). Teavitamisplaan võiks sisaldada vajadusel infot ka selle kohta, kas ning mil moel tuleks protsessi kaasata ka andmekaitsespetsialist ja organisatsiooni juristid.

Täiendavad kontrollküsimused:

- Kas kasutajaid informeeritakse regulaarselt selle kohta, et kõrvalekallete ilmnemisel on kohustuslik nendest kohe informeerida andmebaasi administraatorit?
- Kas seda ettekirjutust järgitakse?
- Kas on olemas vastavate teadmistega andmebaasi haldavad administraatorid?
- Kas on olemas taastekontseptsioon ning teavitamisplaan?
- Kas paroolide kiireks ja turvaliseks väljajagamiseks on kasutusele võetud asjakohane protseduur ning kas seda on piisavalt testitud?

M 6.49 Andmebaasi varundamine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator

Operatsioonisüsteemide andmevarundusprogrammide kasutamine ei ole andmebaasisüsteemi andmete täielikuks varundamiseks reeglina piisav. Vastavad programmid moodustavad sageli ainult vahelüli, mille kaudu saab varundamisele kuuluvaid andmeid kirjutada mõnele andmekandjale. DBMSi ja andmete varundamiseks tuleb enamike andmebaasitoodete puhul rakendada vastavaid DBMSi teenusprogramme. Kõige lihtsam andmete varundamisviis, mis on ühtlasi ka kõige turvalisem valik, on andmebaasi andmetest täieliku varukoopia loomineväljalülitatud seisundis. Varunduse käigus salvestatakse kõik andmebaasi kuuluvad andmed varunduse andmekandjale. Tihti pole aga antud protseduuri teostamine võimalik, kas nt andmebaasile kehtivate käideldavusnõuete või varundamisele kuuluva suure andmemahu tõttu.

Eelpool kirjeldatud täieliku varukoopia loomise alternatiiviks on andmebaasi online -varundus. Selle variandi puhul leiab varundus aset igapäevase kasutuse raames, st andmebaasi ei ole tarvis tööst välja lülitada. Antud varundusvariandi puudusteks on asjaolu, et ebakõlasid pole võimalik täielikult vältida ning fakt, et andmebaasi hävimise juhuks peab ka selle variandi puhul siiski eksisteerima ka veel täiendav offline -varundus, mille abil saab online -varundust taastada. Sel põhjusel tuleks online -andmevarundusi teha ainult siis, kui andmebaasi puhul nõutakse permanentset käideldavust. Sellele vaatamata ei tohiks täies mahus offline -varundusest loobuda, vaid need vastuvõetavate pikemate ajavahemike möödudes siiski läbi viia.

Üheks täiendavaks võimaluseks on andmebaasi osaline varundamine. Seda tuleks rakendada alati neil juhtudel, kus varundatava andmebaasi maht on liiga suur, et seda täies mahus korraga varundada. Vastavad piirangud võivad tekkida nt asjaolust, et varunduse andmekandjate salvestusruum ei ole piisav, või siis napib ajalist ressurssi täieliku andmevarunduse läbiviimiseks.

Võimalusel tuleks alati kahe offline -varunduse vahele jäävad transaktsioonid arhiveerida. Oracle pakub nt võimalust lülitada andmebaasis sisse nn ARCHIVE Mode . Transaktsioonid salvestatakse Oracle puhul nn log -failidesse, millest eksisteerib erinevaid versioone. Kõik logifailid täituvad üksteise järel infoga ning kui kõik logifailid saavad täis, hakatakse neid algusest jälle üle kirjutama. ARCHIVE-Mode loob nimetatud log -failidest enne nende ülekirjutamist varukoopiad. Sellise lahenduse puhul on võimalik andmebaasi hävimise korral kõiki aset leidnud transaktsioone taastada täies mahus. Ka selle variandi puhul on siiski eelduseks, et andmebaasist peab eksisteerima täiemahuline varukoopia. Asjakohase Recorvery -protsessi kestus kasvab vastavalt sellele, kui paljusid arhiveeritud log -faile on tarvis uuesti sisse lugeda.

Andmebaasisüsteemi andmete varundamiseks on tarvis luua eraldi andmevarunduskontseptsioon. Nimetatud kontseptsiooni mõjutavad järgnevad faktorid:

- Andmebaasi käideldavusnõuded - Juhul, kui andmebaas peab olema tööpäeviti ööpäevaringselt käideldav, saab täielikku andmevarundust läbi viia ainult nädalavahetusel, kuna enamasti tuleb andmebaas selleks otstarbeks eelnevalt välja lülitada.

- Andmemahud - Varundamisele kuuluvate andmete kogumahtu tuleb võrrelda kasutada olevate varundusandmekandjate salvestusruumiga. Võrdluse käigus tuleb kindlaks teha, kas andmekandjate salvestusruum (nt üks DAT-lint ühe varunduse kohta) on piisav andmebaasis oleva andmemahu varundamiseks. Juhul, kui see ei ole piisav, tuleb koostada andmevarunduskontseptsioon, mis näeb ette varundamisprotsessi jagamise osadeks. See võib nt tähendada, et erinevate rakenduste või andmebaasi erinevate osade andmeid varundatakse alati vahelduvalt, st varundatakse ainult värsked muudatused. Osalise andmevarunduse võimalikkus sõltub kasutatavast andmebaasi tarkvarast.
- Maksimaalselt talutav andmekadu - Siin tuleb kindlaks määrata, kas andmebaasi hävimise puhul on ühe päeva andmete kaotsiminek vastuvõetav, või tuleb andmebaas taastada kuni viimase asetleidnud transaktsioonini. Täielik taastamine on vajalik enamasti neil juhtudel, kus andmetele on kehtestatud kõrged käideldavus- või terviklusnõuded.
- Taaskäivitusaeg - Kindlaks tuleb määrata ka aeg, mis tohib kuluda andmebaasi taastamiseks pärast avariid, ilma et see rikuks andmebaasi käideldavusnõudeid.
- Andmebaasitarkvara poolt pakutavad andmevarunduslahendused - Andmebaasitarkvarad ei toeta reeglina kõiki mõeldavaid andmevarudnusvõimalusi, nt puudub paljudel osalise andmevarunduse tugi. Seetõttu tuleb igal konkreetsel juhul kontrollida, kas koostatud andmevarunduskontseptsiooni on ka reaalselt võimalik olemasolevate mehhanismidega ellu rakendada.

Selle loetletud info põhjal on võimalik koostada andmebaasidele vajalik andmevarunduskontseptsioon. Vastavas varunduskontseptsioonis (vt B 1.4 Andmevarunduspoliitika) määratakse muuhulgas kindlaks järgnevad aspektid:

- Korrakohase andmevarunduse läbiviimise eest vastutavad isikud
- Andmebaasi varundamise ajalised intervallid
- Andmebaasi varundamise viis
- Andmebaasi varundamistööde ajad
- Varundatava andmemahu spetsifikatsioon varunduse lõikes
- Andmevarunduse dokumenteerimise viis
- Andmevarunduseks kasutatavate andmekandjate hoiukoht

Näide
Varundamine esmaspäevast laupäevani.

- Algusaeg: hommikuti kell 3.00.
- Andmetest luuakse täielik varukoopia, milleks ei lülitata andmebaasi välja, vaid rakendatakse DBMSi online -varundamisvõimalust.

Varundamine pühapäeviti

- Algusaeg: hommikuti kell 3.00.

- Andmebaas lülitatakse välja ning kogu andmebaasi mahus luuakse täielik varukoopia.

Täiendavad kontrollküsimused:

- Kas on olemas dokumentatsioon, mis kirjeldab, kuidas taastada andmebaasi pärast selle avariid?
- Kas institutsioonil on olemas dokumenteeritud värske andmebaaside andmevarunduskontseptsioon?
- Kuidas toimub töötajate teavitamine neid puudutava kontseptsiooni osa kohta?
- Kas kontseptsiooni järgimist kontrollitakse?
- Kuidas arvestatakse mõjufaktorite võimalikku muutumist?

M 6.50z Andmehulkade arhiveerimine

Algatamise eest vastutavad: IT-turvaosakond, IT-juht

Rakendamise eest vastutavad: administraator

Kui andmebaasis olevate andmete puhul tekib vajadus neid arhiveerida, tuleb selleks koostada asjakohane kontseptsioon, mis peab tagama, et arhiveeritud andmehulgad oleksid tulevikus täies mahus kasutatavad, ning et neis ei esineks tervikluse kadusid. Siinkohal tuleb arvestada järgnevate punktidega:

Arhiveerimine

- Tuleb tuvastada, milliseid arhiveerimisvõimalusi saab arhiveerimiseks kasutada.
- Tuleb dokumenteerida, milline andmemudel võetakse arhiveeritavate andmete aluseks.
- Tuleb dokumenteerida arhiveerimise läbiviimise aeg.
- Tuleb dokumenteerida andmebaasi haldussüsteemi ning kasutatud teenusprogrammide versioon.
- Tuleb täpsustada arhiivi ülesehitus, süstemaatika ja korrakriteeriumid.
- Kõikidele arhiveerimisel kasutatavatele andmekandjatele tuleb tootjaandmete ja kasutuskogemuste põhjal määrata nende maksimaalne kasutusiga. Seoses kasutuseaga tuleb kindlaks määrata ka arhiveeritud andmehulkade värskendamine.
- Arhiveeritud andmehulkade nõutud käideldavust tuleb regulaarselt kontrollida ning viia vajadusel kooskõlla vastavate konkreetsete nõuetega. Hädavajalikud kohandamised mõjutavad muuhulgas arhiveerimiseks kasutatava andmekandja valikut ning ka arhiveerimisprotseduuri. Kõrgete käideldavusnõuete puhul tuleb vajadusel hoida ühest ja samast andmebaasist korraga mitut paralleelset ligipääsetavat ajaloolist andmebaasi versiooni.
- Tuleb tagada, et kehtestatud säilitusaegadest peetaks täpselt kinni.

Uuesti sisselugemine

- Arhiveeritud andmete uuesti sisselugemine ei tohi mõjutada värsket andmemahtu.
- Arhiveeritud andmehulkade uuesti sisselugemiseks peab olema piisavalt salvestiruumi.
- Arhiveeritud andmehulkasid peab olema võimalik taastada ka siis, kui vahepeal on aset leidnud muudatused andmemudelis või andmebaasi versioonis. Sellistel juhtudel peab olema andmete taastamiseks teada, millist andmemudelit ja milliseid teenusprogramme arhiveerimise hetkel kasutati.
- Kui uuesti sisseloetavaid andmed peavad olema mõne teenusprogrammi poolt töödeldavad, peab vajaminevast rakendusest eksisteerima ka selline versioon, mis on võimeline „vana“ andmemudelit töötlema.
- Regulaarselt tuleb kontrollida, kas arhiveeritud andmehulki on võimalik uuesti sisse lugeda.

Isikuandmeid sisaldavate andmehulkade arhiveerimisel tuleb lisaks eelnevale järgida veel ka andmekaitseseadusest tulenevaid nõudeid ja sellega seotud ettekirjutusi. See võib nt tähendada, et puudutatud isikutel võib olla õigus nõuda

nende kohta salvestatud andmete parandamist, kasutamise tõkestamist või kustutamist. Sõltuvalt asjaoludest võib andmetele olla kehtestatud nõue, et teatud aja möödudes tuleb need täies ulatuses, st ka nende kohta eksisteerivad varukoopiad ja arhiveeritud andmed kustutada. Selle tagamiseks tuleb välja töötada asjakohased tehnilis-organisatsioonilised meetmed. Eriti oluline on tagada, et pärast vanade andmemahtude uuesti sisselugemist säiliksid siiski ka kõik korrektuurid, muudatused, tõkked ja kustutused, mis on tehtud uuesti sisseloetava andmemahu varundamise ajahetke ja selle uuesti sisselugemise vahel.

Täiendavad kontrollküsimused:

- Kas on olemas dokumentatsioon, mis käsitleb arhiveeritud andmehulkade uuesti sisselugemist?
- Kas institutsioonil on olemas dokumenteeritud värske arhiveerimiskontseptsioon?
- Kuidas arvestatakse mõjufaktorite võimalikku muutumist?

M 6.51 Andmebaasi taastamine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator

Andmebaasi taastamiseks tuleb koostada kontseptsioon, mis reguleerib andmebaasist loodud varukoopiate uuesti sisselugemist. Vastava kontseptsiooni aluseks on järgnevad punktid:

- Andmevarunduskontseptsioon (vt M 6.49 Andmebaasi varundamine)
- Võimalikud veasituatsioonid, mis võivad tekitada vajaduse andmebaasist loodud varunduste sisselugemiseks (vt M 6.48 Protseduurid andmebaasi tervikluse kao puhuks).

Nende punktide alusel tuleb välja selgitada, milliseid andmebaasivarundusi on tarvis teatud konkreetsel kujul uuesti sisse lugeda.

Andmebaasi taastamine võib kujuneda keerukaks ülesandeks, mis nõuab ülimalt hoolikat protseduuri järgimist, mille erinevaid samme on tarvis regulaarsete testimistega hoolikalt üle kontrollida. Sellele vaatamata võib siiski juhtuda, et taastamisprotsess ei kulge sujuvalt ega veavabalt.

Taastamise puhul on tarvis omavahel kooskõlla viia kaks aspekti. Ühelt poolt on tarvis vastav andmebaas nii kiiresti kui vähegi võimalik kasutajatele jälle töökorda seada, teiselt poolt jällegi tuleb andmebaas taastada võimalikult värskete andmetega ning peale selle peab analüüsima ka veel kahju tekkimise põhjuseid. Kui andmebaasi avariid ei saa üheselt seostada riistavaras asetleidnud rikkega, on tihti väga raske tuvastada, kui laialdase tervikluse kaoga võib olla tegemist. Samuti pole andmebaasi alati võimalik niisama lihtsalt ilma probleemideta taastada seisundis, mis kajastaks ka viimast tegevust enne vea tuvastamist.

Sellistel juhtudel tuleb otsustada, kumba varianti parasjagu eelistatakse, kas mõningase uuema informatsiooni kadu, või pikemaajalist tööseisakut. See sõltub suuresti ka andmebaasi kasutusvaldkonnast, vea liigist ning ajast, mis jääb vea tekkimise ja tema avastamise vahele, st ajast, mil veale reageeritakse. Tihti on kahjude ulatust raske kindlaks teha siis, kui need võivad olla põhjustatud väärast haldamisest või volitamata manipuleerimisest.

Sellisteks juhtudeks tuleks koostada otsustamist aitavad suunised ja asjakohased tegutsemisjuhised, mis peaksid leidma oma kindla koha taastekontseptsioonis. Selleks, et andmebaasi oleks võimalik jälle kiiresti töökorda seada, tuleks vastav andmebaas taastada kas mõnes eraldatud süsteemis või eraldi salvestiruumi piires ja seejärel kasutajatele kättesaadavaks teha. Kui juurdepääsufunktsioonid on andmetest eraldatud, (vt M 2.134 Andmebaasipäringute suunised), saab seda enamatel juhtudel teostada kasutajate jaoks piisavalt läbipaistvalt.

Hävinud andmebaasi ei tohi mitte mingil juhul ilma kontrollimata (vt M 6.48 Protseduurid andmebaasi tervikluse kao puhuks) lihtsalt andmevarunduse sisselugemisega üle kirjutada. Andmebaase, mille puhul arvatakse, et need on kaotanud oma tervikluse, on tihti võimalik taastada, ilma et selleks oleks tarvis andmebaasi täies mahus uuesti luua. Pigem on tarvis taastada ainult mõningaid üksikud andmehulgad. Osalise taastamise puhul tuleks samuti kaaluda, kas taastada andmebaas esmalt võib-olla mõnes muus asukohas, nt testsüsteemis ning seada originaalandmebaas töökorda alles pärast seda, kui on kindel, et seda on ka reaalselt võimalik korrakohaselt taastada. Ka neil juhtudel, kui on kindel, et andmebaasi ei õnnestu enam parandada, tuleks vastavat andmebaasi siiski säilitada, et seda analüüsida ja selgitada välja vea põhjus.

Taastekontseptsioonis peaks olema kindlaks määratud, millises ulatuses tuleb avariijuhtudeks valmis hoida erinevaid ressursse. Märksõnadeks, millega tuleb siinkohal kindlasti arvestada, on salvestusmahud ja kõvaketta sektorid. Neid suurusi tuleb regulaarselt värske andmebaasi suuruse alusel üle kontrollida, et avarii korral oleks selle mõju teistele andmebaasidele võimalikult minimaalne.

Täiendavad kontrollküsimused:

- Kas andmebaasidest loodud varukoopiate uuesti sisselugemise kohta on koostatud kontseptsioon?
- Millal harjutati viimati andmebaasivarunduste uuesti sisselugemist?
- Kas avariijuhtudeks hoitakse piisavat andmekandjate varu?

M 6.52 Võrgu aktiivkomponentide konfiguratsiooniandmete regulaarne varundamine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator

Tsentraalsetele võrgu aktiivkomponentidele tuleb reeglina seada kõrged käideldavusnõuded, kuna kohtvõrgu sujuvast töötamisest sõltuvad reeglina korraga paljud kasutajad. Selleks, et vea esinemise järel võimalikult kiiresti tööd jätkata, tuleb elektroonilisel kujul varundada aktiivsete võrgukomponentide konfiguratsiooniandmeid (vt M 6.32 Regulaarne andmevarundus ja M 6.91 Marsruuterite ja kommutaatorite andmete varundus ja taaste). Seda varundust võib üldjuhul teha ka lokaalselt üksikute komponentide juures eraldi, või siis läbi võrgu, nt võrguhaldustööriista kaasabil. Juhtudel, kus andmed on varundatud elektroonilisel kujul, on konfiguratsioone võimalik taastada palju kiiremini ja turvalisemalt kui neil juhtudel, mil konfiguratsioonid on suure ajakuluga käsitsi üles kirjutatud. Andmete sisselugemine võib toimuda sellistel juhtudel automaatselt, nt võrguhaldustööriista abil või käsitsi, administraatori sekkumisel.

Vältige TFTPd

Konfiguratsiooniandmete varundamisel läbi võrgu tuleb vastupidiselt lokaalsele varundamisele arvestada, et andmete võrgu kaudu edastamisel võib tekkida võimalus nende volitamata lugemiseks, mis tähendab, et potentsiaalsel ründajal võib tekkida võimalus ligi pääseda aktiivsete võrgukomponentide turvalisuse seisukohast kriitilise tähtsusega infole nagu paroolidele, mille tagajärjel võib ründaja välja selgitada terve võrgu konfiguratsiooni. Tihti kasutatakse selleks protokolle nagu TFTP (Trivial File Transfer Protocol) või RCP (Remote Copy Protocol), kusjuures võimalusel tuleks kasutada RCPd koos autentimisega (vt M 5.20 rlogin, rsh ja rcp turbemehhanismid). TFTP seevastu ei paku konfiguratsiooniandmete volitamata juurdepääs vastu mitte ühtki kaitsemehhanismi (vt M 5.21 telneti, ftp, tftp, rexeci turvaline kasutamine), mistõttu tuleks selle kasutamisest loobuda.

Taastatavuse kontrollimine

Kõikide varundamismeetodite puhul tuleb läbi viia test ja välja selgitada, kas varundus on tehtud korralikult, ning kas varundusest on võimalik andmeid taastada. Eriti kehtib see võrgu kaudu tehtavate varunduste puhul, kuna mõnikord võib võrk olla ka sellises seisundis, et võrgu kaudu taastamine ei ole enam võimalik.

Kontrollküsimused:

- Kas kõikide aktiivsete võrgukomponentide konfiguratsiooniandmed on varundatud?
- Kas andmevarundusprotseduur on dokumenteeritud?
- Kas andmevarunduseks kasutatav protseduur on kooskõlas olemasoleva andmevarunduskontseptsiooniga?

M 6.53z Võrgukomponentide liiasus

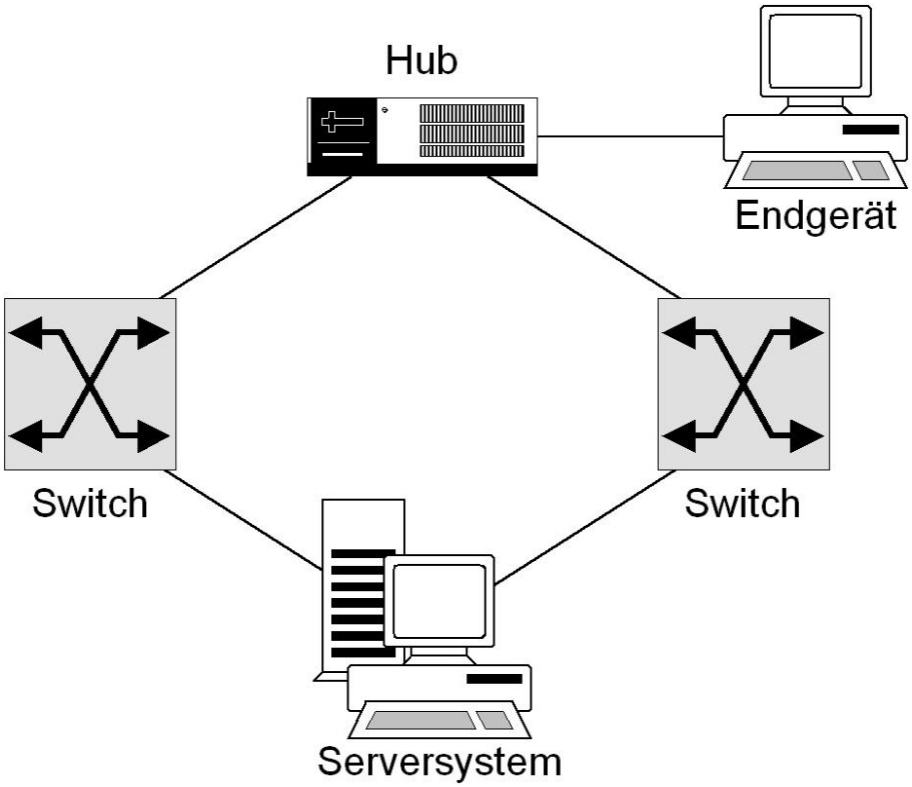
Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator, varumisosakond

Tsentraalsetele võrgukomponentidele tuleb reeglina seada kõrged käideldavusnõuded, kuna kohtvõrgu sujuvast töötamisest sõltuvad reeglina korraga paljud kasutajad. Selleks, et vea korral saaks tööga võimalik kiiresti edasi minna, tuleb sõltuvalt kehtivatest käideldavusnõuetest luua vastavates valdkondades liiasus, mis peab suutma ennetada oluliste võrgukomponentide osalist või täielikku avariid.

Liiasuse loomiseks on valida erinevate võimaluste vahel:

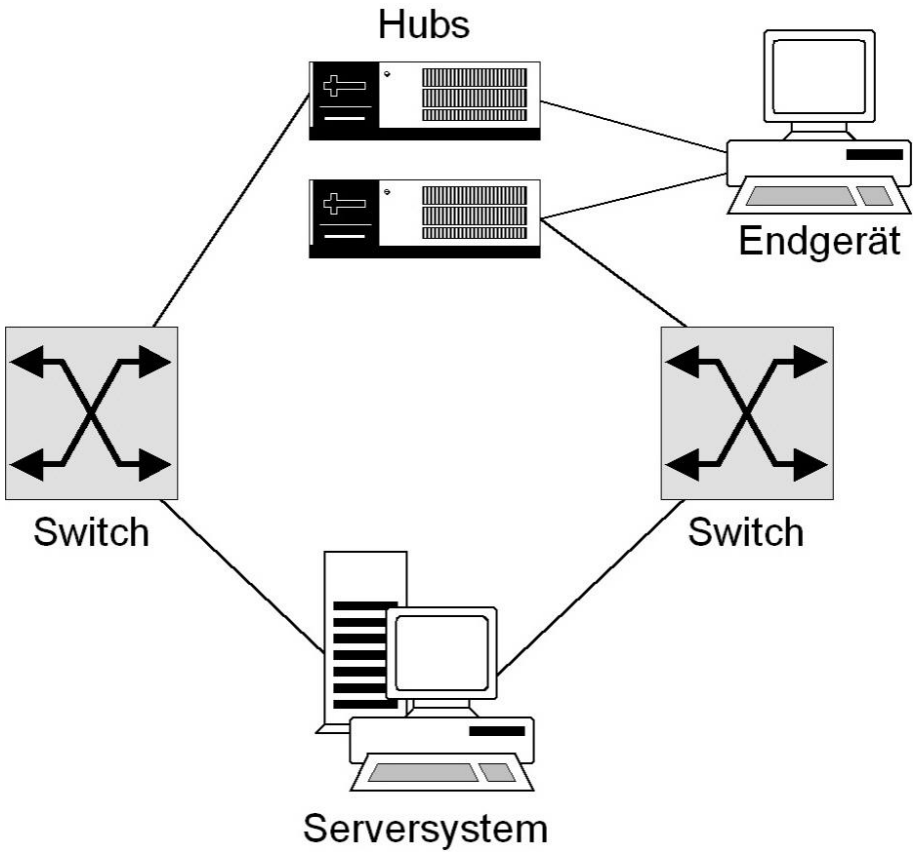
- Võrgukomponentide varuseadmeid võib hoida laos, et avarii korral oleks võimalik neid lühikese aja jooksul välja vahetada. Kui seda põhimõtet ei järgita, tuleb enne rikke kõrvaldamist tihti läbi teha soetamisprotseduurid, mis nõuavad palju aega. Alternatiivseks lahenduseks on sõlmida vastavate tootjatega hooldus- või tarnelepingud, mis garanteeriksid defektsete komponentide kiire asendamise. Seejärel võib varundatud konfiguratsiooniandmed uuesti sisse lugeda, et avariist puudutatud võrgusegmentide seisakuajad oleksid võimalikult lühikesed (vt M 6.52 Võrgu aktiivkomponentide konfiguratsiooniandmete regulaarne varundamine).
- Lisaks on mõttekas juba võrgu kontseptsiooni väljatöötamise käigus planeerida ka võrgukomponentide liiasus. Selle alusel peaksid kõik kesksed kommutaatorid ning sõltuvalt kasutatavatest protokollidest ka kõik marsruuterid olema võrku ühendatud topelt, et tagada liiasused serveriühendustes ning üksikute võrgukomponentide omavahelistes ühendustes (vt joonis 1). Korrektne funktsioneerimine tuleb tagada sobiva loogilise võrgukonfiguratsiooniga.



Joonis 1: võrgukomponentide liiasusega ühendused

Hub – jaotur, Endgerät – lõppseade, Switch – kommutaator, Serversytem - serverisüsteem

Juhul, kui sõltuvalt käideldavusnõuetest on liiasusega tarvis varustada ka lõppseadmed, tuleb täiendavalt ka kõik lõppseadmed varustada kahe võrguadapteriga (vt joonis 2).



Joonis 2: kuni lõppseadmeteni ulatuv liiasus

Hubs – jaoturid, Endgerät – lõppseade, Switch – kommutaator, Serversytem - serverisüsteem

Igal konkreetsel juhul tuleb kontrollida, kas rakendatavad aktiivsed võrgukomponendid ja operatsioonisüsteemid toetavad sellist tehnikat.

Lisaks on aktiivsete võrgukomponentide puhul sagedaseks rikkepõhjuseks nende toiteallikas, kuna see sõltub elektritoite stabiilsusest. Seetõttu on paljusid võrgukomponente võimalik varustada mitme toiteallikatega või on need koguni nendega juba varustatud. Niimoodi on võimalik tõsta võrgukomponentide avariikindlust, ilma et tuleks rakendada korraga kahte võrgukomponenti. Samas tuleb aga arvestada, et sellised meetmed ei tõsta võrgukomponentide tegeliku funktsiooni avariikindlust. Kõikidel juhtudel tuleb hoolika analüüsimisega välja selgitada, millised konkreetsed käideldavusnõuded parasjagu kehtivad. Süsteemi- ja võrguarhitektuuri detailse planeerimistöö raames tuleb seejärel välja töötada sobiv liiasuse kontseptsioon, mis peab täitma vajalikke nõudeid. Antud kontekstis tuleks järgida ka meedet M 6.18 Varuliinid .

Täiendavad kontrollküsimused:

- Kas võrgu käideldavusnõuded on tuvastatud ja dokumenteeritud?
- Kas kõikidest olulistest võrgukomponentidest eksisteerivad laovarud või eksisteerivad nende kohta tarnelepingud?
- Kas võrgu planeerimistööde raames arvestati ka komponentide liiasuste loomisega?

M 6.54 Protseduurid võrgu tervikluse kao puhuks

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator, kasutaja

Väärkasutuse sarnane kasutus

Juhul, kui võrk ei käitu nii nagu ette nähtud (nt puudub juurdepääs serveritele, võrguressurssidele ei ole võimalik juurde pääseda, võrgu jõudlus katkeb pidevalt), võib tegu olla võrgu tervikluse kaoga. See võib olla põhjustatud võrgu väärkasutusele sarnanevast kasutamisest, nt aktiivsete võrgukomponentide konfiguratsiooni muutmisest või nende kahjustamisest.

Neil juhtudel peaksid kasutajad arvestama järgnevate punktidega:

- Salvestage oma töö ja sulgege aktiivsed programmid.
- Administraatori teavitamine - Kasutajad peavad sobiva teavitamiskanali (nt kasutajate abiliini) kaudu informeerima olukorrast administraatorit. Siinkohal tuleb muuhulgas hoolitseda ka selle eest, et teavitamine ei segaks administraatorit liigselt tema olulistes töödes.

Võrguadministraator peaks läbi tegema järgnevad sammud:

- Veakäitumise piiritlemine, tuvastades konkreetse võrgusegmendi ehk võrgukomponendi
- Sealsete aktiivsete võrgukomponentide konfiguratsiooni kontrollimine (siia alla kuulub ka paroolide kontrollimine)

Logifailide varukoopiate loomine

- Kõikide failide , mis võiksid anda infot tekkinud probleemi liigi ja põhjuse kohta (nt kas tegu oli reaalse ründega ning millisel viisil õnnestus ründa- jal süsteemi sisse tungida) varundamine, st eriti oluline on varundada kõik olulised logifailid
- Vajadusel originaal-konfiguratsiooniandmete uuesti sisselugemine (vt M 6.52 Võrgu aktiivkomponentide konfiguratsiooniandmete regulaarne varundamine),
- Vajadusel kasutatava riistvara (juhtmestiku, pistikühenduste, aktiivsete võrgukomponentide) kontrollimine defektide suhtes

Teavitamisplaani kasutamine

- Kõikide kasutajate teavitamine koos palvega, et nad kontrolliksid ebareeglipärasuste ilmnemist oma kasutusvaldkonnas.

Kui peaks ilmnema, et võrgu suhtes pannakse toime ettekavatsetud rünnet, on kahjude minimeerimiseks ja võimalike täiendavate kahjude ärahoidmiseks tarvis kiiresti tegutseda. Selleks on vaja teavitamisplaani, mis sisaldaks loetelu kõikidest vajalikest sammudest ja määratleks, milliseid isikuid tuleb vastavast intsidendist informeerida (vt M 6.60 Turvaintsidentide käsitlusprotseduurid ja teavitamiskanalid). Teavitamisplaan võiks sisaldada infot ka selle kohta, kas ning mil moel tuleks protsessi kaasata ka andmekaitsespetsialist ja organisatsiooni juristid.

Kontrollküsimused:

- Kuidas tagatakse administraatori efektiivne teavitamine?
- Kas seda ettekirjutust järgitakse?
- Kas paroolide kiireks väljajagamiseks on kasutusele võetud asjakohane protseduur ning kas seda on piisavalt testitud?

M 6.56 Andmevarundus krüptoprotseduuride kasutamisel

Algatamise eest vastutavad: IT-juht, IT turvaosakond

Rakendamise eest vastutavad: IT turbespetsialist

Krüptograafiliste protseduuride rakendamisel ei ole andmevarundusega seotud küsimused sugugi teisejärgulised. Lisaks küsimusele, kuidas oleks kõige mõistlikum krüpteeritud andmeid varundada, tuleks ka järele mõelda, kas ja kuidas peaks salvestama kasutatavaid krüptograafilisi võtmeid. Lisaks oleks mõttekas luua varukoopiad ka täiendavalt rakendatavate krüpteerimistoodete konfiguratsiooniandmetest.

Võtmete andmevarundus

Kasutatavate krüptograafiliste võtmete puhul tuleks väga täpselt järele mõelda, kas ja kuidas neid salvestada, kuna iga võtmekoopia kujutab endast potentsiaalset riski. Sellele vaatamata võib krüptograafiliste võtmete salvestamine olla erinevatel põhjustel lausa möödapääsmatu.

Võtmete salvestamiseks saab kasutada mitmeid erinevaid meetodeid:

- salvestamine transportimise eesmärgil kaasaskantava andmekandja peale, nt disketile, kiipkaardile (rakendatakse ennekõike võtmete väljajagamiseks ja võtmevahetuseks, vt M 2.46 Krüpteerimise õige korraldus);
- salvestamine IT-komponentidesse, millel peab olema pidev juurdepääs krüptograafilistele võtmetele, nt andmeside krüpteerimiseks;
- võtmete deponeerimine eesmärgiga ennetada nende kaotsiminekut või selleks, et rakendada neid töötajate asenduste käigus.

Siinkohal tuleb arvestada järgmiste aspektidega:

- Krüptograafilisi võtmeid tuleks salvestada ja hoida selliselt, et volitamata isikutel ei tekiks võimalust neid märkamatult välja lugeda. Võtmeid võiks salvestada nt spetsiaalsesse turvariistvarasse, mis suudab võtmed ründe korral automaatselt kustutada. Tarkvarasse salvestamise puhul tuleb need igal juhul üle krüpteerida. Siinkohal tuleb arvestada, et enamik standardseid rakendusi, mille puhul võtmed või paroolid salvestatakse otse rakenduse enda alla, toimub salvestamine selliste protseduuridega, mida on küllaltki lihtne murda. Täiendava variandina saab võtmete salvestamiseks rakendada nelja silma põhimõtet, st salvestada võti poole või erinevate osade kaupa.
- Andmesidevõtmete ja muude lühiajaliste võtmete puhul tuleks varukoopiate tegemisest loobuda. Volitamata kasutuse välistamiseks tuleks üldjuhul loobuda koopiate tegemisest ka privaatsete allkirjavõtmete puhul. Kui aga võtmete salvestamiseks on valitud puhtalt tarkvaraline lahendus, st kui ei kasutata kiipkaarte ega muud sarnast, tekib kõrgendatud oht võtme kadumiseks, nt bitivigade või kõvaketta defekti näol. Sellistel juhtudel võib võtmete piisavalt turvalise deponeerimisvõimaluse loomine osutuda tunduvalt vähem tülikaks kui kohustus hakata iga võtmekaotuse puhul vastavast sündmusest oma sidepartnereid informeerima.

- Pikaealistest võtmetest, mida rakendatakse nt andmete arhiveerimiseks või andmesidevõtmete genereerimiseks, tuleks ilmtingimata luua ka vastavad varukoopiad.

Krüpteeritud andmete varundamine

Krüpteeritud andmete varundamisel ehk krüpteerimise kasutamisel andmevarunduse käigus tuleb olla väga hoolikas. Kui protsessi käigus peaks tekkima viga, pole sellest puudutatud mitte ainult mõningad andmehulgad, vaid kasutuskõlbmatuks muutuvad tihti kõik andmed.

Täiendavaid probleeme toob endaga kaasa veel ka olukord, kus krüpteeritud või digitaalselt allkirjastatud andmeid on tarvis salvestada pikemaajalise ladustamise eesmärgil. Siinkohal pole mitte ainult tarvis tagada, et andmekandjaid regulaarselt värskendataks ja et säilitataks andmete töötlemiseks vajalikud tehnilised komponendid, vaid ka seda, et kasutatud krüptograafilised algoritmid ja võtmepikkus vastaksid kaasaegsetele tehnilistele nõuetele. Andmete pikemaajalise arhiveerimise puhul võib seetõttu olla mõttekam salvestada need krüpteerimata kujul ning hoolitseda pigem nende turvalise ladustamise eest, hoides neid nt seifis.

Ettevaatlikkusest lähtudes tuleks ka kasutatud krüptomoodulid alati arhiveerida, kuna kogemused näitavad, et ka aastaid hiljem võidakse avastada andmeid, mida ei hoitud arhiivis.

Rakendatud toodete konfiguratsiooniandmete andmevarundus

Keerulisemate krüpteerimistoodete puhul ei tohiks unustada nende konfiguratsioonide varundamist (vt M 4.78 Konfiguratsioonimuudatuste hoolikas teostamine). Valitud konfiguratsioon tuleks dokumenteerida selliselt, et süsteemi võimalikuavarii või taasinstalleerimise korral oleks võimalik seda kiirelt taastada.

Kontrollküsimused:

- Kas ettevõttes või ametiasutuses on loodud ettekirjutused, kuidas peaks toimuma krüpteerimisvõtmete deponeerimine?
- Kuidas tagatakse, et krüpteeritult salvestatud andmed on ka pikema aja möödudes jätkuvalt ligipääsetavad?

M 6.57 Avariiplaani koostamine haldussüsteemi avarii puhuks

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator

Haldussüsteemi avarii võib tekkida erinevatel põhjustel nagu nt tarkvarast või riistvarast tingitud arvutirike, elektrikatkestus või sabotaaž. Kuna haldussüsteeme rakendatakse enamasti suuremate süsteemide puhul, tuleks sellistele süsteemidele koostada nii avariiennetuskontseptsioon vastavalt moodulile B 1.3 Hädaplaanimine kui ka andmevarunduse kontseptsioon (vt B 1.4 Andmevarunduspoliitika). Avariiennetuskontseptsioonis tuleb kehtestada ja dokumenteerida ka juhised haldussüsteemi avarii puhuks. Eriti oluline on välja töötada käitumisreeglid haldussüsteemi erinevate komponentide (*Manager, Management Server, Management Console*) avariide puhuks.

Sellele lisaks tuleb koostada haldussüsteemile kas tervikuna või siis selle üksikute komponentide lõikes taasteplaan. Ideaaljuhul peaks haldussüsteem oma funktsiooni taastama automaatselt. Andmevarunduse raames tuleks pöördumatu andmekao (ketta kokkujooksmise) ennetamiseks luua haldussüsteemi tarkvarast varukoopiad. Nende hoiukoht tuleb üles märkida avariikäsiraamatusse. Käsiraamatusse tuleks muuhulgas üles märkida ka informatsioon, mis on vajalik hoiukohta sissepääsemiseks või sellesse juurdepääsu loomiseks, nt kolleegide nimed ja telefoninumbrid, kes teavad vajalikku seifikombinatsiooni või paroole (vt M 2.22 Paroolide deponeerimine).

M 6.58 Turvaintsidentide käsitluse haldussüsteemi rajamine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond
Rakendamise eest vastutavad: IT turvaosakond

IT valdkonna osatähtsuse kasvuga paljude ametiasutuste ja ettevõtete igapäevastes tööprotsessides kasvab üha enam ka sõltuvus IT korrektsest toimimisest.

Seetõttu on IT turvaosakonna üks olulisi ülesandeid valmistada ennast piisavalt hästi ette kõikvõimalike turvaintsidentide käsitlemiseks. Turvaintsidente võivad põhjustada paljud erinevat liiki sündmused, mille tagajärjeks võib olla nt andmete, üksiku IT-süsteemi või terve võrgu käideldavuse, tervikluse ja/või konfidentsiaalsuse kadu. IT turvahalduse raames käsitlemist vajavad intsidendid on juhtumid, millega tuleb spetsiaalselt tegeleda seetõttu, et need sisaldavad potentsiaali suurte kahjude tekkeks. Turvaprobleemid, mis tekitavad piiratud kujul kahju ainult kohapeal või mis võiksid sellist kahju tekitada, peaks lahendama kohapealsed vastutavad töötajad, et IT turvahaldust mitte üle koormata.

Turvaintsidentide käsitlemisega seotud eesmärgid

Turvaintsidentide käsitlemine kui IT turvahalduse osa täidab järgmisi eesmärke:

- Reageerimisvõime tagamine, et turvaintsidente ja turvaprobleeme oleks võimalik õigel ajal avastada ja sellest vastutavatele osakondadele teada anda.
- Otsustusvõime tagamine, et hinnata, kas sündmuse puhul on tegu lokaalse turvaprobleemi või turvaintsidendiga.
- Tegutsemisvõime tagamine, et turvaintsidendi puhul rakendataks võimalikult kiiresti vajalikke vastumeetmeid.
- Kahjude minimeerimine, teavitades õigel ajal ka kõiki teisi potentsiaalselt ohustatud osapooli.
- Efektiivsuse tagamine, hoolitsedes turvaintsidentide käsitlemist kajastavate õppuste läbiviimise ja nende kontrollimise eest.

Juhtkonna tasandi kaasamine

Nimetatud eesmärkide saavutamiseks on tarvis sisse seada turvaintsidente käsitlev haldussüsteem. Üks vältimatuid eeldusi on siinkohal ettevõtte või ametiasutuse juhtkonna kaasamine, kelle kohustuste hulka kuulub vastava haldussüsteemi elluviimine ja kes peab hoolitsema vajamineva IT turbe alase teavitustöö, otsustusõiguste määramise ning IT-turbeesmärkide saavutamise eest.

Turvaintsidente käsitleva haldussüsteemi juurutamisel võib umbkaudu lähtuda järgmistest sammudest:

1. samm: valdkonna kajastamine turvapoliitika raames.

Turvaintsidentide käsitlemine kui IT turvahalduse osa peaks olema lahti kirjutatud ettevõtte või ametiasutuse turvapoliitikas või siis selle turvakontseptsioonis. Siinkohal tuleb kindlaks määrata, kuidas peavad kasutajad ja teised puudutatud osapooled teavitama turvaprobleemidest ja turvaintsidentidest vastavaid turbe eest vastutavaid töötajaid. Lisaks tuleb kirjeldada ka otsuse langetamise protsesse ning luua hädavalik motivatsioon. Kõnealuse teema kajastamisega turvapoliitikas luuakse selge märk sellest, et ettevõtte või ametiasutuse juhtkond toetab IT turvet.

2. samm: vastutusalade defineerimine

Selle sammuga määratakse erinevate töötajate vastutus seoses turvaintsidentide esinemisega.

Järgnevate näidisülesannete eest kannavad vastutust nt järgmised grupid:

- IT kasutajad: info edastamine turvaprobleemide ja -intsidentide esinemise kohta.
- IT administraatorid: teadete vastuvõtmine ning esimese otsuse langetamise ettevalmistamine, et hinnata, kas tegemist on turvaprobleemi või turvaintsidendiga ning kas sündmust tuleb suunata kõrgemale otsustustasandile või mitte.
- IT-rakenduste eest vastutajad: kaasamine puudutatud süsteemide kaitsevajaduste kandjatena otsuste langetamisel ja abimeetmete valikul.
- IT turvaspetsialist või IT turvaosakond: teadete vastuvõtmine ja otsuse langetamise, kas tegemist on turvaprobleemi või turvaintsidendiga, ning eskalatsiooniprotseduuri ja vajalike abimeetmete algatamine.
- Turvaintsidendi meeskond: puudutatud IT administraatoritest, IT kasutajatest, IT turbespetsialistist, avalike suhete töötajast ja vajaduse korral ka juhtkonna liikmest koosnev meeskond, kes peab tegelema turvaintsidendi lahendamisega.
- Avalike suhete osakond või pressikeskus: vajaduse korral turvaintsidenti käsitleva infopoliitika ettevalmistamine.
- IT turvarevisjon: haldussüsteemi kontrollimine ja turvaintsidendi järelanalüüs.
- Ametiasutuse/ettevõtte juhtkond: kokkuvõtva otsuse langetamine.

Vastutusalad tuleb kindlaks määrata ja kehtestada. Täiendavat infot leiate meetmest M 6.59 Turvaintsidentide käsitlemise eest vastutavate isikute määramine eest vastutavate isikute määramine.

3. samm: turvaintsidentidega seotud käitumisreeglid ja teavitamiskanalid

Turvaintsidentide efektiivse käsitlemise tagamisel on määrava tähtsusega puudutatud isikute õige käitumine, mis tähendab, et nad peavad säilitama rahu ja andma info tekkinud olukorra kohta viivitamata edasi. Selleks on vaja kehtestada käitumisreeglid (rahu säilitamine, teavitamiskohustus, täiendava info edastamise kohustus seoses raamtingimustega jms) ning lisaks tuleb töötajaid selles vallas ka vastavalt koolitada. Eriti oluline on siinjuures kindlaks määrata isikud, keda tuleb IT turvaprobleemist või turvaintsidendist informeerida.

Eelnev arvestamine tüüpiliste turvaintsidentidega

Seoses tüüpiliste esineda võivate turvaintsidentidega (nt arvutiviiruste avastamise, siseringist pärit isiku läbiviidud andmemanipulatsioonide, võõraste isikute häkkimiskatsete jms) on võimalik juba eelnevalt välja töötada asjakohased tegutsemisjuhised, kust peaks selguma, mida niisugustel juhtudel teha tuleb. Niimoodi kiirendatakse reageerimisvõimet hädaolukorras ja aidatakse minimeerida potentsiaalseid kahjusid. Kuna vastavate tegutsemisjuhiste väljatöötamisega seotud vaev ei ole just tühine, tuleks piirduda olulisemate planeeritavate valdkondadega (vt M 6.60 Turvaintsidentide käsitlusprotseduurid ja teavitamiskanalid).

4. samm: turvaintsidentide eskalatsioonistrateegia

Mida kriitilisema turvaintsidendiga on tegu, seda rohkem kompetentsi on reeglina vaja selle käsitlemiseks. Olukord võib jõuda selleni, et protsessist tuleb informeerida ja sellesse kaasata ka ametiasutuse või ettevõtte juhtkond, et võtta vajaduse korral kasutusele hädavajalikke meetmeid, nagu info levitamise keeld, politsei kaasamine, suurte väljaminekutega seotud asendusmeetmed jne. Selle toimimiseks on aga juba eelnevalt tarvis välja töötada eskalatsioonistrateegia, kus kirjeldatakse, keda täpselt tuleb hädaolukorras protsessi kaasata. Täiendavat infot leiate meetmest M 6.61 Turvaintsidentide käsitluse eskalatsioonistrateegia .

5. samm: prioriteetide kehtestamine

Kuna turvaintsident tekib reeglina erinevate põhjuste koosmõjul ja mõjutab IT erinevaid rakendusvaldkondi, tuleks rakendatavad abimeetmed seada tähtsuse järjekorda. Prioriteetide kehtestamine sõltub kaitsevajadusest, IT kasutusvaldkondadest, IT-rakendustest ja ka ametiasutuse või ettevõtte individuaalsetest tingimustest. Analoogselt kaitsevajaduse väljaselgitamisele tuleks juba eelnevalt määrata tähtsuse järjekord, et oleks teada, millist tööde järjekorda tuleks turvaintsidendi tagajärjel tekkinud kahjuga tegelemisel järgida (vt M 6.62z Prioriteetide kindlaksmääramine turvaintsidentide käsitlemiseks).

6. samm: turvaintsidentide uurimis- ja hindamismetoodika koostamine

Pärast teate saabumist turvalisusega seotud ebareeglipärasuse kohta tuleb esmalt otsustada, kas tegemist on lokaalse turvaprobleemi või hoopis turvaintsidendiga, mille puhul tuleb võib-olla karta ka suuremate kahjude tekkimist. Otsuse langetamisel tuleb arvestada erinevate teguritega (potentsiaalse kahju suurus ja hilisemad kahjud, põhjus, puudutatud IT-süsteemid, hädavajalikud kohesed meetmed) ja need üksteise suhtes läbi kaaluda. Vajaduse korral tuleb eskalatsioonistrateegia kohaselt kaasata protsessi järgmised haldustasandid.

7. samm: turvaintsidentide kõrvaldamisega seotud abimeetmete rakendamine

Turvaintsidentide kõrvaldamisega seotud meetmete rakendamise puhul tuleb arvestada, et kõik vastavad meetmed võetakse tihti suure ajasurve all. Seetõttu pole sugugi välistatud, et selliste meetmete käigus võivad tekkida omakorda uued probleemid. Sel põhjusel on mõistlik dokumenteerida meetmed piisavalt põhjalikult. Lisaks tuleks juhtumi puhul mõelda ka sellele, kuidas karistada vastavat (siseringi) „kurjategijat" eeldusel, et tegemist on ettekavatsetud tegevusega. Olenevalt olukorrast tuleb kaaluda muutusi personalis (vt M 6.64 Turvaintsidentide likvideerimine).

8. samm: asjassepuutuvate osapoolte teavitamine

Olukorras, kus turvaintsidendi puhul peaks selguma, et selle mõju võib avalduda ka väljaspool oma ametiasutuse, ettevõtte või selle üksikute allüksuste piire, tuleb kahjude minimeerimise eesmärgil teavitada sündmustest ka kõiki potentsiaalselt puudutatud osapooli. Selleks tuleb juba eelnevalt kindlaks määrata asjakohased sidekanalid ja läbi viia sõltuvusanalüüs, et teavitamisprotseduuri kiirendada (vt M 6.65 Asjassepuutuvate isikute teavitamine turvaintsidentidest).

9. samm: turvaintsidendi järelanalüüs

Selleks, et asetleidnud turvaintsidendist ka midagi kasulikku õppida ja infot koguda, tuleks kehtestada nõue, et turvaintsidentidele tuleb teha ka järelanalüüs. Tihti on niimoodi võimalik saada infot, mille alusel saab turvaintsidentide käsitlemist muuta veelgi paremaks, või andmeid, mille põhjal saab hinnata IT rakendatud turvakontseptsiooni tõhusust. Muu hulgas tuleb arvestada järgmiste aspektidega (vt lisaks M 6.66 Turvaintsidentide järelhindamine):

- reageerimisaeg,
- teavitamiskanali tundmine,
- eskalatsioonistrateegia tõhusus,
- kontrolli efektiivsus,
- asjassepuutuvate osapoolte teavitamisvõimalused.

10. samm: turvaintsidentide avastamismeetmed

Mida kiiremini turvaintsident avastatakse ja sellekohane info edastatakse, seda efektiivsemalt saab kasutusele võtta vastuabinõusid. Siinkohal võib olla mõttekas rakendada tehnilisi tuvastusmeetmeid, et vähendada inimese sekkumisel tekkivaid viivitusi. Eraldi tuleks siinkohal esile tuua viirusetõrjetarkvara, logiandmete analüüsimine ja sissetungi tuvastamise süsteemid. Vastavate meetmete valikut, aktiveerimist ja nende teavitamiskanaleid kirjeldatakse lähemalt meetmes M 6.67 Turvaintsidentide avastamismeetmete rakendamine.

11. samm: efektiivsuse kontrollimine

Kontseptsiooni koostamine ja selle regulaarne värskendamine

Turvaintsidentide käsitlemiseks rakendatava haldussüsteemi efektiivsuse hindamiseks ja sellega seotud haldusülesannete praktilise teostuse soodustamiseks tuleb selle kasutamist harjutada, st situatsioone läbi mängida. Kuna see kõik nõuab suure hulga personali kaasamist ja võib muutuda igapäevatöös liiga häirivaks, tuleks harjutamisel piirduda olulisemate valdkondadega (vt lisaks M 6.68 Turvaintsidentide käsitluse süsteemi tõhususe testimine).

Loetletud sammude tulemused tuleks mõistagi dokumenteerida, koostades selle põhjal vastava „Turvaintsidentide käsitlemiskontseptsiooni”. Kontseptsiooni tuleb regulaarsete ajavahemike tagant värskendada ja teha see sobival moel puudutatud isikutele teatavaks.

Kontrollküsimused:

- Kas erinevat liiki turvaintsidentide käsitlemiseks on olemas selgelt defineeritud protseduurid ja reeglid?
- Kas turvaintsidentidega seotud käitumisreeglid ja teavitamiskanalid on kirjalikult fikseeritud?
- Kas need on kõigile töötajatele teada?

M 6.59 Turvaintsidentide käsitlemise eest vastutavate isikute määramine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT turvaosakond

Rakendamise eest vastutavad: IT turvaosakond

Ülesannete ja kompetentsi määramine

Turvaintsidentidega seotud vastutuse määramisel on võimalik lähtuda ettekujutatavatest ajalistest etappidest, mida turvaintsident võib läbida. Intsidentidega tegelevate isikugruppide puhul tuleb määrata kindlaks nende ülesanded ja kompetents ning see, millisel viisil neid selleks kohustatakse ja koolitatakse. Järgnev kirjeldus on toodud näitena tüüpiliste asjast puudutatud isikugruppide kohta.

IT kasutajad

- Ülesanne: kohe, kui IT kasutajad märkavad mõnda turvalisuse seisukohast olulist ebareeglipärasust, peavad nad järgima neile kehtestatud käitumisreegleid ja andma vastavast ebareeglipärasusest teada.
- Kompetents: IT kasutajad peavad langetama otsuse, millist teavitamiskanalit konkreetse juhtumi puhul kasutada (vt M 6.60 Turvaintsidentide käsitlusprotseduurid ja teavitamiskanalid).
- Kohustamine/koolitamine: iga IT kasutaja peaks olema kohustatud järgima organisatsioonis kehtivat turvapoliitikat, edastades infot võimalike turbega seotud ebareeglipärasuste kohta. Lisaks eelnevale tuleks kõikidele kasutajatele kätte jagada ka kirjalikud tegutsemisjuhised, kus õpetatakse, kuidas käituda ja keda tuleb erinevatest juhtumitest informeerida.

IT administraator

- Ülesanne: IT administraatori ülesanne selles kontekstis on võtta vastu teateid turvalisusega seotud ebareeglipärasuste kohta, mis puudutavad tema hallatavaid IT-süsteeme. Seejärel peab ta otsustama, kas ta likvideerib selle ebareeglipärasuse ise, või peab ta suunama info edasi järgmisele otsustustasandile.
- Kompetents: administraator peab suutma otsustada, kas vastava sündmuse puhul on tegemist turvaprobleemiga, mida ta on võimeline omal vastutusel kõrvaldama, või tuleb tal kaasata protsessi viivitamata ka täiendavaid isikuid (eskalatsiooniplaani järgi) ja seda, keda ta olukorrast informeerib.
- Kohustamine/koolitamine: vastavad punktid peavad olema määratletud tööülesannetes ja turvaintsidentide käsitlemise kontseptsioonis.

IT turvaspetsialist / IT turvaosakond

- Ülesanne: IT turvaspetsialist võtab vastu turvaintsidente kajastavaid teateid. Tema ülesanne on viia läbi turvaintsidendi uurimine ja hindamine. Tema valib välja hädavajalikud abimeetmed ning annab oma kompetentsi piires käsu nende täitmiseks. Vajaduse korral kutsub ta kokku turvaintsidendi meeskonna või nõustab edasise eskalatsiooni suhtes juhtkonda.

- Kompetents: ta on pädev läbi viima turvaintsidendi hindamist ja korraldama turvaintsidendi suunamist erinevatele vastutustasanditele. Lisaks on tema käsutusse antud finants- ja personaliressursid (nt 100 000 eurot ja kahe inimese tööaeg kahe kuu vältel), mida tal on õigus kasutada oma äranägemise järgi intsidentide likvideerimiseks.
- Kohustamine/koolitamine: IT turvaosakond töötab välja turvaintsidentide käsitlemiskontseptsiooni. Seetõttu peaksid kõik IT turvaspetsialistid olema teadlikud sellest, millised on nende ülesanded ja kompetentsipiirid seoses turvaintsidentide käsitlemisega.

IT turvarevisjon

- Ülesanne: IT turvarevisjonile võib panna ülesandeks kontrollida teatud ajavahemike tagant turvaintsidentide haldussüsteemi tõhusust. Lisaks võib neid kohustada osalema turvaintsidentide järelanalüüsis.
- Kompetents: kokkuleppel juhatusega on neil õigus algatada ja läbi viia eespool nimetatud kontrolle.
- Kohustamine/koolitamine: vastavad punktid peavad olema määratletud tööülesannetes ja turvaintsidentide käsitlemiskontseptsioonis.

Avalike suhete osakond / pressikeskus

- Ülesanne: raskekujuliste turvaintsidentide korral tuleks avalikkusele edastada infot eranditult läbi pressikeskuse. Info edastamise käigus ei tuleks turvaintsidenti ei ilustada ega ka selle tõsidust maha vaikida, vaid tuleb jääda asjalikuks, et mitte kannatada hiljem maine kahjustumise all, mis võib olla põhjustatud vastuolulise info avaldamisest.
- Kompetents: pressikeskus peab turvaintsidenti käsitleva info valmistama ette koostöös tehniliste ekspertidega ning enne avaldamist selle juhatuse tasandil kooskõlastama.
- Kohustamine/koolitamine: vastavad punktid peavad olema määratletud tööülesannetes ja turvaintsidentide käsitlemiskontseptsioonis.

Ametiasutuse/ettevõtte juhtkond

- Ülesanne: juhatust informeeritakse raskekujuliste turvaintsidentide esinemisest ja vajaduse korral palutakse neil langetada asjakohaseid otsuseid.
- Kompetents: koguvastutust kandva organina on juhatusel õigus delegeerida oma vastutus eespool nimetud gruppidele. Lisaks võib juhatus kahtluse korral, et tegu võib olla kriminaalse tegevusega, kaasata protsessi ka politsei ja kriminaaljälitusorganid.
- Kohustamine/koolitamine: ametiasutuse või ettevõtte juhtkond peab turvaintsidentide käsitlemiskontseptsiooni ja sellega kaasnevad esklatsiooniplaanid heaks kiitma. Selle käigus edastatakse juhatusele ka informatsioon nende rollist turvaintsidentide käsitlemisel.

Turvaintsidendi meeskond

Lisaks nimetatud gruppidele võib keeruliste või raskekujuliste turvaintsidentide puhul tekkida vajadus kutsuda turvaintsidendi käsitlemiseks kokku ajutine turvaintsidendi meeskond. Reeglina algatab selle protsessi IT turvaspetsialist, kes kooskõlastab selle vajaduse korral eelnevalt ka juhtkonna tasandiga.

Liikmete ja ülesannete määramine

Vaatamata sellele, et turvaintsidendi meeskond kutsutakse kokku ainult konkreetse turvaintsidendi lahendamiseks, peab juba eelnevalt olema teada, kes määratakse selle liikmeks ja milliste ülesannetega peavad meeskonna erinevad liikmed tegelema, et tagada turvaintsidendi korral võimalikult kiire reageerimine. Turvaintsidendi meeskonna liikmetele tuleb anda volitused, mis võimaldavad neil oma ülesandeid täita isiklikul vastutusel. Selleks vajalikud ettekirjutused tuleb fikseerida kirjalikult ja ametiasutuse või ettevõtte juhtkond peab need kinnitama. Eriti oluline on määrata, kes peab võtma enda kanda vastava meeskonna juhtimiskohustuse.

Turvaintsidendi meeskonda võivad kuuluda (olenevalt turvaintsidendi liigist) järgmised isikud:

- ametiasutuse või ettevõtte juhtkond,
- IT turvaosakond / IT turvaspetsialist,
- IT-juht,
- pressikeskus,
- andmekaitsespetsialist,
- jurist,
- töökeskkonnavolinik.

Vajaduse korral tuleb meeskonda kaasata täiendavaid liikmeid, näiteks

- puudutatud osakonnad (osakonnajuhataja, IT-protseduuride eest vastutav töötaja)
- IT administraatorid,
- varumisosakond, tehnikaosakond, sisekommunikatsiooniosakond, organisatsioon, personal,
- tuleohutusspetsialist.

Lisatöö tingimused

Juba eelnevalt peab olema selge, kuidas käiakse ümber turvaintsidentide raames tekkiva lisatööga, nt kas ametiasutuse või ettevõtte tööajatingimusi on võibolla tarvis täiendada, koostades vastavad eriolukorda kajastavad lisad, kus sätestatakse tööaja arvestamine seoses turvaintsidenti käsitlemisega (lisatöö, töö nädalavahetustel jne). Lisaks on tarvis tagada, et vastaval meeskonnal oleks võimalik kasutada oma tööruume ka väljapool tavapärast tööaega.

Kontrollküsimused:

- Kas turvaintsidendi meeskond on ametisse määratud?

- Kas meeskonda kuuluvatele isikutele on tutvustatud neile kehtestatud töö-ülesandeid?
- Kes koordineerib erinevate meetmete rakendamist?
- Millal värskendati viimati katastroofihaldusmeeskonna liikmete nimekirja?

M 6.60 Turvaintsidentide käsitlusprotseduurid ja teavitamiskanalid

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT turvaosakond
Rakendamise eest vastutavad: IT turvaosakond

Paljud turvaintsidendid kasvavad suureks probleemiks üksnes vale reageerimise tõttu, kuna asjakohaseid otsuseid võetakse vastu pikemalt mõtlemata, nt otsustatakse spontaanselt kustutada mõningad andmed, mille puhul hiljem selgub, et need olid sündmuse analüüsimise seisukohast ülimalt olulised. Siinkohal tuleb eristada üldkehtivaid käitumisreegleid, mis on kehtestatud kõikidele võimalikele turvaintsidentidele, ning käitumisreegleid, mis arvestavad IT spetsiifikaga.

Kõikvõimalike ebareeglipärasuste puhul, mis võivad olla seotud turvalisusega, võib kehtestada järgmised üldised käitumisreeglid:

- Ärge sattuge paanikasse! – Kõik puudutatud isikud peaksid säilitama rahu ning vältima abimeetmete võtmisel liigset kiirustamist.
- Tegutsege süstemaatiliselt! – Ebareeglipärasuste esinemisest tuleks viivitamata teavitamisplaani kohaselt teada anda.
- Ärge hakake midagi varjama! – Vastumeetmeid tohib rakendada alles pärast seda, kui pädevad osapooled on andnud vastava korralduse. Kahjude minimeerimise eesmärgil tuleb kogu taustteave edastada ilustamata kujul ja ausalt.
- Kahju ulatuse hindamine – tuleks koostada esimene isiklikel kogemustel põhinev hinnang selle kohta, milline võiks olla kahju võimalik suurus, hiljem avalduva kahju suurus, kes on potentsiaalselt puudutatud isikud organisatsiooni sees ja väljaspool ning millised on olukorra võimalikud tagajärjed.

Turvaintsidenti puudutavat infot ei tohi jagada kolmandatele isikutele ilma vastavasisulise konkreetse loata. Loetletud üldised käitumisreeglid tuleb teha sobival kujul teatavaks kõikidele potentsiaalselt puudutatud osapooltele ametiasutuse või ettevõtte sees.

Käitumisreeglite avaldamine

Lisaks eelnevale võib puudutatud osapooltele kehtestada ka veel spetsiifilisi käitumisreegleid, eriti neile, kelle ülesanne on turvaintsidente puudutava info vastuvõtmine ja kes peavad langetama esimese otsuse või võtma esimesed vastumeetmed. Siia all kuuluvad IT-administraatorid, IT-rakenduste eest vastutavad töötajad ning IT turvaosakond.

Vastavate käitumisreeglite hulka kuuluvad järgmised meetmed:

- M 6.23 Käitumisreeglid arvutiviiruste esinemisel
- M 6.31 Protseduurid süsteemi tervikluse kao puhuks

- M 6.48 Protseduurid andmebaasi tervikluse kao puhuks
- M 6.54 Protseduurid võrgu tervikluse kao puhuks

Lisaks käitumisreeglite kehtestamisele tuleb kindlaks määrata ka teavitamiskanalid. Siinkohal võib lähtuda järgmistest põhimõtetest:

- ohtude puhul, mille on põhjustanud vääramatu jõud, nagu tuli, vesi, elektrikatkestus, sissemurdmine ja vargused, tuleb olukorrast teavitada kohalikke abijõude (tuletõrjet, tehnikaosakonda, valvelauda, turvatöötajaid jne);
- riistvara puudutavate tehniliste probleemide ning IT-käituses esinevate ebareeglipärasuste korral tuleb teavitada süsteemide eest vastutavat IT-administraatorit;
- oletatavate ettekavatsetud rünnete ja muude sündmuste puhul, mida ei osata täpselt liigitada (nt andmemanipulatsioonid, õiguste volitamata rakendamine, spionaaži- ja sabotaažikahtlus), tuleb olukorrast teavitada IT turvaspetsialisti või IT turvaosakonda.

Teavitamiskanalite avaldamine

Siinkohal on eriti oluline, et kõik töötajad teaksid, kes on nende asjakohased kontaktisikud ning milliseid teavitamiskanaleid tuleb erinevat liiki turvaintsidentide puhul kasutada. Selleks võib nt majasiseses telefoniraamatus või intranetis olla ära toodud vastavate kontaktisikute loetelu, mis sisaldab nimesid, telefoninumbreid ja e-posti aadresse. Samas tuleb aga ka arvestada, et kahtluse korral informatsiooni edastamine ei tohi olla ei keeruline ega ka aeganõudev. Selleks peavad eksisteerima kiired ja turvalised sideühendused. Tuleb tagada sidepartnerite autentimine ja kahtluse korral edastava informatsiooni konfidentsiaalsuse säilimine. Kõik töötajad peaksid olema informeeritud ka sellest, et kolmandatele osapooltele tohib turvaintsidendi kohta infot edastada vaid IT turvaosakond (vt M 6.65 Asjassepuutuvate isikute teavitamine turvaintsidentidest).

Õppuste korraldamine

Õppuste abil tuleks pisteliselt kontrollida, kas turvaintsidentidele kehtestatud käitumisreeglid on sobivad ja teostatavad, ning kas kõik töötajad on nendest teadlikud (vt M 6.68 Turvaintsidentide käsitluse süsteemi tõhususe testimine). Turvaintsidentidest viivitamata teatamine ning avatus sellega tegelemisel sõltub suuresti heast töökliimast ja toimivast suhtluskultuurist (vt M 3.8z Tööõhkkonda kahjustavate tegurite vältimine).

Infoleht teavitamisplaani ja olulisemate käitumisreeglitega

Ühe näitena, kuidas käitumisreegleid ja teavitamisplaani puudutatud töötajatele teatavaks teha, on koostada selleks ametiasutuse või ettevõtte juhtkonna allkirjastatud infoleht, mis sisaldab kokkuvõtet olulisest infost. Vastav infoleht tuleks hoida töökohal käepärast ja täiendavalt tuleks seda hoida ka intranetis. Vastava infolehe näite leiate IT etalonturbe abivahendite alt. Selleks, et tagada informatsiooni kättesaadavus avariiolukorras, ei ole mõttekas hoida seda infot ainult elektroonilisel kujul, kuna ka just seesama info võib olla turvaintsidendist puudutatud. Tagamaks, et kõik loetletud käitumisreeglid oleksid jätkuvalt tõhusad, ning et teavitamiskanalid alati toimiksid, tuleb kõik potentsiaalseid turvaintsidente käsitlevad infolehed läbi töötada ja värskendada kohe pärast seda, kui organisatsioonis on aset leidnud olulised muudatused.

Kontrollküsimused:

- Kas erinevat liiki turvaintsidentide käsitlemiseks on olemas selgelt defineeritud käitumisreeglid?
- Kas need on kõigile töötajatele teada?
- Millal toimus viimati vastava info värskendamine?

M 6.61 Turvaintsidentide käsitluse eskalatsioonistrateegia

Algatamise eest vastutavad: ametiasutuse / ettevõtte juhtkond, IT turvaosakond, ametiasutuse/ettevõtte juhtkond

Rakendamise eest vastutavad: IT turvaosakond

Pärast seda, kui turvaintsidentidega seotud vastutusalad on määratud (vt M 6.59 Turvaintsidentide käsitlemise eest vastutavate isikute määramine) ning kõikidele puudutatud isikutele on edastatud info käitumisreeglite ja teavitamiskanalite kohta (vt M 6.60 Turvaintsidentide käsitlusprotseduurid ja teavitamiskanalid), tuleb järgmisena paika panna, kuidas hakatakse tegelema laekuvate teadetega.

Isik, kes on saanud teate turvaintsidendi kohta, peab vastavat teadet esmalt uurima ja hindama. Kui tegu peaks olema tõepoolest turvaintsidendiga, tuleb võtta täiendavaid meetmeid.

Sellega seoses tuleks esitada järgmised küsimused:

- Kes on need isikud, keda tuleb eskalatsiooni ehk tegevusahela laiendamise puhul olukorrast teavitada?
- Millistel juhtudel tuleb viivitamata rakendada eskalatsiooniprotsessi?
- Millistel muudel tingimustel tuleb rakendada eskalatsiooniprotsessi?
- Millal alustatakse eskalatsiooniprotsessiga (kohe, järgmisel päeval, järgmisel tööpäeval)?
- Milliseid teavitamiskanaleid kasutatakse teate edastamiseks?

Vastused nimetatud küsimustele tuleb kokku koguda eskalatsioonistrateegiasse ja teha teatavaks. Eskalatsioonistrateegia võib koostada kolmes tööetapis:

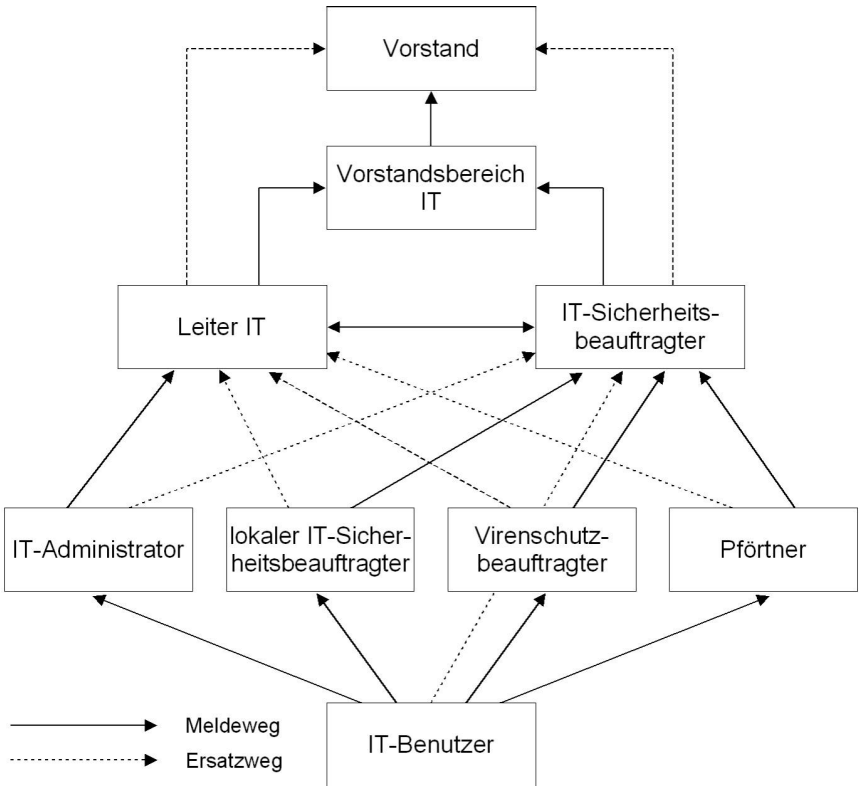
1. samm: eskalatsiooniprotseduuride määratlemine

Kes informeerib keda?

Turvaintsidentide käsitlemise eest vastutavad isikud said määratud meetmega M 6.59 Turvaintsidentide käsitlemise eest vastutavate isikute määramine . Eskalatsiooniprotseduuri määratlemisel tuleb defineerida, kes peab kellele edastama asjakohase teate. Kõige lihtsam viis seda teha on koostada vastav graafik.

Andmete näitlikustamisel tuleks arvestada nii tavapäraste eskalatsioonikanalite kui ka nende toimimisega töötajate asenduste puhul.

Näide:



Joonis: teavitamiskanalid

Vorstand – juhatus, Vorstandsbereich IT – IT eest vastutav juhatuse osa, Leiter IT – IT-juht, IT-Sicherheitsbeauftragter – IT turvaspetsialist, IT-Administrator – IT administraator, Lokaler IT-Sicherheitsbeauftragter – kohapealne IT turvaspetsialist, Virenschutzbeauftragter – viirusetõrjespetsialist, Pförtner – uksehoidja, IT-Benutzer – IT kasutajad, Meldeweg – teavitamiskanal, Ersatzweg – teavitamise varuvariant

Keda tuleb kui kiiresti informeerida?

2. samm: abi saamine eskalatsiooniotsuse tegemisel

Teises tööetapis tuleks kõigepealt defineerida, millistel juhtudel tuleb viivitamata ilma olukorda pikemalt analüüsimata ja hindamata rakendada eskalatsiooni.

Tabeli kujul võiks vastav loetelu välja näha järgmine:

Sündmus	Viivitamatult tuleb teavitada
Arvutiviiruse tuvastamine	Viirusetõrjespetsialisti, administraatorit
Tulekahju	Uksehoidjat, tuletõrjet
Ründed ja oletatavad kriminaalsed tegevused	IT-turvaspetsialisti
Tööstusspionaaži kahtlus	IT-turvaspetsialisti, juhatust
Vajadus kaasata protsessi politsei ja kriminaaljälitusorganid	Juhatust
Eksistentsi ohustavad kahjustused	Juhatust

Tabel: sündmused ja informeerimine

Seejärel tuleb määratleda eskalatsiooni ajahetk kõikide muude juhtude puhuks. Põhjused võivad olla järgmised:

- Kahju eeldatav suurus ületab teate vastu võtnud instantsis vastutuse piirid.
- Kahju kõrvaldamisega seotud kulud ja ressursside rakendamine ületab isiku kompetentsi piirid.
- Turvaintsident on piisavalt keeruline, et ületab vastava instantsi kompetentsuse ja vastutusala piirid.

3. samm: eskalatsiooni läbiviimine

Kuidas teavitatakse ohust?

Siin tuleb kindlaks määrata, kuidas antakse informatsioon edasi eskalatsiooniahela järgmisele lülile. Valida on järgmiste võimaluste vahel:

- isiklik kohalkäimine,
- kirjalik aruanne,
- e-kiri,
- telefon, mobiiltelefon,
- kättetoimetamine suletud ümbrikus.

Samuti tuleb määratleda, kui kiiresti vastavad teated edasi antakse.

Näited:

- Teate viivitamata edastamist nõudvad sündmused: kohe, ühe tunni jooksul
- Sündmused, mis on küll kontrolli all, kuid nõuavad siiski ka järgmise eskalatsiooniastme teavitamist: järgmisel tööpäeval.

Lisatöö tingimused

Kiire reageerimise tagamiseks tuleb kõigile turvaintsidente käsitlevate teadete potentsiaalsetele vastuvõtjatele kätte jagada vastava eskalatsioonistrateegia koopia.

Turvaintsidendi piiritlemiseks tuleb reeglina tegutseda kiiresti. Vajaduse korral tuleb töötajad nende muude projektide juurest ära kutsuda või paluda neil töötada koguni üle tavapärase tööaja. Seetõttu peab olema reguleeritud ka tekkiva lisatöö hindamine ja töötajate kohustus olla vajaduse korral telefonivalves (vt M 6.59 Turvaintsidentide käsitlemise eest vastutavate isikute määramine).

Kontrollküsimused:

- Millal värskendati viimati eskalatsioonistrateegiat?
- Kas eskalatsioonikanalite toimimist on õppuste raames testitud?

M 6.62z Prioriteetide kindlaksmääramine turvaintsidentide käsitlemiseks

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT turvaosakond
Rakendamise eest vastutavad: IT turvaosakond

Kogemustele toetudes võib väita, et turvaintsident tekib reeglina erinevate põhjuste koosmõjul. Sellest tulenevalt esineb tihti ka olukordi, kus turvaintsidendi tagajärjel tekkivaid potentsiaalseid kahjusid on võimalik liigitada erinevate kahjukategooriate alla. Seetõttu on oluline, et juba võimalikult varakult oleks teada, millised on probleemide kõrvaldamisele kehtivad prioriteedid. Prioriteetide liigitusest sõltub muu hulgas ka tööde järjekord, mida tuleb järgida probleeme kõrvaldama hakates.

Turvaintsidendid ja muulaadsed probleemid on omavahel konkurentsis

Prioriteetide määratlemine sõltub suuresti konkreetse organisatsiooni kohapealsetest oludest. Prioriteetide liigitamisel tuleb leida vastused järgmistele küsimustele:

- Millised on organisatsiooni jaoks olulised kahjukategooriad?
- Millises järjekorras tuleks hakata tegelema erinevatesse kahjukategooriatesse liigituvate probleemide kõrvaldamisega?

Nimetatud küsimustele aitab vastust leida IT etalonturbe põhimõtete alusel läbi viidud kaitsevajaduse tuvastamine. Kaitsevajaduse tuvastamise käigus selgitatakse välja organisatsiooni jaoks olulised kahjukategooriad.

Näide:

Kui raskeloomuliste kahjudega on tegemist? Olulised kahjukategooriad on järgmised:

- seaduste, eeskirjade või lepingute rikkumine;
- informatsioonialase enesemääratlusõiguse piiramine;
- isikliku puutumatuse rikkumine;
- tööülesannete täitmise piiramine;
- negatiivsed välismõjud;
- rahalised mõjud.

Lisaks töötatakse kaitsevajaduse tuvastamise käigus välja definitsioonid, mille põhjal liigitatakse kahjud nende suurusest lähtudes erinevatesse kahjukategooriatesse.

Näide:

Rahaliste mõjude kahjukategooria
Rahaliste mõjude kahjukategooria
Keskmine kahju
Kahju alla 25 000 €
Suur kahju
Kahju, mis jääb 25 000 ja 5 000 000 € vahele
Väga suur kahju
Kahju üle 5 000 000 €
Tabel: kahjudega seotud rahalised tagajärjed

Prioriteetide määratlemine kolme astme või järjekorra alusel

Toetudes nimetatud kategooriatele ja kahju suurust käsitlevatele eeskirjadele saab alljärgnevalt kirjeldatud moel hakata looma prioriteetide järjekorda. Iga kahjukategooria ja kahju suuruse kombinatsioonile määratakse oma prioriteet.

Prioriteetide kehtestamisel võib kasutada prioriteetide klassifitseerimist jaotuse alusel, nagu nt

1. = eriti oluline
2. = oluline
3. = vähemoluline

või nii, et kehtestatakse vastav järjekord.

Näide:

Organisatsioonina vaadeldakse linnavalitsust, kes võimaldab oma linnakodanikel kasutada teenuseid ka läbi interneti. Linnakodanikel on võimalik esitada linnavalitsusele meili teel erinevaid avaldusi ja seejärel saavad nad interneti vahendusel jälgida, millises tööetapis nende avaldus parasjagu on. Infoteenusena rakendab linnavalitsus internetiserverit.

Kahjukategooria	Keskmine kahju	Suur kahju	Väga suur kahju
Seaduste, ettekirjutuste või lepingute rikkumine	2	2	2
Informatsioonialase enesemääratlemisõiguse piiramine	2	2	1

Isikliku puutumatuse rikkumine	2	1	1
Tööülesannete täitmise piiramine	3	3	2
Negatiivsed välismõjud	3	2	1
Rahalised mõjud	3	3	2

Tabel: näidistulemus prioriteetide liigitamise kohta

Kahjukategooria	Keskmine kahju	Suur kahju	Väga suur kahju
Seaduste, ettekirjutuste või lepingute rikkumine	13	12	11
Informatsioonialase enesemääratlemisõiguse piiramine	8	6	3
Isikliku puutumatuse rikkumine	5	2	1
Tööülesannete täitmise piiramine	15	14	7
Negatiivsed välismõjud	17	9	4
Rahalised mõjud	18	16	10

Tabel: näidistulemus prioriteetide liigitamisest järjekorra alusel

Juhatuse kinnitus

Ametiasutuse või ettevõtte juhtkond peab vastava prioriteetide liigituse vastu võtma ja kehtestama. Kehtestatud prioriteedid tuleb teha teatavaks kõigile isikutele, kes peavad turvaintsidentide käsitlemise raames olulisi otsuseid vastu võtma. Turvaintsidendi esinemisel saab eelnevalt kehtestatud prioriteete rakendada alljärgnevalt kirjeldatud moel. Pärast turvaintsidendi uurimist ja hindamist on võimalik teha oletusi potentsiaalse kahju eeldatava suuruse kohta. Vastavaid kahjusid saab liigitada teadaolevate kahjukategooriate lõikes. Seejärel tuleb vastavad kahjud liigitada klassidesse „keskmine", „suur" ja „väga suur". Kehtestatud prioriteetidest loodud tabeli alusel on seejärel võimalik välja lugeda, millises järjekorras tuleb hakata tekkinud kahjusid kõrvaldama. Siin tuleb siiski arvestada ka sellega, et eelnevalt kehtestatud prioriteedid suudavad pakkuda abi vaid esmasel orienteerumisel. Vajaduse korral tuleb prioriteete kohandada konkreetsete olude alusel.

Näide:

Eespool nimetatud linnavalitsuses kahtlustatakse, et mõnel häkkeril on õnnestunud internetipõhise infoserveri andmetega manipuleerida, mille tagajärjel leiab aset linnavalitsuse laimamine. Olukord tuvastatakse ruttu, protsessi lülitatakse IT turvaosakond ja viiakse läbi ka eespool kirjeldatud kahjude hindamine. Hindamise käigus selgub, et oodata võib järgnevate kahjude tekkimist:

Kahjukategooria	Keskmine kahju	Suur kahju	Väga suur kahju
Seaduste, ettekirjutuste või lepingute rikkumine	S1		
Informatsioonialase enesemääratlemisõiguse piiramine			
Isikliku puutumatuse rikkumine			
Tööülesannete täitmise piiramine	S2		

Negatiivsed välismõjud	S3
Rahalised mõjud	S4

Tabel: kahjukategooriate jaotumine

Kehtestatud prioriteetide alusel seotakse kahjudega S1,. . . , S4 järgmised prioriteedid:

Prioriteetide liigitus: S1 = 2, S2 = 3, S3 = 1, S4 = 3

Prioriteetide järjekord: S1 = 13, S2 = 15, S3 = 4, S4 = 18

Mõlema liigutuse puhul selgub, et kahjude piiritlemise esimene prioriteet, millele tuleb keskenduda enne kõikide muude kahjudega tegelema hakkamist, on kahju S3 (negatiivne välismõju). Kirjeldatud näitejuhtumi puhul tuleks esimese sammuna negatiivse välismõju piiritlemiseks eraldada võrgust manipuleeritud internetiserver ja hakata seejärel tegelema ülejäänud vastumeetmetega.

Juhul kui negatiivsetele välismõjudele oleks kehtestatud madalam prioriteet ja tööülesannete täitmise piiramist oleks hinnatud kõrgema prioriteediga, tuleks olenevalt olukorrast internetiserveri väljalülitamist viivitamata võetava meetmena võibolla vältida.

Kontrollküsimused:

- Kas kehtestatud prioriteedid on ettevõtte või ametiasutuse juhtkonnaga kokku lepitud?
- Kas kõik haldussüsteemis osalevad isikud, kes peavad käsitlema turvaintsidente, on kehtestatud prioriteetidest teadlikud?
- Millal toimus kehtestatud prioriteetide viimane värskendamine?

M 6.64 Turvaintsidentide likvideerimine

Algatamise eest vastutavad: IT turvaosakond, IT-juht
Rakendamise eest vastutavad: IT turvaosakond, administraator, IT-juht

Kohe pärast seda, kui turvaintsidendi põhjus on tuvastatud, tuleks valida asjakohased meetmed ja hakata turvaintsidenti likvideerima. Selleks tuleb probleem esmalt piiritleda ja kõrvalda ning seejärel taastada „normaalne" seisund.

Hädavajalike ekspertteadmiste kaasamine

Nimekiri ekspertide aadressidega

Turvaaugu uurimise ja kõrvaldamise üks vältimatuid eeldusi on asjakohase oskusteabe olemasolu. Selleks tuleb kas olemasolevat personali piisaval määral koolitada või kutsuda nõustamiseks appi vastavad eksperdid. Selleks peaks olema koostatud nimekiri erinevate valdkondade nii organisatsioonist endast kui ka väljastpoolt organisatsiooni pärit ekspertidest koos kontaktaadressidega, mida saaks vajaduse korral kiiresti kasutada.

Väliste ekspertide alla kuuluvad muu hulgas

- arvutiavariide tõrje rühmad (computer emergency response teams, CERT) (vt M 2.35 Teabe hankimine turvaaukude kohta)
- puudutatud IT-süsteemide tootjad ja edasimüüjad (vt M 4.107 Tootja ressursside kasutamine)
- rakendatavate turvasüsteemide, nagu viirusetõrjetarkvara, tulemüüri, sissepääsukontrollisüsteemide tootjad ja edasimüüjad jne
- välised turvatehniliste eriteadmistega nõustajad

Turvalise seisundi taastamine

Puudutatud süsteemide uurimine

Turvaaukude kõrvaldamiseks tuleb puudutatud süsteemid võrgust eemaldada ja luua kõikidest failidest, mis võiksid anda infot tekkinud probleemi liigi ja põhjuse kohta, varukoopiad. Siia alla kuuluvad ennekõike kõikvõimalikud olulised logifailid.

Kuna tervet süsteemi tuleks vaadelda ebaturvalise ja manipuleeritava süsteemina, tuleb võimalike muudatuste suhtes üle kontrollida ka operatsioonisüsteem ja rakendused. Lisaks programmidele tuleks potentsiaalseid manipulatsioone otsida ka konfiguratsioonifailidest ja kasutajafailidest. Siinkohal oleks mõttekas kasutada kontrollsummaprotseduure. See eeldab aga, et kontrollsummad peavad olema juba eelnevalt nende „turvalises" seisundis kokku kogutud ja kirjutuskaitsega varustatud andmekandjatele hoiule pandud (vt M 4.93z Regulaarne tervikluse kontroll).

Ettevaatusabinõud andmevarunduste sisselugemisel!

Paroolid tuleb ära muuta!

Veendumaks, et ründaja sisse toodud Trooja hobused on tõepoolest kõrvaldatud, tuleks originaalfailid kirjutuskaitsega varustatud andmekandjatelt uuesti sisse lugeda. Sealjuures tuleb pöörata tähelepanu sellele, koos kõige muuga loetaks uuesti sisse ka kõik turvalisuse seisukohast olulised konfiguratsioonid ja turvapaigad. Andmevarundustest andmete sisselugemisel tuleb tagada, et need oleksid kindlasti turvaintsidendi mõjust puutumata jäänud, nt et need poleks nakatunud arvutiviirusega. Andmevarunduste uurimine võib olla muu hulgas abiks ründe algusaja või arvutiviirusesse nakatumise alguse tuvastamisel.

Puudutatud IT-süsteemide seire

Pärast toimunud rünnet, enne IT-süsteemide uuesti kasutuselevõtmist, tuleb kindlasti ära muuta kõik nende paroolid. Paroolid tuleb vahetada ka neis IT-süsteemides, mis polnud otseselt manipulatsioonist puudutatud, kuid mille abil võis ründaja hankida endale infot kasutajate ja/või nende paroolide kohta. Pärast „turvalise" seisundi taastamist tuleb olla valmis olukorraks, kus ründaja võib proovida oma tegu korrata. Sel otstarbel tuleks IT-süsteemid, eriti aga võrguüleminekud varustada asjakohaste seiretööriistadega (vt M 5.71z Sissetungi tuvastuse ja sellele reageerimise süsteemid).

Dokumentatsioon

Turvaprobleemi likvideerimise käigus tuleks kõik sooritatud tegevused dokumenteerida võimalikult detailselt eesmärgiga

- säilitada olukorrast ülevaade,
- saada tekkinud probleemidest aru,
- suuta kõrvaldada vigu, mis võisid tekkida sageli liiga kiiresti läbiviidud vastumeetmete rakendamise tõttu,
- likvideerida juba tuttavaid probleeme nende esinemisel kiiremini,
- sulgeda turvaaugud ja töötada välja sobivad vastumeetmed ning
- koguda tõendeid võimaliku kriminaaljälituse otstarbeks.

Sellise dokumentatsiooni juurde ei kuulu mitte ainult läbiviidud tegevuste kirjeldused koos aja fikseerimisega, vaid ka puudutatud IT-süsteemide logifailid.

Reageerimine rünnetele

Turvaintsidentide puhul, mis on alguse saanud ründajast, tuleb langetada otsus, kas tuvastatud rünne tuleks võtta jälgimise alla või rakendada sellele hoopis võimalikult kiiresti vastumeetmeid. Loomulikult võib proovida ründajat ka „otse teolt tabada", kuid sellise lähenemisega kaasneb ka suur oht, et ründajal võib õnnestuda vahepeal andmed kas hävitada, neid manipuleerida või need oma valdusesse saada.

Oma töötajatest kurikaeltega ümberkäimine

Kahjuks jõutakse turvaprobleemide analüüsimisel tihti tulemuseni, et need on põhjustanud asutuse või ettevõtte enda töötajad. Turvaprobleemid võivad olla tekkinud ka kogemata, vigaste tööprotsesside või tehniliste probleemide tagajärjel, kuid neid võivad põhjustada ka turvameetmete eiramine ja ettekavatsetud tegevus. Kõikide siseringist alguse saanud turvaprobleemide puhul tuleb uurida ka selle põhjustajat. Paljudel juhtudel jõutakse siinkohal tulemuseni, et probleemide tekkepõhjuseks on vigased või arusaamatud ettekirjutused. Sellistel juhtudel

tuleb ettekirjutusi vastavalt muuta või võtta kasutusele täiendavad, nt tehnilised abimeetmed. Kui turvaprobleemide põhjuseks on ettekavatsetud tegevus või hooletus, tuleks rakendada sobivaid distsiplinaarkaristusi.

Kontrollküsimused:

- Millal värskendati viimati turvaekspertide nimekirja?
- Kas on esinenud oma töötajate toime pandud ründeid?

M 6.65 Asjassepuutuvate isikute teavitamine turvaintsidentidest

Algatamise eest vastutavad: IT turvaosakond
Rakendamise eest vastutavad: IT turvaosakond, IT-juht, administraator

Turvaintsidendi esinemisel tuleb sellest infomeerida puudutatud osapooli nii ettevõtte sees (juhtkond, äripoole esindajad jne) kui ka väljaspool ettevõtet (CERT-EE-d). Eriti oluline on informeerida neid osapooli, kes võivad turvaintsidendist kõige otsesemat kahju kannatada, kes peavad viivitamata võtma vastumeetmed ja neid, kes peavad hakkama turvaintsidenti uurima ning aitavad kaasa nende ennetamisele ja likvideerimisele. Vajaduse korral tuleks teha selgitustööd ka avalikkusele.

Kes informeerib keda?
Selleks tuleb individuaalselt vastava turvaintsidendi tarbeks koostada juhend / kord / teavitamise skeem vms, kes peab keda millises järjekorras ja kui põhjalikult informeerima. Selleks on tarvis tagada, et turvaintsidendi kohta jagaksid infot ainult selle eest vastutavaks määratud isikud, nagu nt IT turvaosakonna või pressikeskuse töötajad. Riigi Infosüsteemi Amet on oma veebilehel välja toonud juhendi ja raportite vormid, millal ja kuidas tuleb turvaintsidentidest teavitada CERT-EE-d.

Näide:
Pärast olulise turvaintsidendi avastamist võtab asutuse infoturbejuht, IT-juht või infoturbe eest vastutav isik viivitamata ühendust CERT-EE-ga ja kirjeldab probleemi. Teavitamisel edastatakse turvaintsidendi kohta nii palju infot, kui teavitamise hetkel võimalik. Teavitamine intsidendi avastamisel võib toimuda eri viisidel:

- helistades numbril 663 0299;
- kirjutades e-posti aadressil cert@cert.

Intsidendi lahendamise järel või kui on teada probleemi või katkestuse olemus, täidab asutuse infoturbejuht, IT-juht või infoturbe eest vastutav isik vormikohase turvaintsidendi raporti. Vormi leiate Riigi Infosüsteemi Ameti veebilehelt. CERT-EE-d ei pea teavitama sisemistest teguritest põhjustatud turvaintsidentidest, mis ei vii asutuste töö või oluliste teenuste katkestuse ohuni ega mõjuta teisi süsteeme ega võrgupõhiseid lahendusi.

Olulise turvaintsidendi mõiste on lahti kirjutatud Riigi Infosüsteemi Ameti turvaintsidentidest teavitamise juhendis, mille leiate RIA veebilehelt.

Kontrollküsimused:

- Kas on loodud protsess turvaintsidentide teavituse kohta asutuses?
- Kas korrapäraseid turvaintsidente puudutavaid raporteid edastatakse CERT-EE-le?

M 6.66 Turvaintsidentide järelhindamine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond, IT turvaosakond

Rakendamise eest vastutavad: IT turvaosakond, revident

Igast turvaintsidendist on midagi õppida. Selleks, et turvaintsident oleks võimalikult õpetlik, ei tohi alahinnata intsidendi järelhindamist. Tihti on niimoodi võimalik saada infot, mille alusel muuta turvaintsidentide käsitlemist veelgi paremaks või koguda andmeid, mille põhjal teha järeldusi IT turvaosakonna või olemasolevate IT turvameetmete tõhususe kohta. Muu hulgas tuleb arvestada järgmiste aspektidega:

Reageerimisaeg

Tuleks uurida, kui ruttu turvaintsidenti märgati. Seejuures tuleb kontrollida, kas on tarvis täiendada tehnilisi tuvastamismeetmeid. Kas info liikus korralikult? Lisaks tuleb kindlaks teha, kui kaua kulus aega, kuni teade jõudis läbi vajaliku teavitamiskanali soovitud sihtpunkti. Lõpuks tuleb selgitada, kui kiirelt langetati otsus vajalike meetmete kohta, kui kaua läks nende elluviimisega ja millal teavitati olukorrast puudutatud asutusesiseseid ja -väliseid osakondi. Teavitamisprotseduuri tagasiulatuval analüüsimisel tuleks kontrollida, kas vajalik teavitamisprotseduur oli kõigile teada või on tarvis veel täiendavat selgitamist ja töötajate informeerimist.

Eskalatsioonistrateegia tõhusus

Konkreetse turvaintsidendi alusel tuleks kontrollida, kas kehtestatud eskalatsioonistrateegiast peeti kinni, millist lisainfot läheb töötajatel tarvis ning kas eskalatsioonistrateegiat on vaja kohandada.

Kontrolli tõhusus

Tagasivaatavalt tuleks hinnata, kas turvaintsidendi tekitatud kahjude hindamine oli õige, kas tööde aluseks võetud prioriteedid olid õiged ja kas uurimistööde läbiviimisel kasutati sobivalt koostatud turvaintsidendi meeskonda. Asjassepuutuvate osapoolte teavitamine

Tuleks kontrollida, kas kõiki asjassepuutuvad osapooli tõepoolest informeeriti olukorrast ning kas teavitamine toimus piisavalt kiiresti. Vajaduse korral tuleb teavitamiseks leida meetodid, mis toimiksid kiiremini.

Vastus teate edastanud osakonnale

Neid osakondi, kes avastasid turvaintsidendi ja teatasid sellest vastutavale eksperdile, tuleks pärast intsidendi kõrvaldamist informeerida tekkinud kahjude ja turvaintsidendi kõrvaldamiseks võetud meetmetest. Selline tagasiside näitab, et vastavasisulistesse teadetesse suhtutakse tõsiselt ning see tõstab töötajate motivatsiooni. Lisaks võib teate korrektse edastamise eest avaldada kiitust või pakkuda autasu, edastamaks signaali, et teadete edastamine on turvaintsidentidega toimetulemisel ülimalt oluline.

Teo toimepanija motiivid

Kui selgub, et turvaintsident on tekitatud tahtlikult, tuleb uurida teo toimepanija motiive. Eriti oluline on motiivide väljaselgitamine siis, kui vastava teo on toime pannud oma asutuse töötaja. Kui selgub, et põhjus peitub organisatsioonis valitsevas tööõhkkonnas, tuleb sellest teatada ka juhtkonnale, kuna sellistel juhtudel on põhjust oodata vastavate vigade ja ettekavatsetud rünnete kordumist.

Olenevalt järelhindamise tulemuste kaalukusest tuleb nendest vajaduse korral teavitada ka juhtkonda, et sellel oleks võimalik olukorda parandada. Seega võib olla kasulik lasta järelhindamisega tegelda organisatsiooni sellisel allüksusel, mis ei ole kaasatud teavitamisplaani.

Tegutsemisjuhise väljatöötamine

Turvaintsidendi järelhindamise raames tuleks saadud kogemuste põhjal koostada toimimisjuhis või kohandada olemasolevat juhist, et samalaadse turvaintsidendi esinemise korral oleks täpselt teada, kuidas tegutseda. Kuna nüüdseks on probleem juba reaalselt esinenud, saab seda kasutada senise teoreetilise stsenaariumi asemel, et töötada välja veelgi tõhusam tegutsemisjuhis. Lisaks tõestab juba esinenud turvaintsident ka seda, et vastavat liiki turvaintsidendi jaoks on sobivat toimimisjuhist tõepoolest ka reaalselt tarvis. Selliselt koostatud tegutsemisjuhis tuleb sobival viisil edastada asjassepuutuvatele isikugruppidele.

Kontrollküsimused:

- Kas viimati esinenud turvaintsidendi kohta on tehtud järelhindamine?
- Kas juhtkonda informeeritakse vähemalt kord aastas esinenud turvaintsidentidest?
- Kuidas toimub konkreetsete toimimisjuhiste värskendamine ja nende teatavaks tegemine?

M 6.67z Turvaintsidentide avastamismeetmete rakendamine

Algatamise eest vastutavad: IT turvaosakond
Rakendamise eest vastutavad: IT turvaosakond

Turvaintsidentide avastamine

Lisaks turvaintsidentide ärahoidmisele on väga oluline ka nende avastamine. Paljude turvalisust mõjutavate kõrvalekallete avastamist saab vastava tehnilise toega muuta automaatseks ja seeläbi võimalikult kiireks. Sellised avastamismeetmed suurendavad tavaliselt avastamisprotsessi usaldusväärsust ja lühendavad aega, mis jääb kõrvalekalde tekkimise ja selle avastamise vahele. Eelnevalt tuleks siiski hinnata, kas võit reageerimisvõimes ja -ajas on piisav, et õigustada süsteemi paigaldamise ja kontrollimisega kaasnevat täiendavat töömahtu. Sellised avastamismeetmed on praktiliselt asendamatud, kui kahjustuste korral on oodata väga suuri kahjusid, mis võivad ulatuda lausa isikukahjudeni.

Vastavad tehnilised avastamismeetmed on nt järgmised:

- ohuteavitussüsteem (vt M 1.18 Valve- ja tuletõrjesignalisatsioon);
- tõrgete kaugindikatsioon (vt M 1.31z Tõrgete kaugindikatsioon);
- arvutiviiruste otsiprogrammid (vt M 2.157 Sobiva viiruseskanneri valimine);
- sissetungi tuvastamise ja sellele reageerimise süsteemid (vt M 5.71z Sissetungi tuvastuse ja sellele reageerimise süsteemid);
- krüptograafilised kontrollkoodid (vt M 4.34z Krüpteerimise, kontrollsummade ja digitaalallkirjade rakendamine);
- turvalisuse monitooring reaalajas z/OS-süsteemidele, et tuvastada kiirelt turvaeeskirjade rikkumisi.

Tehniliste ja organisatoorsete meetmete kombineerimine

Kõik turvaintsidendid ei ole ainult tehniliste meetmetega õigel ajal tuvastatavad. Sageli tuleb rakendada täiendavaid organisatsioonilisi meetmeid. Tehniliste avastamismeetmete usaldusväärsus sõltub üldiselt nende värskusest ja sellest, kui hästi on neid kohandatud tegelike oludega. Organisatoorsete avastamismeetmete usaldusväärsus sõltub olulisel määral sellest, kui usaldusväärsed on neid rakendavad isikud, kuid vähemoluline pole ka see, mil määral on võimalik vastavaid meetmeid reaalselt igapäevatöös ellu viia.

Täielikult või osaliselt organisatsioonilised avastamismeetmed on tavaliselt järgmised:

- teabe hankimine turvaaukude kohta (vt M 2.35 Teabe hankimine turvaaukude kohta);
- valitud IT-süsteemide regulaarne turvakontroll (vt M 4.93z Regulaarne tervikluse kontroll , M 5.8 Võrgu regulaarne turvakontroll ja M 5.141 Regulaarsed traadita kohtvõrgu turvakontrollid);

- logifailide regulaarne analüüs (vt M 2.64 Logifailide kontroll , M 4.5 Kodukeskjaama (PBX) haldustööde logi , M 4.25 Logimine Unix-süsteemis , M 4.47 Turvalüüsi operatsioonide logimine ja M 5.7 Võrguhaldus);
- SMF-andmehulkade analüüs z/OS-i all. Nende SMF-andmehulkade infot saab kasutada pakk-raportite (batch-reports) jaoks või andmeallikana reaalajas toimiva seiresüsteemi jaoks, mis suudavad omalt poolt juhtida keskset kontrollikonsooli. Selliseid keskseid konsoole pakuvad oma automatiseerimistoodete hulgas mitmed tootjad.

Kontrollküsimused:

- Milliseid avastamismeetmeid kasutatakse?
- Kas on tagatud, et edastatakse informatsiooni logiandmetes esinevatest ebatavalistest väärtustest?

M 6.68 Turvaintsidentide käsitluse süsteemi tõhususe testimine

Algatamise eest vastutavad: IT turvaosakond

Rakendamise eest vastutavad: IT turvaosakond, revident

Turvaintsidentide käsitluse haldussüsteemi värskust ja tõhusust tuleb regulaarselt kontrollida.

Lisaks tuleb regulaarselt testida ka selles formuleeritud meetmeid, et selgitada välja, kas

- asjassepuutuvad töötajad on nendest teadlikud;
- meetmed on teostatavad ka stressiolukorras, seega turvaintsidendi puhul, mille tagajärjeks on ebakorrapärane töö;
- meetmeid on võimalik integreerida igapäevastesse tööprotsessidesse.

Haldussüsteemi kontroll

Tõhususe testimiseks tuleks simuleerida avariiolukordi, et kontrollida, kas määratud tegutsemisjärjekorrast peetakse kinni või kas selle järgimine on üleüldse võimalik. Kui see pole nii, tuleb teha vastavad muudatused. Lisaks võib korraldada nii etteteatamisega kui ka ootamatuid õppuseid.

Õppused ei tohi põhjustada reaalseid kahjustusi!

Ootamatute õppustega ei tohi tekitada olukordi, mille tagajärjel tekivad pöördumatud või raskesti kõrvaldatavad kahjustused IT-süsteemides, andmetes või muudes seotud valdkondades. Enne igat õppust tuleb täpselt kindlaks määrata, kellele tuleb eelnevalt kõigest teatada. Ametkonna/ettevõtte juhtkond peab õppuse tingimata heaks kiitma. Mõnikord võib olla vajalik teatud gruppidele õppuste toimumisest mitte teada anda, nt jätta uksehoidjad või administraatorid informeerimata. Sellele vaatamata tuleb alati tagada, et olukord ei väljuks kontrolli alt. Seega tuleks vältida politsei või tuletõrje kohalekutsumist või ametiasutuse/ettevõtte kõikide võrguühenduste katkestamist.

Näited:

Simuleeritud avariiolukorrad

- Helistage oma ettevõtte/ametiasutuse üldtelefonile ja teeselge häkkerit, kes on tunginud sisevõrku. Häkkeri asemel võib ennast esitleda ka ajakirjanikuna, kellele olevat laekunud info, et häkker on tunginud sisevõrku ja kopeerinud sealt endale konfidentsiaalseid faile. Helistada võib ka sellistele töötajatele, kelle poole palutakse tavaliselt sellistes olukordades pöörduda, nt pressiesindajale või IT-juhile. Sellise kõnega peaks saama tuvastada, kas tagajärjeks on paanika või olukorrale vastav adekvaatne reageerimine.
- Suvalisel päeval võib testida kõiki arvutiviirustesse nakatumisega seotud tegevusi ja teavitamiskanaleid. See ei nõua ilmtingimata kõikide asjaosaliste eelnevalt teavitamist, kuid seda tuleb teha siiski hiljemalt sel hetkel, mil nad kaasatakse tegevusahelasse.

Kontrollküsimused:

- Milliseid õppuseid viimati läbi viidi?
- Kas õppused kooskõlastatakse eelnevalt juhtkonnaga?

M 6.69 Faksiserverite avariiplaan ja rikkekindluse tagamine

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator, faks-postikeskus

Faksiserverite avariiennetamise ja töökindluse tagamise meetmed sõltuvad andmehulkadest, mis üle faksiserveri või faksiserverite liiguvad ja nõuetest, mis esitatakse selle teenuse käideldavusele.

Konfiguratsioonipara-meetrite dokumenteerimine

Esmalt tuleb veenduda, et kasutatavate kommunikatsioonikaartide, rakendatava operatsioonisüsteemi ja faksiserveri rakenduse kõik konfiguratsiooniparameetrid oleks dokumenteeritud. Konfiguratsioonis tehtavate muudatuste korral tuleb vastavalt täiendada ka dokumentatsiooni. Ainult nii saab tagada, et hädaolukorras on faksiserver kiirelt taaspaigaldatav.

Regulaarne andmevarundus

Lisaks tuleb andmeid regulaarselt varundada, lähtudes andmevarunduse kontseptsioonist ja andmevarundusele kehtivast turvapoliitikast. Lisaks andmepartitsioonidele tuleks andmevarundusse kaasata ka need partitsioonid, millel asuvad operatsioonisüsteem ja faksiserveri rakendused. Faksiserverile salvestatud faksisaadetistest tuleb regulaarselt koostada varukoopiad. Kui faksiandmeid on tarvis püsivalt arhiveerida, tuleks selleks faksiserveri asemel kasutada väliseid andmekandjaid.

Tavapäraste faksiaparaatide varu hoidmine

Selleks, et tagada võimalus fakse saata ja vastu võtta ka faksiserveri või võrgu avarii korral, tuleks võimalusel varuks hoida ühte või mitut tavapärast faksiaparaati. Vajalike seadmete arv sõltub avariiolukorras saabuvate ja väljuvate fakside arvukusest. Mõistlik on varuna alles hoida need faksiaparaadid, mida kasutati juba enne faksiserveri paigaldamist. Kõik täiendavad avariikindlust tagavad meetmed põhjustavad osalt suuri lisakulutusi ja on seepärast mõeldavad ainult kõrgendatud käideldavusnõuete puhul ning nende otstarbekust tuleb kaaluda iga juhtumi puhul eraldi.

RAID-süsteemide kasutamine

Esmalt võib IT-süsteemi, millel asub faksiserver, varustada RAID-süsteemiga. Vastava lahenduse puhul koondatakse mitu kõvaketast kokku ja nendel asuvad andmed jaotatakse koos liiasuse moodustamisega erinevatele ketastele. Näiteks nn RAID Level 5 puhul ei esine ka ühe kõvaketta väljalangemise korral üldse andmekadu. Samas väheneb RAID-tehnoloogia kasutamisel loodava liiasuse tõttu kõvaketaste vaba salvestusruum. Samuti tuleb arvestada sellega, et see lahendus ei asenda välist andmevarundust ja ei kaitse süsteemi täieliku avarii eest.

Mitme faksiserveri kasutamine

Rikkekindluse tagamiseks võib kasutada ka mitut faksiserverit. Ühe serveri avarii korral saab koormuse jaotada ülejäänute peale. Lisaks kaasneb selle lahendusega eelis, et koormus on jaotatud ja üksiku faksiserveri ülekoormamise oht on väiksem. Puuduseks on tõsiasi, et saabunud faksid, mis asuvad avariilises serveris, ei ole vähemalt avarii kestvuse ajal käideldavad.

Liiasusega faksiserverite kasutamine

Kui faksiserveritele kehtestatud käideldavusnõuded lubavad avariisid, mis võivad maksimaalselt kesta ainult mõne minuti, on kõige parem kasutada liiasusega servereid. Iga liiasuskontseptsiooni kaasatud faksiserveri jaoks peab sellisel juhul eksisteerima veel ka teine server, mille peale toimub vastavate andmete replikeerimine. Selline lahendus pakub – vajadusel kombinatsioonis RAID-

süsteemidega – maksimaalset avariikindlust, kuid põhjustab ka märkimisväärseid kulutusi.

Täiendavad kontrollküsimused:

- Kas konfiguratsiooni dokumentatsioon on värske?
- Kes vastutab andmevarunduse eest?
- Kas avariiolukorra jaoks on olemas tavalised faksiaparaadid?

M 6.71 Mobiilse IT-süsteemi andmevarundus

Algatamise eest vastutavad: IT-turvaosakonna meeskond, IT-juht

Rakendamise eest vastutavad: administraator, kasutaja

Mobiilselt kasutatavad IT-süsteemid (nt sülearvutid) ei ole tavaliselt püsivalt võrku ühendatud. Andmevahetus teiste IT-süsteemidega toimub tavaliselt andmekandjate või ajutiste võrguühenduste kaudu. Võrguühendused võivad aset leida nt kaugpöörduse vahendusel või siis luuakse pärast töökohale naasmist otseühendus kohtvõrguga. Erinevalt statsionaarsetest klientidest on seega mobiilsete IT-süsteemide puhul vältimatu, et andmeid salvestatakse tsentraalse serveri asemel vähemalt ajutiselt ka lokaalsesse süsteemi. Selliste andmete kaotsiminekut tuleb ennetada sobivate andmevarundusmeetmete rakendamisega. Enamatel juhtudel saab andmevarunduseks kasutada järgnevaid protseduure:

- Andmete varundamine välistele andmekandjatele - Selle meetodi eeliseks on, et andmevarundus saab toimuda praktiliselt kõikjal ja igal ajal. Puuduseks on vajadus sobiva kettaseadme ja piisava hulga andmekandjate kaasaskandmise järele ning lisaks peab kasutaja olema piisavalt hoolikas, et andmekandjaid õigesti käsitseda. Andmekandjate salvestusmaht peab olema piisavalt suur, et kasutaja ei peaks ühe varundamise ajal sisestama kettaseadmesse mitut andmekandjat. Krüpteerimata andmetalletuse puhul esineb lisaks ka andmekandjate kadumise ning seega ka konfidentsiaalsete andmete kompromiteerimise oht. Andmekandjaid ja mobiilseid IT-süsteeme tuleks hoida võimalikult eraldi, et IT-süsteemi kaotamise või varguse korral ei läheks kaduma ka andmekandjad. Andmete varundamine välistele andmekandjatele on eriti sobilik neil juhtudel, kus väliseid andmekandjaid kasutatakse ka andmevahetuseks teiste IT-süsteemidega. See võib luua võimaluse nende kahe protsessi kombineerimiseks. Pärast töökohale naasmist tuleb andmekandjatele talletatud andmevarundused üle kanda varundussüsteemi, tootmissüsteemi või siis asutuse kesksesse andmetalletussüsteemi.
- Andmevarundus ajutiste võrguühenduste kaudu - Kui IT-süsteeme saab ühendada regulaarselt võrguga, näiteks kaugpöörduse kaudu, võib lokaalsete andmete varundus toimuda ka võrguühenduse kaudu. Eeliseks on, et kasutaja ei pea muretsema andmekandjate haldamise pärast ning samuti pole vajadust vastavat kettaseadet kaasas kanda. Lisaks saab seda protseduuri teatud määral automatiseerida, nt võib andmevarundus käivituda iga kaugpöörduse korral automaatselt pärast sissevalimist. Ajutuse võrguühenduse kaudu toimuva andmevarunduse korral on oluline, et varundatava andmemahu jaoks eksisteeriks võrguühenduses piisav ribalaius. Andmeedastus ei tohi kesta liiga kaua ega põhjustada üleliigseid viivitusi olukorras, kus kasutaja peab samal ajal ligi pääsema eemalasuvatele ressurssidele. Enamlevinud juurdepääsutehnoloogiate puhul (nt ISDN'i, modemi, mobiiltelefoni) puhul tähendab see seda, et varundusprotseduuri ajal saab edastada ainult väikseid andmehulki. Seetõttu pakuvad mõningad andmevarundusprogrammid võimalust edastada ainult andmetes tehtud muudatused, mis on tekkinud pärast viimast võrgu kaudu toimunud andmevarundust. Paljudel juhtudel on seeläbi võimalik transporditavaid andmemahtusid oluliselt vähendada. Üheks tähtsaks nõudeks andmevarunduseks kasutatavale

tarkvarale on selle võime tuvastada ühenduse ootamatuid katkemisi ja nendega korrektselt ümber käia. Ühenduste katkemised ei tohi mõjutada varundatavaid andmeid.

Mõlema andmevarundusprotseduuri puhul on soovitatav varundamisele kuuluvat andmehulka minimeerida. Lisaks kaovabade tihendusprotseduuride rakendamisele, mis on paljudesse andmevarundustarkvaradesse juba integreeritud, võib rakendada ka inkrementaalset või diferentseeritud andmevarundust (vt M 6.35 Andmevarunduseks vajalike protseduuride määratlemine). Seeläbi võib sõltuvalt olukorrast siiski suureneda andmevarunduse taastamise töömaht. Andmete varundamine peaks toimuma võimalikult automaatselt, et kasutaja tööoperatsioonide hulk oleks selle puhul võimalikult väike. Kui andmete varundamisprotsessi on tarvis kaasata ka töötajad, tuleb töötajatele kehtestada kohustus viia regulaarselt läbi andmevarundusi (vt M 2.41 Töötajate kaasamine andmevarundusse). Lisaks tuleks pisteliselt kontrollida, kas loodud andmevarundustest on võimalik andmeid ka taastada.

Täiendavad kontrollküsimused:

- Kas mobiilsetele IT-süsteemidele salvestatavaid andmeid varundatakse regulaarselt?
- Kas andmevarunduseks välja valitud protseduur on tekkiva andmemahu jaoks sobiv?
- Kas andmevarundus nõuab võimalikult vähe kasutajapoolset sekkumist?

M 6.72 Ettevaatusabinõud mobiiltelefoni tõrgete puhuks

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: IT-juht, kasutajad

Toide

Mobiiltelefon võib erinevatel põhjustel rikki minna või töötada ainult osaliselt. Eriti ärritav on see loomulikult siis, kui telefoni on hädasti tarvis või kui seeläbi lähevad kaotsi olulised andmed. Seega tuleks eelnevalt võtta tarvitusele vastavad meetmed, et ennetada tõrkeid ja vähendada nendega kaasnevaid probleeme. Mobiiltelefoni aku laetust ja töökindlust tuleb regulaarselt kontrollida (vt M 4.115 Mobiiltelefonide toite tagamine).

Regulaarne andmevarundus

Kõik mobiili salvestatud andmed, nt telefoniraamatusse tehtud sissekanded, sõnumid jms tuleks regulaarselt ümber salvestada mõnele teisele andmekandjale, et neid saaks vajadusel taastada. Selleks on mitu võimalust:

- Olulisemad seadistused, nt PIN-koodid ja turvamehhanismide konfiguratsioonid tuleks kirjalikult dokumenteerida ja panna vastavalt nende kaitsevajadusele turvaliselt hoiule.
- Kõiki SIM-kaardile salvestatud andmeid, nt kontakte, saab SIM-kaardi lugeja ja vastava tarkvaraga arvutisse ümber salvestada ja seal hallata. Lisaks on siinkohal eeliseks, et andmete haldamine on arvutis kergem ning andmeid saab kergemini teiste aadressiandmebaasidega sünkroniseerida. Eriti just mitme mobiili kasutamisel (vt M 2.190 Mobiilikogu sisseseadmine) on mõistlik sel moel telefoniraamatuid võrdsustada. Kui varundatakse ainult SIM-kaardile salvestatud andmeid, tuleb kõiki kasutajaid teavitada, et telefoninumbreid jms tuleks salvestada ainult kaardile.
- Andmevahetuse eesmärgil saab mobiiltelefoni ühendada ka teiste IT-süsteemidega, nt sülearvuti või elektroonilise märkmikuga (vt M 5.81 Turvaline andmeedastus mobiiltelefoni kaudu). Seejuures saab varundada niihästi SIM-kaardile kui ka seadmesse salvestatud andmeid.

Varu käepärast hoidmine

Kui mobiiltelefon peab alati käepärast olema, tuleks endaga kaasas kanda varumobiiltelefoni või vähemalt varuakut. Kui mobiiltelefone kasutatakse häireteadete edastamiseks, nt kui vargasignalisatsioonid saadavad teateid GSMi kaudu või kui avariipersonal peab olema mobiiltelefonide kaudu kättesaadav, tuleb alati tagada varuvariandi olemasolu.

Parandamine

Mobiili puhul võib rikki minna seade tervikuna või ka ainult mõni üksikkomponent. Parandamine tohiks usaldada ainult usaldusväärsetele ettevõtetele. Seetõttu peab eksisteerima ülevaade sobilikest ettevõtetest. Paljud edasimüüjad pakuvad parandamise ajaks asendusseadmeid. Lühikese kasutuseaga mobiilsete seadmete (nt mobiiltelefonide) puhul võib parandamine osutuda sageli mõttetuks, mistõttu pakutakse mõnikord ka asendusseadmeid. Kuna eriti just mobiil peab olema alati käepärast, on mobiiltelefoni ja selle edasimüüja valimisel oluline jälgida, et vastavaid teenuseid ka pakutaks. Enne mobiili üleandmist parandusele, tuleb võimaluse piires kustutada kõik isikuid kajastavad andmed, seega nt kõnede numbrimälu, salvestatud meilid ja kontaktid (vt M 2.4 Hooldus- ja remonditööde reeglid). Enne kustutamist tuleb andmed loomulikult varundada. Lisaks tuleb seadmest eemaldada SIM-kaart.

Kontrollküsimused:

- Kas mobiiltelefonidel salvestatud andmeid varundatakse regulaarsete ajavahemike tagant teisele andmekandjale?
- Kas enne parandamist kustutatakse mobiiltelefonist kõik konfidentsiaalsed andmed (mis on eelnevalt varundatud)?

M 6.73 Hädaolukorraplaani koostamine Lotus Notes süsteemi tõrgete puhuks

Algatamise eest vastutavad: IT-juht, ametiasutuse / ettevõtte juhtkond

Rakendamise eest vastutavad: administraator

Notes-süsteemi osaline või täielik avarii mõjutab sageli väga tugevalt kasutajate töövõimalusi, kuna avarii tagajärjel on kas osad või kõik serveripõhised tegevused on häiritud. Avariiennetamise raames tuleb seega luua kontseptsioon, mis aitaks hoida avarii tagajärgi võimalikult minimaalsetena ja määraks, millised sammud on avarii korral kohustuslikud.

Siinkohal tuleb arvestada järgnevate aspektidega:

- Replikeerimine- Notes-süsteemi avariiplaan tuleb integreerida olemasolevasse avariiplaani (vt B 1.3 Hädaplaanimine). Olulised andmebaasid tuleks replikeerimise abil jaotada mitme serveri peale, kuna üksiku serveri tõrke korral saab siis kasutada replikatsioone.
- Andmevarundus- kontseptsioon - Süsteemi avariiga võivad kaasneda muuhulgas ka andmekaod. Seega tuleb luua Lotus Notes'i jaoks andmevarunduse kontseptsioon, mis tuleks integreerida olemasolevasse andmevarunduse kontseptsiooni (vt B 1.4 Andmevarunduspoliitika). Siinkohal tuleks arvestada Lotus Notes süsteemi kõikide komponentidega, eriti aga klientidega.
- Klasterdamine - Notes pakub nn klasterdamisega võimalust käitada mitut füüsilist serverit korraga ühe virtuaalse serverina. Ühe serveri tõrke korral toimub automaatne Failover ja klastri ülejäänud serverid võtavad avariilise serveri ülesanded enda kanda. Kas vastav valik on Lotus Notes töökontseptsiooni raames mõistlik või mitte, tuleb otsustada iga konkreetse olukorra puhul eraldi.
- Notes-IDde taastamine - Notes-IDde jaoks pakub Lotus Notes taastamismehhanismi. Seda saab kasutada kahel moel: ühe valiku puhul saab taastada kogu Notes-ID-faili, kui see on muutunud kasutuskõlbmatuks või kustutatud. Teise valikuga on võimalik viia unustatud Notes-ID-paroolid paroolide taastamismehhanismiga tagasi nende algolekusse. Sel juhul peab kasutaja küsima ühelt või mitmelt administraatorilt nn taastamisparoolid ning seejärel saab määrata uue Notes-ID-parooli.
- Oluliste System-Notes-ID'de varukoopiate hoidmine - Olulised System-Notes-ID'd (Root-Certifier, Certifier, Server, Administrator) tuleb alati vähemalt ühe eraldiseisvana koopiana alles hoida.
- Dokumentatsioon peab sobima avariiolukorras kasutamiseks - Süsteemi konfiguratsioon tuleb dokumenteerida. Olulisi ülesandeid tuleb kirjeldada selliselt, et vajadusel suudaksid neid teostada ka isikud, kellel on pikaajaline kogemus tehnikaga ümberkäimisel, kuid kes on konkreetses valdkonnas võhikud.
- Taasteplaan - Tuleb luua taasteplaan, mis tagaks süsteemi korrakohase sisselülitamise.
- Avariiplaan - Avariiplaan peab arvestama oluliste Notes-serverite eripäradega (nt sertifitseerimisüksuse eripäradega) ja olema kohandatud sellega sobivaks. Avariiennetamise raames tuleb arvestada ka erinevate kompromiteerimisvõimalustega (nt Root-Certifier-ID kompromiteerimisega) ja sellega, kuidas niisugustel juhtudel asjakohaselt reageerida.

Täiendavad kontrollküsimused:

- Kas Lotus Notes süsteemi avarii puhuks on koostatud avariiplaan?
- Kas Lotus Notes süsteemi jaoks on olemas andmevarunduskontseptsioon, mis hõlmab kõiki komponente?

M 6.74z Avariiarhiiv

Algatamise eest vastutavad: ametiasutuse / ettevõtte juhtkond, IT-juht

Rakendamise eest vastutavad: IT-juht

Avariiarhiiv sisaldab selliseid varundusandmeid, mille põhjal saab kogu süsteemi terviklikult taastada.

Varundatud andmete hoidmine muudes ohualades

Vastav andmevarundus ei tohi mitte mingil juhul hävida samadel põhjustel, mis ähvardavad tootmisandmeid. See peab olema kättesaadav ka pärast katastroofi, st juurdepääs varunduse andmekandjatele ja nende transport peab mahtuma sellesse ajavahemikku, mis on kehtestatud taasteplaaniga. Hoidmine andmekandjaseifis või andmekandjate turvaarhiivis ei ole selleks piisav järgmistel põhjustel:

- Juurdepääs võib olla takistatud näiteks rusude tõttu
- Tuletõrje või juhtumit uurivad ametiasutused võivad juurdepääsu vastavale kohale mitmeks päevaks sulgeda
- Sisenemine ei ole lihtsalt võimalik, kuna hoone on muutunud liiga varisemisohtlikuks.

Niisuguste probleemide lahendamiseks tuleb andmevarundust sisaldavaid andmekandjaid hoida väljapool asutust. Siinkohal on võimalikud järgmised variandid:

Andmekandjate transportimine avariiarhiivi

- Avariiarhiivi võib sisse seada mõnes muus hooneosas (tavaliselt kahe tuletõkketsooni kaugusel) või siis mõnes muus hoones. Varundusi sisaldavad andmekandjad tuleb aegsasti sinna kohale transportida. Sinna ladustatavad andmevarundused peavad olema kaitstud volitamata juurdepääsu ja sabotaaži eest. Sõltuvalt riskiastmest tuleb mõelda ka kaitsele selliste tegurite vastu nagu tulekahju, suitsugaasid, veekahjustus ja andmekandjaid hävitavad magnetväljad. Seega võib kasutada sobivasse kaitseklassi kuuluvat andmeseifi või andmevarundusarhiivi.

Andmekogude edastamine võrgu kaudu

- Andmekandjaid ei transpordita ladustuskohta, selle asemel edastatakse varundatud andmed kas sideliinide kaudu robotarhiivi või kaugemal asuvatesse peegeldatud kettakogumitesse. Suurte andmemahtude jaoks on kõige parem kasutada valguskaableid mis võimaldavad edastada suuri andmehulkasid pikkade vahemaade taha. Käideldavuse tõstmise eesmärgil tuleks selle lahenduse puhul kaaluda varuliinide kasutamist (vt M 6.18 Varuliinid). Avariiarhiivi käitamise võib jätta välise teenusepakkuja hoolde, kes pakub nii andmete edastamis- kui ka salvestamisteenust. Avariiolukorras peaksid need ettevõtted tegema vajadusel kättesaadavaks ka täiendavad riistvarakomponendid, et asutus saaks kiirelt infotöötlusega jätkata. Välise teenusepakkuja valimisel tuleb sõlmida täpne leping ning kehtestada teenuse mahtu ja vajalikke turvameetmeid kajastavad tingimused (vt M 5.87 Leping kolmandate poolte võrkudega ühendamise kohta).

Kontrollküsimused:

- Kas avariiarhiivi vajalikkust on uuritud?

- Kas andmevarundusi sisaldavaid andmekandjaid hoitakse võrreldes IT-süsteemidega erinevas tuletõkketsoonis?
- Kas avariiarhiiviga loodava ühenduse jaoks on tarvis liiasusega varuliine?
- Kas on tagatud, et hädaolukorra arhiivi andmevarundus ei ole ohustatud sama kahju põhjustaja poolt nagu tootmisandmed?

M 6.75z Varu-sidekanalid

Algatamise eest vastutavad: IT-juht, IT-turvaosakonna meeskond

Rakendamise eest vastutavad: administraator

Sõltuvalt käideldavusele esitatavatest nõuetest võib kommunikatsiooniühenduste tõrge või puudumine endaga kaasa tuua tõsiseid probleeme. See kehtib nii telefoni-, LAN- kui ka WAN-ühenduste puhul. Veaallikad võivad olla väga erinevad, millest tulenevalt on põhjuse leidmine tihti väga keeruline. Kuna tüüpiline töökeskkond on üha enam ühenduses teiste omasugustega, võib kommunikatsiooniühenduse tõrke tagajärjel tekkida olukord, kus olulisi andmeid ja infot ei saa enam omavahel vahetada. Senikaua, kui ühendused taastatakse või leitakse sobivad varuvariandid, võib tekkida tööseisak. Seetõttu on kasulik hoida erinevate kommunikatsiooniühenduste jaoks valmis ka võimalikud varuvariandid (sõltuvalt nende kaitsevajadusest).

Näited:

- Telefoniühendus keskjaamaga peaks lisaks püsivõrgule olema tagatud ka mobiiltelefoni kaudu.
- Meiliserveri ühendamiseks välismaailmaga peaks lisaks tavapärasele interneti-teenusepakkujale olema võimalik kasutada veel ka mõnda teist teenusepakkujat.
- Lisaks meiliühendusele või lisaks faksiserverile peaks olemas olema ka faksiaparaat, mida saab kasutada olukorras, kus võrguühendus või server ei tööta.

Seejuures pole alati vajalik hoida varuks sama ribalaiuse ja kvaliteediga ühendust. Paljudel juhtudel on piisav, kui avariiolukorras on võimalik tööd jätkata vähemalt piiratud võimlaustega (vt B 1.3 Hädaplaanimine).

Täiendavad kontrollküsimused:

- Kas oluliste kommunikatsiooniühenduste jaoks on olemas varulahendused?
- Kas varuvariante täiendatakse regulaarselt kooskõlas tehnika arenguga?

M 6.76 Avariiplaani koostamine Windowsi süsteemi tõrke puhuks

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: IT-juht, administraator

Avariidokumentatsiooni tuleb käsitleda konfidentsiaalse infona

Ühe või mitme Windows-süsteemi avarii võib vastava serverirolli täitmise korral mõjutada tõsiselt IT-keskkonda, kuna kasutaja ei pääse enam serverisüsteemile ligi. Tuleb määratleda, millised on vajalikud abinõud, et vältida avariilaadseid situatsioone, minimeerida avarii tagajärgi ning tagada kiire ja tõhus taaskäivitus. Avarii (serveri avarii) puhul vajalik dokumentatsioon ja tegutsemisjuhised võivad sisaldada konfidentsiaalset infot. Neid tuleb hoida turvalises kohas, et vältida vastava info kuritarvitamist.

Konfidentsiaalne info võib olla näiteks:

- Konfiguratsiooniandmed
- Litsentsivõtmed, sõltuvalt olukorrast ka hulgilitsentsi andmekandjad
- (Administratiivsed) kasutajakontod ja paroolid
- Muu autentimis teave (Windows 7 Bitlocker Drive Encryptioni võti)

Samas tuleb aga organisatoorsete meetmetega tagada, et vajalik info oleks avarii korral kättesaadav isikutele, kes vastutavad taastamise eest. Windowssüsteemide avariiplaan tuleb integreerida avariikontseptsiooni (vt B 1.2 Personal ja M 6.96 Serveri avariiplaan) ning see peab olema kooskõlas meetmega M 6.96 Serveri avariiplaan .

Alustage avariiplaani koostamisega juba süsteemi planeerimisel

Avariiplaani koostamisega tuleks alustada juba süsteemi planeerimisel, et saaks juba aegsasti arvestada võimalike spetsiaalsete käideldavusnõuetega, mis võivad nt ette näha serverite varustamise liiasusega (vt M 6.1 Käideldavusnõuete inventuur). Avariiplaan peab sisaldama selgeid kriteeriumeid, mis määraksid, millistele Windows-süsteemidele avariiplaani rakendatakse.

Andmevarundus

Windows-süsteemide avariiplaanis tuleb viidata asjaolule, et avariiolukorraga toimetulekuks peavad moodulis B 1.4 Andmevarunduspoliitika kirjeldatud meetmed olema juba ellu rakendatud.

Andmevarunduse dokumenteerimine

Andmevarundust kajastav dokumentatsioon on avariiplaani jaoks väga oluline. Dokumentatsiooni värskust tuleks hooldustööde käigus regulaarselt kontrollida. Ennekõike peab dokumentatsioonist saama välja lugeda, millises mahus andmeid varundati, millal toimus viimane edukas varundamine ning millist tark- ja riistvara andmevarunduseks kasutati. Valitud andmevarundusprotseduur ning rakendatav riist- ja tarkvara peavad suutma täita taastamisnõuetes kehtestatud taastamisaja piiranguid.

Tehniline dokumentatsioon

Süsteemide kohta peab eksisteerima piisav tehniline dokumentatsioon, mida saaks avarii korral kasutada.

Dokumentatsioon peaks sisaldama vähemalt järgnevaid punkte:

- BIOSi ja püsivara versioonid
- Riistvara
- Installeeritud Windows-komponendid
- Installeeritud lisatarkvara
- Võrgu konfiguratsioon
- Teenused
- Kõvaketaste või ühendatud kõvakettasüsteemi partitsioonide jaotumine
- Kasutajakontod ja volitustega grupid
- Kasutusload ja kasutuslubade volitused, NTFS volitused
- Seadistused turvapoliitikates (mallide abil)

Kogu dokumentatsiooni kaasamine avariiplaani koostamisse

Selleks, et avariiolukorras ei selguks, et olulised funktsioonid on jäetud tähelepanuta, tuleb avariiplaani koostamisel arvestada kogu olemasoleva dokumentatsiooniga ning vajadusel seda ka veel täiendada. Dokumentatsiooni tuleb kohandada hooldustööde käigus, pärast riistvaras ja tarkvaras tehtud muudatusi ning samuti süsteemikonfiguratsiooni muutmise järel.

Kogu dokumentatsioon peab olema saadaval offline töörežiimis

Tehnilise dokumentatsiooni ja seega ka avariiplaani värskendamine on osa muudatuste haldusest. Peab olema arusaadav, millised isikud tegid muudatusi ja kes uuendas dokumentatsiooni. Avariiplaani jaoks peab kogu dokumentatsioon, kaasa arvatud tootjapoolne dokumentatsioon eksisteerima trükivormis, kuna avariiolukorras pole elektrooniline juurdepääs alati tagatud.

Töötamine alternatiivsüsteemidel

Kui organisatsiooni seisukohast on talutavad on ainult lühiajalised tööseisakud, tuleb tagada alternatiivsete süsteemide kasutusvõimalus. Süsteemide koguvõimsus peaks olema planeeritud selliselt, et üksiku süsteemi avarii korral suudaksid asutuse ülejäänud süsteemid avariilise süsteemi rollid ja funktsioonid võimalikult suures mahus enda peale võtta. Siinkohal tuleb arvestada meetmetega M 4.418 Windows Server 2008 kasutamise planeerimine või M 4.420 Windows 7 tegevuskeskuse turvaline kasutamine .

Varuseadmed

Windows-serverite puhul tuleks kaaluda varuseadmete soetamist, mis võimaldaks jätkata Windows-serveri ja teatud rakenduste käitamist ka neil juhtudel, mil avarii võib esineda korraga mitmes serveris. Ümberlülitusaja minimeerimiseks peavad need seadmed olema eelnevalt installeeritud ning neid tuleb regulaarselt käivitada ja hooldada. See kehtib Windows 7 ja Windows Server 2008 kasutamisel ka neis seadmetes, milles rakendatakse KMS-i (Key Management Service) või MAK-proksit (Multi Activation Key Proxy), juhul kui neid aktiveerimisliike kasutatakse hulgilitsentside jaoks. Alternatiivsüsteemide kasutusprotseduuride väljatöötamine võib olla väga töömahukas. Seetõttu on alternatiivsüsteemide kasutusprotseduuride väljatöötamisega soovitatav alustada juba serverikasutuse planeerimisel. Alternatiivsüsteemide kasutuselevõtu jaoks peavad olema koostatud konkreetsed tegevusjuhised.

Konkreetsed tegutsemisjuhised alternatiivsüsteemidega töötamiseks

Alternatiivsüsteemide kasutamisprotseduuride väljatöötamine võib olla väga töömahukas. Seetõttu on alternatiivsüsteemide kasutamisprotseduuride väljatöötamisega soovitatav alustada juba serverikasutuse planeerimisfaasis. Alternatiivsüsteemide käikuvõtmise jaoks peavad eksisteerima konkreetsed tegutsemisjuhised.

Taasteplaan

Sõltuvalt serveri rollist ja IT-keskkonna eripärast kehtestatakse Windowssüsteemide avariijärgsele taaskäivitusele erinevaid nõudeid. Siinkohal tuleb lisaks vaatluse all olevale serverile arvestada ka ühendatud IT-keskkonna (nt marsruuteri, teiste serverite, asukoha konnektorite) käivitusaegadega. Käivitusplaan on seda keerukam, mida suurem on IT-süsteem ning see tuleb koostada kooskõlas domeeni struktuuri ja rakendatavate serverirollidega. Liikmesserverit tuleks uuesti käivitada alles siis, kui eelnevalt on käivitatud vähemalt üks globaalse kataloogiga domeenikontroller, üks sertifikaatide server sertifikaatide keelunimekirjade päringuteks (kui on olemas) ja kõik infrastruktuuriserverid.

Avariiplaani testimine

Hooldusplaani raames tuleks avariiplaani regulaarselt (nt kord kvartalis) testida testimiskeskkonnas, mõnikord siiski ka tootmiskeskkonnas, mis nõuab aga loomulikult erilist hoolt. Mida sagedasemad on konfiguratsioonis tehtavad muudatused, seda sagedamini tuleb avariiplaani selle värskuse tagamiseks testida. Tulemused tuleb dokumenteerida ja vajadusel sellest lähtuvalt olemasolevat avariiplaani muuta. Taastamisstsenaariumeid tuleb kontrollida ja tulemused dokumenteerida.

Taastamine

Avariiplaanis peavad olema kirjas reinstalleerimistööde abil tehtavaks taastamiseks vajalikud eeldused. Tuleb arvestada ettevalmistamise kontseptsiooniga või olemasolevate installeerimiskontseptsioonidega. Kriitilise tähtsusega on nt kasutatav riistvara ja vajalikud draiverid. Teatud RAID-kontrollerite puhul võib osutuda vajalikuks paigaldada draivereid installeerimise käigus. Tavaliselt annab tootja draiverid eraldi andmekandjal koos tootega kaasa või tagab nende kättesaadavuse internetis. Andmekandjal peab olema vastava draiveri hetkel kasutuses olev versioon.

Installeerimisallikad ja litsentsid

Taastamine nõuab originaaltarkvara olemasolu originaalandmekandjatel koos tootevõtmete ja litsentsiinfoga. Kui hulgilitsentsiprogrammi ei kasutada, tuleb Windows-süsteemide võimaliku aktiveerimisvajaduse korral juhtida tähelepanu sellele, et Interneti kaudu toimuv mitmekordne aktiveerimine ühe ja sama tootevõtmega erinevatel kõvaketastel võib ebaõnnestuda. Selle tagajärjel võib olla vajalik võtta otse telefoni teel ühendust Microsoftiga. Microsofti tuleb teavitada süsteemi avariist. Windows 7 kliendid tuleb reaktiveerida ka siis, kui kasutatakse Windows 7 hulgilitsentse. Windows 7 kasutamisel tuleb muu hulgas pöörata tähelepanu sellele, et alati oleks olemas piisav arv litsentse. Uuesti installimise korral ja juhtudel, kus aktiveerimine leiab aset automaatselt kas MAK-proksi või KMS-iga, küsivad Windows 7 kliendid litsentse. Litsentsihaldus peab tagama, et aktiveerimiseks oleks olemas piisav hulk litsentse.

Lisateavet aktiveerimise kohta leiate meetmetest M 4.336 Hulgilitsentslepinguga Windowsi süsteemide aktiveerimine alates Windows Server 2008-st ja M 4.343z Hulgilitsentsilepinguga Windowsi süsteemide reaktiveerimine alates Windows Vistast või Windows Server 2008-st tuleb tagada, et taastamisvõtmeid oleks vajaduse korral võimalik lühikeseks ajaks kättesaadavaks teha. Edastamisel peab volitamata tutvumine olema välistatud. Süsteemide uuesti installimise korral muutuvad seni kasutatud autentimislahendused ja BitLocker Drive Encryptioni taastamisvõtmed kehtetuks. Uute, st äsja koostatud autentimis- ja taastamisvõtmete puhul tuleb tagada, et neile pääsevad juurde üksnes volitatud isikud (vt M 4.337z BitLockeri Drive Encryption kasutamine).

Replikaatide varu hoidmine

Luues olulisest infost ja failidest replikaate erinevatele serveritele, saab üksikute serverite avariide korral kasutada vastavaid replikaate. Seeläbi saab kasutajatele kiirelt kättesaadavaks teha andmetest loodud koopiaid. Avariiplaani raames tuleks kontrollida, kas ja milliste andmete jaoks on see vajalik. Windows-Serverid pakuvad selleks replikeerimisteenust FRS (File Replication Service), mida saab kasutada ka koos DFSiga (Distributed File Service).

Avariiplaani koostamisel tuleb täiemahulise taastamise eesmärgil eristada Windows-süsteemide teatud rolle nagu nt DNS-server ja sertifikaadiserver. Selle juurde kuulub rollipõhiste süsteemikomponentide (nt DNS-teenuse või sertifitseerimisüksuse andmebaaside) varundamine, samuti põhjalik dokumentatsioon vastavate rollidega seotud seadistuste kohta.

Kontrollküsimused:

- Kas isikutel, kes vastutavad taastamise eest, on IT-süsteemi rikke korral juurdepääs kõikidele vajalikele andmetele, nagu konfigureerimisandmed, litsentsivõtmed, administratiivsed kasutajakontod ja paroolid?
- Kas on olemas hädaolukorraks valmisoleku plaan ja kas see on asutuse hädaolukorra kontseptsiooni osa?
- Varusüsteemide kasutamine: Kas süsteemide koguvõimsus on rollide ja funktsioonide võimaliku ülevõtmise korral piisav, et asendada rivist välja langenud süsteeme?
- Kas hädaolukorraks valmisoleku plaani ajakohasus on tagatud ka pärast konfiguratsioonimuudatusi?
- Kas hädaolukorraks valmisoleku plaanis peetakse kinni reinstalleerimistööde abil tehtavaks taastamiseks vajalikest eeldustest?
- Kas süsteemi taastamisel võetakse arvesse olemasolevat kasutusse andmise ja installeerimise kontseptsiooni?
- Kas on tagatud rollipõhiste süsteemikomponentide täielik taastamine ja kas rollidega seotud seadistused on dokumenteeritud?

M 6.78 Andmete varundamine Windowsi klientsüsteemides

Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: kasutajad
Andmevarunduse käigus tuleb pöörata tähelepanu järgnevale:
Oluliste süsteemifailide varundamine

- Varundustarkvara suudab varundada olulisi süsteemifaile, nt lokaalse arvuti registrit, COM+ registriandmeid ning ka käivitusfaile. Seda tuleks teha regulaarsete ajavahemike tagant ning pärast suuremaid muudatusi konfiguratsioonis. Selleks tuleb valiku System Status all aktiveerida vastavad valikukastid.
- Domeenikontrolleritel saab lisaks varundada ka Active Directory andmeid ja SYSVOL-kataloogi andmeid. Seda tuleks teha iga varunduse käigus. Domeenikontrolleritel leiab olulised valikud samuti valiku System Status alt.

Logifaili genereerimine

- Varundusprotseduuri kohta tuleb kindlasti luua ka logifail. Pärast tööde lõppu tuleks logifaili analüüsida, et välja selgitada, kas kõik andmed, mida varundada taheti, ka tõepoolest varundati ning kas varundusprotsessi käigus on esinenud vigu. Seejuures on soovitatav aktiveerida Tools / Options / Backup Log all valik Details , kuna sellega on võimalik kindlaks teha, kas kõik varundamisele kuulunud andmed varundati ning kas vastavad kataloogid, mida varundusprotsessi lülitada taheti ka tõepoolest sellesse kaasati.

Juurdepääsukaitse taastamine

- Varundatud andmete taastamisel saab taastada ka nende juurdepääsukaitse, juhul, kui taastamistöö käigus on tehtud vastav valik (nupp (Start Restore / Advanced buttons). Standardina on see valik sisse lülitatud. Seejuures on seda võimalik kasutada ainult NTFS-failisüsteemist pärinevate andmete puhul.
- Varundatavad failid ja kataloogid saab salvestada ühtsesse faili, et neid valikuid sealt hiljem tagasi laadida. See mehhanism võimaldab luua varundustest eri versioone, mis hõlmavad erinevaid andmeid.
- Varundada tuleks regulaarsete ajavahemike möödudes.

Planeerige varundustöö kindlatele aegadele. Niimoodi on võimalik varundamist automatiseerida. Kui suurte süsteemide või kõrgete käideldavusnõuete puhuks otsustatakse täiendava andmevarundustarkvara kasuks, tuleb tarkvara valimisel jälgida, et see täidaks järgnevaid nõudeid:

- Varundamisel ja taastamisel peab olema tagatud kasutatud failisüsteemide tugi, seega peaks tarkvara toetama FATi, NTFSi ja vajadusel ka HPFSi.
- Varundada peab saama nii Active Directory andmeid kui ka SYSVOLkataloogi andmeid.

Automaatne tagasiside

- Andmevarundusi peaks olema võimalik teostada automaatselt, kas eelvalikuga määratava ajahetke või reguleeritavate intervallide alusel, ilma et selleks oleks tarvis käsitsi sekkuda (sõltuvalt olukorrast tuleb võib-olla tegeleda siiski ka varunduseks vajalike andmekandjate valmisseadmisega).
- Tarkvara peaks suutma teavitada üht või mitut valitavat kasutajat automaatselt andmevarundusprotsessi tulemuste kohta ning olema võimeline edastama veateateid, kasutades selleks kas meili vms mehhanisme.
- Andmevarundustarkvara peaks toetama varukoopiat sisaldava andmekandja kaitsmist kas parooli või veel parem, krüpteerimisega. Lisaks peaks tarkvara suutma varundatud faile salvestada tihendatud kujul.

Include - ja Exclude -loendid

- Failide ja kataloogide valimisel peab olema võimalik vastavate Include - ja Exclude -loendite abil täpselt määrata, milliseid andmeid tuleb varundada ja milliseid mitte. Nimetatud leoendeid peab olema võimalik kokku liita varundusprofiilideks, neid peab olema võimalik salvestada ning hiljem varunduse otstarbel uuesti kasutada.
- Varundamisse kaasatavaid andmeid peab olema võimalik valida nende loomise kuupäeva ja viimase muudatuskuupäeva alusel.

Automaatvõrdlus

- Varundustarkvara peaks toetama täielike loogiliste ja füüsiliste varukoopiate ning inkrementaalsete varukoopiate (muudatusi kajastavate koopiate) loomist.
- Varundamisprotsess peaks toimima ka kõvaketastel ja võrguajamitel.
- Varundamistarkvara peaks suutma läbi viia automaatseid analüüse ja võrdlema pärast varundamise lõppu omavahel varundust ja originaalandmeid ning pärast andmete taastamist taastatud andmeid ja andmevarunduse andmekandja sisu.
- Failide taastamise puhul peaks olema võimalik ise valida, kas andmed taastatakse nende algsele asukohale või mõnele muule kettale või mõne muu kataloogi alla. Samuti peaks olema võimalik tarkvara juhtida ka sellistes olukordades, kus sihtkohas võib juba ees olla mõni sama nimega fail. Seejuures peab saama seadistada, et vastavat faili ei tohi mitte kunagi üle kirjutada, tohib alati üle kirjutada või tohib üle kirjutada vaid juhul, kui see on vanem kui taastatav fail, või et vastaval juhul esitatakse kasutajale enne toimingut konkreetne asjakohane küsimus.

Kontrollküsimused:

- Kas andmevarundusprotseduur on dokumenteeritud?
- Kas andmevarunduseks kasutatav protseduur on kooskõlas olemasoleva andmevarunduskontseptsiooniga?

M 6.79 Andmete varundamine Internet-PCde kasutamisel

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator

Internet-PCsid saab kasutada erinevatel otstarvetel. Ühest küljest saab Internet-PC paigaldada täiendava juurdepääsuvõimaluse loomiseks internetile, nt kui töökohaarvutil on küll internetijuurdepääs olemas, kuid seal ei saa turvalisuse põhjustel käivitada aktiivsisu, nt JavaScript'i. Teisalt pakuvad Internet-PCd sageli ainsat võimalust kasutada WWWd, meili või muid internetiteenuseid.

Käideldavuse suurendamine

Nimetatud erinevatest kasutusvaldkondadest tulenevad ka erinevad nõuded Internet-PCde käideldavusele. Kõrgete käideldavusnõuete puhul saab kasutada liiasusega Internet-PCsid ja internetiühendust. Internet-PC kiire taastamise tagamiseks avarii, tehnilise tõrke või edukaks osutunud ründe korral, tuleks igal juhul luua asjakohane andmevarunduse kontseptsioon. Seejuures tuleb eristada süsteemi-, programmi- ja konfiguratsioonifaile ning rakendusandmeid.

Süsteemi-, programmi- ja konfiguratsioonifailide varundamine

Image andmevarunduse alusena

Internet-PC võimalikult kiireks taastamiseks, tuleks pärast kõikide vajalike operatsioonisüsteemi koostisosade ja tarkvarakomponentide paigaldamist ning sellele järgnevat konfigureerimist teha süsteemist kujutis (*Image*). Selleks varundatakse kõik süsteemi-, programmi- ja konfiguratsioonifailid varundusprogrammi abil või kasutatakse eriprogrammi, mis salvestab kogu kõvaketta sisu baithaaval ümber. Viimasel juhul ei tohiks sel ajal kõvakettal asuda rakendusandmeid. Süsteemikujutis tuleks luua järgnevatel juhtudel:

- Esimene kord vahetult pärast Internet-PC installeerimist ja selle konfigureerimist,
- Iga kord, kui mõni operatsioonisüsteemi või tarkvara komponent on installeeritud, eemaldatud või uuendatud, nt pärast paikade installeerimist,
- Iga kord, kui konfiguratsioonis on tehtud olulisi või turvalisust mõjutavaid muudatusi.

Niimoodi toimides ei pea pärast Internet-PC avariid kõiki tarkvarakomponente ükshaaval uuesti installeerima ja konfigureerima hakkama. Selle asemel saab süsteemi taastada tervikuna.

Rakendusandmete varundamine

Kataloogide määratlemine

Kui kasutuskontseptsioon näeb ette lokaalset andmetalletust, tuleb lisaks süsteemiandmetele *regulaarselt* varundada ka rakendusandmeid. Selleks on soovitatav luua Internet-PC all üks või mitu kataloogi, millesse tohib salvestada rakendusandmeid. Nende kataloogide sisu kaasatakse varundusse. Kasutajatele tuleb selgitada, milliseid kataloge varundatakse ja kuidas faile sinna salvestada. Varundatavate rakendusandmete hulk võib kiiresti kasvada. Seetõttu tuleb andmevarunduse kontseptsioonis kindlaks määrata, millised on varunduse salvestusmahu piirangud ja mida teha mahu ületamise korral.

Andmevarunduskontseptsioon

Andmevarunduse protseduur peab olema dokumenteeritud vastavas kontseptsioonis. Kontseptsioon peaks sisaldama vähemalt järgnevaid punkte:

- Andmevarunduse maht (kataloogid, partitsioonid, jne)
- Andmevarunduse sagedus ja aeg
- Andmevarunduseks kasutatav andmekandja
- Andmevarundusega seotud vastutusalad
- Varukoopiaid sisaldavate andmekandjate hoiukoht

Kasutajate informeerimine
Kõik Internet-PC kasutajad peavad olema andmevarunduskontseptsioonist teadlikud. Täiendavaid soovitusi andmevarunduskontseptsiooni koostamise kohta leiate M 6.33 Andmevarunduskontseptsiooni loomine .
Näited

- Internet-PCde kasutamine ettevõttes lisavõimalusena, kuna majasisese võrgu kaudu internetti kasutades ei tohi käivitada aktiivsisu. Süsteemi installeeritakse *Image* abil uuesti kord nädalas. Kasutajaid on teavitatud, et kui tahavad oma Internet-PC andmeid ka edaspidi kasutada, peavad nad neid varundama iseseisvalt.
- Ettevõtte majasisene võrk ei ole Internetiga ühenduses. Meiliteenuse kasutamiseks paigaldatakse seetõttu mitu Internet-PCd ja ühendatakse omavahel võrku. Sisenevad ja väljuvad meilid varundatakse iga päev ühte Internet-PCsse paigaldatud CD-kirjutaja abil. Administraator ja tema asendaja vastutavad CD-R või CD-RW andmekandjate kirjutusseadmesse asetamise ja andmevarunduse käivitamise eest.

Täiendavad kontrollküsimused:

- Kas Internet-PC jaoks on koostatud andmevarunduskontseptsioon?
- Kas andmevarunduskontseptsioon arvestab ka võimalike lokaalselt salvestatud rakendusandmetega?
- Kas kõik kasutajad on andmevarunduskontseptsioonist teadlikud?

M 6.81 Novell eDirectory andmete varundamine

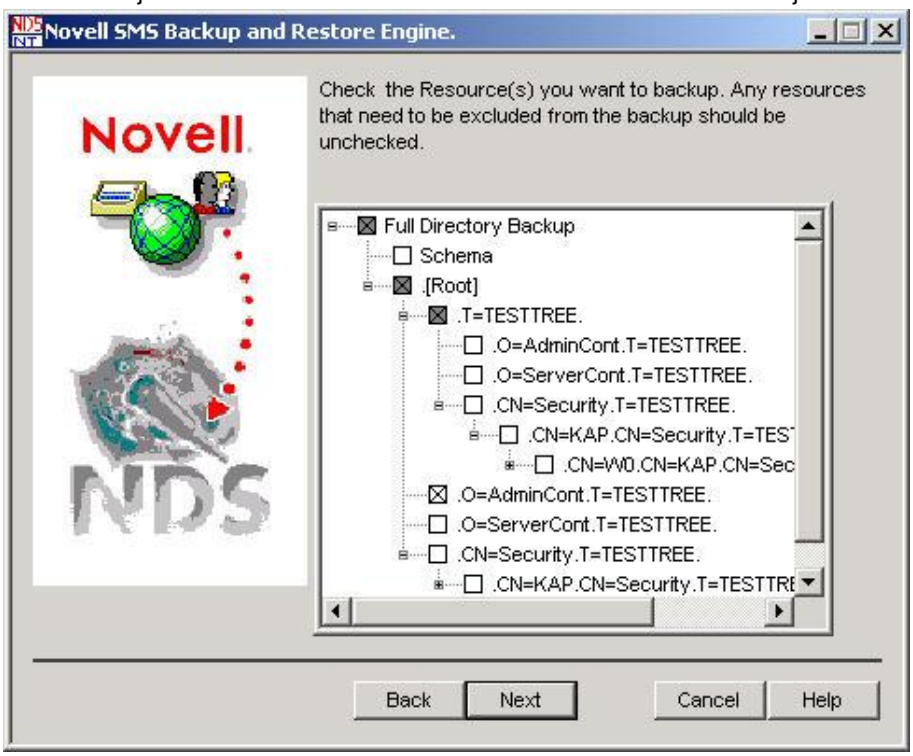
Algatamise eest vastutavad: IT-juht, IT-turvaosakond
Rakendamise eest vastutavad: administraator

eDirectory-kataloogiteenuse andmete varundamine tuleks läbi viia koos üldise serveriandmete varundamisega, et hiljem oleks võimalik taastada serverite üldseisundit. Sel põhjusel sõltub varundusprotsessi valik ka kasutatavast operatsioonisüsteemist. Tagamaks eDirectory-andmekogumi ühtset varundamist serveril, tuleks kasutada spetsiaalset varundusprogrammi.

eDirectory varundamiseks saab kasutada järgnevaid programme:

- Netware: SBCON.NLM
- Linux, Sun Solaris: ndsbackup utility

Lisaks kataloogi täielikule varundamisele pakuvad Novell-programmid võimalust varundada ka ainult teatud eDirectory osasid. Üksikute eDirectory-objektide arhiveerimiseks või taastamiseks tuleb määratleda objekti täielik eraldusnimi (distinguished name). Kogu puu varundamiseks tuleb määratleda vastav Tree-objekt. Eraldi on võimalik varundada ka skeemi, milleks tuleb välja valida vastav skeem - objekt. Varundada saab ka eDirectory-puu üksikosi, milleks tuleb valida puu vastav konteiner. Seejärel varundatakse kõik vastava konteineri alla kuuluvad objektid.



Joonis: Novell SMS Backup and Restore Engine

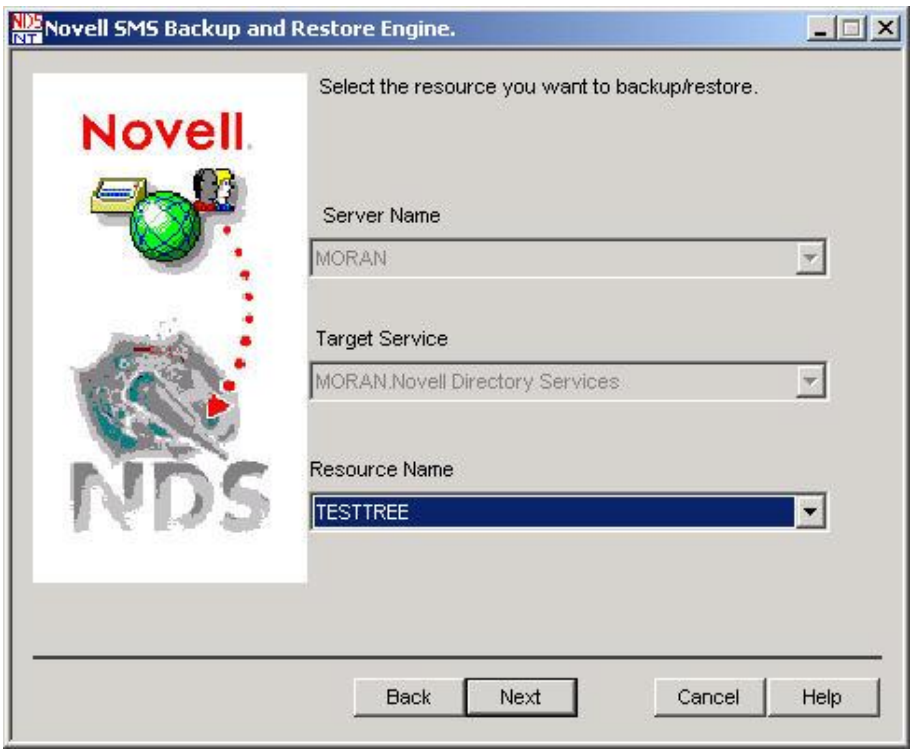
Dokumentatsioon tuleb välja printida!
Nimetatud varundusprogrammidega ei saa varundada partitsiooni infot. Taastamise korral tuleb vastavad kohad tagantjärgi partitsioonideks jaotada. Sel põhjusel tuleb puustruktuuri kohta kindlasti välja printida koopiad, mida tuleb ka regulaarselt värskendada.

eDirectory-utiliitide varundusprotsessi saab kohandada sobivaks kasutaja vajadustega. Valikuga Exclude/Include saab teatud eDirectory-objekte andmevarundusest välja jätta või sellesse juurde liita.

Andmevarunduse logimine
Varukoopiaid tuleks reeglina teha kord nädalas või sagedamini. See sõltub sellest, kui sageli oluline kataloogiinfo muutub. Varundusprotsess peaks olema arusaadaval kujul logitud ning logi alusel tuleks kontrollida, kas kõik failid on veatult varundatud.

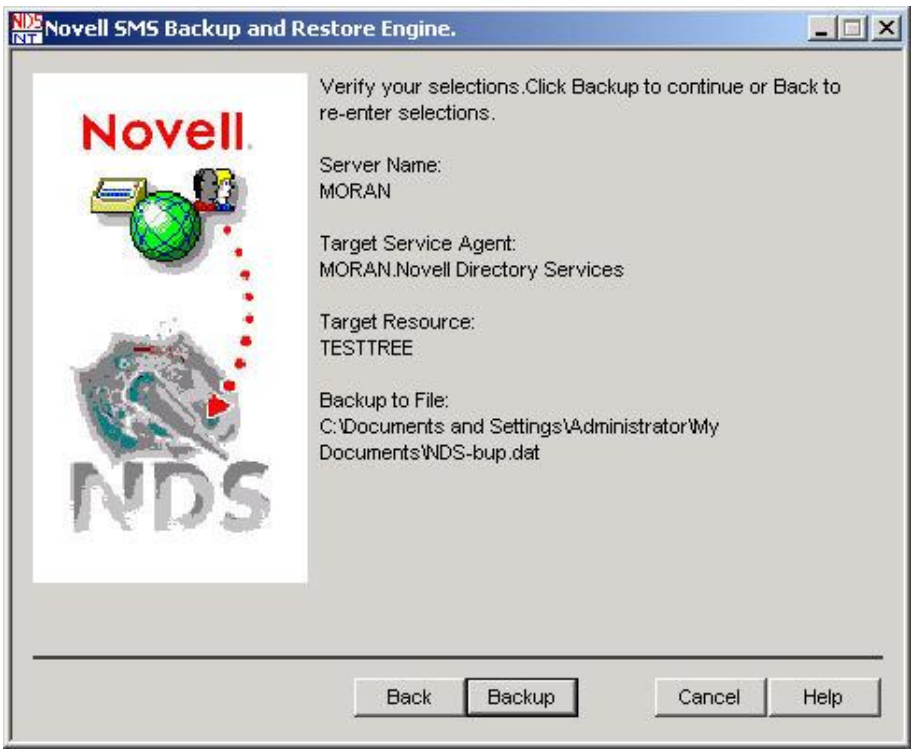
Varundamine Netware'i all
Netware-operatsioonisüsteemi üks osa on SBCON.NLM, nn Storage Management Engine (SME). See kujutab endast tagaprogrammi (Back End 'i), mis teostab Backup/Restore -päringuid. Enne SBCON.NLM kasutamist tuleb siiski laadida QMAN.NLM , et töödelda SBCON.NLM poolt loodud Backup/Restore -töid. Selle asemel võib töötada ka SMS-ühilduvate Backup/Restore -utiliitidega.

Storage Management Data Requester (SMDR) suhtleb SME ja Target Service Agent (TSA)-tarkvara vahel. SMDR.NLM esmakordsel laadimisel küsitakse kasutajalt erinevaid küsimusi konfiguratsioonivalikute kohta, muuhulgas ka seda, kas luua eDirectory-kataloogipuusse SMDR-objekt.



Joonis: Resource Name

SME ja TSA võivad asuda samal arvutil või ka erinevatel arvutitel. Jaotatud variandi puhul peab mõlemale olema installeeritud SMDR. Target Service Agents for NDS (TSANDS) suunavad päringuid SMDR ja eDirectory-andmebaasi vahel.



Joonis: *Verify Backup* seadistused

Varundamine Linuxi ja Sun Solarise all
Linuxi ja Sun Solarise all saab andmete varundamiseks kasutada programmi ndsbackup. Programm käivitatakse käsuviiba kaudu ning see võimaldab salvestada eDirectory-objekte eraldiseisvasse faili ndsbackupfile. eDirectory-objektide varundamiseks tuleb määrata nende täielik eraldusnimi, FDN (full distinguished name). Kogu puu salvestamiseks tuleb valida vastav puu-objekt. Käsuviibal saab programmi jaoks kasutada mitmeid funktsioonitähti, nt c - create , r - restore jne, samuti parameetreid. Täpsema info leiate administreerimise käsiraamatust.

Kontrollküsimused:

- Kas eDirectory partitsioonide loomine on dokumenteeritud selliselt, et selle saaks pärast süsteemi avariid käsitsi taastada?
- Kas andmevarundusprotseduur on dokumenteeritud?
- Kas andmevarunduseks kasutatav protseduur on kooskõlas olemasoleva andmevarunduskontseptsiooniga?

M 6.82 Avariiplaani koostamine Exchange-süsteemi avarii puhuks

Algatamise eest vastutavad: IT-juht, IT-turvaosakond

Rakendamise eest vastutavad: administraator

Exchange-süsteemi osaline või täielik avarii mõjutab sageli väga tugevalt meilikasutajate töövõimalusi, kuna avarii tagajärjel pole kõik serveripõhised tegevused enam käideldavad. Avariiennetamise raames tuleb seega luua kontseptsioon, mis aitaks hoida avarii tagajärgi võimalikult minimaalsetena ja määraks, millised sammud on avarii korral kohustuslikud.

Süsteemi konfiguratsiooni dokumenteerimine

Exchange-süsteemi avariiplaan peab arvestama organisatsiooni olemasoleva avariiplaaniga (vt B 1.3 Hädaplaanimine). Lisaks tuleb Exchange 2000 avariiplaan seejuures integreerida ka vastava Windows 2000 võrgu avariiplaani (vt M 6.76 Avariiplaani koostamine Windowsi süsteemi tõrke puhuks). Süsteemi konfiguratsioon tuleb dokumenteerida. Selle juurde kuulub kõvaketta partitsioonide ja nende kasutusotstarvete kirjeldus (süsteem, ülekandeprotokoll, andmebaas jne), samuti riistvara ja operatsioonisüsteemi dokumentatsioon. Olulisi ülesandeid tuleb kirjeldada selliselt, et avariiolukorras suudaks neid kohe teostada ka vastava koolituse läbinud personal. Dokumentatsiooni vajalik täpsus sõltub seejuures vastava personali teadmistest, kes peab avariiolukorras reageerima. Kui organisatsiooni palgal on mitmeliikmeline koolitatud Exchange-administraatorite grupp, võib avariidokumentatsioonist teatud info välja jätta. Kui aga organisatsioonis töötab ainult üks koolitatud Exchange-administraator, peaks avariidokumentatsioon kirjeldama olulisi meetmeid selliselt, et vajadusel suudaksid neid teostada ka isikud, kellel on pikaajaline kogemus tehnikaga ümberkäimisel, kuid kes on konkreetses valdkonnas võhikud.

Andmevarunduse kontseptsiooni koostamine

Avariiplaan peab arvestama lisaks Exchange/Outlook 2000le ka teiste oluliste Windows 2000 Serverite omapäradega, nt sertifitseerimisüksusega, ja olema vastavalt kohandatud.

Taasteplaani koostamine

Süsteemi avariiga võivad kaasneda muuhulgas ka andmekaod. Seega tuleb luua Exchange 2000 jaoks andmevarunduskontseptsioon, mis tuleks integreerida olemasolevasse andmevarunduskontseptsiooni (vt B 1.4 Andmevarunduspoliitika). Seejuures ei tuleks arvestada mitte ainult Exchange-serveriga, vaid ka Exchange-klientidega, eriti Outlook 2000 klientidega. Lisainfot andmevarunduse kohta leiate M 4.166 Exchange/Outlook 2000 turvaline käitamine . Tuleb luua taasteplaan, mis tagaks pärast toimunud avariid süsteemi korrakohase sisselülitamise. Selleks võib kasutada ka Exchange 2000 Server paigaldusprogrammi *Disaster-Recovery-režiimis*. Avariiennetuse raames tuleks arvestada erinevate kompromiteerimisohtudega ning välja töötada vastavad juhised, kuidas tegutseda serveri, üksikute teenuste või kasutajakontode kompromiteerimise puhul.

Avariiõppuste läbiviimine

Tungivalt soovitav on korraldada regulaarselt süsteemitaaste avariiõppuseid. Avariiõppused peaksid arvestama kõikide aspektidega, mis on olulised süsteemi avarii või kompromiteerimise korral. Vastutavad isikud peaksid selleks loodud testimiskeskkonnas harjutama esmajoones andmete taastamist, üksikute teenuste parandamist või nende uuestikonfigureerimist (nt pärast kompromiteerimist). Testimissüsteem peab olema tootmissüsteemiga võimalikult sarnane. Mõnel juhul läheb andmete taastamiseks või süsteemi parandamiseks tarvis konfidentsiaalset

juurdepääsuinfot, nt krüptograafilisi võtmeid või paroole. Tuleb jälgida, et avariiplaan määratleks selliseks juhuks vajalikud toimingud. Lisaks tuleb andmete varundamise või muude meetmetega tagada, et nimetatud info oleks hädaolukorras kättesaadav.

Täiendavad kontrollküsimused:

- Kas Exchange-süsteemi jaoks on olemas avariiplaan?
- Kas Exchange/Outlook 2000 jaoks on olemas kõikide selle oluliste komponentidega arvestav andmevarunduskontseptsioon?
- Kas avariiõppuseid korraldatakse regulaarselt?

M 6.83 Väljasttellimise avariiplaan

Algatamise eest vastutavad: IT turvaosakond, IT-juht

Rakendamise eest vastutavad: IT turvaosakond, IT-juht, administraator

Väljasttellimisel kehtivad avariiennetusele üldjuhul samad nõuded nagu nendele IT-süsteemidele, mille käitamine ei ole organisatsioonist välja viidud.

Väljasttellitava IT-käituse eripärad tulenevad sellest, et ka vastav avariiennetus jaotub mitme osapoole vahel ning ka sellest, et IT-komponentide laialijaotamise tõttu lisanduvad avariiennetusse täiendavad komponendid.

Avariiennetus-kontseptsiooni jaotamine

Üldjuhul peab süsteemide avariiennetuskontseptsioon olemas olema nii tellija ja välise teenusetarnija süsteemide kui ka tellija ja teenusepakkuja vaheliste liideste jaoks (nt võrguühenduse, marsruuteri, telekommunikatsiooniteenuse pakkuja jaoks). Meetmes M 2.253 Välise teenusepakkujaga sõlmitava lepingu koostamine on mõned nõuanded selle kohta, millised aspektid peaksid olema reguleeritud juba teenusetasemelepetes. Avariiennetuskontseptsioonis tuleb täpsustada ja detailselt kirjeldada järgnevaid nõudeid:

Detailsed kokkulepped

- Vastutusalad, kontaktisikud ja protseduurid peavad olema täpselt reguleeritud ja täies mahus dokumenteeritud.
- Tuleb luua täpsed andmevarundust puudutavad eeskirjad (nt eraldi varukoopia-andmekandjad iga kliendi jaoks, käideldavus, töötajate asenduse korraldamine, turvaintsidentide käsitlemine, viirusetõrje).
- Konkreetsete veasituatsioonide jaoks tuleb luua täpsed, konkreetsete nõudmistega tööjuhised.
- Tuleb luua kontseptsioon, mis tagaks avariiõppuste regulaarse läbiviimise.

Tööjuhiste tähendus

IT turvalisus sõltub avariiolukordades olulisel määral välise teenusetarnija personalile mõeldud tööjuhiste kvaliteedist. Sageli käitab teenusepakkuja personal küll tellija süsteeme, kuid puuduvad täpsed teadmised rakendustest, mida vastavates IT-süsteemides käitatakse. Vastutus rakenduse eest on siiski täielikult tellija kanda. Kui rakenduses esineb mõni viga, peab väline teenusetarnija vea kõrvaldama, kuid puudutatud süsteemist ei pruugi tal olla põhjalikke teadmisi. Seega peab ootamatuste ennetamise kontseptsioon tagama välisele teenusetarnijale juhised, kuidas tal on lubatud vastavates olukordades toimida. Seejuures võib olla mõistlik defineerida tegevused, mis on rangelt keelatud, nagu nt masina rebuutimine. Rakenduse rikkekäitumise põhjus võib olla tehniline (nt täis andmekandja, võrguprobleemid) või rakenduspõhine (vale andmekogumi töötlemine, programmiviga, vale seadistus).

Kui tegu on tehniliste vigadega, mis ei mõjuta teisi rakendusi, suudab väline tee-

nusetarnija vea tavaliselt ka iseseisvalt kõrvaldada. Siiski läheb enamasti tarvis ka koostööd tellijaga, et vältida soovimatuid kõrvalmõjusid rakenduse tasandil. Kui probleemid tulenevad rakendusest, vajab väline teenusetarnija detailseid ja põhjalikke juhiseid ja tellijapoolsete kontaktisikute nimekirju, et olukorrale õigesti reageerida. Eriti just keerukate rakendustega seotud probleemide või mahukate pakktööde puhul läheb sageli tarvis teadmisi, mis on olemas vaid tellijal. Sellistel juhtudel on oluline varustada teenusetarnija infoga asjassepuutuvatest andmetest ja süsteemide turbevajadusest, et tarnija suudaks olla piisavalt ettevaatlik.

Kontrollküsimused:

- Kas kõik avariiennetuskontseptsioonid (tellija, teenusetarnija, liides) on välja töötatud?
- Kas isikud, kes peavad hakkama avariiennetuskontseptsiooni kasutama, on kontrollinud nende arusaadavust ja kasutuskõlblikkust?
- Kas teenusetarnijal on olemas kogu vajalik info, et avariiolukorras mõistlikult tegutseda?
- Kas tellija ja teenusetarnija on avariiennetuskontseptsioonid omavahel kooskõlastanud?
- Kas avariiolukorras käitumist on avariiõppuste käigus harjutatud?

M 6.84 Süsteemi- ja arhiiviandmete regulaarne varundamine

Algatamise eest vastutavad: IT-juht
Rakendamise eest vastutavad: IT-juht, administraator

Nagu teisigi IT-süsteeme, ohustab ka elektroonilisi arhiivisüsteeme andmekadu. Sobivate andmekandjate, näiteks optiliste arhiivi-andmekandjate valik üksi ei taga piisavat kaitset andmekao vältimiseks, näiteks arhiivi andmekandja enda hävimise või varguse korral. Seetõttu on arhiiviandmete, selle juurde kuuluva indeksiandmebaasi ja süsteemiandmete varukoopiate tegemine hädavajalik. Andmete varundamiseks tuleb põhimõtteliselt rakendada moodulis B 1.4 Andmevarunduspoliitika esitatud nõudmisi.

Alternatiivina arhiiviandmete varundamisele võib toimuda ka varukoopiad salvestada ka füüsiliselt eraldatud ja erinevatesse tuletõkkesektsioonidesse paigaldatud arhiivisüsteemidesse. Mõned arhiivisüsteemide tootjad pakuvad selleks kõrge käideldavusega lahendusi. Vaatamata sellele peab ka sel juhul toimuma nii arhiivisüsteemi enda kui ka indeksiandmebaasi andmete varundamine.

Andmete varundamisel ja andmekandjate kasutamisel tuleb täita alljärgnevaid nõudeid:

- Tuleb sisse seada regulaarne arhiividokumentide ja nende juurde kuuluva indeksiandmebaasi varundamine. Selleks võib kasutada näiteks ühte järgmistest meetoditest:
- igapäevane varundamine (automaatne muutunud failide varundamine tööpäevadel),
- iganädalane varundamine (automaatne muutunud failide varundamine),
- kõigi failide varundamine üks kord kuus ning konfiguratsiooni loomisel ja muutmisel.

Järgida tuleb tootja spetsifikatsioone:

- Kasutada tohib eranditult vaid tootja spetsifikatsioonidele vastavaid andmekandjaid.
- Kui arhiveerimiseks kasutatakse salvestusüksusena jukebox'i, kehtib nõue, et andmekandjaid tohib jukebox'ist võtta ja sellesse panna vaid programmi juhtimisel. Välistada tuleb andmekandjate väljavõtmine ja sisse asetamine käsitsi, kuna seda ei ole võimalik kontrollida.
- Tuleb dokumenteerida, millised andmekandjad mis ajaks arhiivisüsteemi sisestati ja sealt välja võeti, et vältida andmete autoriseerimata kustutamist või lisamist väljavõetud andmekandjatel.

Andmekandjad tuleb pealkirjastada:

- Kõik andmekandjad tuleb selliselt pealkirjastada, et need ei läheks segamini.
- Vallasrežiimis andmekandjaid tuleb hoolikalt säilitada ja tagada, et nendele pääseks ligi vaid administraatorid ning et need oleks kaitstud kahjulike keskkonnamõjude eest. Selleks tuleks neid hoida suletud tulekindlas ja sissemurdmise eest kaitstud teraskapis (S 120 DIS, VdS klass III).
- Üksikute andmekandjate varukoopiad tuleb kohe pärast nende loomist arhiivisüsteemist selliselt eraldada, et ka pärast arhiivi hävimist oleks võimalik selles olnud andmeid täielikult taastada. Volitamata isikutele ei tohi võimaldada pääsu ruumidesse.

Andmete varundamine tuleb dokumenteerida:

- Andmete varundamiseks valitud meetod tuleb dokumenteerida. Lisaks sellele tuleb dokumenteerida, millal millised varukoopiad on loodud ja kuhu need salvestati (vt M 6.37 Andmevarunduse dokumenteerimine).
- Kuna kõikidel varundusandmekandjatel on piiratud eluiga, tuleb need regulaarselt tootja soovituste kohaselt uute vastu välja vahetada.
- Kõikide varundatud andmete loetavust tuleb regulaarselt testida ja vajaduse korral salvestada need uutele andmekandjatele.

Kontrollida tuleb taaskäivitus- ja andmetaaste võimet

- Andmevarunduse rakendatavust ja süsteemi taaskäivitus- ja andmetaaste võimet tuleb kontrollida regulaarsete ajavahemike järel ning konfiguratsioonimuutuste korral. Selle testi käigus ei kontrollita ainult seda, kas varundatud andmed on loetavad, vaid ka seda, kas arhiivi on võimalik varundatud andmete abil ilma andmekaota uuesti taastada. Tulemus tuleb dokumenteerida.
- Arhiiviandmete uuesti krüpteerimisel (vt M 2.264 Krüpteeritud andmete regulaarne regenereerimine arhiveerimisel) tuleb ka varundusandmekandjatel asuvad andmed uuesti krüpteerida ning vanad andmekandjad kustutada või hävitada.
- Kui varundatud andmed installeeritakse uuesti arhiivisüsteemi, tuleb kontrollida, kas seetõttu on esinenud andmekadu, niisiis kas arhiveeritavad andmed tuleb uuesti salvestada. Lisaks sellele tuleb kontrollida, kas uuesti sisestatud andmeid ei ole markeeritud kustutamiseks.

Kontrollküsimused:

- Kas arhiveeritavate dokumentide varundamiseks on ette nähtud varuarhiivisüsteemid või varundussüsteemid?
- Kas arhiivi andmekandja defekti korral on võimalik üksikuid andmeid varundatud andmete hulgast jälle taastada?
- Kas varundusandmekandjaid hoitakse arhiivisüsteemist ruumiliselt eraldatult?

M 6.88 Veebiserveri hädaolukorraks valmisoleku plaani koostamine

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: administraator

Veebiserveri osalise või täieliku väljalangemisega kaasnevad paljudel juhtudel rasked tagajärjed. Veebiserver võib olla asutusesiseste tööprotsesside kulgemise või e-kommerts- või e-riigisüsteemi oluliseks koostisosaks. Sel juhul toob veebiserveri väljalangemine endaga kaasa kogu süsteemi väljalangemise. Kui veebiserveri näol on tegemist avaliku veebisaidiga, saab avalikkus selle väljalangemisest või tõrkest ka kiiresti teada. Seetõttu tuleb ootamatuseplaani koostamisel luua kontseptsioon, mis võimaldab minimeerida väljalangemise tagajärgi ning määratleb toimingud, mis tuleb väljalangemise korral läbi viia.

Üldine ootamatuseplaan

Arvestada tuleks järgmiste aspektidega:

- Veebiserveri hädaolukorraks valmisoleku plaan tuleb integreerida olemasolevasse hädaolukorraks valmisoleku plaani (vt B 1.3 Hädaplaanimine).
- Regulaarne andmevarundus - Süsteemi väljalangemisel võib ette tulla ka andmete kadu. Seetõttu tuleb kõigi veebiserverite jaoks luua andmevarunduskontseptsioon, mis tuleb integreerida olemasolevasse andmevarunduskontseptsiooni (vt B 1.4 Andmevarunduspoliitika). See peab hõlmama mitte ainult veebiserverit, vaid ka kogu süsteemi, milles veebiserverit kasutatakse. Nende hulka kuuluvad teatud juhtudel andmebaasid, rakendusserverid või proksiinstallatsioonid koormuse jaotamiseks.
- Kui veebiserveri käideldavusele esitatakse kõrgendatud nõudeid, tuleks paigaldada vajalikud komponendid liiasusega. Ka veebiserverit ennast on mõnedes rakendustes ühise välise salvestussüsteemi kasutamisel võimalik paigaldada liiasusega.
- Veebiserveri kasutamise eelduseks Internetis on funktsioneeriv internetiühendus. Teatud konfiguratsioonide korral on vajalik ka laitmatult funktsioneeriv DNS-server. Seepärast tuleb arvestada ka nimetatud komponentide väljalangemisega.
- Kui veebiserveril kasutatakse turvasoklite kihti (SSL), peab süsteemi taaskäivitumisel olema kättesaadav ka SSL-sertifikaadi privaatvõti. Kuna privaatvõti peaks olema kaitstud parooliga, peab see olema turvaliselt deponeeritud, et see oleks taaskäivitamise tarbeks kättesaadav (vt M 2.22 Paroolide deponeerimine).
- Süsteemi konfiguratsioon tuleb dokumenteerida. Olulisi ülesandeid tuleb kirjeldada nii, et hädaolukorras oleksid kogu süsteemi töö võimelised taastama tavakasutajad, kes ei oma eelnevaid teadmisi selle konfiguratsioonist.
- Tuleb luua taaskäivitusplaan, mis tagab süsteemi plaanipärase üleslaadimise.

Täiendavad kontrollküsimused:

- Kas veebiserveri tõrke puhuks on olemas hädaolukorraks valmisoleku plaan?
- Kas on olemas hädaolukorraks valmisoleku plaanid teiste süsteemide jaoks, mida vajatakse veebiserveri kasutamiseks?
- Kas on olemas hädaolukorraks valmisoleku plaanid internetiühenduse katkemise puhuks, juhul kui veebiserverit kasutatakse Internetis.

- Kas veebiserveri jaoks on olemas andmevarunduskontseptsioon?

M 6.90 Andmete varundamine ja arhiveerimine rühmatarkvara ja e-posti puhul

Algatamise eest vastutavad: infoturbespetsialist
Rakendamise eest vastutavad: administraator, kasutaja

Rühmatarkvarasüsteemi korral tuleb andmeid regulaarselt varundada. Üks rakendustest, mille juures on regulaarne andmevarundus eriti oluline, on meilisüsteem. Meilide tähtsus asutusesiseses ja -välises suhtluses kasvab pidevalt, mistõttu on oluline, et saadetud või vastuvõetud teated oleksid kättesaadavad pikema aja jooksul. Lisaks on olemas ka seaduslikud määrused, mis nõuavad ettevõtte jaoks oluliste meilide pikaajalisemat revisjonikindlat arhiveerimist. Rühmatarkvarasüsteemid koosnevad paljudest komponentidest, mis tuleb konfiguratsioonist olenevalt andmevarundusega siduda. Seetõttu tuleks rühmatarkvara jaoks luua andmevarunduskontseptsioon, mille peaks paigutama asutuse juba olemasolevasse andmevarunduskontseptsiooni (vt B 1.4 Andmevarunduspoliitika). Serveri poolelt salvestavad rühmatarkvarasüsteemid olulise teabe ja andmed andmebaasidesse. Selleks tuleks rakendada üldiste andmebaaside andmevarunduse infoturbesoovitusi (vt M 6.49 Andmebaasi varundamine). Isegi kui rühmatarkvaraserveri andmevarundus on üldjuhul hästi reguleeritud, tekivad meilide varundamisel ja arhiveerimisel tihti suured regulatsioonilüngad. Tavaliselt paigutatakse keskses rühmatarkvara- või meiliserveris meilid esmalt kasutajate arvutitele või kasutajate kaustadesse, kus neid töödeldakse ja kust need edasi saadetakse või kuhu need ladustatakse. Kui serveritel paiknevaid meile salvestatakse regulaarselt, siis kliendil paiknevate meilide korral tehakse seda tihtipeale ebapiisavalt või üldse mitte. Ka selle jaoks peaks olema reguleeritud tegevusviis. Meilide vastuvõtmiseks on võimalik seadistada kasutaja- või ülesandespetsiifilised meiliaadressid. Paljud kasutajaspetsiifilistele meiliaadressidele suunatud meilid peaksid aga olema kättesaadavad mitmele isikule, näiteks mõne grupiprojekti korral. Seetõttu on oluline salvestada need serveril paiknevatesse spetsiaalsetesse projektikataloogidesse. Ametlike dokumentidena tuleb selliste meilide salvestamisel arvestada minimaalse ja maksimaalse salvestusperioodiga (vt B 1.12 Arhiveerimine). Põhimõtteliselt peaks olema reguleeritud, kuidas, millal ja kus saadetud ning vastuvõetud meile arhiveeritakse, näiteks kas kasutajad teevad seda keskselt või mitte.

Krüpteeritud meilide arhiveerimisel tuleb arvestada mõningate punktidega (vt M 6.56 Andmevarundus krüptoprotseduuride kasutamisel):

- Meilid, mida soovitakse salvestada pikemaks ajaks, ei pruugi enam loetavad olla, kuna kasutajatel ei ole enam nende avamiseks vajalikke krüptograafilisi võtmeid.
- Krüpteeritud meilide arhiveerimist ja hilisemat kasutamist tuleb hoolikalt planeerida. Üheks võimaluseks on salvestada teated avatekstina. Sel juhul tuleb konfidentsiaalsus tagada muul moel. Krüpteeritud salvestamisel tuleb salvestada ka ligipääsuandmed, mida saaks hiljem kasutada andmete taastamiseks.

Täiendavad kontrollküsimused:

- Kas kasutatava rühmatarkvarasüsteemi jaoks on olemas andmevarunduskontseptsioon, mis arvestaks kõigi seotud komponentidega?
- Kas rühmatarkvarasüsteemide andmepanku varundatakse regulaarselt?
- Kas saadetud ja vastuvõetud meilide arhiveerimiseks on olemas reguleeritud tegevusviis?

M 6.91 Marsruuterite ja kommutaatorite andmete varundus ja taaste

Algatamise eest vastutavad: IT-juht, infoturbe osakond
Rakendamise eest vastutavad: administraator

Ka marsruuterid ja kommutaatorid tuleks kaasata üleorganisatsioonilisse andmevarunduspoliitikasse. Seejuures tuleb eriti suurt tähtsust omistada konfiguratsioonifailide varundamisele. Võrgu aktiivkomponentide failisüsteemide varundamine ei ole võimalik. Kuna tsentraalse haldamise käigus hoitakse konfiguratsioonifaile tihti eraldi serveritel ning sealt ka laetakse, võib varundamine toimuda nende serverite kaudu. Konfiguratsioonifaile tuleb nimetatud serveritel kaitsta volitamata juurdepääsu eest. See kehtib eriti juhul, kui konfiguratsioonifailides on paroolid salvestatud klaartekstina.

Kui konfiguratsioonifailide varundamiseks kasutatakse TFTP- serverit, võib see olla kättesaadav vaid haldusvõrgus. Alternatiivina võib mõnede süsteemide juures toimuda andmete salvestamine ka PCMCIA pistikkaartide abil. Et olla valmis andmevarunduse praktiliseks läbiviimiseks, tuleb andmete taastamist regulaarselt harjutada.

Täiendavad meetmed:

- M 6.35 Andmevarunduseks vajalike protseduuride määratlemine
- M 6.36 Minimaalse andmevarunduse kontseptsiooni määratlemine
- M 6.37 Andmevarunduse dokumenteerimine

Kontrollküsimused:

- Kas toimub regulaarne konfiguratsioonifailide andmevarundus?
- Kas turvapoliitika näeb ette regulaarset andmete varundamist?
- Kas varundatud konfiguratsioonifailide haldamine toimub turvaliselt ja tsentraalselt?

M 6.92 Marsruuterite ja kommutaatorite hädaolukorraks valmisoleku plaan

Algatamise eest vastutavad: IT-juht, infoturbeosakond
Rakendamise eest vastutavad: administraator

Marsruuterite ja kommutaatorite vigade käsitlemine

Igas IT-töö valdkonnas tekib tõrkeid, mis võivad ulatuda aeg-ajalt esinevatest arvutiriketest kuni mingi seadme täieliku väljalangemiseni ning sellest põhjustatud võrkude väljalangemiseni. Turvalise tööprotsessi põhialuseks on ettevalmistus tõrkeolukordadeks. Siia kuuluvad riistvara ja tarkvara väljalangemised ja rikked, mis võivad olla põhjustatud defektidest või kompromiteerimisjuhtudest. Et taolises situatsioonis efektiivselt ja kiiresti reageerida, tuleb diagnostika ja vigade käsitlemine juba eelnevalt planeerida ja ette valmistada. Tüüpiliste tõrgete puhuks ning võttes aluseks juba varem toimunud tõrkeid, tuleks koostada tegutsemisjuhised.

Kokaraamatu tüüpi dokumentatsioonid kõikide vajalike käskudega, nende rakendamine eeldatavate väljundandmetega on situatsioonides, mis nõuavad kiiret reageerimist, eriti suureks abiks. Nende hulka kuuluvad lisaks diagnostikale ja vigade kõrvaldamisele ka normaalses tööprotsessis vajalikud haldustegevused. Viimaseid võiks sisaldada juba tootja dokumentatsioon. Igapäevaseks praktiliseks kasutamiseks on igatahes otstarbekas koostada kogu dokumentatsioon tegevusjuhisena.

Logimine

Diagnostikatööde edukuse eelduseks on ka asjakohane logimine töö käigus (vt M 4.205 Marsruuterite ja kommutaatorite töö logimine). Lisaks sellele tuleks vigade käsitlemiseks kasutada sobivaid instrumente. Selleks on olemas nii vabalt kättesaadavad kui ka kommertsprogrammid, tihti ka seadmete tootjalt. Sobivate instrumentide kasutamine on seda tähtsam, kuna süsteemikäskudega ei näidata mitte alati kõiki konfiguratsiooniseadeid. Osaliselt hõlmavad need vaid standardseadetest erinevaid andmeid. Vigade kõrvaldamise protseduurid võib jaotada halduse, jõudluse mõõtmise ja diagnostika valdkonda. Alljärgnevalt käsitletakse parajasti vaadeldavaid aspekte.

Administratsioon

Tegutsemisjuhendis peaksid olema dokumenteeritud kõik vajalikud administreerimis- ja konfigureerimiskäsud.

Arvestada tuleks alljärgnevate valdkondadega:

- kasutajate konfigureerimine, pääsuõiguste jaotamine;
- operatsioonisüsteemi värskendamine;
- konfigureerimine;
- liidestamine;
- ühenduspordid;
- pääsuloendid (ACLid);

- marsruutimine;
- logimine.

Jõudlus

Jõudluse osas tuleks arvestada järgmiste aspektidega:

- sissetulev ja väljaminev kirjavahetus (liidese või pordi kohta);
- jõudlus või liiklus liidese kohta;
- kasutatud logifailide statistiline informatsioon.

Diagnostika

Diagnostikaks peaks olema dokumenteeritud kõik vajalikud käsud ja kogusüsteemi, liideste ja nende konfiguratsiooni seisundi näitajate eeldatavad väljundandmed. Paljud käsud võimaldavad lisaks sellele debug režiimi ulatusliku staatuse info väljastamiseks. Muuhulgas on vigade diagnostika jaoks oluline alljärgnev info:

- Võrguliideste ja teiste ühenduste olukord
- TCP ja UDP võrguteenuste staatus
- Ülevaade kogu konfiguratsioonist
- Protsessid
- Marsruutimistabelid ja kasutatud marsruutimisprotokollid
- ARP tabel
- Sisseloginud kasutajad
- DNS ja nslookup teenuse abil saadav info
- Logimine (log level 'i kasutamine, logimisinfo tõlgendamine)

Valmisolek käideldavuse tõstmiseks hädaolukorras

Tõrgete puhul läbiviidavate protseduuride planeerimisega on võimalik minimeerida taastamiseks kuluvat aega ning teatud juhtudel üldse leida lahendus. Planeerimine tuleb kooskõlla viia kõikehõlmava tõrke- ja avariiplaaniga ning peaks lähtuma üldisest hädaolukorraks valmisoleku kontseptsioonist (vt B 1.3 Hädaplaanimine). Siinkohal formuleeritakse avariiolukorraks valmisoleku dokumentidele esitatavad nõuded kogu IT-töö valdkonnas. Need määravad ideaalvariandina kindlaks ühtsed ja kohustuslikud nõuded, täpsemalt ülesehituse, sisu ja vormi.

Hädaolukorraks valmisoleku planeerimisel omavad suurt tähtsust alljärgnevad probleemid:

- Millised nõuded esitatakse monitooringule?
- Info kokkupanek, mille analüüs toimub alati võrgukomponentide töö eest vastutavates kohtades (vt ka lõiku Logimine).
- Kuidas saab tagada varajase tõrgete kindlaksmääramise?
- Millised on võimalike tõrgete põhjused?
- Riistvara defektid;
- Liiga väike dimensioneerimine (väljalangemine koormuse tõusmisel).
- Milliseid ettevaatusabinõusid on võimalik tarvitusele võtta?

- Tagavaraseadmed
- Tagavaraosad
- Tõrkesiirde funktsioonide juurutamine, mis võimaldab töö käigus ümberlülitumist alternatiivseadmele;
- Hooldusleping
- Töötajate väljaõpe
- Millised teenusetasemelepped (SLA) on olemas ja millised tuleks sõlmida?
- Riistvara tarnijad (näiteks teatud komponentide koha peal väljavahetamine ajalise garantiiga);
- Teenusetasemelepetele esitavad nõuded
- Kuidas peab toimuma diagnostika?
- Staatuse päringud
- Konfiguratsiooni näit
- Protsessid
- Marsruutimine
- Sisseloginud kasutajad
- Logimine
- Millised tõrgete kõrvaldamise protseduurid tuleb läbi viia?
- Protseduurid kogu süsteemi väljalangemisel (operatsioonisüsteemi ja konfiguratsiooni taastamine)
- Protseduurid osakomponentide, näiteks mäluseadme väljalangemisel
- Keda tuleb tõrke korral informeerida?
- Serveri- ja rakendushaldurit
- Riistvara tarnijat/hooldusleping kontaktisikut
- Millised dokumendid peavad olema tõrke korral kättesaadavad olema?
- Konfiguratsioon
- Pääsuloendid (reeglistik)
- Sisseseatud kasutajad ja volitused
- Paroolid

Dokumentatsioon ka paberkandjal

Dokumentatsioon ei tohiks mitte mingil juhul olemas olla vaid elektroonilisel kujul. Tegevusjuhised peaksid olemas olema vähemalt ka paberkandjal.

Teatud juhtudel võib konfiguratsioonifaile deponeerida eraldi ka CD-ROMidel või teistel andmekandjatel.

- Kuidas toimub taaskäivitamine?
- Sõltuvus teistest võrgukomponentidest või IT-koosluse valdkondadest
- Operatsioonisüsteemi uuesti installeerimine ja konfigureerimine
- Varundatud konfiguratsiooni taastamine
- Võimalused piirangutega kasutamiseks

Protseduuride katsetamine nende kirjelduste põhjal

Hädaolukorraks valmisolekuks vajalike protseduuride kirjeldused tuleb koostada erilise hoolikusega ning neid tuleb regulaarselt katsetada. Vajadusel tuleb erinevate seadmetüüpide ja operatsioonisüsteemide korral võtta vaatluse alla erinevad protseduurid. Kõige tähtsam meede käideldavuse tõstmiseks on tõenäoliselt tagavaraosade kasutusvalmis hoidmine, et viia riistvara tõrgete korral väljalangemisaeg miinimumini. Alternatiivina või sellele lisaks võib tootjaga sõlmida hooldusleping, mis tagavad käideldavuse garanteeritud reageerimis- või isegi parandusaegade kaudu. Sellega on võimalik vähendada ladustamisele tehtavaid kulutusi või muuta riistvara käideldavus veelgi efektiivsemaks. Sellise lepinguga on võimalik reguleerida ka varustamist tarkvara täiendustega.

Kontrollküsimused:

- Kas turvakontseptsioonis on kirjeldatud tõrgete ja hädaolukordade käsitlemisprotseduure?
- Kas on defineeritud vastutusalad hädaolukorraks?
- Kas toimub regulaarne tõrke- ja hädaabiprotseduuride testimine?

M 6.93 z/OS süsteemide hädaolukorraks valmisoleku plaan

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: administraator

z/OS süsteemide turvalise töö tagamiseks on vaja olla valmis erinevateks avariiolukordadeks. Nende hulka kuuluvad näiteks:

- Hädaolukorra kasutajatunnuse protseduur, mis muutub vajalikuks, kui käsutuses ei ole enam kindla funktsionaalsusega tunnust
- Meetod funktsioneeriva RACF-andmebaasi taastamiseks
- Koheselt aktiveeritav z/OS varundussüsteem
- Hädaabisüsteem, mida vajatakse teatud juhtudel üksiksüsteemide jaoks, et oleks võimalik läbi viia vigade parandust

Järgnevalt on lähemalt kirjeldatud mitmesuguseid soovitatavaid toiminguid, mis tagavad valmisoleku hädaolukorraks.

Hädaolukorra kasutajatunnuse protseduur

Hädaolukorraks valmisolekuks tuleb sisse seada hädaolukorra kasutajatunnuse protseduur. Hädaolukorra kasutajatunnust on võimalik kasutada, kui hädaolukorras ei ole RACF-haldur (*Resource Access Control Facility*) kättesaadav või kui tunnused on *SPECIAL* -õigustega tühistatud. Võimalik on sisse seada üks või mitu hädaolukorra kasutajatunnust.

Järgida tuleb järgmisi reegleid:

- *Juurdepääs hädaolukorra kasutajatunnusele* -Kuna hädaolukorra kasutajatunnusel on süsteemis väga suured volitused (*SPECIAL*), tuleb neid kasutajatunnuseid jaotada piirangutega. Hädaolukorra kasutajatunnusele tohib olla juurdepääs vaid eelnevalt kindlaks määratud isikutel. Sellele peaks omama ligipääsu vaid RACF-administraatorid ja RACF-väljaõppe saanud süsteemi programmeerijad.
- *Hädaabi kasutajatunnuse kasutamisest teatamine ja dokumenteerimine* - Hädaabi kasutajatunnuse kasutamisest tuleb nii ruttu kui võimalik informeerida RACF- administratsiooni, audiitorit ja IT-turvaosakonda. Teavitada tuleb alljärgnev info: Kes kasutas hädaabi kasutajatunnust? Mis põhjusel oli hädaabi kasutajatunnust vajalik kasutada? Millal seda kasutati? Mida tehti hädaabi kasutajatunnuse volitustega? Kõik hädaabi kasutajatunnusega tehtud toimingud tuleb arusaadavalt dokumenteerida ja arhiveerida.
- *Hädaabi kasutajatunnuse parool* - Kui logimisel kasutatakse hädaabi kasutajatunnust, peab kasutaja parooli koheselt muutma. Selle tagab RACF, kui hädaabi kasutajatunnus on varustatud uue salasõnaga. Pärast hädaabi kasutajatunnuse kasutamist tuleb selle juurde kuuluv parool RACF- halduri kaudu uuesti kindlaks määrata ja deponeerida.
- *Hädaabi kasutajatunnuse protseduuri kuritarvitamine* - Hädaabi kasutajatunnuse protseduuri ei tohi kuritarvitada volituste laiendamiseks, kui hädaolukord puudub. Takistada tuleb hädaabi kasutajatunnust kasutamist mugavuse pärast, et eirata kindlaksmääratud haldus- ja otsustusprotsesse.

- *Hädaabi kasutajatunnuse blokeerimise takistamine* - Kõik tunnused võib teatud etteantud aja tagant passiivsuse tõttu blokeerida. Vastav seadistamine toimub *RACF-* i *SETROPTS* -parameetrites. Selliselt võib blokeerida ka hädaabi kasutajatunnused, kui neid ei kasutata pikema aja jooksul. Automaatset blokeerimist on võimalik pakktöötluse kasutamise abil takistada. Pakktöötlus peaks regulaarselt kasutama hädaabi kasutajatunnuseid (näiteks kord kuus). Seeläbi uuendatakse ajatempleid RACF-andmebaasis. Nimetatud pakktöötlust on võimalik algatada tööde planeerija (*job scheduler*) abil. Tagada tuleb, et hädaabi kasutajatunnuse parool ei saaks teatavaks kellelegi peale selleks selgesõnaliselt volitatud töötajate. Kasutusele tuleks võtta RACF-klassi *SURROGAT* , et töökeelde (*Job Control Language*) ei oleks vaja seadistada parooli.

z/OS RACF andmebaasi taastamiseks kasutatavad protseduurid

RACF-andmebaas on z/OS-süsteemi turvaseadistuste tähtsaim ja tsentraalne salvestuskoht. Kui on vaja tagada turvaline kasutamine, peab RACF-andmebaas korrektselt funktsioneerima. Käsutuses mitte olevate ja defektsete RACF-andmebaaside probleemidega toimetulekuks tuleb järgida alljärgnevaid soovitusi:

- *RACF-andmebaaside varundamine* - RACF-andmebaaside sünkroniseerimine tuleb läbi viia laitmatult. Seetõttu tuleb aktiivsete andmebaaside varundamiseks (andmebaasid, mis on *RVARY* -monitoril aktiivsena tähistatud) kasutada kas *RACF-Utility IRRUT200* (soovitatud IBM poolt) või *IRRUT400.* Varundamise käigus teostatakse arvukaid *LOCK* -funktsioone. Seetõttu tuleks varundamist läbiviiv pakktöötlus paigutada võimalikult väikese koormusega ajavahemikku. Varukoopiaid ei tohi salvestada samale kõvakettale, millel asuvad kasutuses olevad RACF-andmebaasid. Otstarbekas oleks säilitada mitmed varukoopiate generatsioonid. Seejuures tuleks arvestada ka nädalavahetusega. Andmebaaside varukoopiaid tuleb, nagu RACF-andmebaase, kaitsta vastavate RACF-profiilide abil (vt M 4.211 z/OS turvasüsteemi RACF kasutamine).
- *RACF-andmebaasi taastamine* - z/OS süsteemis on RACF andmebaasi põhi- ja varusüsteem. Neid saab tööprotsessis ümber lülitada. Turvalisuse tagamiseks tuleb mõlemad andmebaasid paigutada erinevatele ketastele. Kui põhiandmebaasis esineb vigu, on võimalik muuta RACF varuandmebaas *RVARY SWITCH* käsu abil põhiandmebaasiks ja põhiandmebaas varuandmebaasiks. Vigase RACF varuandmebaas saab seejärel reeglina kustutada ning uuega asendada. Kui mõlemad RACF-andmebaasid on vigased, on võimalik vigane RACF-andmebaas asendada kehtiva varukoopiaga ning sellega süsteemi töö uuesti taastada (mõningatel juhtudel mõnest teisest süsteemist). Üksiksüsteemide korral on selleks vajalik avariisüsteem.
- *Jälitatavus vigade esinemisel* - RACF-andmebaasi varundamiseks ja taastamiseks on vaja sisse seada protseduurid. Vaja on sisse seada protseduur, et muutused RACF-andmebaasis RACF-andmebaasi viimase varundamise ja tekkinud hädaolukorra ajamomendi vahel oleks jälitatavad. Üheks võimaluseks on näiteks, et RACF-muudatusi tohib läbi viia vaid dokumenteeritud pakitöötluse kaudu. Teiseks võimaluseks on, et kohe pärast RACF-muutusi

toimub SMF-andmekogude hindamine. Mõlemad protseduurid peavad olema arusaadavalt dokumenteeritud. Dokumentatsioon peab olema administraatoritele kättesaadav.

z/OS varundussüsteem

Süsteemi vigade korral, kui z/OS-süsteemi (või ka kogu *Parallel Sysplex klastrit)* pole enam võimalik käivitada, on tähtis süsteem või süsteemid võimalikult kiiresti viia töökindlasse seisundisse. Taoliste väljalangemiste põhjuseks võivad olla näiteks tehnilised vead või vigased käsitsi tehtud sissekanded. Seetõttu peaks olema valmis pandud komplekt kõvakettaid, mis sisaldab kasutatava operatsioonisüsteemi koopiat. Vaid IPL-aadressi muutmisega (*Initial Program Load*) on z/OS- operatsioonisüsteemi enamikel juhtudel võimalik kiiresti reaktiveerida. Seejuures tuleks täita järgmisi soovitusi:

Kõvaketta kontseptsioon

z/OS-operatsioonisüsteemi kõvaketta kontseptsioon ja selle juurde kuuluvad programmitooted (näiteks plaanur, *Output Manger* ja teised) peavad olema loogiliselt üles ehitatud ja selgesti äratuntavad. Kokkukuuluvaid faile, näiteks operatsioonisüsteemi faile, ei tohi laiali jaotada ja salvestada paljudele eraldi kõvaketastele. Tuleb kasutada võimalikult vähe kõvakettaid, et oleks võimalik suhteliselt lihtsalt luua täiuslikud varukoopiad.

Kloonimisprotsess

Varukõvaketaste loomiseks on vaja välja töötada kloonimisprotseduur, mille käigus teostatakse vähemalt järgmised toimingud:

- Süsteemi paiknemiskohtade (*system residence*) kopeerimine
- Programmitoodete kõvaketaste kopeerimine
- HFS-kõvaketaste kopeerimine (*Hierarchical File System*)
- SMP/E-kõvaketaste kopeerimine (*System Modification Program*)
- Andmekandjal olevate andmete muutmine SMP/E-s *ZONEEDIT* - funktsiooni (vanade andmete asendamine uutega) abil
- Andmekandjal olevate andmete sobitamine *Parmlib IEASYMnn* liikmes

Hooldustööde kontseptsioon

Et tööprotsessi mitte ohustada, kasutatakse z/OS operatsioonisüsteemi hooldamiseks reeglina eraldi kõvakettaid. Neid on otstarbekas kasutada pärast hooldustööde läbiviimist uue aktiivse kõvakettakomplektina ning endisi kõvakettaid varukomplektina.

Süsteemi muutujate kasutamine

Defineerimise kergendamiseks tuleks kõikjal, kus see on tehniliselt vähegi võimalik ja otstarbekas, kasutada sümbolitega muutujaid (alates z/OS 1.4 on defineeritavad kuni 800 sellist muutujat). Otstarbekas oleks teha ülemkataloogi sissekanded ja nende *ALIAS* -sissekanded sellist tehnikat kasutades, et igal ajal oleks võimalik vahetamine ilma täiendava sekkumiseta. Sümbolitest muutujate kasutamine on võimalik paljudes definitsioonides, kuid tuleb silmas pidada, et mõned definitsioonid ei toeta veel muutujaid.

Tööfailide haldamine

Hooldamiseks tehtavate asjatute kulutuste tegemise vältimiseks ei tuleks tööfaile, näiteks katalooge, *Parmlibs* , *Proclibs* ja programmitoodete andmebaase pidada topelt ega mitmekordselt.

z/OS hädaabisüsteemi loomine

Olulistes tarkvarakomponentides, näiteks RACF- (*Resource Access Control Facility*) või ülemkataloogis esinevate vigade korral võib tekkida tõrge kogu süsteemis. Üksiksüsteemide korral peab sellistel puhkudel olema lühiajaliselt kättesaadav hädaabisüsteem, mida on võimalik probleemideta käivitada ning mille abil on võimalik defektne süsteem parandada. Vastupidiselt varundussüsteemidele ei ole hädaabisüsteem mõeldud aktiivseks kasutamiseks. Hädaabisüsteemide loomisel tuleb pöörata tähelepanu alljärgnevatele aspektidele:

- *Sõltumatus* - Hädaabisüsteem tuleb tervenisti sisse seada sõltumata failidest ja tootmissüsteemide definitsioonidest.
- *Piirdumine olulisega* - Hädaabisüsteem ei peaks sisaldama rohkem tarkvarafunktsioone kui parandustöödeks ilmtingimata vajalik, et süsteemi jaoks ei oleks vaja rohkem kui ühte kõvaketast. Nende hulka kuuluvad programmid JESx (*Job Entry Subsystem*), VTAM (*Virtual Telecommunication Access Method)* ja TSO (*Time Sharing Option*) sinna juurde kuuluvate ISPF-failidega (*Interactive Support Programming Facility*). Võib kaaluda ka JES–ita süsteemi kasutamist. Siis ei saa aga kasutada pakktöötlust.
- *Salvestusüksuse andmed* - Kõik protseduurid on vaja varustada salvestusüksuse andmetega, et vältida sõltuvust kataloogidest. Seetõttu ei tohiks kasutada ka SMS-faile (*System Managed Storage*).
- *VTAM terminalid* - Tuleb sisse seada võimalikult lihtne VTAM protseduur, mille puhul on ette nähtud vähemalt üks VTAM *Local Node*, mis sisaldab ühe MCS-konsooli (*Multiple Console Support*) aadressi. Sellega on võimalik luua VTAM ühendus ning defektsesse süsteemi sisse logida. VTAM konfiguratsioonide muutuste korral tuleb vastavalt muuta ka VTAM *Local Node* definitsiooni.
- *Hädaabisüsteemi komponendid* - Hädaabisüsteem peaks paiknema kõvakettal, mis sisaldab vähemalt IPL teksti, ülemkataloogi, JESx kontrollpunkti ja *spool* faili, lehekülgede andmestikku, süsteemifaile (MANx, STGINDEX, LOGREC, DAE), *Parmlieb, Proclib* (sisselogimisprotseduuri mitte unustada), SMF-faile (SYS1.MANx), BROADCAST- ja UADS-faile ja RACF-andmebaasi.
- *Kasutajatunnused hädaolukorraks* - Hädaabisüsteemil peab olema vähemalt kaks kasutajatunnust, mida käsitletakse hädaabi kasutajatunnustena.
- *Pidev hooldus* - Juurdepääs hädaabisüsteemile peab olema kaitstud. Tavasüsteemis tehtavad muutused peavad olema kiiresti jälitatavad ka hädaabisüsteemis, kui need on hädaabisüsteemi seisukohalt olulised. Hädaabisüsteemi funktsionaalsust tuleb perioodiliselt kontrollida.

Täiendavad kontrollküsimused:

- Kas on olemas hädaabi kasutajatunnuse protseduur?

- Kas on teada kõvaketas, millel asub RACF- andmebaasi varukoopia?
- Kas on olemas z/OS varundussüsteem?
- Kas üksiksüsteemidel on olemas hädaabisüsteem?

M 6.94 Turvalüüside hädaolukorraks valmisoleku plaan

Algatamise eest vastutavad: IT-juht, infoturbeosakond
Rakendamise eest vastutavad: administraator

Turvalüüside vigade käsitlus

Turvalüüsid täidavad organisatsiooni võrguühenduse käideldavuse osas keskset rolli. Turvalüüside või üksikkomponentide vigadel või tõrgetel (regulaarselt esinevatest vigadest kuni seadme väljalangemiseni ning sellest põhjustatud võrgu väljalangemiseni) võivad olla vahetud ja rasked tagajärjed, kui ootamatusteks ei olda piisavalt ette valmistatud. Et taolises situatsioonis efektiivselt ja kiiresti reageerida, tuleb diagnostika ja vigade kõrvaldamine juba eelnevalt planeerida ja ette valmistada. Tüüpiliste tõrgete puhuks tuleks koostada tegutsemisjuhised, võttes aluseks juba varem toimunud tõrked. Kokaraamatulaadsed dokumendid, milles on üles loetletud kõik vajalikud etapid, on kiiret tegutsemist nõudvates situatsioonides eriti suureks abiks. Nende hulka kuuluvad lisaks diagnostikale ja vigade kõrvaldamisele ka normaalses tööprotsessis vajalikud haldustegevused. Viimaseid võiks sisaldada juba tootja dokumentatsioon. Igapäevaseks praktiliseks kasutamiseks on igatahes otstarbekas koostada kogu dokumentatsioon tegevusjuhisena.

Logimine

Diagnostikatööde edukuse eelduseks on ka asjakohane logimine töö käigus (vt M 4.47 Turvalüüsi operatsioonide logimine). Lisaks sellele tuleks vigade kõrvaldamiseks kasutada sobivaid instrumente. Vigade käsitlemise protseduurid võib jaotada halduse, jõudluse mõõtmise ja diagnostika valdkonda. Alljärgnevalt kirjeldatakse aspekte, millele tuleb tähelepanu pöörata. Marsruuterite puhul, mis on paketifiltrina üks turvalüüsi osa, tuleks rakendada M 6.92 Marsruuterite ja kommutaatorite hädaolukorraks valmisoleku plaan .

Administratsioon

Turvalüüside üksikkomponentide kasutusjuhendis peaksid olema dokumenteeritud kõik halduseks ja konfigureerimiseks vajalikud käsud ja tööetapid. Parema ülevaate saavutamiseks on soovitatav teha seda iga komponendi jaoks eraldi ning lisaks sellele luua ülevaatlik dokument.

Arvestada tuleks alljärgnevate valdkondadega:

- Operatsioonisüsteemi konfiguratsioon, eriti võrguliideste konfiguratsioon
- Operatsioonisüsteemi värskendamine
- Funktsioonikomponentide konfiguratsioon (paketifiltrid, turvaproksid, viiruseskannerid jne)
- Eriti suure tähtsusega käsud teenuste alustamiseks ja lõpetamiseks
- Konfiguratsioonifailide ja –andmebaaside salvestuskoht, vajadusel vastavate konfiguratsiooniinstrumentide kasutamine
- Turvaprokside puhul (näiteks HTTP-proksi, meili turvalüüs) ka andmekataloogide asukoht (partitsioon / failisüsteem)
- Logimine

Jõudlus

Jõudluse osas tuleks arvestada järgmiste aspektidega:

- Paketifiltrite kaudu sisse tulev ja väljuv kirjavahetus ning kõik logifailid, milleks turvaproksit kasutatakse
- Kasutatud logifailide statistiline informatsioon

Diagnostika

Diagnostikaks peaks olema dokumenteeritud kõik vajalikud käsud ja turvalüüside ning nende konfiguratsioonide kõikide komponentide tööseisundi kirjeldamiseks eeldatav väljundinfo.

Muuhulgas on vigade diagnostika jaoks oluline alljärgnev info:

- Ülevaade kogu konfiguratsioonist
- Võrguliideste ja teiste ühenduste olukord ja konfiguratsioon
- Olemasolevate võrguteenuste olukord
- Protsessid
- Sisseloginud kasutajad
- Logimine (log level 'i kasutamine, logimisinfo interpreteerimine)

Täiendavaid abinõusid kirjeldatakse M 2.215 Tõrkekäsitlus .

Valmisolek käideldavuse tõstmiseks hädaolukorras

Tõrgete puhul läbiviidavate toimingute planeerimise teel on võimalik süsteemi töö taastamiseks kuluv aeg minimeerida ning teatud juhtudel leida lahendused. Plaanid tuleb viia kooskõlla üldise tõrgeteks ja hädaolukorraks valmisoleku plaaniga ning selle teostamisel tuleks võtta aluseks võtta üldine hädaolukorraks valmisoleku plaan (vt B 1.3 Hädaplaanimine). Selles formuleeritakse põhilised nõuded, mida esitatakse kogu IT-tööd hõlmavaks hädaolukorraks valmisoleku planeerimise dokumentatsioonile. Need määravad ideaalvariandis kindlaks ühtsed ja kohustuslikud nõuded, täpsemalt ülesehituse, sisu ja vormi.

Hädaolukorraks valmisoleku planeerimisel omavad suurt tähtsust alljärgnevad probleemid:

- Milliseid nõudeid esitatakse monitooringule?
- Informatsiooni kokkupanek, mille analüüs toimub alati võrgukomponentide töö eest vastutavates kohtades (vt ka lõiku Logimine).
- Kuidas saab võimalikuks varajane tõrgete kindlaksmääramine? Kas on olemas vahendid, mis võimaldavad kasutada automaatset häiresüsteemi?
- Millised on võimalike tõrgete põhjused?
- Ründed;
- Riistvara defektid;
- Liiga väike dimensioneerimine (väljalangemine koormuse tõusmisel).
- Milliseid ettevaatusabinõusid on võimalik rakendada?

- Alternatiivkonfiguratsioonide ja “tagasipöördumisstrateegiate” väljatöötamine teatud liiki tõrgete ja rünnete korral (näiteks muutunud marsruutimine, alternatiivsed paketifiltri reeglid)
- Varuseadmed; tõrkesiirde funktsioonide juurutamine, mis võimaldavad töö käigus ümberlülitumist alternatiivseadmele
- Hooldusleping
- Töötajate väljaõpe
- Millised teenusetasemelepped (SLA) on olemas ja millised tuleks sõlmida?Riistvara tarnijad (näiteks teatud komponentide koha peal väljavahetamine ajalise garantiiga, eriti rakenduste juures)
- Teenusetasemelepingutele esitatavad nõuded
- Kuidas peab toimuma diagnostika?
- Staatuse päringud
- Konfiguratsiooni kuvamine
- Logimine
- Millised tõrgete kõrvaldamise protseduurid tuleb läbi viia?
- Protseduurid kogusüsteemi väljalangemisel (operatsioonisüsteemi ja konfiguratsiooni taastamine)
- Toimingud osakomponentide väljalangemisel (näiteks salvestusseade, kõvakettad, võrgukaardid)
- Keda tuleb tõrke korral informeerida?
- Serveri- ja rakendushaldurit
- Riistvara tarnijat/hooldusleping kontaktisikut
- Millised dokumendid peavad olema tõrke korral kättesaadavad?
- Konfiguratsioon
- Paketifiltri reeglid, turvaprokside konfiguratsioon
- Paroolid

Dokumentatsioon ka paberkandjal

Dokumentatsioon ei tohiks mitte mingil juhul olemas olla vaid elektroonilisel kujul. Tegevusjuhised peaksid olema olemas vähemalt ka paberkandjal.

Teatud juhtudel võib konfiguratsioonifaile deponeerida eraldi ka CD-ROM-idel või teistel andmekandjatel.

- Kuidas toimub taaskäivitamine?
- Sõltuvus teistest IT-koosluse valdkondadest
- Operatsioonisüsteemi uuesti installeerimine ja konfiguratsioon
- Varundatud konfiguratsiooni taastamine
- Piiratud kasutamisvõimalused

Ettevaatust piirangutega kasutamisel

Piirangutega kasutamise planeerimisel tuleb silmas pidada, et turvalüüside piirangutega kasutamise tagajärjel ei tohi tekkida olukord, kus ei ole tagatud oma võrgu piisav kaitse. Kahtluse korral tuleks pigem leppida mingi teenuse pikemaajalise tõrkega kui ohuga, et “piiratud turvalisus” toob endaga kaasa lisaprobleeme.

Protseduuride katsetamine nende kirjelduste põhjal

Hädaolukorraks valmisolekuks vajalike toimingute kirjeldused tuleb võimalikult hoolikalt koostada ja neid tuleb regulaarselt katsetada. Vajadusel tuleb erinevate seadmetüüpide ja operatsioonisüsteemide korral võtta vaatluse alla erinevad protseduurid. Tsentraalsete komponentide puhul, milleks võivad näiteks olla turvalüüsi paketifiltrid, mis on paigutatud sisevõrgu ja Interneti vahele, võib turvalüüsi ühe komponendi väljalangemine endaga kaasa tuua kogu internetiühenduse katkemise.

Kõige tähtsam meede käideldavuse tõstmiseks on seetõttu tagavaraosade kasutusvalmina hoidmine, et viia riistvara tõrgete korral väljalangemisaeg miinimumini. Alternatiivina või täienduseks võib tootjaga sõlmida hooldusleping, mis tagavad käideldavuse garanteeritud reageerimis- või isegi parandusaegade kaudu. Sellega on võimalik vähendada hoidmisele tehtavaid kulutusi või muuta riist- vara käideldavus veelgi efektiivsemaks. Sellise lepinguga on võimalik reguleerida ka varustamist tarkvara täiendustega.

Kontrollküsimused:

- Kas turvakontseptsioonis on kirjeldatud tõrgete ja hädaolukordade käsitlemisprotseduure?
- Kas on defineeritud vastutusalad hädaolukorra puhul?
- Kas tõrke- ja hädaabiprotseduure testitakse regulaarselt?

M 6.95 Nutitelefonide ning tahvel- ja pihuarvutite andmevarundus ja muud tõrgete vältimise meetodid

Algatamise eest vastutavad: infoturbeametnik, IT-juht

Rakendamise eest vastutavad: administraator, kasutaja

Nutitelefon, tahvel- või pihuarvuti võib väga erinevatel põhjustel kas rikki minna või töötada ainult osaliselt. Eriti ärritav on see loomulikult siis, kui telefoni on hädasti tarvis või kui seeläbi lähevad kaotsi olulised andmed. Seega tuleks eelnevalt võtta vastavad meetmed, et ennetada tõrkeid ja vähendada nendega kaasnevaid probleeme.

Mobiiltelefoni aku laetust ja töökindlust tuleb regulaarselt kontrollida (vt ka M 4.31 Toite tagamine mobiilsel kasutamisel).

Kõik kaasaskantaval lõppseadmel salvestatud andmed nagu telefoniraamatu kirjed, märkmed jne tuleks regulaarsete ajavahemike tagant salvestada teisele andmekandjale, et neid oleks võimalik kahtluse korral sealt taastada.
Selleks on mitu võimalust:

- olulisemad seadistused, nt paroolid ja turvamehhanismide konfiguratsioonid tuleks kirjalikult dokumenteerida ja panna vastavalt nende kaitsevajadusele turvaliselt hoiule. Kui lõppseadmeid juhitakse tsentraalselt Mobile-Device-Management-Software'i kaudu, tuleb lõppseadmete vastavad profiilid varundada, nii et neid oleks võimalik kiiresti jälle sisestada.
- Nutitelefonis, tahvel- või pihuarvutis olevad andmed tuleks regulaarselt sünkroniseerida muu kohaga, nt arvuti, asutuse serveriteenuse või vajaduse korral välise teenusepakkujaga. See ei asenda siiski täielikku andmevarundust.
- Seetõttu tuleks regulaarselt läbi viia ka nutitelefoni, tahvel- või pihuarvuti andmevarundus teisele IT-süsteemile, nt sülearvutile või laua-PC-le. Eriti soovitatav on täielik andmevarundus täieliku süsteemi kujutisega (Snapshot). Lahendus on mugav ja hoiab oluliselt kokku uue seadme installeerimisele ja konfigureerimisele kuluvat aega. Kui selle lahenduse jaoks on vaja IT-süsteemi sügavamalt manipuleerida, nt juurimise või alternatiivsete, Androidi taastamisel põhinevate seadmetega, tuleks põhjalikult kaaluda manipuleerimise riski võrreldes kiirema kättesaadavuse eelisega. Antud juhul on täiendavad infoturbemeetmed, mis on juurimise või muude meetmete kasutamisel vajalikud, nii kõrged, et puudub eelis, võrreldes vähem mugava varundusmeetodiga ilma süsteemikujutiseta.
- Kuna nutitelefonidel, tahvel- ja pihuarvutitel on olemasolev mäluruum piiratud, saab enamikku mudeleid täiendada väliste andmekandjatega (vt ka M 4.232 Mälulaienduskaartide turvaline kasutamine). Selle jaoks on levinud mälukaardid, nt Memory-Cards, mida saab kiiresti vahetada, nii et need sobivad hästi ka teel olles varukoopiate tegemiseks. See on eelkõige siis kasulik, kui kasutaja on pikalt eemal ja seetõttu ei toimu pikemat aega sünkroniseerimist IT-süsteemi ja nutitelefoni, tahvel- või pihuarvuti vahel. Nagu üldiselt andmevarunduse puhul, kehtib ka siin, et neid tuleb säilitada turvaliselt. Kui mälukaardid jäetakse lõppseadmes või mujal järelevalveta, võivad

volitamata isikud kopeerida nendele salvestatud andmeid. Kui hiljem mälukaart tagasi pannakse, ei ole sellest tegevusest ühtegi jälge.
- Kõiki andmeid, mis on salvestatud vahetatavatele mälukaartidele, tuleb samuti varundada, hiljemalt järgmisel sünkroniseerimisel.

Enamikul nutitelefonidel, tahvel- või pihuarvutitel asub operatsioonisüsteem välkmälus, millel on sageli piisavalt ruumi vähemalt kõige olulisemate andmete nagu Personal Information Manager'i (PIM) sisude varundamiseks. Selle mugavaks teostamiseks on olenevalt tootjast olemas kas komplekti kuuluvad või täiendavad tööriistad. Siinjuures tuleks tähele panna, et pärast täielikku lähtestamist kustutatakse kõik väljaspool välkmälu olevad andmed, ka kõik paroolid juurdepääsu kaitseks. Seetõttu võib ründe toimepanija saada hõlpsalt juurdepääsu välkmälule ja seal salvestatud andmetele. Enne kui nutitelefon, tahvel- või pihuarvuti edasi antakse, nt parandamiseks või teisele kasutajale, tuleks kõik andmed, ka välkmälust, kustutada.

Kui nutitelefon, tahvel- või pihuarvuti peab olema pidevalt kasutatav, tuleks alati kaasas kanda varuakut.

Parandamine

Nutitelefoni, tahvel- ja pihuarvuti või üksikute komponentide vigade korral tuleks parandamist läbi viia ainult usaldusväärsete spetsialistide juures. Seetõttu peab eksisteerima ülevaade sobilikest ettevõtetest.

Paljud edasimüüjad pakuvad parandamise ajaks asendusseadmeid. Lühikese kasutusajaga seadmete nagu nutitelefonide, tahvel- või pihuarvutite puhul võib parandamine osutuda sageli mõttetuks, mistõttu pakutakse mõnikord ka asendusseadmeid. Et just nutitelefon, tahvel- või pihuarvuti peaks pidevalt kasutuses olema, tuleb lõppseadme või edasimüüja valikult pöörata tähelepanu sellele, milliseid teenuseid pakutakse.

Enne kui nutitelefon, tahvel- või pihuarvuti parandusse antakse, tuleb kõik isikuandmed nt salvestatud e-kirjad ja telefoniraamat seadmes kustutada (vt ka M 2.4 Hooldus- ja remonditööde reeglid), st juhul, kui see veel võimalik on. Enne kustutamist tuleb andmed loomulikult varundada. Eemaldada tuleb ka lisakaardid.

Kontrollküsimused

- Kas pihuarvutite akude laetust ja töökindlust kontrollitakse regulaarselt?
- Kas pihuarvutites salvestatud andmeid varundatakse regulaarselt?
- Kas enne pihuarvutite edasiandmist kustutatakse kõik andmed?

M 6.96 Serveri avariiplaan

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: administraator

Serveri osaline või täielik väljalangemine võib olla raskendavaks asjaoluks, kui server on asutusesiseste tööprotsesside oluline osa või toetab avalikult juurdepääsetavat veebilehte (näiteks e-kommerts või e-valitsuse rakendustes). Seetõttu tuleb hädaolukorraks valmisoleku plaani koostamisel luua kontseptsioon, mis aitaks minimeerida väljalangemise tagajärgi ning mis annab ülevaate väljalangemise korral läbiviidavatest toimingutest.

Seejuures tuleks arvestada järgmiste aspektidega:

- Serveri hädaolukorraks valmisoleku plaan tuleb integreerida olemasolevasse hädaolukorraks valmisoleku plaani (vt B 1.3 Hädaplaanimine).
- Süsteemi väljalangemisel võib tekkida ka andmete kadu. Seepärast tuleb üldise andmevarunduskontseptsiooni käigus (vt B 1.4 Andmevarunduspoliitika) luua ka serveri andmevarunduskontseptsioon. Sellesse ei tule kaasata ainuüksi server, vaid ka süsteemid, millest sõltub serveri töö.
- Hooldus- ja teenusetasemelepingute raames või oma lao pidamisega tuleb teatud tähtaja jooksul tagada varustamine varuosadega. Väljalangemisaega tuleb vähendada nii palju kui vähegi võimalik. Kui serveri käideldavusele esitatakse kõrgendatud nõudeid, tuleb selle saavutamiseks kasutada ka kõrgendatud nõuete täitmist võimaldavaid lahendusi.
- Süsteemi konfiguratsioon tuleb dokumenteerida. Olulised ülesanded tuleb kirjeldada nii, et hädaolukorras suudaksid kogu süsteemi töö taastada tavakasutajad, kes ei oma eelnevaid teadmisi selle konfiguratsioonist. Dokumentatsioon ei tohiks mitte mingil juhul olemas olla vaid elektroonilisel kujul, vaid kasutusjuhised peaks olema olemas ka paberkandjal. Vajadusel võib konfiguratsiooniandmed deponeerida ka eraldi CDle.
- Luua tuleb taaskäivitusplaan, mis tagab süsteemi korrakohase üleslaadimise.
- Kõiki vajalikke toimingute kirjeldusi tuleb regulaarselt kontrollida ja testida. Vajadusel tuleb erinevate operatsioonisüsteemide korral võtta vaatluse alla erinevad protseduurid.

Kontrollküsimused:

- Kas serveri tõrke puhuks on olemas hädaolukorraks valmisoleku plaan?
- Kas on olemas hädaolukorraks valmisoleku plaanid teiste süsteemide jaoks, mida vajatakse serveri kasutamiseks?
- Kas serveri jaoks on olemas andmevarunduskontseptsioon?
- Kas tõrke- ja hädaabiprotseduure testitakse regulaarselt?

M 6.97 SAP süsteemi valmisolek hädaolukorraks

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: administraator

SAP süsteemi jaoks tuleb sarnaselt teistele süsteemidele luua hädaolukorraks valmisoleku plaan. Et ettevalmistused selleks kulgeksid eesmärgikindlalt, tuleb planeerimise ja kontseptsiooni koostamise faasis luua hädaolukorraks valmisoleku kontseptsioon (vt M 2.341 SAP kasutuselevõtu planeerimine), milles on defineeritud ka hädaolukorrad, millega tuleb kontseptsiooni koostamisel arvestada. Põhimõtteliselt ei erine SAP süsteemi hädaolukorraks valmisoleku planeerimine teiste süsteemide omast. Seetõttu tuleb rakendada ka teiste oluliste moodulite hädaabimeetmeid, mis on rakendatavad IT-süsteemides (näiteks serverarvuti, klientarvuti, andmebaas), millest koosneb SAP-süsteem. Hädaolukorraks valmisoleku kontseptsioon peaks hõlmama vähemalt järgmisi meetmeid ning seda tuleks vastavalt individuaalsetele vajadustele laiendada.

- Tuleb konfigureerida hädaolukorra administraatori konto ning määrata kindlaks selle kasutamisreeglid.
- SAP süsteemi andmevarundust tuleb regulaarselt läbi viia. Protseduurid ja sagedus tuleb fikseerida andmevarunduskontseptsioonis.
- Tuleb määrata kindlaks SAP süsteemi taastamisprotseduurid.
- Kõrgete käideldavusnõuete korral on vajalik varusüsteemi olemasolu.

Olenevalt kasutusotstarbest võib hädaolukorraks valmisoleku kontseptsiooni kuuluda ka kaitse arvutiviiruste eest (vt M 4.271 SAP süsteemi viirusetõrje).

Administreerimine hädaolukorras

Juhuks, kui tavapäraste administraatori kasutajatunnustega ei pääse enam SAP süsteemi, on vajalik hädaolukorra administraatori konto. Kuna ABAP ja Java protokollistikul on eraldi kasutajate haldussüsteemid, tuleb hädaolukorra administraatori konto luua iga protokollistiku jaoks eraldi. ABAP protokollistikus võib sellele anda volitused, mis vastavad profiilide SAP_ALL ja SAP_NEW summale. Nii omab hädaolukorra administraatori kasutajatunnus täielikku kontrolli SAP süsteemi ABAP-protokollistiku üle. Java protokollistikus peab hädaolukorra konto kuuluma gruppi Administraatorid. Standardi kohaselt omab administraatorite grupp täielikku kontrolli Java protokollistiku üle. Alates platvormist NetWeaver 04 (Java 6.40) toimub kasutajahaldus Javas *User Management Engine* (UME) kaudu (vt M 4.267 SAP Java pinu turvaline kasutajate haldus). See baseerub gruppidel ja rollidel ning toetab kasutajakontode erinevaid salvestuskohti. Administraatorite gruppi nimetatakse olenevalt salvestuskohast erinevalt. Kui kasutajakontod on salvestatud andmebaasi või LDAP-kausta, on selle nimi „ *Administrators* ”. Kui kasutajakontod salvestatakse ABAP protokollistikus, on selle nimi „SAP_J2EE_ADMIN”: Selle grupi kasutajatel ei ole täielikke administratiivseid õigusi, vaid on õigused Java protokollistiku baas- ja kasutajahalduseks. Üldine hädaolukorra konto Java protokollistiku jaoks on SAP-süsteemi poolt etteantud kasutajakonto „SAP”, mida on võimalik kasutada aga ainult olukorras, kui Java protokollistik on lülitatud niinimetatud üksikkasutajarežiimi (*Single User Mode*). Selles režiimis saab end sisse logida eranditult vaid kasutaja „SAP*”. Seetõttu on vajalik veel üks hädaolukorra konto, mis on rakendatav ka tavarežiimis.

Hädaolukorra halduseks kasutatavad kontod on varustatud turvaliste paroolidega. Vastutavad isikud peaksid olema paroolide deponeerimise kohast informeeritud. Pärast hädaolukorda tuleb paroolid muuta selliselt, et need saavad teatavaks vaid juhul, kui kasutatakse hädaolukorra haldusprotseduure. Hädaolukorra halduseks kasutatavad kontod peaksid olema alati kättesaadavad. Neid ei tohi ka deaktiveerida või blokeerida. Sellepärast peavad pääsuandmed olema turvaliselt kaitstud. Hädaolukorra konto kasutamisel ei ole hiljem enam võimalik kindlaks teha, milline isik SAP süsteemi kasutas. Seetõttu peab süsteemi administraatoreid ja infoturbeosakonda hädaolukorrast viivitamatult informeerima. Seejuures tuleb anda informatsiooni järgmiste aspektide kohta:

- Milline hädaolukord tekkis?
- Kes ja millal kontot kasutas?
- Milliseid toiminguid ja muudatusi tehti?

Andmevarundus

Hädaolukorraks valmisolekuks regulaarselt läbiviidavate meetmete hulka kuulub SAP süsteemi andmevarundus. Üleorganisatsioonilise varunduspoliitika väljatöötamise raames tuleb planeerimisfaasis kavandada ka SAP süsteemi andmevarundus. SAP süsteemi andmed salvestatakse küll põhiliselt andmebaasi, andmete varundamine piirdub aga siiski vaid ABAP protokollistiku installatsioonide korral (nt SAP R/3 süsteemide korral) andmebaasi varundamisega. Iseäranis Java protokollistiku puhul kehtib ka teiste andmete varundamise nõue. Nende hulka kuuluvad eelkõige SAP kataloogipuus paiknevad failisüsteemi andmed.

SAP infoallikad

Java protokollistiku jaoks tuleb lisaks varundada andmed (nt teised andmebaasid või failid), mida kasutavad installeeritud rakendused. Kui neid ei varundata, võib rakendusandmetes esineda ebakõlasid. Vastutavad administraatorid peavad lisaks olema informeeritud varukoopia andmekandjate asukohast ja taasteprotseduuridest. Teisi dokumentatsioone kirjeldatakse M 2.346 SAP dokumentatsiooni kasutamine .

Varusüsteem

Väikesed ettevõtted ja asutused kasutavad teatud juhtudel SAP süsteemi, mille puhul on kõik komponendid installeeritud ühte arvutisse (*Single Server Installation*). Hädaolukorra puhul, mida ei ole võimalik kõrvaldada varundatud andmete taastamisega, näiteks riistvara defekti korral, tuleb soetada varusüsteem. Kuna varusüsteemi soetamiseks kulub tavaliselt aega, võib esineda pikaajalisi tõrkeid. Seetõttu on soovitatav hoida kasutusvalmis varusüsteem, mis on ette valmistatud selliselt, et tööprotsessi taastamiseks on vaja salvestada vaid viimati varundatud andmed.

Täiendavad kontrollküsimused:

- Kas on olemas SAP süsteemide hädaolukorraks valmisoleku plaan?
- Kas hädaolukorra administraatori konto on sisse seatud?
- Kas vastutavad töötajad on teadlikud sellest, kus hoitakse hädaolukorra administraatori konto pääsuandmeid?
- Kas SAP süsteemi andmeid varundatakse regulaarselt?
- Kas on teada, kus asuvad varundusandmekandjad ning kuidas toimub SAP süsteemi taastamine varukoopiast?
- Kas on olemas varusüsteem?

M 6.98 Salvestisüsteemide hädaolukordadeks ettevalmistamine ja reageerimine hädaolukorras

Algatamise eest vastutavad: IT-juht, infoturbeametnik

Rakendamise eest vastutavad: administraator, IT-juht

Selleks, et tagada salvestisüsteemi kättesaadavus ja terviklus, on vajalikud ulatuslikud hädaolukorra ettevalmistamise meetmed. Ühelt poolt võivad need seisneda selles, et tuvastada õigeaegselt vigu ja neid käsitleda, teiselt poolt võivad need tuleneda nõuetest korrakohasele tööle. Seetõttu on vajalik hädaolukorra ettevalmistamise meetmete dokumentatsioon, et tagada hädaolukorras sobilik reageerimine.

Salvestisüsteemi vigade käsitlemine

Igas IT-süsteemis esinevad rikked, mis võivad ulatuda komponendi juhuslikust valest käitumisest kuni seadme selgelt piiritletava tõrkeni. Turvalise käitamise alus on ettevalmistus sellisteks tõrkeolukordadeks. Siia kuuluvad riistvara või tarkvara tõrked või kahjustused näiteks vigade või kompromiteerimise alusel.

Seda tüüpi olukordades kiireks reageerimiseks tuleb juba eelnevalt planeerida ja ette valmistada diagnoosimist ning vigade kõrvaldamist. Tüüpiliste ja juba esinenud veaolukordade jaoks peaksid olema koostatud käsitlusjuhendid. Kokaraamatusarnane dokumentatsioon meetmetest ja käskudest, mis toetavad veaanalüüsi ja vigade parandamist, on eriti kasulik. Kui asutuses on olemas ulatuslik hädaolukorra haldus (vt moodulit B 1.3 Hädaplaanimine), peaksid olemas olema näited selliste taastamisplaanide jaoks, mida siin kasutada tuleks. Nii saab tagada, et hädaolukorra meeskonnal on kõik andmed sobival kujul olemas.

Just keeruliste süsteemide nagu salvestisüsteemi korral on rikete hindamise ning kiire ja eesmärgipärase sekkumise seisukohast otsustava tähtsusega selliste ühenduste ja sõltuvuste kujutamine, mille iga asutus individuaalselt loob.

Edukate diagnoositööde eeldus on nõuetekohane logimine käitamise ajal (vt ka M 2.359 Salvestisüsteemide seire ja haldamine). Lisaks tuleks vigade kõrvaldamisel kasutada sobivaid tööriistu. Selleks on olemas nii tasuta saadavad kui ka tasulised programmid, sageli ka salvestisüsteemi ja selle komponentide tootjalt. Sobivate tööriistade kasutamine on seda olulisem, et keeruliste lahenduste korral ei nõuta üksikute komponentide kontrollimist ja juhtimist, vaid ülevaadet sageli väga heterogeense üldlahenduse riist- ja tarkvara koostoimest.

Rikete käsitlemise plaane ja ka automaatseid hädaolukorra protseduure

(ümberlülitamine teistele SAN-idele, replikatsioonitestid) tuleb testida ja neid tuleks harjutada hädaolukorra harjutuste raames. Salvestisüsteemidega seotud hädaolukorra testide ja harjutuste korral ilmneb järelmeetmete eripära, et testide ja harjutustega toodetakse suuri andmehulki. Nendel andmetel võib olla konfidentsiaalsuse suhtes eriline kaitsevajadus või need sisaldavad isikuandmeid. Eriti sellisel juhul, aga ka tavapärase kaitsevajaduse korral tuleb andmed pärast harjutuse lõppemist turvaliselt ja nõuetekohaselt kustutada (vt meede M 2.527 Turvaline kustutamine SAN-keskkonnas). Siinjuures vajalikud kulutused tuleb arvesse võtta testide ja harjutuste planeerimisel. Ka taaskäivitamise ja taastamise plaanid peavad arvesse võtma üleliigsete andmete kustutamist, mis genereeriti hädaolukorra likvideerimise raames.

Peab olema selge, et pärast rikkeid ja hädaolukordi, mis on seotud andmekaotusega, on salvestisüsteemide tagasiviimine tavarežiimi ainult siis võimalik, kui on olemas kohane andmevarundus. Andmevarunduste taastatavuse kontrolli tuleb läbi viia regulaarselt.

Salvestisüsteemide vigade käsitlemise protseduur tuleb ära jaotada halduse, jõudluse mõõtmise ja diagnoosimise vahel. Alljärgnevalt esitatakse aspekte, mida tuleb alati arvesse võtta.

Administreerimine

Käitamisraamatus peaksid olema dokumenteeritud kõik vajalikud käsud haldusele ja konfigureerimisele.

Arvesse tuleb võtta järgmisi valdkondi:

- (administratiivsete) kasutajate seadistamine, volituste andmine,
- püsivara ja operatsioonisüsteemi värskendamine,
- konfiguratsioon,
- alvestiressursid,
- administratiivsed juurdepääsud,
- ühendatud server ja andmevarundusseadmed,
- logimine.

Jõudlus

Jõudluse osas tuleks arvesse võtta järgmisi tähelepanekuid ja väiteid:

- andmekandjate hõivatus (loogilise või füüsilise seadme kohta),
- läbilaskevõime liidese kohta (IP, FC jne), võttes arvesse terviksüsteemi,
- statistiline teave kasutamiseks.

Diagnoos

Kõik vigade diagnoosimiseks (Debugging) vajalikud käsud ja oodatavad väited ning nende tähendus tuleb dokumenteerida. Siia kuulvad näiteks väited erinevate süsteemikomponentide ja liideste olekute ning ka tegelike konfiguratsioonide

kohta.

Muu hulgas kuuluvad vigade diagnoosimise juurde järgmised andmed:

- võrguliideste ja muude ühenduste olek,
- võrguteenuste olek (TCP/IP NAS-süsteemide korral, spetsiifilised andmed SAN-i korral, nt SAN-kommutaatorite olek),
- täiendavate komponentide olek (nt salvesti virtualiseerimine),
- üldkonfiguratsioon ülevaatena,
- protsessid,
- jaotus,
- sisseloginud kasutajad,
- logimine (logitasandi kasutamine, logiandmete tõlgendamine).

Hädaolukorra ettevalmistamine kättesaadavuse tõstmiseks

Rikete käsitlemise planeerimisega saab taastamise aega minimeerida ja teatud juhtudel üldse lahendust võimaldada. Planeerimised tuleb kooskõlastada üldise hädaolukorra haldusega ja need peaksid orienteeruma üldises hädaolukorra kontseptsioonis (vt moodulit B 1.2 Personal). Üldises hädaolukorra kontseptsioonis sõnastatakse üldised nõuded hädaolukorra dokumentidele kogu IT-süsteemis. Need määravad ideaalsel juhul kindlaks ühtsed ja siduvad nõuded ülesehituse, sisu ja vormi kohta. Siiski ei tohiks integreerimisel üldisesse hädaolukorra haldusesse jääda tähelepanuta salvestisüsteemide hädaolukorra ettevalmistamise ja käsitlemise eripärad. Salvestisüsteemidele esitatavad kättesaadavuse nõuded peavad olema selgelt määratletud.

Alljärgnevad küsimused on hädaolukorra ettevalmistamisel asjakohased.

- Mis on võimalike rikete põhjused?
  - riistvara vead;
  - liiga vähene dimensioneerimine (rike või tõrge kasutamise suurenemisel).
- Millised on nõuded seirele hädaolukordade vältimiseks?
- Kuidas saab tagada varajase rikke tuvastamise?
  - Andmete kogumine, mida hindavad alati salvestilahenduste töö eest vastutavad asutused.
- Milliseid ennetusmeetmeid võib kasutada?
  - varuseadmete olemasolu;
  - varuosade olemasolu;
  - Failover-lahenduste rakendamine, mis võivaldavad jooksva töö käigus ümber lülitada alternatiivsele seadmele;
  - hoolduslepingute lõpetamine;
  - töötajate koolitus;
  - replikatsioonimeetmete võtmine;
  - ühendused tuleb rakendada liiasusega;
  - liiasusega ühendused erinevate trasside kaudu;
  - erinevad kandjad ühendustel;

- liinivõimsuste piisav dimensioneerimine (hädaolukord);
- andmete taastamise meetmete võtmine;
- käitamisraamatu koostamine;
- hädaolukorra plaani koostamine;
- andmete koostise säilitamine;
- kui salvestisüsteemi kasutatakse arhiivina, mida enam ei varundata, peab iga objekti kohta olemas olema vähemalt üks lisakoopia.

- Andmetalletus
  - hädaolukorra puhul tuleb kinni pidada käitamiskontseptsioonist, milliseid andmeid peegeldada (hoida varuna) või millised andmed hädaolukorras varundatud andmetest taastada. Selle meetodi põhimõte tuleneb olemasolevatest SLA-dest;
  - IP- ja FC-võrkude liiasusega väljaehitamine;
  - liiasusega FC-topoloogia, järgides üheselt mõistetava WWN-i andmist;
  - liiasusega FC-topoloogia, järgides üheselt mõistetava IP-aadressi andmist;
  - segmenteerimise ja tsoneerimise tõrkekindlus tuleb tagada vastavate võrgukomponentide väljaehitamisega koos liiasusega.
- Milliseid Service Level Agreements'e (SLA-d) tuleks kasutada?
  - riistvara tarnijad (nt vahetamine kohapeal koos ajagarantiiga teatud komponentide jaoks);
  - Service Level Agreements'i haldus: peab olema tagatud, et SLA-d pikendatakse õigeaegselt või kohandatakse õigeaegselt ajakohastele nõuetele.

Teenusetaseme lepingute (Service Level Agreements) haldus

SLA-d sõlmitakse tavaliselt piiratud ajaks ja neid ei pikendata alati automaatselt. Seetõttu juhtub sageli, et SLA-de pikendamise hinnad pikemaks ajavahemikuks tõusevad oluliselt või et neid vananenud süsteemidele enam ei pakutagi. Sellisel juhul tuleks kontrollida, kas ehk investeering uude salvestisüsteemi ei ole pikaajalises perspektiivis odavam. Seda tuleb õigel ajal arvesse võtta ja planeerida.

Hädaolukorra ettevalmistamise dokumentatsioon

Täpset tegevust kindlates hädaolukordades tuleb kirjeldada hädaolukorra plaanis. Tegevus peab sisaldama järgmisi punkte.

Kuidas diagnoosimine läbi viia? Seejuures on abiks järgmised andmed:

- olekupäringud,
- konfiguratsiooni näit,
- toimuva protsessi näit,
- sisseloginud kasutajad,
- logimine.

- Milliseid vigade kõrvaldamise protseduure tuleks läbi viia?
  - tegevus salvestisüsteemi töö täieliku katkemise korral (operatsioonisüsteemi ja konfiguratsiooni taastamine);
  - tegevus osakomponentide tõrke korral (näiteks kõvakettad).
- Keda tuleb kahjujuhtumi korral teavitada?
  - serveri ja rakenduste haldus;

- riistvara tarnija / hooldusleping kontaktisik;
- kõik vajalikud andmed hooldusleping ja teenusetaseme lepingute, teabeliini numbrite, kliendi- või seadme-ID-de kohta.

- Millised dokumendid peavad kahjujuhtumi korral saadaval olema?
  - hooldusleping;
  - aluskonfiguratsioon (uuesti) kasutuselevõtmiseks;
  - aluskonfiguratsiooni muudatused, et seadistada ajakohast töökonfiguratsiooni;
  - reeglistik juurdepääsukontrolli jaoks (Access Control Lists);
  - seadistatud kasutajad ja volitused;
  - paroolid hädaolukorra juurdepääsudele.
- Kuidas toimub taaskäivitamine?
  - sõltuvus IT-koosluse muudest süsteemidest;
  - operatsioonisüsteemi uuesti installeerimine ja konfigureerimine;
  - varundatud konfiguratsiooni taastamine;
  - piiratud käitamise võimalused;
  - kaugtöö teises asukohas.

Hädaolukorra ettevalmistamiseks vajalikud tegevuste kirjeldused tuleb koostada võimalikult hoolikalt ja neid tuleb regulaarselt järele proovida. Arvesse tuleb võtta varieeruvaid tegevusviise erinevate seadmetüüpide ja operatsioonisüsteemide korral.

Dokumentatsioon ei tohi kindlasti eksisteerida ainult elektroonilisel kujul. Tegevusjuhised peavad olemas olema vähemalt ka paberkujul. Vajaduse korral võib konfigureerimisfailid salvestada eraldi ka välistele andmekandjatele nagu CD-ROM või USB-mälupulk.

Ilmselt kõige tähtsam meede kättesaadavuse suurendamiseks on varuosade olemasolu, et minimeerida riistvaravigade korral katkestusaegasid. Alternatiivselt või täiendusena sellele võib sõlmida tootjaga hooldusleping, mis tagavad garanteeritud reaktsiooni- või isegi remondiaegadega kättesaadavuse. Seeläbi alanevad laos hoidmise hinnad või saavutatakse veelgi suurem riistvara kättesaadavus. Sellise lepinguga saab reguleerida ka varustamist tarkvaravärskendustega (tarkvarahooldus). Vajaduse korral on üldise hädaolukorra halduse raames ette nähtud salvestisüsteemi etapiviisiline taaskäivitamine. Sellisel juhul võetakse kasutusse kõigepealt üks salvestisüsteemi osa, et ajakriitilised äriprotsessid saaksid töötada avariirežiimi vajalikus ulatuses. Sellisel juhul eksisteerivad taastusplaanide kõrval ka taaskäivitusplaanid, mis alluvad samadele nõuetele kui taastusplaanid.

Salvesti virtualiseerimise kasutamisega tekivad hädaolukorra ettevalmistamise jaoks uued võimalused. Nii saab näiteks salvesti virtualiseerimise kaudu (Distributed LUN) tagada liiasusega salvestamise erinevatel salvestisüsteemidel. Sel moel

viiakse ellu salvestisüsteemi Hot-Standby, tänu millele on võimalik katkestusaegasid peaaegu täielikult vältida.

Kontrollküsimused

- Kas tegevusjuhised on olemas meetmete ja käskude kujul, mis toetavad veaanalüüsi ja vigade parandamist?
- Kas vigade kõrvaldamiseks kasutatakse sobivaid tööriistu?
- Kas rakendatud salvestisüsteemi jaoks on olemas hädaolukorraplaan, mis kirjeldab täpset tegevust teatud hädaolukordades?
- Kas hädaolukorra ettevalmistamiseks vajalikke tegevuskirjeldusi testitakse regulaarselt?
- Kas testide ja harjutuste korral ning ka hädaolukorras kustutatakse üleliigsed andmed vastavalt nende kaitsevajadusele?

M 6.99 Windows Serverite tähtsate süsteemikomponentide regulaarne varundus

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: andmevarunduse eest vastutavad töötajad

Andmevarunduskontseptsioon

Varundustarkvara

Windows Serverite süsteemikomponente tuleb regulaarselt varundada, kuna server allub oma serverirolli tõttu pidevatele konfiguratsioonimuutustele. Planeerimata muudatused, mis võivad põhjustada süsteemis vigu, näiteks uuenduste vigast installeerimist, võivad muuta vajalikuks tähtsate süsteemikomponentide taastamise. Tähtsate süsteemikomponentide hulka ei kuulu mitte ainult tegelikud süsteemifailid, vaid ka konfiguratsiooniandmed (näiteks registri andmebaas, IIS metabaas, konfiguratsioonifailid), staatust puudutav informatsioon (registri andmebaas, DHCP andmebaas, WINS jne) ning logimisandmed. Andmevarundus võib toimuda varundustarkvara abil või selektiivselt failisüsteemi kaudu, näiteks skripti abil.

Üldiselt tuleb vähemalt staatust puudutav informatsioon ja logifailid varundada iga päev vastavalt andmevarunduskontseptsiooni eeskirjadele (vt B 1.4 Andmevarunduspoliitika).

Süsteemi staatuse varundamine (System State)

Alates versioonist Windows Server 2008 juurutas Microsoft uue, andmete varundamiseks ja taastamiseks mõeldud lahenduse, mille kasutamiseks tuleb Microsoft Management Console'is käivitada snap-in Windows Server Backup. Kuna see komponent ei kuulu standardinstallatsiooni hulka, tuleb see eraldi juurde installida. Olulised süsteemikomponendid võivad paikneda nii süsteemipartitsioonil kui ka teistel kõvaketta partitsioonidel. See oleneb muu hulgas sellest, kas komponendi installimise käigus on valitud standardist erinev andmetee, nt logifailide puhul. Süsteemiandmeid võib varundada Windowsi enda asjakohase varundusprogrammiga.

Varundusprogrammiga saab salvestada ka süsteemi seisundit. Näiteks kui varundusprogrammi kasutatakse domeenikontrolleri jaoks ja kui programmi töös on aktiveeritud süsteemiseisundi varundamise suvand, hõlmab varundamine kõiki installimise käigus valitud salvestuskohas asuvaid süsteemikomponente ja kõiki jaotatud teenuseid, mille töö sõltub Active Directoryst. Alllpool on toodud näited süsteemi staatuse andmete kohta.

Süsteemi staatuse andmed vastavalt põhiinstallatsioonile:

- Andmed süsteemi käivitamiseks
- Süsteemi registreerimine

- Registreeritud COM-komponentide andmebaas (laienemine komponentobjektide mudeliks)
- Logifailid
- Täiendavad süsteemi staatuse andmed domeenikontrolleril (näitlik)

1. SYSVOL kataloog
2. DNS andmebaas
3. Active Directory

Näited teiste rollispetsiifiliste süsteemi staatuse andmete kohta:

- klastriteenuse staatus (kui on installeeritud);
- sertifikaaditeenuste andmebaas (kui on installeeritud).

Teiste tootjate programmid

Varundusprogrammid

Varundusprogramm Backup sisaldab vaid andmevarundusprogrammi põhifunktsioone ning on kasutatav vaid madala turbevajaduse korral. Muuhulgas on piiratud selle usaldusväärsus (kontrollmehhanismid ei loo kontrollkoode) ja riistvara toetus ning see võimaldab vaid algelist logimist, monitooringut ja aja planeerimist. Olenevalt serveri rollist ja andmevarundusele esitatavatest nõuetest, tuleb kontrollida, kas tuleks eelistada teiste tootjate programme. Need peaksid toetama NT-Backup-API -t.

Täielik süsteemistaatuse varundus ja osaline taaste

Süsteemistaatuse failide taastamine

Windowsi varundusprogramm suudab taastada vaid kogu süsteemi staatuse. Kolmandate tootjate programmid võimaldavad taastada üksikute rollide konfiguratsiooniandmeid, näiteks Active Directory. Igal juhul peab enne taastamist olema operatsioonisüsteem identselt konfigureeritud, vastasel korral lõpeb taastamine kas veaga või mittefunktsioneerivate parameetritega.

Tuleb välja selgitada järgmised baasparameetrid:

- Millist teenusepaketti kasutatakse?
- Millise litsentsitüübi kasuks otsustati?
- Millisel viisil tuleb toode aktiveerida?
- Kuidas on arvuti nimi?
- Kuidas on riistvara konfigureeritud? (Riistvara väikseid muutusi kompenseerib isehäälestumist võimaldav tarkvaratugi -PnP).

Andmete taaste eraldi testimissüsteemilSüsteemi staatuse taastamist ei tohi kunagi viia läbi töötaval serveril, ka mitte kontrollimise eesmärgil. Kui see ei rahulda süsteemi kaitsevajadust, tuleb mõelda alternatiivsetele süsteemi staatuse varundusstrateegiatele (nt kõvaketta kujutised, serveri virtualiseerimine). Kontrollimismudeli näide: Süsteemipartitsioon asub draivil RAID-tasemega 1 (peegeldus). Üks kõvaketas eemaldatakse RAID-kooslusest ning katkestatakse side Internetiga (offline), nii et süsteemi originaalseisund konserveeritakse. Seejärel viiakse katseliselt läbi süsteemi staatuse taaste ning kontrollitakse süsteemi funktsioneerimist. Pärast testi läbiviimist taastatakse eraldatud ketta side Internetiga (online) ja peegeldatakse tagasi, et originaalseisund on taastatud.

Avariitaaste (Disaster Recovery)

ASR: varundusfunktsioon ja taastefunktsioon

Alates versioonist Windows Server 2008 saab Windows Server Backupi varundusfunktsiooniga luua andmetest ka selliseid varukoopiaid, mille põhjal saab taastada süsteemi. Selleks võib valida kas täieliku serverivarunduse (kõik failisüsteemid) või Bare Metal Recovery varunduse (ainult süsteemile hädavajalikud failisüsteemid). Taastamisprotsess toimub Windowsi taastamiskeskkonnas ning selle saab käivitada kolmel moel: setup andmekandjaga, süsteemi käivitamise ajal klahviga F8 või parandamisfunktsiooniga Repair your Computer.

Kontrollküsimused:

- Kas on testimise teel välja selgitatud, kas eeldefineeritud süsteemi staatuse varundus on mahu poolest piisav?
- Kas on testimise teel välja selgitatud, kas on vajalik võtta kasutusele kolmandate tootjate varundustooted?
- Kas on tagatud, et enne süsteemistaatuse andmete taastamist on operatsioonisüsteem identselt konfigureeritud ja taastamist ei viida läbi töötaval süsteemil?
- Kas vastavalt serverirollile ja käideldavusnõuetele toimub serveri ootamatuseplaani raames taastamise ja taasteaja testimine ja parendamine?

M 6.100 IP-kõne (VOIP) hädaolukorraks valmisoleku plaani koostamine

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: administraator

IP-kõne osaline või täielik väljalangemine on paljudel juhtudel raskendavaks asjaoluks, sest telefoniside on enamasti asutuse üheks tähtsamaks teenuseks. Selle väljalangemisel võib olla mitmeid põhjusi. Lisaks tüüpilistele IP-kõne probleemidele võib ka üksikute võrgukomponentide tõrge põhjustada IP-kõne teenuse täielikku väljalangemist. Seetõttu tuleb hädaolukorraks valmisoleku plaani koostamisel luua kontseptsioon, mis võimaldab minimeerida väljalangemise tagajärgi ning kehtestab toimingud, mida tuleb läbi viia väljalangemise korral. Seejuures tuleks arvestada järgmiste aspektidega:

- IP-kõne hädaolukorraks valmisoleku plaan tuleb integreerida olemasolevasse avariiplaani (vt B 1.3 Hädaplaanimine).
- IP-kõne tõrke puhul peab sidepidamise võimalus alles jääma. Seepärast tuleb välja selgitada, kas IP-kõne tõrke puhul on võimalik vähemalt hädavajalik sidepidamise võimalus (vähemalt politsei ja tuletõrjega). Lisaks peab olema võimalik kiiresti informeerida välist kasutajatoe teenusetarnijat väljalangemisest, et viga saaks kõrvaldatud. Väljalangemise korral võib sidepidamiseks kasutada näiteks mobiiltelefone, selleks on aga vaja valmis olla.
- Süsteemi väljalangemisel võib ette tulla ka andmete kadu. Seepärast tuleb üldise andmevarunduspoliitika koostamise käigus (vt B 1.4 Andmevarunduspoliitika) luua ka reeglid IP-kõne komponentide varundamiseks. Selleks ei tule võtta vaatluse alla mitte ainult IP-kõne vahendustarkvara, vaid ka kasutaja poolt seadistatud lõppseadmed, näiteks telefoniraamatud.
- Tuleb võtta tarvitusele abinõud IT-süsteem, milles kasutatakse tarkvaratelefoni, korda tegemiseks. Kui kasutajad peavad oma ülesannete täitmiseks olema telefoni teel kättesaadavad, tuleb see tagada vastavate meetmete rakendamisega.

Täiendavad kontrollküsimused:

- Kas IP-kõne tõrke puhuks on olemas hädaolukorraks valmisoleku plaan?
- Kas on olemas telefoniside varulahendused, näiteks mobiiltelefonid?

M 6.101 IP-kõne (VOIP) andmevarundus

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: administraator

Et konfiguratsioonivea või väljalangemise korral, mida on võimalik kõrvaldada vaid komponentide väljavahetamise teel, oleks võimalik IP-kõne kiiresti taastada, tuleb kõik konfiguratsiooniandmed regulaarselt varundada. Andmete varundamiseks tuleb põhimõtteliselt rakendada B 1.4 Andmevarunduspoliitika kirjeldatud tegutsemisviisi. Varundatavate failide hulk tuleb välja selgitada kasutatavate IP-kõne komponentide abil. Nende hulka kuuluvad muuhulgas:

- Kõik IP-kõne spetsiifilised konfiguratsiooniseaded
- Üldised konfiguratsiooniseaded, näiteks IP-aadressid, paroolid ja kasutatava operatsioonisüsteemi kõik olulise tähtsusega konfiguratsioonid
- Logimisandmed
- Kasutaja sisestatud personaalsed andmed, näiteks isiklikud telefoniraamatud

Nimetatud konfiguratsiooniseadeid tuleb regulaarselt varundada. Andmevarundus tuleb läbi viia ka enne ja pärast igakordset konfiguratsiooni muutmist. Seejuures tuleb pöörata tähelepanu asjaolule, et hallatakse paljusid varundusfailide versioone (generatsioone). Vigast konfiguratsiooni on tihti võimalik kõrvaldada enne seda genereeritud versiooni installeerimise teel. Tuleb arvestada, et pärast tarkvara uue redaktsiooni kasutuselevõtmist ei ole alati võimalik kasutada vanu konfiguratsioonifaile. Kui pärast riistvara tõrget võetakse kasutusele seade, millel on uuem või varasem tarkvararedaktsioon, võib juhtuda, et konfiguratsioonifaile ei saa otse üle võtta. Seepärast tuleb tarkvara väljavahetamisel pöörata tähelepanu uusimale tootja informatsioonile, näiteks *Changelog* failidest. Kui konfiguratsioonifaile tuleb tarkvararedaktsiooni vahetamisel kohandada, tuleb varundada nii vana kui ka uus versioon. Probleemide korral uuema redaktsiooniga võib ka hiljem uuesti üle minna vanale versioonile, mis võib olla stabiilsem. Andmed tuleb varundada IT-süsteemidele ja andmekandjatele, mis on sõltumatud tööks kasutatavatest IT-süsteemidest ja andmekandjatest. Nendeks võivad olla näiteks lindid, CD-RWd või teised IT-süsteemid. Kui andmevarundus teise süsteemi toimub võrgu kaudu, tuleks mõelda andmete krüpteerimisele või kasutada oma administratiivset võrku, et kaitsta andmeid pealtkuulamise ja manipuleerimise eest.

Täiendavad kontrollküsimused:

- Kas konfiguratsioonifaile varundatakse regulaarselt?
- Kas testitakse regulaarselt, kas varundatud andmeid on võimalik taastada?

M 6.102 Käitumisreeglid traadita kohtvõrkude turvaintsidentide puhul

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutavad: administraator, kasutajad

Kui kohtvõrgu käitumises tekivad kõrvalekalded ettenähtust (nt kohtvõrk ei ole pikemat aega kättesaadav, juurdepääs võrguressurssidele ei ole võimalik, võrgu jõudlus kaob pidevalt), võib see olla põhjustatud turvaintsidentidest. Eeltoodu võib olla põhjustatud ründest, valest konfiguratsioonist või vigadest süsteemis. Kasutajad peavad pöörama tähelepanu järgmistele soovitustele:

- Töö tulemused tuleks varundada, traadita kohtvõrgu kasutamine lõpetada ja kliendi traadita kohtvõrgu liides deaktiveerida.
- Võimalikud veateated või kliendi ebanormaalse käitumise peaks kasutaja täpselt dokumenteerima. Lisaks tuleb dokumenteerida, mida kasutaja tegi enne turvaintsidenti või selle toimumise ajal. See loob administraatoritele eeldused intsidendi põhjuse kiiremaks tuvastamiseks ja vastumeetmete rakendamiseks.
- Kasutajad peavad administraatoreid sobiva eskalatsiooniastme kaudu (nt *User Help Desk*) teavitama. Seejuures tuleb tagada, et administraatorit teavitamisprotsessiga tema töös oluliselt ei segataks.

Administraatorite poolsed vastumeetmed

Administraatorid peavad turvaintsidentide korral rakendama sobivaid vastumeetmeid. Võimalikud tegevused võiksid olla järgnevad:

- Pääsupunktide väljalülitamine;
- Kommunikatsiooni sulgemine pääsupunktis jaotusvõrgu ja kohtvõrgu/Interneti vahel;
- Serverite seiskamine (veebiserver või töökeskkonna juhtserver või muu taoline server);
- Klientide traadita kohtvõrgu liidese deaktiveerimine;
- Pääsupunktide konfiguratsiooni kontrollimine;
- Kõikide failide varundamine, mis võivad osutuda vajalikuks intsidendi edasisel uurimisel (nt kas rünne on tõepoolest toimunud ning mil moel ründaja süsteemi pääses), see tähendab eelkõige kõikide tähtsate logifailide varundamist
- Vajadusel varundatud originaal-konfiguratsiooniandmete taastamine (vt M 6.52 Võrgu aktiivkomponentide konfiguratsiooniandmete regulaarne varundamine)
- Kasutajate informeerimine ja palve kontrollida oma töövaldkondi võimalike muudatuste osas

Kui pääsupunktid on varastatud, tuleb rakendada sobivaid turvameetmeid, näiteks:

- Kõikide seadmete poolt kasutatavate krüptovõtmete muutmine, näiteks puudutab see eelsisestatud võtmeid (PSK-d) WPA-PSK või WPA2-PSK kasutamisel
- Konfiguratsioonimuudatuste tegemine RADIUS-serverites varastatud pääsupunkti blokeerimiseks (IP, nimi, RADIUS-klient, *Shared Secret* , IPSec)

Lisaks tuleb uurida turvaintsidentide võimalikke mõjusid. Lõpuks tuleb rakendada kõiki vajalikke meetmeid, et välistada varastatud seadmete kuritahtlikku kasutamist asutuse võrgule juurdepääsemiseks. Näiteks kui WLAN-klient on varastatud, tuleb sertifikaadipõhise autentimise korral tühistada ka kliendisertifikaadid.

Täiendavad kontrollküsimused:

- Kas on tagatud administraatori efektiivne teavitamine?
- Kas kasutajad ja administraatorid tunnevad kõiki vajalikke käitumisreegleid, millest oleks vaja kinni pidada traadita kohtvõrgu turvaintsidentide korral?
- Kas toimub võimalike turvakriitiliste intsidentide analüüs?

M 6.103z Primaarkaabelduse liiasus

Algatamise eest vastutavad: IT-juht

Rakendamise eest vastutavad: IT-juht

Tihti on suurematel kinnistutel mitmed hooned ühendatud tähekujuliselt ühes nendest hoonetes asuva arvutuskeskusega. Tuleb kindlaks teha, kas vähemalt tähtsate hoonete jaoks tuleb luua varuga üle sõltumatute trasside kulgev primaarne IT-juhtmestik. Lisaks tuleb välja selgitada, kas ühendused IT- või PBX-tarnijaga on vajalik planeerida varuga? Tõelise varu loomiseks tuleb tarnijaga kokku leppida, kas erinevates kohtades (jaotuskohtades) tõesti luuakse ühendus sidevõrguga. Vajadus varuga primaarjuhtmestiku või varuga ühenduse järele tarnijaga sõltub asutuse käideldavusele esitatavatest nõuetest.

Paralleelkasutus

Hoones tuleb sobivate võrgu aktiivkomponentide kasutamisega tagada, et töö käigus toimuks automaatselt varuliinide paralleelne kasutamine. Nii toimub luuakse samaaegselt varu ning suurendatakse jõudlust. Seejuures tuleb silmas pidada, et ühe liini tõrke korral edastusmaht väheneb. Nimetatud edastusmahu vähenemisega tuleb arvestada hädaolukorraks valmisoleku kontseptsiooni koostamisel.

Ümberlülitamine

Kui kasutatav tehnika või juhtmestiku kaudu realiseeritavad teenused ei võimalda varuliinide paralleelset kasutamist, tuleb kasutatava liini tõrke korral varuliinile ümber lülituda. Ümberlülitamine võib toimuda automaatselt või käsitsi.Kui paralleelkasutus ei ole võimalik, tuleks mõistliku aja jooksul varuliinidele ümber lülituda, ka juhul, kui tegemist ei ole tõrkega. See on vajalik varuliinide funktsionaalsuse kontrollimiseks. Kontrollimissageduse aluseks tuleks võtta käideldavusnõuded.

Monitooring

Varuga paigaldatud sideliinid suudavad reeglina käideldavuse taset oluliselt tõsta vaid juhul, kui liinide funktsionaalsust hoitakse kontrolli all. Monitooring on vajalik tõrgete, probleemide ja muude ebareeglipärasuste varajaseks avastamiseks, et probleemid kõrvaldataks õigeaegselt või neid õnnestuks isegi vältida. Ilma monitooringuta suureneb oht, et liinide tõrkeid ei avastata ning et sel juhul on tegemist vaid näilise, mitte aga tegeliku varuga.

Kontrollküsimused:

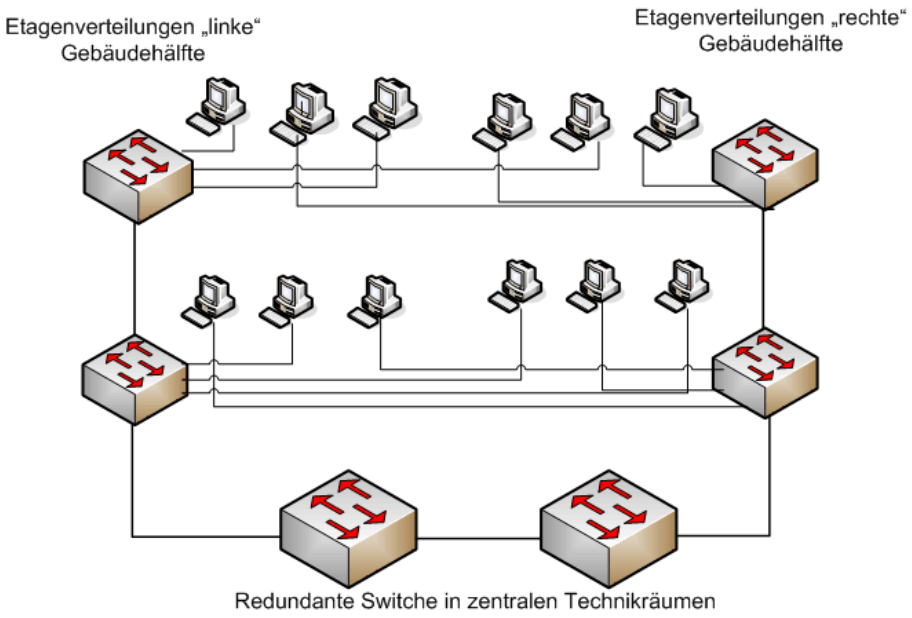
- Kas käideldavusnõuetele vastavalt on varuga paigaldatud primaarjuhtmestik või varuga ühendus tarnijaga õigustatud?
- Kas varujuhtmestiku toimimist kontrollitakse regulaarselt?

M 6.104z Hoone kaabelduse liiasus

Algatamise eest vastutavad: IT-juht
Rakendamise eest vastutavad: tehnikaosakond, IT-juht

Kõrgete käideldavusnõuete korral tuleks kaaluda olulise tähtsusega hoonetes sekundaar- ja tertsiaarjuhtmestiku varuga paigaldamist. Selleks paigaldatakse sekundaarjuhtmestik, st korrustevaheline ühendus vähemalt kahe vertikaalse tunneli kaudu, mis peavad paiknema hoone erinevates tuletõkkesektsioonides. Näiteks võiks sekundaarjuhtmestiku paigaldada vastamisi asetsevatesse hoone osadesse (nt põhi ja lõuna või ida ja lääs). Kõik varustamist vajavad ruumid ühendatakse mõlema sekundaarjuhtmestikuga. Pooled ühenduskohtadest ühes ruumis ühendatakse jagajaga ühel hoone poolel, teine pool hoone teisel poolel.

Alljärgneval joonisel kujutatakse mõlemat hoone poolt skemaatiliselt „vasak-“ ja „parempoolse” küljena.



Joonis 1: Kasutajate varuga ühendamine

Joonise juurde : Etagenverteilungen “linke” Gebäudehälfte – Jaotumine korrustele, hoone vasak tiib; Etagenverteilungen “rechte” Gebäudehälfte – Jaotumine korrustele, hoone parem tiib; Redundante Switche in zentralen Technikräumen – Varuga paigaldatud switch ’id tsentraalsetes tehnikaruumides.

Selliselt on ka raske kahjustuse korral võimalik töö jätkumist korrustel kasvõi ajutiselt säilitada, niikaua kui kahjustus ei hõlma mõlemat hoone poolt.

Kontrollküsimused:

- Kas käideldavusele esitatavatest nõuetest tuleneb vajadus sekundaar- ja tertsiaalkaabli varuga paigaldamiseks?

M 6.105 Printerite, koopiamasinate ja multifunktsionaalsete seadmete hädaolukorraks valmisoleku plaan

Algatamise eest vastutavad: IT-juht, infoturbeosakond

Rakendamise eest vastutab: administraator

Olemasolevate printerite, koopiamasinate ja multifunktsionaalsete seadmete väljalangemine pikemaks ajaks ei ole aktsepteeritav. Iseäranis tsentraalsete komponentide tõrge, mis on vajalik kogu printerite infrastruktuuri jaoks, võib tööprotsesside toimumist tuntavalt häirida. Olenevalt käideldavusele esitatavatest nõuetest tuleb rakendada meetmeid, et väljalangemisaega, täpsemalt öeldes väljalangemisest põhjustatud mõjusid vähendada.

Kulumaterjalid

Tuleb jälgida, et alati oleks olemas küllaldaselt kulumaterjale, näiteks toonerit ja paberit. Kui kulumaterjali on alles teatud hulk, mis sõltub tarvidusest, tuleb hankida ja kättesaadavana hoida uus kulumaterjal (vt M 2.52 Faksimaterjalide varude jälgimine ja täiendamine).

Konfiguratsiooniseaded

Iga koopiamasina, printeri ja teiste printimissüsteemi komponentide juures tuleb teostada erinevad konfiguratsiooniseaded. Et neid seadeid pärast väljalangemist või väljavahetamist jälle kiiresti sisse seada, tuleb konfiguratsioonid süstemaatiliselt dokumenteerida (vt M 2.25 Süsteemi konfiguratsiooni dokumenteerimine).

Tsentraalsed seadmed

Mida vähem printereid või koopiamasinaid kasutuses on, seda raskemad tagajärjed on ühe seadme väljalangemisel. Printserveri väljalangemine on eriti probleemaatiline, kuna neid on tavaliselt ainult üks või mõned üksikud. Et oleks võimalik hädaolukordadele reageerida, tuleks ühelt poolt vahet teha tsentraalsete komponentide ning teiselt poolt printerite ja koopiamasinate vahel. Kõrgema kaitsevajaduse korral seoses käideldavusnõuetega tuleks kaaluda tsentraalsete komponentide, näiteks printserverite varuga paigaldamist. Kui ainuke olemasolev tsentraalne server välja langeb, ei saa teatud juhtudel kogu kohtvõrgus enam väljatrükki teha. Detsentraalsed komponendid, näiteks printerid, asuvad tihti mitmel korrusel või hoone erinevates büroodes.

Üldiselt tuleks printerid paigutada selliselt, et kasutaja saaks ühe printeri väljalangemisel probleemideta kasutada teist.

- Tuleks kaaluda lokaalsetele printeritele, millel on vastavalt käideldavusnõuetele kõrgem kaitsevajadus ning mis ühendatakse otse töökohaarvutiga, varuseadmete paigaldamist (Cold Standby). Väljalangemise korral saaks defektse printeri kiiresti varuseadme vastu välja vahetada.
- Suurte koopiamasinate ja printerite puhul, mida kasutavad paljud inimesed, tuleks sõlmida hooldusleping, milles on kindlaks määratud kaitsevajadusele vastav reageerimisaeg.
- Tuleks koostada nimekiri müügifirmadest, kust saaks probleemideta soetada uue seadme.

- Vajadusel võiks olemas olla tihti vajaminevad tagavaraosad. Viimati nimetatu on otstarbekas vaid juhul, kui omatakse erialaseid teadmisi, mis võimaldavad varuosi iseseisvalt välja vahetada.

Kontrollküsimused:

- Kas on kindlaks tehtud vajadus tsentraalsete komponentide varuga paigaldamiseks?
- Kas hooldusleping on sõlmitud?
- Kas konfiguratsiooniseadeid varundatakse süstemaatiliselt?

M 6.106z Kataloogiteenuse hädaolukorraks valmisoleku plaani koostamine

Algatamise eest vastutavad: IT-juht, infoturbe eest vastutav töötaja

Rakendamise eest vastutavad: IT-juht, administraator

Kataloogiteenuste osaline või täielik väljalangemine raskendab reeglina olulisel määral kasutajate tööd. Kataloogiteenuste tõrke korral ei saa näiteks läbi viia serveri baasil teostatavaid toiminguid. Seetõttu tuleb hädaolukorraks valmisoleku plaani koostamisel luua kontseptsioon, mis võimaldab minimeerida kataloogiteenuste komponentide väljalangemise tagajärgi ning kehtestada toimingud, mida tuleb väljalangemise korral läbi viia.

Seejuures tuleks arvestada järgmiste aspektidega:

- Kataloogiteenuste süsteemi hädaolukorraks valmisoleku plaan tuleb integreerida olemasolevasse hädaolukorraks valmisoleku plaani (vt B 1.3 Hädaplaanimine).
- Süsteemi väljalangemisel võib ette tulla ka andmete kadu. Seetõttu tuleb koostada kataloogandmebaasi andmevarunduse plaan, mida on võimalik integreerida olemasolevasse andmevarundusplaani või mis seda asendab (Vt B 1.4 Andmevarunduspoliitika ja M 6.107 Kataloogiteenuste andmevarundus)
- Kui koopiad olulisest informatsioonist ja failidest salvestatakse mitmele serverile, saab ühe kataloogiteenuste serveri tõrke korral kasutada neid koopiaid.

Kataloogiteenuste rimismehhanismide abil on võimalik anda kasutajate käsutusse ruumiliselt lähedane andmete koopia, et tagada kiire juurdepääs serverile ja selle kõrge käideldavus (vt M 2.409 Kataloogiteenuse partitsioonide loomise ja replikeerimise planeerimine).

- Kataloogiteenus loob võimaluse kataloogandmebaasi jaotamise (partitsioneerimise) mitmele kataloogiteenuse serverile, nii et igal serveril oleks vaid üks osa andmetest. Ühe kataloogiteenuse serveri tõrge mõjutab seega vaid sellele serverile salvestatud kataloogi partitsiooni. Avariiplaani koostamisel tuleb arvestada kõigi kataloogiteenuse installatsiooni partitsioonidega.
- Kogu kataloogiteenuse komponentide süsteemi konfiguratsioon tuleb dokumenteerida. Kõik süsteemi taastamiseks läbiviidavad toimingud peavad olema kirjeldatud selliselt, et neid on hädaolukorras võimeline läbi viima ka personal, kes ei oma üksikasjalikke teadmisi eelnevalt olemasolevast süsteemikonfiguratsioonist.
- Hädaolukorraks valmisoleku plaani koostamisega tuleb tagada, et hädaolukorras oleks kättesaadav vastava koolituse läbinud personal.
- Tuleb luua taasteplaan, mis tagab kataloogiteenuse süsteemi korrakohase taaskäivitamise.
- Hädaolukorraks valmisoleku plaani koostamisel tuleks arvestada olulise tähtsusega kataloogiteenuse serverite omapärasid ning need plaani kaasata.

Hädaolukorraks valmisoleku plaani koostamisel tuleks arvestada erinevate olukordadega, millesse sattudes toimub kataloogiteenuse süsteemi või selle osaline kompromiteerimine. Nimetatud olukordade tekkimise puhuks tuleks hädaolukorraks valmisoleku plaanis võimalikult täpselt kirjeldada, kuidas mingil juhul tuleb reageerida ning millised toimingud tuleb läbi viia. Olukordadele reageerimist tuleks regulaarselt harjutada.

Õigeaegne etteantud tegevusjuhistega hädaolukorraks valmisoleku plaani koostamine, mida on võimelised läbi viima ka isikud, kes ei ole kursis süsteemi haldamisega, võib aidata avarii korral selle tagajärgi leevendada. Tuleb silmas pidada, et kuna avariiolukorra dokumendid sisaldavad tähtsat ja konfidentsiaalset informatsiooni, tuleb neid turvaliselt säilitada.Vaatamata sellele peavad volitatud isikud omama neile hädaolukorras juurdepääsu.

Üksikasjalikult tuleks vaatluse alla võtta vähemalt järgmised hädaolukorrad:

Ründed

Kui paljastatakse ründed kataloogiteenusele, mille põhjuseks võib olla kasutajaõiguste laiendamine, ei saa detailse turvaanalüüsita lähtuda sellest, et ründe põhjuseks oleva konto kustutamine taastab ründest puudutatud süsteemide turvalise seisundi. Pigem tuleb pöörata tähelepanu asjaolule, et on läbi viidud süsteemi konfiguratsiooni muudatused või installeeritud kahjurprogrammid (nt tagauksed, Trooja hobused). Võimalike kahjurprogrammide usaldusväärseks eemaldamiseks soovitatakse kahjustatud kataloogiteenuse komponendid täielikult taastada, et tagada usaldusväärne baas.

Selleks tuleb kasutada varundatud andmeid, aga ka salvestusi täpse konfiguratsiooni kohta ning kataloogiteenuse turvasuuniseid. Lisaks tuleb kontrollida vähemalt kõigi laiendatud õigustega kontode (eriti puudutab see administraatorite gruppe) grupikuuluvust ning varustada need viivitamata uute paroolidega, et minimeerida võimalike järgnevate rünnakute õnnestumist. Ka kasutajakontode paroolid tuleks muuta. Lisaks tuleb tegelda põhjuste uurimisega ning tulemused ja kogemused olemasolevasse turvakontseptsiooni sisse viia.

Vargus

Kataloogiteenuse komponentide varguse korral tuleb viivitamata kõik kontod, eriti laiendatud õigustega kontod, varustada uute paroolidega. Lisaks on ka siinjuures vajalik teostada põhjalik turvaanalüüs ja selgitada välja põhjused ning saadud tulemuste põhjal eelkõige läbi viia infrastruktuuri turvaeeskirjade laiaulatuslik kohandamine. Kahtluse korral tuleks kogu kataloogiteenuse struktuur uuesti käivitada. Nii toimunud ründe kui ka varguse puhul tuleb vastutavaid isikuid informeerida turvakontseptsioonis tehtud parandustest ning nõuda nende täitmist.

Väär konfigureerimine

Süsteemihalduse väär konfigureerimine võib hakata avaldama negatiivset mõju kataloogiteenuse kogustruktuurile. Kataloogiteenuse süsteeme tuleks regulaarselt väära konfigureerimise suhtes kontrollida. Niipea, kui midagi taolist avastatakse, tuleb anda hinnang selle ulatusele ning võtta kasutusele parandusmeetmed. Vajalikud muudatused konfiguratsioonivigade kõrvaldamiseks võib vastavalt ver-

sioonile läbi viia kohe, kuid suuremate probleemide korral tuleb taastada süsteemi olemasolevad varundatud andmed kuni süsteemi uuesti installeerimiseni. Kui väära konfigureerimise mõju või põhjust ei ole võimalik täpselt välja selgitada, on soovitatav taastada kataloogiteenuse usaldusväärne seisund. Et samu probleeme tulevikus vältida, tuleb läbi töötada turvameetmed ning neid vajadusel kohandada. Lisaks tuleb analüüsida testvõrgus ja töökeskkonnas teostatavaid protseduure, et testvõrgus kogutud kogemuste abil minimeerida väljalangemisaegu ja töökeskkonna vääri konfiguratsioone.

Vääramatu jõu poolt põhjustatud tõrked

Vääramatu jõu tõttu tekkivad ohud, näiteks maavärisemine, üleujutused, kahjutuli, tormikahjustused, kahjustatud kaablid, võivad kataloogiteenuse kättesaadavust negatiivselt mõjutada. Teenuse kättesaadavuse parandamiseks tuleks kaaluda sobivate meetmete rakendamist, näiteks varu sideliinide või IT-süsteemide kasutuselevõtmist.

Kontrollküsimused:

- Kas on koostatud vajadustele vastav hädaolukorraks valmisoleku plaan?
- Kas on olemas hädaolukorraks valmisoleku plaanid olulise tähtsusega kataloogiteenuse süsteemide tõrke puhuks?
- Kas kõik protseduurid kataloogiteenuse komponentide tõrke puhuks on dokumenteeritud?
- Kas hädaolukorraks valmisoleku plaan on viidud vastavusse kataloogiteenuste andmevarunduspoliitikaga?

M 6.107 Kataloogiteenuste andmevarundus

Algatamise eest vastutavad: IT-juht, infoturbe eest vastutav töötaja
Rakendamise eest vastutabvad: administraator

Kataloogiteenuse andmevarundus tuleks integreerida asutuse üldisesse andmevarunduspoliitikasse.

Et hoida ühel serveril kataloogi andmekogu konsistentseid andmevarusid, tuleks kasutada spetsiaalset varundusinstrumenti. Lisaks kataloogi täielikule varundamisele pakuvad instrumendid ka võimalust kataloogiteenuse osaliseks varundamiseks. Kataloogiteenuse objektide arhiveerimiseks või taastamiseks tuleb spetsifitseerida objekti täielik eraldusnimi. Kogu puu varundamiseks tuleb ära märkida vastav puuobjekt. Skeemi eraldi varundamiseks on vaja välja valida skeemi objekt. Lõpuks on võimalik varundada ka kataloogiteenuse puu osad, selleks on vaja valida vastav puu ümbris.

Seejärel toimub kõigi selle ümbrise alla kuuluvate objektide varundamine. Partitsioonide infot ei saa nende varundusseadmetega varundada. Taaste korral tuleb vastavad osad tagantjärele sektsioneerida. Seepärast tuleb kataloogiteenuse partitsioonide loomine kirjalikult dokumenteerida, et seda oleks süsteemi tõrke korral võimalik käsitsi taastada. Selleks otstarbeks tuleks kindlasti valmistada puustruktuuri ja partitsioonide trükitud koopiad ning neid regulaarselt uuendada.

Kontrollküsimused:

- Kas kataloogiteenuse andmevarundus toimub vastavalt olemasolevale andmevarunduskontseptsioonile?
- Kas kataloogiteenuse partitsioonide loomine on kirjalikult dokumenteeritud, et seda oleks võimalik süsteemi tõrke korral käsitsi taastada?

M 6.108 Domeenikontrollerite andmevarundus

Algatamise eest vastutavad: IT-juht, vastava ala spetsialist

Rakendamise eest vastutavad: administraator

Kuna domeenikontrollerid täidavad reeglina tsentraalseid autentimis- ja autoriseerimimisülesandeid juurdepääsuks olulise tähtsusega ressurssidele võrgus, tekitab nende väljalangemine võrgus vahetult raskeid kahjustusi. Seetõttu tuleb domeenikontrollerite kui tsentraalsete IT-komponentide andmevarunduse läbiviimiseks kindlaks määrata sobivad protseduurid. Need tuleks dokumenteerida kas asutuse andmevarunduskontseptsioonis või omaette andmevarundussuunistes (vt B 1.4 Andmevarunduspoliitika). Lisaks domeenikontrollerite eripärale tuleb andmevarundussuuniste väljatöötamisel arvestada ka *Active Directory* eripäraga. Nimetatud reeglistikus tuleb pöörata tähelepanu järgmistele aspektidele:

- Domeenikontrolleritel tuleb regulaarselt ja arusaadavalt läbi viia andmevarundus
- Andmevarunduseks ei tohiks kasutada üleorganisatsioonilisi üldisi kasutajakontosid
- Andmevarundussüsteemid tuleks paigaldada vaid kohtadesse, kus on tagatud riistvara ja andmekandjate turvalisus
- Vajalik on regulaarselt testida, kas domeenikontrollereid saab varundusandmekandjate kasutamisel taastada
- Väljapraagitud varundusandmekandjad tuleb hävitada.

Erinevalt tavapärasest serverite varundusest tuleks domeenikontrollerite puhul arvestada ka järgmiste aspektidega:

- Väljalangenud domeenikontrolleri taastamine toimub harva vaid varundusandmekandjate abil. Õigustanud on end domeeni liikmele domeenikontrolleri õiguste andmine ning sellele järgnev *Active Directory* andmete replikeerimine teiselt domeenikontrollerilt. Seda meetodit saab kasutada vaid juhul, kui mitmete domeenikontrollerite kasutamise tõttu pärast ühe või mitme süsteemi väljalangemist on olemas vähemalt veel üks kehtiv *Active Directory* duplikaat.
- Kui on olemas vaid üks domeenikontroller või ei ole pärast domeenikontrolleri väljalangemist enam ühtegi *Active Directory* duplikaati, peab taastamine toimuma varundusandmekandjate kaudu. Seejuures tuleb jälgida, et teatud juhtudel võivad vastutavatele isikutele tekitada probleeme vigased varundusandmekandjad, mittetäielikud taastamisprotseduurid või puuduvad teadmised protseduuridest. Nende probleemide ületamiseks tuleb tagada, et administraatorid kogustruktuuri taastamisprotseduuridega tuttavad.

Sobiva varundustarkvara valik

Kui andmevarundusprogramm ei käsitle varundavate failide metaandmeid korrektselt, võib selle tagajärjeks olla, nagu ebasobivate viirusetõrjeprogrammide kasutamise korral, liigne failide kopeerimine *File Replication Service* (FRS) (vt G 4.68 Ebavajalikust replikeerimisest tingitud tõrked Active Directory töös). Seetõttu

on sarnaselt viirusetõrjeprogrammi kasutamisele (vt M 2.414 Domeenikontrollerite kaitse arvutiviiruste eest) andmevarundustarkvara valikul ülimalt tähtis jälgida, et domeenikontrollerite andmevarunduseks kasutataval tarkvaral oleks tootjapoolne kasutusluba.

Kõrgendatud turvanõuded

Teenuskontol, millega domeenikontrollerid varundatakse, peavad olema teenuste administraatori õigused ning seega väga suured õigused. Nende õiguste kuritarvitamise vältimiseks peaks kasutajate ring, kellel on juurdepääs nendele kontodele, olema võimalikult väike.

Domeenikontode kasutamine andmete varunduseks

Seetõttu on soovitatav kasutada varundusagendi jaoks domeenikontrolleritel teisi teenuskontosid kui asutuse ülejäänud serveritel. Erinevad kasutajakontod domeenikontrolleritel ja teistel serveritel kaitsevad domeenikontrollerit ka juhul, kui organisatsiooni tavakohane serverit kompromiteeriti. Lisaks peaksid grupi „Varundusoperaatorid" liikmeteks olema vaid kasutajad, kes on vajalikud süsteemifailide andmevarunduse läbiviimiseks. Kasutajad, kes vastutavad rakendusandmete varundamise eest, ei tohiks olla domeenikontrolleri grupi „Varundusoperaatorid" liikmeteks. Pigem tuleks need kasutajad registreerida vastava rakendusserveri lokaalse grupi „Varundusoperaatorid" liikmeteks. Domeenigrupp „Varundusoperaatorid" ei ole standardile vastavalt eriti kaitstud. Et saavutada vajalikku kaitset, tuleb juurdepääs vastavale *AdminSDHolder* -objektile (konteinerobjekt volituste salvestamiseks) võimalikult kitsalt reglementeerida.

Varundamise sagedus

Domeenikontrollerite andmevarundus peab toimuma regulaarsete vaheaegade järel. Sobiva varundamissageduse kindlaksmääramisel tuleb jälgida, et kustutamiseks markeeritud *Active Directory* objekte ei eemaldata sellest otse, vaid paigutatakse kõigepealt *Active Directory* spetsiaalsesse konteinerisse („Kustutatud objektid"). Selliseid kustutamiseks markeeritud objekte nimetatakse vananenud või ka *Tombstone*- objektideks. Seadistatava ajavahemiku möödudes (standard – 60 päeva) kustutatakse vananenud objektid jäädavalt. Selle protseduuri eeliseks on asjaolu, et ekslikult kustutatud objekte on kindlaksmääratud aja jooksul võimalik uuesti aktiveerida. Kustutamisel konto deaktiveeritakse ning seda ei ole enam võimalik kasutada. Kui selgub, et konto on ennatlikult kustutatud, on seda võimalik kiiremini taastada. Et vältida kopeerimisel probleeme, tuleb jälgida, et varundatud andmed ei sisaldaks või sisaldaksid võimalikult vähe vananenud objekte, mille eluiga on ületatud. Selle tagamiseks tuleks varundusandmekandjad, kui vanade objektide eeldatavast elueast on läbi 75%, regulaarse varundamise käigus üle kirjutada. Ühesõnaga, neid tuleks võimalikult sagedasti varundada - *Backup* -andmekandjad tuleb iga 45 päeva tagant (kui objekti eluiga on 60 päeva) uuesti üle kirjutada, et välistada vananenud objektide taastamist.

Varundusandmekandjate turvaline säilitamine

Kuna domeenikontrollerite varundusandmekandjad sisaldavad *Active Directory* andmebaasi kogu informatsiooni, tuleks nende kaitseks rakendada samasuguseid füüsilisi turvameetmeid nagu domeenikontrollerite puhul (vt M 4.313 Turvaliste domeenikontrollerite kasutuse võimaldamine , lõik *Füüsiline turvalisus*). Eriti filiaalides tuleb varundamise läbiviimisel üle kontrollida, kas on võimalik tagada varundusriistvara ja –andmekandjate turvalisus. Selleks võib kasutada järgmisi võimalusi:

- Filiaalides ei viida läbi domeenikontrollerite andmevarundust

- Andmevarundus filiaalides toimub *Remote* -varundussüsteemide (*Offline* andmekandjad) abil turvalistesse arvutuskeskustesse
- Andmevarundus filiaalides toimub lokaalse varundusena andmekandjatel (*Online* andmekandjad)

Neid võimalusi tuleb kontrollida lähtudes administratiivsete kulutuste suurusest, taastamisaja hilinemisest ja turvalisuse tagamisest. Varundusandmekandjate seisundit ja kõlblikkust tuleb regulaarsete vaheaegade järel kontrollida - selleks viiakse läbi andmete taastamine.

Remote -andmevarundus

Andmete muutmise või varguse vältimiseks tuleb kohapeal kasutatavaid varundusandmekandjaid säilitada turvalises ning valve all olevas kohas. Andmekandja ise tuleb asetada vastavasse draivi vaid andmete varundamise ja taastamise ajaks. Samuti tuleks kindlaks määrata protseduurid, mis sisaldavad nõuet volitatud administraatorite allkirja kohta arhiivivarundusmeediate tagastamisel.

Piirdumine turvaliste asukohtadega

Kui domeenikontrollerid asuvad erinevates kohtades (näiteks haruettevõtetes), tuleks kasutada andmevarundusmeetodeid, mis võimaldavad *Backup* -protseduuri ja selleks vajaminevate andmekandjate sobivat varundamist. Tuleb jälgida, et olenemata asukohast rakendataks andmevarunduskontseptsiooni sobivalt kõikide domeenikontrollerite suhtes. Kui mingis kohas näiteks ei ole varundusandmekandjate jaoks turvalist hoidmisvõimalust, tuleks varundusandmekandjad toimetada selleks sobivasse ja kindlasse kohta. Filiaalide jaoks on mõeldavad *Remote* -lahendused, mille puhul varundatavad andmed kogutakse võrgu kaudu kokku tsentraalsesse kohta. *Remote* -lahenduse korral tuleb pöörata tähelepanu pöörata järgmistele punktidele:

- Andmete tervikluse ja konfidentsiaalsuse kaitseks võrgu kaudu edastamisel tuleb rakendada sobivaid meetmeid, näiteks varundatavate andmete krüpteerimist enne edastamist või selle ajal
- Käsutuses peab olema küllaldaselt ribalaiust, nii et *Remote* -varundamisprotsessi ajal ei oleks häiritud ei töö ega andmevarundus
- Kui kõigepealt viiakse andmevarundus läbi kohapeal ning seejärel kogutakse varundusandmekandjad ühte tsentraalsesse kohta kokku, tuleb kehtestada juurdepääsureeglid, näiteks tuleb juurdepääs vahesalvestusega varundatud failidele võimaldada vaid domeeniadministraatoritele.

Järk-järguline varundamine

Salvestusruumi säästvaks andmevarunduseks kasutatakse süsteemifailide puhul tihti järk-järgulist andmevarundust. Selle meetodi puhul salvestatakse vaid failid, mis on pärast viimast andmevarundust muutunud. Taastamine on selle meetodi puhul siiski seotud suurema ajakuluga. Järk-järgulist andmevarundust ei tuleks domeenikontrollerite puhul kasutada, selline on ka tootja soovitus.

Taastamismeetodid

Kui siiski luuakse järk-järgulisi andmevarusid, kuuluvad varundamisele ainult pärast viimast täielikku varundamist uuesti loodud andmed. Vanemaid andmekogusid ei varundata. Üksikutel juhtudel võib kehtida nõue varem varundatud andmete taastamiseks ja vastavate koopiate tegemiseks, näiteks *Rollback* -aktsiooni käigus. Sellised andmed võib utiliidi *ntdsutil* abil koopia tegemiseks prioriseerida.

Prioriseerimisel määratakse kindlaks, millised andmed varundusest taastatakse või millised andmed tuleb säilitada. Andmete prioriseerimine tuleb läbi viia hoolikalt, kuna vastasel korral võib esineda kogustruktuuri ebakõlasid, näiteks võib juhtuda, et blokeeritud või mittekehtivad kasutajakontod muutuvad jälle kasutatavaks.

Domeenikontrollerite andmevarundus ja taastamine piltide loomise abil ei ole soovitatav, sest *USN-Rollback* (*Update Sequence Number Rollback*) kasutamisel võivad tekkida ebakõlad.

Andmevarunduse regulaarne kontroll

Et varundatud andmed oleks kättesaadavad ka hädaolukorras, tuleb pärast iga varundusprotsessi kontrollida, kas see kulges vigadeta. Kõikides domeenides tuleks regulaarselt läbi viia andmevarunduse kontroll, et garanteerida kolm aspekti:

- Tuleb tagada, et vastaval nädalal viidaks edukalt läbi piisav domeenikontrollerite varundus.
- Tuleb garanteerida, et loodud varundusandmekandjad pealkirjastataks selgelt domeenikontrolleri üheselt mõistetava nimetuse ja andmevarunduse kuupäevaga ning säilitataks seejärel turvaliselt. Seejuures peaks varundusandmekandjate pealkirjastamine andma informatsiooni ka domeenikontrolleri funktsiooni kohta, et kergendada hilisemat identifitseerimist.
- Ebaõnnestunud andmevarunduse korral tuleb viga võimalikult kiiresti kõrvaldada.

Seejuures tuleb regulaarselt testida, kas varundatud andmeid on võimalik taastada. Eduka kontrolli läbinud *Backup* -andmekandjad tuleb vastavalt tähistada. Testimine tuleb läbi viia eraldatud testimiskeskkonnas, mis on töökeskkonnast eraldatud.

Täiendavad kontrollküsimused:

- Kas on olemas domeenikontrollerite andmevarundus- ja taastamissuunised? Kas administraatorid on nende suunistega tuttavad?
- Kas kasutatavat varundustarkvara on selgesõnaliselt lubatud kasutada domeenikontrollerite andmevarunduseks?
- Kas domeenikontrolleritele on sisse seatud eraldi teenuste administraatori õigustega andmevarunduskonto? Kas grupi „Varundusoperaatorid” liikmete arv on viidud miinimumini?
- Kas juurdepääs AdminSDHolder -objektile on piisavalt reglementeeritud?
- Kas domeenikontrollerite andmevarundus toimub regulaarselt ning kas seejuures loobutakse järk-järgulisest andmevarundusmeetodist?
- Kas varundusandmekandjaid säilitatakse sobivas ja turvalises kohas?
- Kas varundusandmekandjate seisundit ja kõlblikkust kontrollitakse regulaarselt?
- Kas andmevarunduse korrektset kulgu kontrollitakse regulaarsete vaheaegade järel? Kas varundatud andmete taastamist testitakse regulaarselt testimiskeskkonnas?

M 6.109 Virtuaalse privaatvõrgu (VPN) hädaolukorraks valmisoleku plaan

Algatamise eest vastutavad: IT-juht, infoturbe eest vastutav töötaja

Rakendamise eest vastutavad: administraator

Olenevalt käideldavusnõuetest võivad virtuaalse privaatvõrgu tõrkel olla rasked tagajärjed. Kahjude vältimiseks või tekkinud kahjude vähendamiseks tuleb käideldavusele esitatavate nõuetega arvestada juba virtuaalse privaatvõrgu süsteemiarhitektuuri defineerimisel. Virtuaalse privaatvõrgu hädaolukorraks valmisoleku plaan on ootamatult tekkinud hädaolukorras (nt füüsiline purustamine, volitamata juurdepääs) juhtnööriks ning see peaks aitama asutusel säilitada ülevaadet hädaolukorras teostatavatest toimingutest. Virtuaalse privaatvõrgu avariiplaan tuleb integreerida olemasolevasse hädaolukorraks valmisoleku plaani (vt B 1.3 Hädaplaanimine). Selleks tuleb kindlaks määrata esmaste meetmete protseduurid ja definitsioonid, et oleks võimalik kiiresti üle minna operatiivsele tööle.

Asukohtade, äriprotsesside või organisatsiooniüksuste prioriseerimise kohaselt tuleb luua individuaalsed virtuaalse privaatvõrgu plaanid, milles kujutatakse olukorrale vastavaid spetsiifilisi asjaolusid.

Virtuaalse privaatvõrgu hädaolukorraks valmisoleku plaani koostamisel tuleb arvestada järgmisi aspekte:

- Millised konkreetsed häired, kahjustused ja kaudsed kahjud kaasnevad virtuaalse privaatvõrgu tõrkega?
- Millised virtuaalse privaatvõrgu ühendused peavad olema kõrge käideldavusega?
- Kui kiiresti on võimalik kindlaks määrata virtuaalse privaatvõrgu tõrget?
- Kas ühendamiseks kasutatud sidevõrkude vigu on võimalik kiiresti avastada? Kas nendest teatatakse vastutavale administraatorile (näiteks probleemid ühenduse saamise, telefoninumbrite edastamise või suletud kasutajagruppide lülitamisega)?
- Kui kiiresti on võimalik virtuaalse privaatvõrgu ühendusi erinevates tõrkeolukordades taastada (seadmete asendamine, süsteemi üleslaadimine)?
- Milliste komponentide väljalangemisel tuleb virtuaalne privaatvõrk välja lülitada, kuigi tehniliselt on võimalik virtuaalse privaatvõrgu ühendusi luua (nt logimise, kommunikatsiooni krüpteerimise või autentimisserveri väljalangemisel)?
- Kas virtuaalse privaatvõrgu haldamiseks hädaolukorras on küllaldaselt kvalifitseeritud personali?

Avariiplaani sisu

Kahjustuste käsitlemiseks oleks vaja välja töötada sobivate protseduuridega avariiolukorra juhend. Sellesse tuleks koondada kõik avariiolukorra kõrvaldamiseks vajalikud andmed ja kujutada neid sellistena, et nendega tuleks toime

ka asenduspersonal. Hädaolukorra juhend peaks lisaks sisaldama informatsiooni alternatiivsete ühenduskanalite, näiteks alternatiivsete sideteenuste tarnijate või ülekandevahendajate kohta.

Vastutusalad hädaolukorrakorras

Personaalsed võtmepositsioonid ja nende ülesanded ning õigused tuleb defineerida ja dokumenteerida (vt M 6.59 Turvaintsidentide käsitlemise eest vastutavate isikute määramine).

Hädaabinumbrite sisseseadmine

Töötajatele, eelkõige mobiilsetele töötajatele ja kaugtöötajatele tuleks teatavaks teha hädaabinumber, et nad saaksid virtuaalse privaatvõrgu probleemidest kiiresti vajalikku kohta teatada. Lisaks sellele peaks virtuaalne privaatvõrk olema kriitilistel aegadel (nt büroo lahtiolekuaegadel ja aegadel, mil peamine andmevahetus toimub virtuaalse privaatvõrgu kaudu) pideva järelevalve all.

Varu-sidekanalid

Olenevalt asukohtade ja nende ärikriitiliste rakenduste prioriseerimisest võib olla vajalik esitada käideldavusele kõrgendatud nõudeid. Kõrgendatud nõuete korral peavad tõrke tekkimisel olema käepärast sekundaarühendused. Sekundaarühendust kasutatakse vaid tõrke puhul ja selleks võib kasutada näiteks DSL- või ISDN-ühendusi. Meetmes M 6.18z Varuliinid pakutakse täiendavaid nõuandeid korrakohaseks realiseerimiseks.

IP-kõne varukomponendid

Olenevalt asukoha käideldavusele esitatavatest nõuetest võib virtuaalse kohtvõrgu komponendi tõrge põhjustada tõsisemaid või vähemtõsiseid probleeme. Virtuaalsele kohtvõrgule esitatavate kõrgete käideldavusnõuete korral peavad vastavad varud olema käepärast.

Seda on nõuete kohaselt võimalik saavutada näiteks järgmiste mehhanismide abil:

- klasterdamine (mitmed võrgustatud komponendid käideldavuse tõstmiseks),
- töötav reserv (initsialiseeritud varuseadmete valmispanek) või
- reserv (väljalülitatud varuseadmete valmispanek).

Eriti tsentraalsete VPN-komponentide, näiteks kaugligipääsu VPN-serverite puhul tuleks kontrollida, kas varuga paigaldamine on vajalik. Informatsiooni edastamine virtuaalse privaatvõrgu kaudu toimub üldjuhul krüpteeritult. Seejuures tuleb jälgida, et krüpteerimiseks peavad olemas olema vastavad varuvõtmed või tuleb genereerida uued võtmed. Nimetatud aspektiga tuleb võtmete haldamisel arvestada. Virtuaalse privaatvõrgu vigade põhjuseks võivad olla mitmesugused allikad, seepärast võib ka meetme M 6.53z Võrgukomponentide liiasus rakendamine aidata kaasa väljalangemisohu vältimisele.

Taasteplaani koostamine

Tööprotsessi võimalikult kiire taastamise tagamiseks tuleb iga kasutuses oleva virtuaalse privaatvõrgu jaoks koostada taasteplaan. Selleks tuleb kindlaks määra-

ta ja dokumenteerida vajalikud etapid. Defektsete VPN-komponentide probleemideta väljavahetamiseks on vaja, et vastavatest konfiguratsiooniandmetest oleks olemas värske varukoopia (vt M 6.52 Võrgu aktiivkomponentide konfiguratsiooniandmete regulaarne varundamine). Tööprotsessi taastamisel tuleb tagada ka andmete järjepidevus.

Andmete tervikluse kontroll pärast tõrget

Ühe või mitme VPN-komponendi süsteemi krahhi või virtuaalse privaatvõrgu muu tõrke korral ei ole enam võimalik garanteerida selle kaudu edastavate andmete järjepidevust. Seetõttu tuleks pärast igakordset tõrget kontrollida nende andmete terviklust ning läbi viia probleemi analüüs, et vältida tõrgete kordumist.

Avariikonfiguratsioon

Teatud situatsioonides võib osutuda vajalikuks virtuaalse privaatvõrgu käitamine piiratud funktsionaalsuse ja jõudlusega. Sel juhul tuleb aktiveerida avariikonfiguratsioon (vt M 4.320 VPNi turvaline konfigureerimine). Seda on vaja selleks, et säilitada virtuaalse privaatvõrgu turvalisus (turvaline pöördus ja pääs, kommunikatsiooni turvalisus) ka piirangutega käitamise korral. Selleks peab eelnevalt olenevalt asukohtade prioriseerimisest olema kindlaks määratud tööprotsessid või organisatsiooniüksused ning see, millistes situatsioonides millise VPN-avariikonfiguratsiooni kasuks otsustatakse.

Valmisolekuharjutuste läbiviimine

Parimastki taasteplaanist on vähe kasu, kui see ei ole praktikas otstarbekas. Seetõttu on eriti tähtis regulaarsete avariiolukorraks valmisoleku harjutuste läbiviimine, et oleks võimalik probleeme ära tunda ja lahendada. Seejuures tuleb tagada VPN-taaste kontrollitav logimine. Kõikide varusideliinide VPN-varukomponentide, andmevarundusseadmete, varundusandmekandjate ja sekundaarliinide funktsionaalsust tuleb regulaarselt kontrollida. Ka vastutavatele isikutele on harjutamise ja teadlikkuse tõstmise meetmetest kasu ning nad suudavad tõsise häire korral kiiremini ja efektiivsemalt reageerida. Virtuaalse privaatvõrgu hädaolukorraks valmisoleku plaan tuleb kohandada asutusespetsiifilise olukorraga ja kujundada selliselt, et kriitilised tööprotsessid oleksid vajaliku aja jooksul teostatavad.

Virtuaalse privaatvõrgu hädaolukorraks valmisoleku plaan peab olema selliselt koostatud, et seda oleks võimeline ellu viima kompetentne kolmas isik. Pidevate tehniliste, organisatoorsete ja personaalsete muutuste tõttu tuleb virtuaalse privaatvõrgu hädaolukorraks valmisoleku kontseptsioon hoida alati ajakohasena.

Kontrollküsimused:

- Kas on olemas ajakohane avariiplaan virtuaalse privaatvõrgu tõrke puhuks?
- Kas on kindlaks määratud, milliseid käideldavusnõudeid esitatakse erinevatele VPN-ühendustele?
- Kas on defineeritud ja dokumenteeritud, kellel on hädaolukorras millised ülesanded ja volitused virtuaalse privaatvõrgu tööks?
- Kas töötajatele antakse hädaabinumber, mille kaudu nad saavad virtuaalse privaatvõrgu probleemidest teatada?

- Kas tehnilised varud vastavad virtuaalse privaatvõrgu kindlaksmääratud käideldavusnõuetel?
- Kas hädaolukorras on virtuaalse privaatvõrgu taastamiseks olemas piisavalt kvalifitseeritud personali?
- Kas virtuaalse privaatvõrgu taastamiseks vajalikud etapid on kindlaks määratud ja dokumenteeritud?
- Kas on olemas konfiguratsiooniandmete värske varunduskoopia?
- Kas toimub regulaarne virtuaalse privaatvõrgu hädaolukorraks valmisoleku harjutamine?

M 6.110 Kehtivusala ja hädaolukorrahalduse strateegia määratlemine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond

Rakendamise eest vastutavad: ametiasutuse või ettevõtte juhtkond, avariiametnik

Hädaolukorra mõiste

Hädaolukord on kahju tekitav olukord, kus institutsiooni protsessid või ressursid ei toimi nii, nagu nad peaksid toimima. Vajalike protsesside ja ressursside käideldavust ei õnnestu selleks ette nähtud aja jooksul taastada. Igapäevased tööprotsessid on tugevalt pärsitud. Võimalikke teenusetasemeleppeid (service-level agreements, SLA) ei suudeta täita. Tekivad suured kuni väga suured kahjud, mis mõjutavad märkimisväärselt ja vastuvõetamatult suurel määral ametiasutuste ülesannete täitmist. Hädaolukordade kõrvaldamiseks ei piisa enam igapäevastest tööprotsessidest. Nende kõrvaldamiseks läheb tarvis eraldi hädaolukordade likvideerimiseks mõeldud töökorraldust. Hädaolukordade haldusest saab lähemalt lugeda BSI standardist 100-4, mille leiate Riigi Infosüsteemi Ameti veebilehelt ISKE alajaotuse dokumentide rubriigi alt.

Hädaolukorra halduse süsteemi algatamise esmane ülesanne on kehtivusala ja halduse strateegia määratlemine. Need kõikide edasiste halduse tööde aluseks olevad sammud peab algatama ja ellu viima institutsiooni juhtkond. Kui hädaolukorrahalduse jaoks on kontaktisik (hädaolukorraülem) juba määratud, abistab ta institutsiooni juhtkonda selle ülesande elluviimisel.

Hädaolukorrahalduse süsteemi kehtivusalasse võib kuuluda kogu institutsioon või ainult mõni selle allüksus. Kehtivusala peaks olema suletud, kuid mitte liiga kitsalt piiritletud, ja peaks sisaldama täielikult väärtuseid loovaid tööprotseduure või olulisi erialaseid ülesandeid, olulisemaid ressursse ning vajalikke toetavaid tööprotseduure. Hädaolukorrakontseptsioonile tuleb kasuks see, kui institutsiooni juhtkond nimetab oma vaatepunktist olulised institutsiooni teenused ja/või tooted. Näiteks kui selle kehtivusala piires jäetakse teatud tööprotseduurid selgelt välja või vaadeldakse neid teatud piirangutega, tuleb see ka vastavalt dokumenteerida. Kuna halduse esmane eesmärk on institutsiooni ellujäämisvõime tagamine ja stabiliseerimine, tuleks püüelda selle poole, et haldus käsitleks tervet institutsiooni. Ainult sel moel on võimalik tagada, et institutsiooni imago ja väärtuseid loovad tegevused ning seega ka oluliste huvigruppide huvid oleksid tõhusalt kaitstud. Hädaolukorrahalduse süsteemi juurutamise järgmiste sammude aluseks on mõistete „hädaolukord", „kriis" ja „hädaolukorrahaldus" määratlemine institutsioonis.

Üksiku tööprotseduuri või terviksüsteemi peatumine võib institutsiooni jaoks olla tõrge, hädaolukord või lausa kriis. Kuna iga institutsiooni piirid on erinevad ning sõltuvad tööprotseduuride ja IT-süsteemide kaitsevajadusest, tuleks institutsioonis need mõisted üldjoontes ära defineerida. Ka hädaolukorrahalduse mõiste vajab täpsustamist. Tuleb kindlaks määrata, millised on haldussüsteemi ülesanded ja võimalused, et võimaldada nende eraldamist institutsiooni teistest loodud haldussüsteemidest ja viimaste liidestest.

Hädaolukorrakontseptsiooni raamistiku määratlemiseks tuleb piiritleda hädaolukorrahalduse strateegia (lühidalt hädaolukorra strateegia), millega tuleb arvestada haldussüsteemi juurutamisel.

Institutsiooni juhtkond peab seega määratlema selged punktid, näiteks

- millised on halduse juurutamise sihid (nt oluliste huvigruppide nõuded),
- milliseid on haldusele esitatavad nõuded,
- milline on valmidus riskida või kui kõrge on riskidega leppimise tase ettevõttes/ametkonnas,
- milliseid katkestusi peetakse tootmises jätkusuutlikkust ohustavaks,
- millisel viisil ja kui intensiivselt tuleks võtta vastumeetmeid ja
- millistest seadustest, lepingute sätetest või ettekirjutustest tuleb kinni pidada.

Hädaolukorrahalduse eesmärkide seadmisel tuleks arvestada üldiste tööeesmärkide ja -ülesannetega ning nende toetamisega. Nende määratlemisel tuleb arvestada ka teiste haldussüsteemide eesmärkidega, eriti aga turvahaldussüsteemi omadega.

Kontrollküsimused:

- Kas hädaolukorrahaldussüsteemi kehtivusala on selgelt määratletud?
- Kas institutsiooni juhtkond on määratlenud hädaolukorrahalduse strateegia, mis iseloomustab institutsiooni sihte ja riskiga leppimise taset?

M 6.111 Hädaolukorrahalduse ja juhtkonnapoolse koguvastutuse võtmise poliitika

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond

Rakendamise eest vastutavad: ametiasutuse või ettevõtte juhtkond, hädaolukorraülem

Hädaolukorrahalduse poliitikaga määratakse halduse kontseptsiooni ja rakendamise selge raamistik. Selles dokumenteeritakse institutsiooni hädaolukorrahalduse olulisemad punktid. Ametkonna/ettevõtte juhatuse kõrgeim tasand näitab sellega, et võtab enda kanda vastutuse halduse eest ja seisab kõikide nõuete ja protseduuride taga.

Hädaolukorrahalduse poliitika sisu

Poliitika peab olema sõnastatud lühidalt ja täpselt. See peab sisaldama järgmisi aspekte:

- lühike ülevaade sellest, mida mõistetakse hädaolukorrahalduse all,
- haldussüsteemi kehtivusala,
- halduse olulisus institutsiooni jaoks,
- halduse eesmärk,
- strateegia tuum,
- vastutuse võtmine institutsiooni juhatuse kõrgeima tasandi poolt, mis dokumenteeritakse täiendavalt selge, kinnitava allkirjaga.

Lisaks võib poliitika sisaldada alljärgnevat infot või viidata vastavale infole:

- halduse süsteemi sidumine institutsiooni olemasoleva haldussüsteemiga,
- halduse (või selle aluseks oleva standardi) sisseseadmise ja käitamise aluseks olev tegutsemismudel,
- halduse ülesehituse struktuur koos olulisemate rollide ja nende vastutusaladega,
- institutsiooni juhtkonna kohustus haldust optimeerida, kasutades regulaarseid kontrolle, teste ja õppuseid,
- asjakohased seadused, direktiivid ja eeskirjad, millega tuleb arvestada,
- üldine info halduse tulemuslikkuse kontrollimise kohta.

Eesti oludes ei ole mõtet nii mitut deklaratiivset dokumenti luua, seetõttu oleks mõistlik poliitika ja strateegia omavahel ühendada, vt M 6.110 Kehtivusala ja hädaolukorrahalduse strateegia määratlemine .

Halduse poliitikast teavitamine

Institutsiooni juhtkonna kõrgeim aste peab hädaolukorrahalduse poliitika kirjalikult kinnitama. See tuleb edastada kõigile sise- ja välistöötajatele ning vajaduse korral ka koostööpartneritele. See peaks toimuma selliselt, et halduse osatähtsus institutsioonis oleks selgesti mõistetav.

Halduse poliitika täiendamine

Selle ajakohasuses veendumiseks tuleb halduse poliitikat regulaarselt ja kindlaksmääratud ajavahemike tagant kontrollida ning vajaduse järgi muuta.

Nõuete, raamtingimuste, ärieesmärkide, hädaolukorrahalduse strateegia ülesannete muudatused ning igasugused muud muudatused peaksid sisse juhatama ka poliitika kontrollimise ja vajaduse korral uuendamise. Tänapäevaste kiirete muudatuste tõttu nii äri- kui ka IT-valdkonnas tuleks hädaolukorrahalduse poliitikat ajakohastada vähemalt kord kahe aasta jooksul.

Kontrollküsimused:

- Kas juhatus on vastu võtnud kehtiva hädaolukorrahaldust reguleeriva poliitika?
- Kas hädaolukorrahalduse poliitikas on kirjas kogu vajalik info?
- Kas hädaolukorrahalduse poliitikat kontrollitakse regulaarselt ja muudetakse vajaduse järgi?
- Kas hädaolukorrahalduse poliitika on kõigile töötajatele teatavaks tehtud?

M 6.112 Sobiva hädaolukorrahalduse organisatsioonilise struktuuri rajamine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond

Rakendamise eest vastutavad: avariiametnik, ametkonna/ettevõtte juhtkond

Hädaolukorrahalduse organisatsioonilise struktuuri kavandamine ja rajamine

Hädaolukorrahalduse protsessi edukas planeerimine, elluviimine ja tööshoidmine eeldab halduse sobivat töökorraldust. Selleks tuleb kindlaks määrata rollid ja vastavad ülesanded, kohustused, õigused ning kompetentsid. Hädaolukorrahalduse organisatsioonilise struktuuri liik ja ulatus sõltub vastava institutsiooni suurusest, omadustest ja struktuurist. Halduse juurutamisel võib selguda, et institutsioonis on hädaolukorrahalduse teatud aspektide eest vastutavad töötajad juba ametisse määratud, kuid puudub neid kõiki hõlmav struktuur. Sellisel juhul tuleb luua institutsioonile sobiv, kõiki hõlmav hädaolukorrahalduse organisatsiooniline struktuur.

Kuna halduse saab jaotada kahte põhifaasi (hädaolukorra ennetamine ja hädaolukorra lahendamine), jaotub ka organisatsiooniline struktuur kaheks valdkonnaks: hädaolukorra ennetamise töökorraldus ja hädaolukorda lahendav töökorraldus.

Hädaolukorra ennetamise rollid

Hädaolukorra ennetamise organisatsioonilise struktuuriga vastutatakse hädaolukorrahalduse kavandamise, ülesehituse, käigushoidmise ja täiustamise eest.

Hädaolukordasid ennetava töökorralduse kesksed rollid on järgmised:

- ettevõtte või ametkonna juhtkond – vastutab tervet institutsiooni hõlmava hädaolukorrahalduse tagamise eest;
- hädaolukorraülem – igas institutsioonis tuleb luua tsentraalne roll, kes on vastutav hädaolukorrahalduse kõikide vajaduste eest;
- hädaolukorra koordinaator;
- hädaolukorra ennetamise meeskond – ajutine, nõustava rolliga üksus hädaolukorraülema kõrval.

Hädaolukorra kõrvaldamise rollid

Hädaolukorra kõrvaldamise organisatsiooniline struktuur hakkab tööle ajutiselt, ainult hädaolukorra või kriisi korral, ning vastutab avarii kiire ja tõhusa kõrvaldamise ja tavapärase töö taasalustamise eest. See tuleb määratleda, luua ja dokumenteerida enne hädaolukorda.

Hädaolukorrahalduse olulisemad rollid on järgmised:

- kriisiotsuste komitee – suunab hädaolukorda või kriisi strateegiliselt ja langetab kriisistaabi juhataja pädevust ületavaid otsuseid;

- hädaolukorra meeskond – hädaolukorrahalduse operatiivüksused. Nende ülesanne on tööprotseduuride, rakenduste või süsteemide taaskäivitamine ja taastamine.

Hädaolukorrahalduse rollide ja nende ülesannete täpse kirjelduse leiate BSI standardist 100-4 „Hädaolukordade haldus".

Institutsiooni hädaolukorrahalduse struktuuri jaoks määratletud rollid tuleb koos nende ülesannete, kohustuste ja õigustega kontrollitavalt dokumenteerida. Siia alla kuuluvad ka üldised töökirjeldused ja töökorralduslikud reeglid. Nende rollide hõivamiseks tuleks koostada nõuete profiilid. Kõikide rollide jaoks tuleb nimetada kvalifitseeritud töötajad.

Hädaolukorrahalduse organisatsioonilise struktuuri kontrollimine

hädaolukorrahalduse organisatsiooniline struktuur ei saa olla muutumatu. Tööprotseduurid ja raamtingimused muutuvad pidevalt, seega tuleb ka halduse organisatsioonilist struktuuri aeg-ajalt kohandada. Seejuures tuleks näiteks selgitada, kas halduse protseduuride ülesanded ja kompetentsid on selgelt defineeritud, kuid ka seda, kas ülesandeid on võimalik täita plaani kohaselt.

Esmajoones on olulised alljärgnevad punktid:

- vastutavate isikute kontrollimine – regulaarselt tuleb kontrollida, kas kõik vastutavad isikud ja vastutusalad on selgelt määratletud ja kas need toimivad ka reaalselt;
- reeglitest kinnipidamise kontrollimine – regulaarselt tuleb kontrollida, kas halduses kehtestatud juhiseid ja protsesse rakendatakse nii, nagu ette nähtud. Samal ajal tuleb kindlaks teha, kas hädaolukorrahalduse jaoks loodud organisatsioonilised struktuurid vastavad nõuetele;
- protsesside ja töökorralduslike reeglite efektiivsuse hindamine – regulaarselt tuleb kontrollida, kas hädaolukorrahalduse kehtestatud erinevad protsessid ja kohustused on praktikas kasutatavad ja tõhusad;
- juhtkonna antavad hinnangud – eespool loetletud kontrollide tulemustest tuleb regulaarselt teavitada ka juhtkonda. Need aruanded on ühest küljest vajalikud pakiliste või aeganõudvate probleemide lahendamiseks, teisest küljest sisaldavad need ka olulist infot, mida juhtkond vajab hädaolukorrahalduse protseduuride juhtimiseks.

Kontrollküsimused:

- Kas hädaolukorrahalduse rollid on määratletud institutsiooni olude kohaselt ning koos kõigi ülesannete, kohustuste ja kompetentsidega dokumenteeritud?
- Kas kõikide rollide jaoks on nimetatud kvalifitseeritud töötajad?
- Kas organisatsiooni struktuuri kontrollitakse regulaarselt seoses praktilisuse, efektiivsuse ja tõhususega?

M 6.113 Hädaolukorrahalduse jaoks sobivate ressursside eraldamine

Algatamise eest vastutavad: ametiasutuse/ettevõtte juhtkond

Rakendamise eest vastutavad: ametiasutuse või ettevõtte juhtkond, hädaolukorraülem

Hädaolukorrahalduse jaoks püstitatud eesmärkide saavutamine eeldab piisavate ressursside olemasolu. Hädaolukorrahalduse planeerimine, rakendamine, käigushoidmine, hooldamine ja tõhustamine vajab piisavaid ressursse nii finantside kui ka personali näol, samuti sobivat varustust. Ametiasutuse või ettevõtte juhtkond peab neid vahendeid eraldama vajaminevas mahus. Hädaolukorraülem peaks ohupotentsiaalist ja hädaolukorrahalduse ning hädaolukordade kõrvaldamise eesmärkidest ja ülesannetest lähtuvalt koostama vajalike ressursside nimekirja. Ühelt poolt aitab see juhtkonnal otsustada ressursside jagamise üle, kuid samas ka planeerida vajalikke projekte ja kehtestada projektide tähtaegu.

Hädaolukorra eest vastutava isiku määramine

Ilma korralikult toimiva avariihalduse organisatsioonilise struktuurita pole isegi kõige kallimatest tehnilistest lahendustest kasu. Seega peab kõrgeima tasandi juhtkond valima juhtkonna hulgast avariihalduse eest vastutava isiku, kellele antakse vajalikud volitused.

Hädaolukorrahalduse planeerimise, elluviimise, käigushoidmise, hooldamise ja tõhustamise eest vastutava isiku nimetamine.

Kõikide hädaolukorrahalduse jaoks vajalike rollide jaoks tuleb määrata sobivad isikud. Rollid peavad katma kõiki protseduuri faase, alates juurutamisest, planeerimisest, elluviimisest, rakendamisest, hooldamisest ja käigushoidmisest kuni kontrollimiseni välja. Arvestada tuleb ka ajutiselt vajaminevate hädaolukorra- ja kriisihalduse rollidega. Eriti oluline on ametisse nimetada hädaolukorraülem, kes oleks keskne kontaktisik ja kõikide ülesannete vastutav koordinaator.

Hädaolukorrahalduse personaliressursid

Kõigil hädaolukorrahalduse meeskonna töötajatel peab olema piisavalt teadmisi ja oskusi, et tulla toime nende rollide alla kuuluvate ülesannetega. Neil peab olema juurdepääs vajalikele ressurssidele, samuti peab neil olema piisavalt aega oma tööülesannete täitmiseks. Sellega tuleb eriti arvestada juhul, kui töötaja peab hädaolukorra haldamise ülesandeid täitma lisaks oma põhiülesannetele. Ametkonna/ettevõtte juhtkond peab kinnitama hädaolukorra haldamise töökorralduse.

IT kasutuseks vajalike ressursside eraldamine

Kui hädaolukorrahaldus esitab IT-süsteemile täiendavaid nõudeid, tuleb tagada, et IT-süsteemide käitamiseks eraldataks ka piisavaid ressursse. Selleks, et avariihalduse meetmed oleksid tõhusad, tuleb reeglina lahendada esmalt IT-süsteemi käitamise tavaprobleemid (väike eelarve, ülekoormatud administraatorid ja vähestruktureeritud või halvasti hooldatud IT-kooslus).

Juurdepääs välistele ressurssidele

Hädaolukorrahalduse üksikutes faasides, nt kavandamise või hädaolukorra kõrvaldamise ajal, tuleb arvestada kuhjuvate tööülesannetega. Nendega toimetulekuks tuleb kasutada rohkem asutuse- või ettevõttesiseseid töötajaid või välisekspertide abi. Samuti võib puuduvate teadmiste või kogemuste puhul olla mõistlik kasutada ajutiselt ekspertide abi. Selleks, et oleks võimalik vajaminevaid ressursse eraldada, peavad ettevõtte/asutuse enda hädaolukorrahaldamise eksperdid vajaduse tekkimisel sellest juhtkonnale teada andma.

Majanduslikud aspektid

Hädaolukordade haldamise turvastrateegia puhul tuleks juba algusest peale arvestada ka selle majanduslike aspektidega. Planeeritavate haldusmeetmete valimisel tuleks arvestada ka olemasolevate ressurssidega. Kui teatud meetmete võtmiseks pole kas piisavalt finantse, tehnilisi lahendusi või personali, tuleb muuta strateegiat. Kui aga sõnastatud eesmärgid ja olemasolevad finantsilised, tehnilised või personaliressursid on siiski liiga erinevad, tuleb nii eesmärgid kui ka strateegia uuesti põhjalikult läbi vaadata.

Sellistel juhtudel tuleb ebakõladest teavitada ka juhtkonda, et neil oleks vajaduse korral võimalik kasutusele võtta abistavaid meetmeid. Ennetavate meetmete kindlaksmääramisel tuleks alati konkreetselt välja tuua ka nende rakendamiseks vajalik rahaline ja personali puudutav ressurss. Lisaks tuleks kindlaks määrata vastutavad töötajad ja muud kontaktisikud ning kehtestada täpsed ajaplaanid ja materjalid, mida on tarvis soetada.

Kõikide plaanitavate ennetavate meetmete puhul tuleks lisaks dokumenteerida, kas planeeritud ressursid eraldati kokkulepitud ajakava kohaselt ning põhjused, miks on projekti rakendamisel tekkinud kõrvalekaldeid. Ainult niimoodi on võimalik ära hoida rikkeid ja tagada, et kõikvõimalikud parandused oleksid piisavalt jätkusuutlikud.

Kontrollküsimused:

- Kas hädaolukorra haldamise eesmärkide saavutamiseks on olemas piisavad finantsilised, tehnilised ja personaliressursid?
- Kas juhtkonnas on nimetatud hädaolukordade haldamise eest vastutav isik? Kas ametisse on nimetatud hädaolukorraülem? Kas kõigi hädaolukordade haldamise seisukohast vajalike rollide täitmiseks on määratud kompetentsed töötajad?
- Kas hädaolukorraülemal ja hädaolukorra meeskonnal on hädaolukorra haldamise seisukohast vajalike ülesannete täitmiseks piisavalt aega?
- Kas planeeritud ressursid on eraldatud kokkulepitud tähtaja kohaselt? Kas meetmete elluviimisel esines pikemaid viivitusi, mille tõttu polnud pikema aja jooksul võimalik tagada eesmärgiks seatud turbeastet?

M 6.114 Hädaolukorraks valmisoleku kontseptsiooni koostamine

Algatamise eest vastutavad: asutuse/ettevõtte juhatus, hädaolukorraks valmisoleku eest vastutav töötaja

Rakendamise eest vastutavad: hädaolukorraks valmisoleku eest vastutav töötaja

Hädaolukorraks valmisoleku kontseptsioon on vajalik hädaolukorraks valmisoleku strateegia elluviimiseks ning selles kirjeldatakse avariiolukorra lahendamiseks püstitatud eesmärkide elluviimiseks kavandatud protseduure. Hädaolukorraks valmisoleku kontseptsioon hõlmab kogu hädaolukorra haldamise protsessis koostatud dokumentatsiooni. See koosneb kahest olulisest komponendist – hädaolukorraks valmisoleku kontseptsioonist ja hädaolukordade lahendamise käsiraamatust. Nendes kajastatakse mõlemat hädaolukorra haldamise seisukohalt olulist ülesannet – äriprotsesside stabiilsuse tugevdamine, et vähendada kahjustava sündmuse tõenäosust ja asutuse või ettevõtte ettevalmistamine hädaolukorra või kriisiga toimetulekuks, et viia kahjustuste mõju miinimumini. Hädaolukorraks valmisoleku kontseptsioonis kirjeldatakse raamtingimusi ning see sisaldab seoses kontseptsiooniga tekkivat koguteavet, mis ei ole otseselt vajalik hädaolukorra lahendamiseks. Hädaolukorra lahendamiseks otseselt vajalik teave, näiteks kontaktandmed ja tegevusjuhised on toodud hädaolukordade lahendamise käsiraamatus.

Iga konkreetse ettevaatusabinõu puhul tuleb lähtuda hädaolukorraks valmisoleku kontseptsioonist. Seetõttu tuleb seda hoolikalt planeerida ja ellu viia. Alljärgnevalt lühidalt puudutatavaid üksikaspekte kirjeldatakse põhjalikumalt BSI standardis 100-4 „Hädaolukorra haldamine”.

Hädaolukorraks valmisoleku kontseptsiooni koostamise eeldus on põhjalikud teadmised asutuse või hädaolukorra haldamiseks määratud kehtivusala kohta ning äritegevuse põhjalik tundmine. Hädaolukorra halduseks peavad olema kättesaadavad asutuse või ettevõtte põhiandmeid ning ülevaade äriprotsessidest. Ülevaade äriprotsessidest peaks sisaldama ka teavet protsessidevaheliste seoste kohta, samuti infot selle kohta, millised äriprotsessid on vajalikud põhitoodete tootmiseks või põhiteenuste osutamiseks. Äriprotsessi ülevaatesse tuleb kaasata ka väljastpoolt tellitavad protsessid, sõltuvussuhete korral ka tarnijad, koostööpartnerid ja välised teenusetarnijad. Üks esimesi samme kontseptsiooni koostamisel on ärimõjude analüüsi (business impact analyse, BIA) läbiviimine. BIA uurib äriprotsesside katkemise mõju, äriprotsessidele esitatavaid käideldavuse nõudeid ja selleks vajalikke ressursse ning taaskäivitamiseks vajaminevat aega. Asutusele tuleb välja valida sobiv meetod BIA läbiviimiseks, määrata kindlaks valitud meetodi parameetrid ja otsused dokumenteerida.

BIA peaks sisaldama vähemalt järgmisi tööetappe:

- Tuleb läbi viia analüüs ja anda hinnang, millist mõju avaldab asutusele või

ettevõttele äriprotsesside või väärtuskettide katkemine ning millised kahjulikud tagajärjed sellega kaasnevad.
- Äriprotsesside taaskäivitamiseks tuleb identifitseerida ja kindlaks määrata parameetrid. Nende hulka kuuluvad:

1. käideldavuse nõue, mis tähistab üleminekut avariiolukorrast hädaolukorraks;
2. maksimaalselt talutav väljalangemisaeg;
3. taaskäivitumisaeg;
4. taaskäivitumisnivoo ning
5. maksimaalselt lubatav andmekadu.

Lisaks sellele on soovitatav kindlaks määrata maksimaalne lubatav taaskäivitamise aeg või maksimaalne lubatav avariikäituse aeg.

- Äriprotsessid tuleb järjestada taaskäivitamise tähtsuse järgi. Otstarbekaks võib osutuda taaskäivitamise klassidesse jagamine. Seejuures tuleb jälgida, et prioriteedid ja taaskäivitamise ajad oleksid majanduslikult ning olemasolevate rahaliste ja inimressurssidega realiseeritavad. Tähelepanu tuleb pöörata ka äriprotsesside vastastikustele seostele. Tuleb kindlaks määrata, millised äriprotsessid liigitada asutuse jaoks kriitiliste hulka ning kaasata hilisemasse kontseptsiooni koostamisse.
- Vähemalt kriitiliste äriprotsesside korral tuleb kindlaks teha vajalikud ressursid käituseks normaal- ja avariiolukorras, samuti kindlaks määrata vastavate äriprotsesside sõltuvus ressurssidest. Kui tehakse kindlaks nõrgad lülid (single points of failure, SPOF), tuleb need kohe kindlasti tähistada. SPOF-idega tähistatakse ressursse, mille väljalangemine põhjustaks äriprotsessside täieliku seiskumise. Nende suhtes on soovitatav läbi viia kiire meetmete kontroll.
- Ressursside puhul tuleb hinnata nende kriitilisuse astet ning käideldavuse nõuet, samuti tuleb kindlaks määrata taaskäivitamis- või taastootmisaeg.

Hädaolukorra lahendamise eest vastutav töötaja koordineerib ja viib hädaolukorra koordinaatorite kaasabil läbi BIA. Olulise tähtsusega kontakt- ja usutluspartnerid BIA läbiviimisel on äriprotsesside toimimise ja ressursside eest vastutavad töötajad. BIA tulemused peavad olema kirjalikult dokumenteeritud ning ettevõtte või asutuse juhtkonna kinnitatud. Üksikasjalikku informatsiooni võimaliku meetodi kohta BIA läbiviimiseks on kirjeldatud BSI standardis 100-4 „Hädaolukorra haldamine”.

Võimalike äriprotsesside katkemise põhjuste väljaselgitamiseks tuleb läbi viia riskianalüüs. Riskianalüüsi läbiviimiseks tuleb kindlaks määrata eesmärgid ja sobivad meetodid ning need dokumenteerida. Riskianalüüsi läbiviimisel võib olla abi, kui kaasata sellesse ka BIA läbiviimise käigus tuvastatud väljalangemiste mõjud ja vastupidi. Riskianalüüsi tulemusena koostatakse nimekiri olulistest riskidest, mis ohustavad äriprotsesside katkematust, ning asutuse või ettevõtte kriitilistest ressurssidest (vt BSI standard 100-3 „Riskianalüüs IT etalonturbe baasil”).

Iga kindlakstehtud riski suhtes tuleb otsustada, milliseid riskistrateegiaid tuleks

kasutada selle mõju ja esinemistõenäosuse vähendamiseks ja süsteemi väljalangemisaja minimeerimiseks. Selleks et üldiste eesmärkide, kindlaksmääratud kaitsevajaduste ja riskide hindamise põhjal oleks võimalik tuletada vajadus konkreetsete kaitsevajaduste ja taaskäivitamise strateegiate kindlaksmääramiseks, on kasu kriitiliste äriprotsesside ja neid toetavate ressursside tegeliku seisundi kindlaksmääramisest. Võrreldes BIA käigus kindlaksmääratud normväärtusi taaskäivitamiseks ja taastootmiseks, samuti asutuse esialgselt kindlaks määratud riskitaluvust (riskide aktsepteerimise tase) tegelikult realiseeritud taaskäivitus- ja turvameetmetega, tehakse kindlaks olemasolevad lüngad taaskäivitamisel ja riskide haldamisel.

Järelduste tegemiseks tuleb edasises kontseptsioonis kindlaks määrata otstarbekohased meetmed, mis vähendavad kriitiliste äriprotsesside ja nende toimimiseks vajalike ressursside väljalangemist, võimaldavad õigeaegset taaskäivitamist ja taastootmist ning piiravad seega avariiolukorra tekkimisel väljalangemisaja pikkust ja kahjustuse suurust.

Soovitatav on arendada mitmesuguseid strateegia suvandeid avariiolukorrast jagusaamiseks, äritegevuse jätkamiseks ning ressursside taastootmiseks ja –käivitumiseks,

- mis vastavad kindlaks määratud nõuetele äritegevuse jätkamisel, taaskäivitamisel ja taastootmisel,
- millel on otstarbekas kulude ja tulude suhe,
- mille tulemusena tekib omavahel kooskõlas olev üldine lahendus ja
- mis arvestavad seejuures ka tähtsamate huvigruppidega või kaasavad need.

Sobivad strateegiad tuleb välja valida ja otsused dokumenteerida. Seejuures tuleks ka fikseerida, kuidas peab hädaolukorras toimuma koostöö tarnijate, koostööpartnerite või väliste teenusetarnijatega. IT-alased meetmed tuleb samuti infoturbeosakonnaga kooskõlastada. Koostada tuleb hädaolukorra kontseptsioon, mis sisaldab kogu kontseptsiooni puudutavat infot, kaasa arvatud sobivad meetmed riskide haldamiseks ja kiire taaskäivitamise ja taastootmise tagamiseks. Hädaolukordade lahendamise käsiraamat sisaldab infot, mis on otseselt vajalik hädaolukordade lahendamiseks. Nimetatud info hulka kuuluvad muu hulgas äritegevuse jätkamise plaanid, taaskäivitamise ja taastootmise plaanid koos varusüsteemi- ja tagavaraplaanidega ning avariiplaanid kohe kasutatavate meetmete rakendamiseks.

Äritegevuse jätkamise, taaskäivitamise ja taastootmise plaanid sisaldavad kogu infot, mis võimaldab kiiret avariikäitust ning protsesside ja ressursside normaalkäituse taastamist. Plaanid peaksid sisaldama infot taaskäivitusaegade ja -protsesside ning ressursside prioriteetide kohta, samuti igasuguseid taaskäivitamise suvandeid mitmesuguste avariiolukordade puhuks. Viivitamata võetavate

meetmete avariiplaanid peaksid muu hulgas tagama avariist puudutatud inimeste heaolu.

Olenevalt asutuse ülesehitusest ja hädaolukorra haldamise integreerimisest asutuse riskide haldusesse, võib otstarbekaks osutuda kriisistaabi juhendi ja kriisikommunikatsiooni plaani koostamine. Kriisistaabi juhend peaks pakkuma kriisistaabile abi strateegiliste otsuste tegemisel. Kriisikommunikatsioon sisaldab infot kommunikatsiooni liigi ja toimumise kohta massiteabevahenditega, aga ka teiste huvigruppidega, ning kriteeriume, millal ja mis põhjustel kommunikatsioon toimub, samuti kommunikatsioonistrateegiat. Erinevad hädaabiplaanid peavad olema üksteisega kooskõlas.

Iga plaan peab sisaldama järgmist teavet:

- kes vastutab dokumendi eest oma allkirjaga;
- milline on plaani kehtivusala;
- milleks on seda võimalik kasutada;
- kes, millistel tingimustel ja kuidas plaani aktiveerib;
- millised on selle valdkonna kommunikatsiooniliinid ning
- üksikasjalikult, millised on ülesanded ja tööetapid hädaolukorraga toimetulekuks.

Kõik plaanid kokku peaksid sisaldama järgmist teavet:

- rollide üksikasjalik iseloomustus hädaolukordade lahendamiseks ülesannete, õiguste ja kohustustega;
- kõikide kaastöötajate kontaktaadressid koos konkreetsete ülesannetega hädaolukorra lahendamiseks, samuti asutuseväliste kontaktisikute, näiteks koostööpartnerite, teenusetarnijate, abiorganisatsioonide või järelevalveasutuste kontaktandmed
- kriteeriumid hädaolukorra lahendamiseks ja vajalike tööetappide kirjeldus;
- andmed selle kohta, kuidas tuleb hädaolukorras protokollida olukord, otsused ja tegevused.

Kõik dokumendid peavad olema kättesaadavad isikutele, kes neid oma ülesannete täitmisel hädaolukorra likvideerimiseks vajavad. Dokumendid peavad olema neid vajavatele isikutele arusaadavalt koostatud. Täpsemat informatsiooni hädaolukorra kontseptsiooni kohta leiab BSI standardist 100-4 „Hädaolukorra haldamine”.

Samal ajal üksikute meetodite väljavalimise ja hädaolukorra kontseptsiooni koostamisega tuleks koostada ka realiseerimisplaan. Selleks tuleb kindlaks määrata, millises ajavahemikus tuleb üksikud meetmed ellu viia ning millised sobivad elluviimiseks omavahel kombineerituna. Lisaks sellele tuleb meetmed elluviimise hädavajalikkuse alusel järjestada.

Elluviimise plaan peaks sisaldama järgmist:

- Prioriteetide kindlaksmääramine (elluviimise järjekord): kõik meetmed tuleks tähtsuse ja efektiivsuse järgi järjestada. Põhimõtteliselt tuleks meetmed eriti raskete riskide vältimiseks ellu viia esmajärjekorras. Kui näiteks finantsilistel põhjustel ei ole võimalik kõiki meetmeid kohe ellu viia, tuleks kõigepealt rakendada kõige ulatuslikuma mõjuga meetmeid. Rakendamisjärjekorra kindlaksmääramisel tuleks arvestada meetmetevahelisi seoseid.
- Vastutusalad: iga meetme puhul on vaja kindlaks määrata, kes vastutab nende algatamise, elluviimise ja kontrolli või auditi eest.

Hädaolukorra meetmete valikul tuleb tähelepanu pöörata nende sobivusele ja majanduslikkusele. Dokumentatsioon peaks sisaldama konkreetseid andmeid vastutusalade ja pädevuste, samuti kontrolli, auditi ja monitooringu läbiviimiseks planeeritud toimingute kohta. Avatud toimingute rakendamise järjekorrast tuleb kinni pidada. Lisaks sellele tuleb dokumenteerida üksikute hädaolukorra meetmete realiseerimiseks planeeritud või kasutatud ressursid.

Hädaolukorra kontseptsiooni juures tuleb tähelepanu pöörata informatsiooni turvalisusele. Hädaolukorras, varulahenduste kasutuselevõtul ja kasutamisel ning normaalkäituse taastamisel tuleb tagada informatsiooni turvalisus. Selle hulka kuulub muu hulgas ka andmete konfidentsiaalsuse tagamine (näiteks juurdepääsuõigused, krüpteerimine), andmevarundusele esitatavatest miinimumnõuetest ja seadusest tulenevatest eeskirjadest kinnipidamine (näiteks asutuse töö seisukohalt tähtsate andmete arhiveerimine).

Kõikide hädaolukorra lahendite jaoks on vaja koostada turvakontseptsioonid ja juurutada turvameetmed. Seetõttu tuleb tagada tihe koostöö infoturbe eest vastutava töötajaga. Hädaolukorra kontseptsioon võib sisaldada konfidentsiaalset teavet, näiteks andmeid turvaaukude või infot turvameetmete kohta. Taolist informatsiooni võib liigitada konfidentsiaalseks ning seda tohib sel juhul edastada vaid volitatud isikutele. Hädaolukorra kontseptsioon tuleks seetõttu liigendada selliselt, et üksikuid osi oleks võimalik edasi anda spetsiaalsele adressaatide ringile.

Kontrollküsimused:

- Kas kriitilised äriprotsessid ja ressursid on välja selgitatud?
- Kas äriprotsesse ja ressursse ohustavad olulise tähtsusega riskid on välja selgitatud ja nende vältimiseks sobivad riskistrateegiad välja valitud?
- Kas on välja töötatud järjepidevuse strateegiad, mis võimaldavad kriitiliste äriprotsesside taaskäivitamist ja taastamist nõutud aja jooksul?
- Kas on olemas ajakohane hädaolukorra kontseptsioon? Kas on välja arendatud ja juurutatud hädaabiplaanid ja -meetmed, mis võimaldavad hädaolukordi efektiivselt likvideerida ja kriitilisi äriprotsesse kiiresti taaskäivitada?
- Kas hädaabi kontseptsioonis on tähelepanu pööratud informatsiooni turvalisusele ja kas hädaolukorra lahendite jaoks on loodud vastavad turvakontseptsioonid?

M 6.115 Kaastöötajate integreerimine hädaolukorra haldusprotsessi

Algatamise eest vastutavad: hädaolukorra lahendamise eest vastutav töötaja

Rakendamise eest vastutavad: hädaolukorra lahendamise eest vastutav töötaja, juhataja, personaliosakond

Hädaolukorra haldamine puudutab kõiki töötajaid. Igaüks peab käituma vastutustundlikult, et ära hoida kahjude tekkimist. Seetõttu tuleb töötajate integreerimiseks hädaolukorra haldusprotsessi võtta meetmeid nende koolitamiseks ja teadlikkuse tõstmiseks – see on ülesanne, millega tuleb tegeleda kogu hädaolukorra haldusprotsessis. Sellest tulenevalt peaks asutus või ettevõte juurutama koolituste ja teadlikkuse tõstmise programmi, mille raames töötatakse välja koolitus- ja teadlikkuse tõstmise kontseptsioon hädaolukordade haldamiseks, valmistatakse ette koolitusmeetmed ning kontrollitakse nende efektiivsust ja kestvust.

Kontseptsiooni koostamisel tuleks arvestada sellega, millised teadmised on töötajatel oma töölõigu kohta hädaolukorra haldamisel juba olemas. Kuna hädaolukorra haldamine on tihedalt seotud infoturbe haldamisega, on otstarbekas teha koostööd ka koolitus- ja teadlikkuse tõstmise meetmete elluviimisel.

Töötajatele tuleb teatavaks teha hädaolukorra haldamise eesmärgid ja vajalikkus. Nad peavad tundma ja mõistma hädaolukorra haldamise tegevusjuhiseid, samuti hädaolukorra haldamise eesmärke ja ülesandeid. Igale töötajale tuleks hädaolukorra halduses määrata selline roll, et ta saaks oma tegevustes järgida hädaolukorra haldamise põhimõtteid. Kõikide töötajate teadlikkust seoses hädaolukorra haldamise ja vajalike hädaolukorra meetmetega tuleb pidevalt tõsta, rakendades selleks pidevalt vajalikke meetmeid. Seejuures on tähtis, et töötajad osaleksid algusest peale hädaolukorra meetmete planeerimisel või organisatoorsete eeskirjade väljatöötamisel. Teadlikkuse tõstmise meetmete eesmärk peab olema töötajatele nende rolli vahendamine ning selgitamine, kuidas nad saavad oma käitumisega hädaolukorra halduse eesmärkide täitmisele kaasa aidata.

Töötajaid, kes on hädaolukorraks valmisolekul või hädaolukorra likvideerimisel võtnud enda kanda mõne rolli, tuleb regulaarselt koolitada. Tuleb tagada, et neil oleks vajalikud teadmised, kompetentsus ja võimed, et nad oleksid hetkel ja tulevikus võimelised täitma oma ülesandeid seoses hädaolukorra haldamisega.

Selleks tuleb välja töötada koolitusprogramm, mille sisu on järgmine:

- töötajate olemasolevate teadmiste analüüs hädaolukorra haldamise alal
- vastava koolituskontseptsiooni väljatöötamine,
- vajalike koolituste organiseerimine või vahendamine,
- regulaarne seire seoses meetmete efektiivsusega ning

- vajaduse korral programmi muutmine ning vastavusse viimine uute nõuetega.

Hädaolukorra halduse teadlikkuse tõstmise ja koolitusprogrammi raames läbitud sammud ja võetud meetmed tuleb kirjalikult fikseerida, et oleks võimalik regulaarselt teostada seiret ka kontrollida efektiivsust.

Kontrollküsimused:

- Kas hädaolukorraks valmisoleku valdkonnas tõstetakse regulaarselt kõigi töötajate teadlikkust?
- Kas hädaolukorra haldamiseks on olemas koolitus- ja teadlikkuse tõstmise kontseptsioon?
- Kas hädaolukorra haldusmeeskonda kuuluvaid töötajaid koolitatakse regulaarselt vajaliku kompetentsusastme kohaselt?

M 6.116 Hädaolukorra halduse integreerimine üleorganisatsioonilistesse protseduuridesse ja protsessidesse

Algatamise eest vastutavad: asutuse/ettevõtte juhatus

Rakendamise eest vastutavad: asutuse/ettevõtte juhatus, hädaolukorra lahendamise eest vastutav töötaja

Eelkõige suuremates asutustes on tihti olemas üldine riski-, turva- ja kriisihalduse osakond. Operatiivsed riskid koos IT riskidega on riski- või turvahalduse lahutamatu koostisosa. Teiste riskidega, mis jäävad vaatamata ennetustööle alles, tegeleb kriisihaldus. Hädaolukorra halduses võetakse vaatluse alla kõik riskid, mis viivad kriitiliste äriprotsesside katkemise või seiskumiseni. Seetõttu on hädaolukorra haldusel palju kokkulangevusi nii riski-, turva- kui ka kriisihaldusega. Seetõttu tuleks riskihalduse meetodid kooskõlastada hädaolukorra halduse alal juba sisseseatud meetoditega. Tähtis on, et ühe asutuse erinevates valdkondades kasutatavates tööjuhendites või teenuslepingutes ei oleks vasturääkivusi.

Hädaolukorra halduse aspektide kaasamine kõikidesse äriprotsessidesse

Asutuse juhatusel peaks olema ülevaade ärikriitilistest ülesannetest või äriprotsessidest ja ärikriitilisest teabest. Vastutavad spetsialistid ja hädaolukorra haldusmeeskond peavad järjepidevuse aspektide kaasamiseks määrama äriprotsesside planeerimisel ja elluviimisel kindlaks konkreetsed reeglid (näiteks kaitsemeetmed ja klassifitseerimine).

Muudatuste haldus

Muudatuste haldus tegeleb protsesside, infrastruktuuri või riist- ja tarkvara muudatuste planeerimisega. Organisatsiooniliste nõuetega tuleb tagada, et selle käigus arvestataks hädaolukorra halduse aspektide ja vajadustega.

Kontrollküsimused:

- Kas on tagatud, et hädaolukorra halduse aspekte arvestataks asutuse kõikides äriprotsessides?
- Kas hädaolukorra halduse protsessid, eeskirjad ja vastutusalad on kooskõlas riski-, turva- ja kriisihaldusega (kui sellised haldussüsteemid on asutuses olemas)?

M 6.117 Testid ja valmisoleku harjutused

Algatamise eest vastutavad: asutuse/ettevõtte juhatus, hädaolukorra lahendamise eest vastutav töötaja
Rakendamise eest vastutavad: hädaolukorra lahendamise eest vastutav töötaja

Meetmete tõhususe kontrollimiseks hädaolukorra halduse alal tuleb regulaarselt läbi viia teste ja valmisoleku harjutusi. Sellega kontrollitakse hädaolukordade lahendamise käsiraamatu usaldusväärsust, käepärasust ja arusaadavust. Olulised eesmärgid on seejuures avastada ebapüsivused hädaolukorra plaanides või puudused hädaolukorra haldusmeetmete planeerimisel ja rakendamisel, samuti harjutada toimingute efektiivset ja sujuvat kulgemist hädaolukorras.

Tüüpiliste harjutuste hulka kuuluvad näiteks:

- funktsioonitestid (näiteks vooluagregaatide, kliimaseadmete, kekserverite testid);
- tuletõrjeõppuste läbiviimine;
- alarmi ja eskalatsiooni läbiviimine;
- staabiharjutused;
- staabi raamharjutused;
- taaskäivitamine pärast üksikute ressursside või äriprotsesside väljalangemist;
- büroohoonest evakueerumine ja siirdumine varupinnale ning
- arvutuskeskuse väljalangemine ning varukeskuse töölerakendamine.

Harjutused võib seejuures läbi viia plaani ülevaate või plaani arutlusena „rohelise laua" taga, simulatsiooni või reaalsuselähedaste tõsiste ülesannetena.

Planeerimine, kontseptsioon, testide ja harjutuste läbiviimine ja analüüs nõuab finants- ja inimressursse. Ressursid peab eraldama asutuse juhtkond. Rollid tuleb kindlaks määrata ja nimetada nende täitmiseks töötajad. Töötajaid, kes võtavad endale mõne rolli planeerimisel, kontseptsiooni koostamisel või testide ja harjutuste läbiviimisel, tuleb vastavate ülesannete täitmiseks koolitada. Testid ja harjutused tuleb planeerida. Ainult nii saab saavutada efektiivse ja majanduslikult tõhusa finants- ja isikuvahendite kasutamise kõikide kehtivusvaldkonnas sisseseatud hädaolukorra meetmete kontrolliks.

Testide ja harjutuste läbiviimine peab toimuma regulaarselt ja vajaduse järgi, kui hädaolukorra halduses tehakse suuremaid muudatusi. Seetõttu tuleb koostada mitme aasta plaan, mis garanteerib, et kogu hädaolukorra halduse kehtivusala saaks kaetud. Seejuures tuleks kasutada mitut liiki teste ja harjutusi, et kontrollida ja testida kõiki hädaolukorra plaane, meetmeid ja hädaolukorra likvideerimise organisatsiooni struktuuri. See üldine plaan peaks sisaldama planeeritud testide liiki, eesmärke, ligikaudset ajakava ja vajalike ressursside loetelu. Iga-aastaselt koostatavas ajakavas tuleks täpsustada ligikaudne ajakava ja määrata kindlaks konkreetsed harjutused.

Asutuse juhtkond peab nii testi kui ka harjutuse üld- ja detailplaneeringu heaks kiitma ning selle allkirjastama. Iga testi ja iga harjutuse jaoks tuleb koostada testi või harjutuse kontseptsioon. Selles määratakse kindlaks üksikasjad, nagu testi või harjutuse liik, ajakava, ressursside kasutus, osavõtjad, taotletavad eesmärgid ja kulg. Kogemus näitab, et testide ja harjutuste kõrvalefektidena võib tekkida avariiolukordi. Detailne planeerimine tuleb seetõttu läbi viia nii, et riskid oleksid minimaalsed. Enne valmisolekuharjutuse läbiviimist tuleb taotleda kirjalik luba detailplaneeringu eest vastutavalt asutuse või ettevõtte juhtkonnalt. Iga testi ja iga harjutuse kulg tuleb protokollina dokumenteerida selliselt, et tulemusi oleks võimalik analüüsida. Testi või harjutuse analüüs tuleb dokumenteerida ning see peaks sisaldama tulemusi, tagasisidet osavõtjatelt ja testitud organisatsiooniüksuselt ning tulemuse võrdlust eesmärgiga, mille saavutamiseks oli harjutuse läbiviimine ette nähtud. Tulemused sisaldavad puudusi, turvaauke ja ettepanekuid nende kõrvaldamiseks. Avastatud puuduste ja turvaaukude kõrvaldamiseks tuleb hädaolukorra likvideerimise planeerimisel kindlaks määrata meetmed, vastutajad nende elluviimisel ja tähtajad. Meetmete õigeaegset elluviimist kontrollib hädaolukorra lahendamise eest vastutav töötaja.

Kontrollküsimused:

- Kas on olemas üldplaan, mis garanteerib, et kõik hädaolukorra haldust puudutavad olulise tähtsusega plaanid ja meetmed saaksid testitud ja läbi harjutatud?
- Kas hädaolukorra halduses on küllaldaselt ressursse planeerimistöödeks, kontseptsiooni koostamiseks, testide ja harjutuste läbiviimiseks ning analüüsimiseks?
- Kas hädaolukorra halduses viiakse regulaarselt ja vajadust mööda läbi erinevat liiki ning erinevate eesmärkidega teste ja valmisolekuharjutusi?
- Kas valmisolekuharjutuste läbiviimisel avastatud puudused ja turvaaugud on küllaldaseks põhjuseks, et hädaolukorra plaanid ja meetmed üle vaadataks ning kas nende rakendamist kontrollitakse?

M 6.118 Hädaolukorra meetmete kontroll ja käigushoidmine

Algatamise eest vastutavad: hädaolukorra lahendamise eest vastutav töötaja
Rakendamise eest vastutavad: hädaolukorra lahendamise eest vastutav töötaja

Hädaolukorra haldus ei kujuta endast mitte ainult soovitava kaitsetaseme saavutamist, vaid ka selle säilitamist ja edasist tõstmist. Seepärast tuleks kõiki hädaolukorra meetmeid regulaarselt kontrollida. Seejuures tuleb eristada kahesugust kontrolli – kas teatud kindlad meetmed on sobivad ja efektiivsed seatud eesmärkide saavutamiseks (täielikkuse või uuenduse kontroll) ning millisel määral on hädaabimeetmeid üksikutes valdkondades rakendatud (audit).

Regulaarne ja vajaduse järgi läbiviidav kontroll

Selleks vajalik kontroll, mida nimetatakse ka auditiks, tuleks läbi viia kindlaksmääratud ajal, kuid teatud põhjustel võib see toimuda ka teistel aegadel. Olemasolevaid hädaolukorra meetmeid tuleks kontrollida vähemalt üks kord aastas.

Olemasolevate meetmete kohandamist nõuab eelkõige just tekkivate hädaolukordade või kriiside kindlakstegemine ja seetõttu tuleb neid kontrollida.

Ka keskkonnamuutuste korral tuleks olemasolevaid meetmeid kohandada, näiteks juhul, kui

- on üles ehitatud uued äriprotsessid, rakendused või komponendid,
- on tehtud suuremaid muudatusi infrastruktuuris (näiteks ümberkolimine),
- seisavad ees suuremad organisatsioonilised muudatused (näiteks väljasttellimine),
- ohtude olemus on oluliselt muutunud,
- on avastatud suured turvaaugud või kahjustused.

Koordineeritud protseduurid

Asutuses või ettevõttes tuleks kindlaks määrata, kuidas tuleb koordineerida kontrolliga seotud tegevusi. Eelkõige vajab koordineerimist IT ja turvahalduse alal läbiviidud kontroll. Selleks on vaja kindlaks määrata, milliseid meetmeid ja millal tuleb kontrollida ning kes seda teeb, et vältida ülesannete dubleerimist ning et asutuses ei jääks ükski valdkond kontrollimata.

Kontrolli objekt

Tuleb kontrollida, kas hädaolukorra meetmetest kinnipidamine ja nende rakendamine on toimunud tõesti nii, nagu näeb ette hädaolukorra kontseptsioon. Seejuures tuleb üle kontrollida, kas tehnilised meetmed on korralikult juurutatud ja konfigureeritud. Kui selgub, et hädaolukorra meetmeid ei ole korralikult rakendatud või need ei toimi praktikas, tuleb välja selgitada kõrvalekallete põhjused.

Hädaolukorra kontseptsiooni tuleb regulaarselt uuendada, täiustada ja uute raamtingimustega kohandada. Tuleb regulaarselt kontrollida, kas valitud meetmed

sobivad veel eesmärkide saavutamiseks (täielikkuse või uuenduse kontroll). Kontrollida tuleks ka rakendatud hädaolukorra meetmete efektiivsust või seda, kas eesmärke ei oleks võimalik saavutada vähem ressursse nõudvate meetmetega.

Kontrolli läbiviimine

Olenevalt kontrolli eesmärgist tuleb kindlaks määrata kontrolli ulatus ja põhjalikkus. Iga kontrolli läbiviimise aluseks on hädaolukorra kontseptsioon ja hädaolukorra haldusprotsessi kohta olemasolev dokumentatsioon. Kontrolli tohivad teostada vaid isikud, kellel on selleks vastav kvalifikatsioon. Samas ei tohi need isikud olla osalenud kontseptsiooni koostamisel, et vältida nn ettevõttepimedust ja konflikte. Kontrollijad või auditi tegijad peavad olema võimalikult sõltumatud ja neutraalsed. Iga kontroll tuleb hoolikalt ette valmistada ja läbi viia. Kõik olulise tähtsusega tähelepanekud ja tulemused tuleb koondada ühte raportisse. See peaks lisaks analüüsile sisaldama ka parandusettepanekuid.

Kontrolli tulemused tuleb dokumenteerida. Lisaks sellele peab olema kindlaks määratud, kuidas peaks toimuma kontrolli tulemuste menetlemine, kuna kontrollil on mõju vaid siis, kui kontrolli tulemuste põhjal võetakse vajalikud parandusmeetmed.

Võimalike parandusmeetmetena tulevad olenevalt põhjusest kõne alla järgmised:

- organisatoorsete meetmete kohandamine;
- personaliga seotud meetmete, näiteks koolitus- ja teadlikkuse tõstmise meetmete kasutamine või distsiplinaarsete meetmete juurutamine;
- infrastruktuuriga seotud meetmete, näiteks ehituslike muudatuste algatamine;
- tehniliste meetmete teostamine, näiteks süsteemide muutmine;
- vastutavate ülemuste otsuste (kuni juhatuse tasemeni) nõutamine.

Raport tuleks üle anda kontrollitud valdkonna juhatajale ning hädaolukorra haldusmeeskonnale, kes peavad selle alusel kavandama järgmised tööetapid. Keerukad probleemid tuleks läbi arutada juhatuse tasemel, et oleks võimalik kiiresti vastu võtta kaugeleulatuvaid otsuseid. Kui kontrollimisel kasutatakse spetsiaalseid vahendeid, peab ka nende suhtes sarnaselt tulemuste dokumentatsiooniga olema tagatud, et juurdepääs neile oleks üksnes autoriseeritud isikutel. Juurdepääs toetavatele instrumentidele ja kontrolli tulemustele peab seetõttu olema eriti hästi kaitstud.

Parandusmeetmed

Avastatud vead ja kitsaskohad tuleb kiiresti kõrvaldada. Rakendada tuleb hädaolukorra meetmete majandusliku kasulikkuse ja efektiivsuse identifitseeritud optimeerimisvajadust. Kontrolli tulemuste põhjal tuleb vastu võtta edasisi protseduure puudutavad otsused. Eriti tähtis on kõikide vajalike parandusmeetmete koondamine rakendusplaani. Tuleb kindlaks määrata ajavahemik ja parandusmeetmete rakendamise eest vastutavad isikud ning varustada need vajalike ressurssidega.

Tuleb algatada protsess, millega juhitakse ja kontrollitakse rakendamist. Hetkeolukord ja rakendamisel tekkivad probleemid tuleb dokumenteerida. Kui vajalikke parandusi kitsaskohtade kõrvaldamiseks ei viida läbi plaanipäraselt, tuleb kogu protsess viia vajaduse korral kõrgemale juhtimistasandile.

Kontrollküsimused:

- Kas hädaolukorra meetmeid kontrollitakse regulaarselt ja vajaduse järgi?
- Kas kontrolli planeeritakse hoolikalt?
- Kas kontrolli tulemusi analüüsitakse ning võetakse vajaduse korral parandusmeetmeid?
- Kas parandusmeetmeid kavandatakse ja kas nende rakendamist kontrollitakse?

M 6.119 Hädaolukorra haldusprotsessi dokumentatsioon

Algatamise eest vastutavad: hädaolukorra lahendamise eest vastutav töötaja
Rakendamise eest vastutavad: hädaolukorra lahendamise eest vastutav töötaja

Hädaolukorra haldusprotsessi kulg, töötulemused eri faasides ja tähtsad otsused tuleb dokumenteerida. Selline dokumentatsioon ja protokollimine on olulised, et hoida protsessi töös ja seda efektiivselt edasi arendada. See aitab leida ja kõrvaldada rikete ning nurjumiste põhjused hädaolukorra haldusprotsessis.

Ainult järjepideva dokumenteerimise abil on võimalik mõista hädaolukorra halduse käigus toimunud arenguid ja tehtud otsuseid. Tuleb sisse seada mõistetav protsess, millega tagatakse, et kõik hädaolukorra haldusprotsessis koostatud dokumendid, protokollid ja märkmed oleksid leitavad, ühemõtteliselt arusaadavad, kiiresti juurdepääsetavad ja loetavad. Iga dokumenti tuleb hoida või säilitada kindlas kohas, ning väärkasutamise vältimiseks tohivad sellele juurdepääsu omada vaid volitatud isikud. Tuleb sisse seada protseduur, millega tagatakse nii regulaarne kui ka vajadust mööda läbiviidav dokumentide uuendamine.

Vananenud dokumendid, mis on asendatud uue versiooniga, tuleb vastavalt märgistada, et vältida nende ettekavatsemata kasutamist. Kõikide hädaolukorra halduse raames koostatud dokumentide juures on tähtis, et mitte ainult uusim versioon, vaid ka kõik varasemad versioonid oleksid tsentraalselt salvestatud ja igal ajal kättesaadavad.

Olenevalt esemest ja kasutusotstarbest tuleb vaadelda järgmisi hädaolukorra halduses ja hädaolukorra haldusprotsessis kasutatavaid dokumentide liike:

- Raportid juhatusele – selleks, et asutuse või ettevõtte juhatus saaks vastu võtta õigeid otsuseid hädaolukorra halduse juhtimiseks, on vaja vastavat informatsiooni. Selleks peaks hädaolukorra lahendamise eest vastutav töötaja või hädaolukorra haldusmeeskond koostama regulaarselt ning vajadust mööda haldusraporteid olukorra kohta hädaolukorra halduses.
- Hädaolukorra halduses kasutatavad dokumendid – hädaolukorra halduseks tuleks koostada järgmist liiki dokumendid:

1. asutuse või ettevõtte suunis hädaolukorra halduseks;
2. rollide kirjeldused ülesannete, õiguste ja kohustustega;
3. ülevaade ressursside vajalikkusest ja valmisolekust;
4. hädaolukorra ennetamise kontseptsioon BIA tulemustega, riskianalüüsi, järjepidevuse strateegia, vajalike meetmete ja nende rakendamisega;
5. hädaolukordade lahendamise käsiraamat hädaolukorra või kriisi efektiivseks lahendamiseks, mis hõlmab organisatsiooni struktuuri hädaolukorra lahendamiseks ja mitmesuguseid hädaolukorra lahendamise plaane;
6. kontseptsioon töötajate teadlikkuse tõstmiseks ja koolitamiseks, meetmete tõendus ning kontrolli dokumentatsioon;

7. testide ja valmisolekuharjutuste planeerimine, kontseptsioon ja läbiviimise protokollid;

8. auditite ja kontrolli planeerimine, läbiviimine ja tulemused (näiteks kontrollnimekirjad ja küsitlusprotokollid);

9. parandus- ja parendusmeetmete planeerimine ja läbiviimine;

10. hädaolukorra haldusmeeskonna olulise tähtsusega tööd ja otsused peaksid olema dokumenteeritud näiteks istungiprotokollide ja otsuste vormis.

- Tööprotsesside dokumentatsioon – tööprotsessid, organisatsioonilised reeglid ja meetmed peavad olema selliselt dokumenteeritud, et ei tekiks kahjustusi teadmatuse või vigade tõttu. Hädaolukordade ja kriiside korral peab olema võimalik taastada äriprotsesside vajalik seisund. Seetõttu tuleb tehnilised üksikasjad ja tööprotsessid dokumenteerida selliselt, et seda saaks teha mõistliku aja jooksul.
- Avariiolukordade dokumentatsioon – hädaolukorrad, kriisid ja nende haldus peavad olema selliselt korraldatud, et kõik sellega seotud toimingud ja otsused oleksid arusaadavad. Lisaks sellele peab dokumentatsioon võimaldama parandusi hädaolukorra ennetamise kontseptsioonis ja hädaolukordade lahendamise käsiraamatus ning vältida tuntud vigu tulevikus.
- Infovool ja teatamiskanalid – hädaolukorra lahendamise juures on tähtis teavitus- ja eskalatsioonikanalite kirjeldamine ja kiire uuendamine.

Dokumentatsiooni olemus

Hädaolukorra lahendamise eest vastutava töötaja ja teda toetava hädaolukorra haldusmeeskonna ülesanne on hoida hädaolukorda puudutavad ajakohased ja informatiivsed dokumendid kasutusvalmis. Kõikidele hädaolukorra protsessi raames koostatud dokumentidele peavad seetõttu olema ette nähtud kindlad toimingud.

Silmas tuleb pidada näiteks järgmisi punkte:

- Dokumendid peavad olema arusaadavad. See tähendab ka, et need tuleb koostada sihtrühma silmas pidades. Juhtkonnale esitatavad rapordid peavad olema teistsugused kui administraatorite mõeldud tehnilised dokumendid.
- Dokumendid peavad olema ajakohased. Peab olema kindlaks määratud, kes nende eest hoolitseb. Need peavad olema selliselt tähistatud ja salvestatud, et neid on vajaduse korral võimalik kiiresti leida. Olemas peavad olema andmed koostamiskuupäeva, allikate ja autorite kohta. Vananenud dokumendid tuleb kohe käigust kõrvaldada ja arhiveerida.
- Kindlaks peaks olema määratud kindel protseduur muudatusettepanekute (koos uute dokumentide koostamisega) sisseviimiseks, hindamiseks ja vajaduse korral arvesse võtmiseks.
- Lisaks kiirele informatsiooni edastamisele volitatud isikutele tuleb tagada ka organisatsioonisiseste andmete konfidentsiaalsus. Konfidentsiaalse sisuga dokumendid tuleb ka klassifitseerida konfidentsiaalseteks ning nende säilitamine ja redigeerimine peab toimuma turvaliselt.

Paljude dokumentide haldamise korral võiks abi olla dokumentide haldusosakonnast. Dokumendid ei pea alati olema paberkandjal. Dokumentide vormi võib

valida vajaduse järgi. Dokumentatsiooni hulka võivad näiteks kuuluda ülevaatediagrammid, lühikesed istungi protokollid, käsitsi kirjutatud märkmed või tarkvaravahendid (näiteks BIA dokumentatsiooni hulka).

Kontrollküsimused:

- Kas hädaolukorra haldussüsteemi ja rakenduse olulise tähtsusega dokumendid on olemas?
- Kas on olemas protseduur, mis garanteerib dokumentide regulaarse uuendamise, võimaldab nende kiiret ülesleidmist ning vaid volitatud isikute juurdepääsu dokumentidele?

M 6.120 Hädaolukorraks valmisoleku süsteemi kontroll ja juhtimine

Algatamise eest vastutavad: asutuse/ettevõtte juhatus, hädaolukorra lahendamise eest vastutav töötaja

Rakendamise eest vastutavad: asutuse/ettevõtte juhatus, hädaolukorra lahendamise eest vastutav töötaja

Asutuse juhtkond vastutab hädaolukorraks valmisoleku süsteemi juhtimise ja paremaks muutmise eest. Vastuvõetavate otsuste puhul on oluline, et asutuse hädaolukorraks valmisolekut puudutav informatsioon oleks ülevaatlik ja sisukas. Hädaolukorraks valmisoleku süsteemi juhtimiseks ja käigushoidmiseks tuleb regulaarselt kontrollida selle toimivust ja efektiivsust ning saadud tulemusi juhatuse tasemel hinnata. Selle eesmärgiks on edasise protseduuri kooskõlastamine hädaolukorraks valmisoleku protsessis. Seetõttu on vaja välja tuua kõik vajalikud muutused ja kohandused hädaolukorra haldusprotsessis, näiteks seoses eesmärkide ja nõudmistega. Tulemused tuleb dokumenteerida ja senised ülestähendused alles hoida.

Regulaarsed haldusaruanded

Selleks et ettevõtte või asutuse juhtkond saaks hädaolukorraks valmisoleku protsessi suunamisel ja juhtimisel õigeid otsuseid langetada, on tal vaja pidepunkte hädaolukorraks valmisoleku olukorra kohta.

Need pidepunktid peaks olema ära toodud haldusaruannetes, mis annavad ülevaate järgmistest punktidest:

- siseauditite ja väliste teenusetarnijate ning allhankijate kontrollimise tulemused koos puuduste loetelu ja parandusettepanekutega;
- testide ja harjutuste tulemused;
- tagasiside erinevatelt huvigruppidelt, kaasa arvatud koostööpartnerid, välised teenusetarnijad, allhankijad ja järelevalveasutused;
- aruanded ajakohaste riskide, vigade ja kahjustuste kohta ning nende põhjal tehtud järeldused ja antud soovitused;
- aruanded kõigi muutuste kohta, mis võivad mõjutada hädaolukorraks valmisolekut (näiteks muutused infrastruktuuris, äriprotsessides, seoses teenuseosutajatega);
- aruanded seoses hädaolukorraks valmisolekuga sätestatud meetmete, realiseerimis- ja parandusprotsessidega;
- aruanded töötajate koolitus- ja teadlikkuse tõstmise meetmete ning nende rakendamise tulemuste kohta;
- aruanded muudatuste kohta hädaolukorraks valmisoleku seaduslikes või lepingulistes nõuetes;
- aruanded seniste tulemuste ja probleemide kohta hädaolukorraks valmisoleku protsessis.

Hädaolukorraks valmisoleku meeskond peab juhatust informeerima regulaarselt sobival viisil hädaolukorra haldusprotsessi kontrolli tulemustest ja olukorrast.

Seejuures tuleks välja tuua probleemid, tulemused ja parandusvõimalused. Haldusaruanne peaks olema lühike ja ülevaatlik. Mitte mingil juhul ei tohi haldusaruannet üle koormata ega olukorra hindamiseks vajalikku teavet maha vaikida.

Niisiis oleks soovitatav esile tuua järgmised punktid:

- millisel määral on hädaolukorraks valmisoleku kontseptsiooni eeskirjad asutuses juba rakendust leidnud;
- millistes kohtades on veel turvaaugud, millega kaasnevad jääkriskid;
- millised avariid on toimunud, millised kahjustused tekkinud ja milliseid kahjustusi oli võimalik ära hoida;
- milliseid tulemusi on andnud sisekontroll;
- mil määral vastab saavutatud kaitsetase asutuse nõuetele ja võimalikele riskidele;
- kas raamtingimused on muutunud selliselt, et tuleb võtta lisameetmeid;
- kas hädaolukorraks valmisoleku meetmed on sobivad või tuleb neid muuta või täiendada;
- millist tagasisidet hädaolukorraks valmisoleku aspektide kohta on saadud klientidelt, äripartneritelt, kaastöötajatelt või avalikkuselt;
- millised ressursid on hädaolukorra halduseks ära kasutatud;
- kas ja kuidas on rakendatud seniseid haldusotsuseid.

Lisaks sellele tuleks anda ülevaade väljavaadetest hädaolukorra halduse üleorganisatsiooniliseks arenguks, tehniliseks ja protseduuriliseks arenguks, mis võiksid kaasa aidata hädaolukorra haldusprotsessi parendamisele. Ikka ja jälle köidavad massimeedia tähelepanu sõnumid äriprotsesside katkemise kohta. Kogemused näitavad, et sellised teistes asutustes juhtunud intsidendid on kasulik kaasata haldusaruannetesse ning näidata, kuidas on asutus taolisteks intsidentideks valmis.

Vajaduse korral koostatavad haldusaruanded

Lisaks regulaarsetele haldusaruannetele võib ootamatult tekkivate probleemide või riskide tõttu osutuda vajalikuks ka täiendavate haldusaruannete koostamine. See on vajalik eriti juhul, kui neid probleeme ei ole võimalik lahendada töötasandil, kui näiteks materiaalseid ressursse vajatakse väljaspool lubatud raame või on vaja kehtestada edasisi personaliga seotud reegleid. Kui toimuvad muutused riskide valdkonnas (näiteks uute ähvarduste, tehnoloogiate või seaduste tõttu), võib otstarbekaks osutuda vajadusest lähtuv haldusaruanne.

Haldusaruannete koostamisel tuleks silmas pidada, et nende lugejaskond ei koosne reeglina tehnilistest ekspertidest. Seetõttu peaks aruande tekst olema hästi mõistetav ja napisõnaline, välja tuleks tuua olulise tähtsusega punktid, näiteks olemasolevad turvaaugud, aga ka saavutused. Haldusaruande lõpus, eriti vajaduse korral koostatud aruannetes, peaksid alati olema välja toodud ettepanekud selgelt eelistatud meetmete kasutuselevõtu kohta, mis on varustatud realistlike hinnangutega oodatavate rakenduslike kulutuste kohta. Sellega tagatakse, et juhatusel on võimalik otsus viivitamata vastu võtta.

Hädaolukorra haldusaruande peab juhtkonnale esitama hädaolukorra haldusmeeskonna liige isiklikult. Nii on võimalik pöörata suuremat tähelepanu olulise tähtsusega põhipunktidele, näiteks olemasolevatele või tekkida võivatele puudustele. Hädaolukorra haldusmeeskonna liikme ülesanne on anda ka tagasisidet ja põhjalikumaid selgitusi, mis võimaldab kogemuste kohaselt langetada otsuseid kiiremini. Lisaks sellele on tähtis ka isiklik kontakt, et juhatuse otsuseid paremini ette valmistada ning probleeme juba eos pehmendada. Abiks on ka see, kui keegi vastava eriala ja huvidega juhatuse liige oleks kontaktisikuna kättesaadav. Isiklik kontakt pakub võimalust „lühikeste ametlike kanalite" sisseseadmiseks, mille olemasolu võib pakilistes hädaolukordades kasulikuks osutuda.

Haldusotsused

Haldusosakond otsustab haldusaruannete põhjal vajalike muutuste, kohanduste ja edasiste protseduuride üle hädaolukorra haldusprotsessis. Seejuures saab asutuse juhatus vajaduse korral toetust hädaolukorraks valmisoleku eest vastutavalt töötajalt. Kõik otsused tuleb dokumenteerida.

Selle alla kuuluvad eriti järgmised punktid:

- kehtivusala kohandamine;
- riskide aktsepteerimise taseme muutmine (riskivalmidus);
- muutused äriprotsesside prioriseerimises;
- muutused hädaolukordadeks valmisoleku strateegias;
- tegevused hädaolukorraks valmisoleku kontseptsiooni efektiivsuse parandamiseks ja selleks vajalikud ressursid;
- muutused, mis võivad mõjutada hädaolukorraks valmisoleku kontseptsiooni, näiteks ärisihid, nõuded ja äriprotsesse puudutavad muudatused.

Dokumentatsioon

Hädaolukorra haldusprotsessi pidevaks jälgimiseks tuleks kõik haldusaruanded ja vastuvõetud otsused süsteemselt arhiveerida. See dokumentatsioon peaks olema vastutavatele isikutele vajaduse korral kiiresti kättesaadav. Kuna hädaolukorra haldusaruanded sisaldavad enamasti konfidentsiaalset informatsiooni olemasolevate turvaaukude ja jääkriskide kohta, tuleb kaitsta nende konfidentsiaalsust. Tuleb kasutusele võtta sobivad kaitseabinõud, et haldusaruannete sisu ei saaks teatavaks volitamata isikutele.

Kontrollküsimused:

- Kas juhatus on teadlik, et tema ülesanne on hädaolukorraks valmisoleku süsteemi regulaarselt kontrollida, hinnata ja vajadust mööda paremaks muuta?
- Kas juhatus saab haldusaruannete kaudu regulaarselt informatsiooni hädaolukorraks valmisoleku süsteemi olukorrast?
- Kas hädaolukorraks valmisoleku haldusaruanded sisaldavad vajalikul määral informatsiooni, et juhatus saaks täita oma kontrolli- ja juhtimisfunktsiooni?

M 6.121 Suuniste väljatöötamine turvaintsidentide käsitlemiseks

Algatamise eest vastutavad: asutuse/ettevõtte juhatus, infoturbespetsialist
Rakendamise eest vastutavad: infoturbespetsialist

Paljud turvaintsidendid muutuvad suuremaks probleemiks alles vale reageerimise tõttu. See võib juhtuda, kui otsuseid võetakse vastu kiirustades või kui administraator kustutab spontaanselt andmeid, mis oleksid olnud vajalikud turvaintsidendi jälitamiseks. Selleks et iga töötaja teaks, kuidas tuleb turvaintsidendi esinemise korral käituda, on soovitatav koostada eri sihtgruppidele mõeldud suunised turvaintsidentide käsitlemiseks. See võimaldab kõigil osalistel ka erandlikes olukordades rahulikult ja kainelt tegutseda.

Administraatoritele ja infoturbeosakonna töötajatele peaksid turvaintsidentide käsitlemiseks haldussüsteemi raames olema koostatud tehnilised tegutsemisjuhised. Sellesse protsessi tuleb aga varakult kaasata ka kasutajad. Samuti peaks suunises olema reguleeritud turvaprobleemide ja turvalisuse seisukohalt olulise tähtsusega hoolduspäringute rikete ja vigade kõrvaldamine (st intsidentide haldus). Soovitatav on avaldada ettevõttes või asutuses suunis, milles kirjeldatakse sobivat protseduuri turvaintsidentide esinemisel ja selgitatakse asutuse kõigile töötajatele siduvalt nii protsessi kui ka teavitus- ja eskalatsioonikanaleid. Suunise väljatöötamisel tuleks tähelepanu pöörata asjaolule, et see oleks täielikult ja praktiliselt rakendatav. Selles peaks kõikide osalejate ülesanded olema selgelt sõnastatud. Suunisele mittevastav käitumine peaks olema lubatud vaid dokumenteeritud erandjuhtudel.

Ärge paanitsege!

Siin tuleb eristada üldisi käitumisreegleid, mis kehtivad igasuguste turvaintsidentide korral, ja IT-spetsiifilisi käitumisreegleid.

Järgmistest üldkehtivatest käitumisreeglitest võib lähtuda igat liiki turvalisuse seisukohalt tähtsate kõrvalekallete korral:

- Kõik asjaosalised peavad säilitama rahu ja võtma kiirustamata asjakohased meetmed.
- Kõrvalekalletest tuleb teatada kohe teatamisplaani järgi ettenähtud kohta.
- Vastumeetmeid tohib võtta vaid pärast selleks volitatud isikute üleskutset.
- Asjaosalised peavad kõiki asjaolusid selgitama ilustamata, avalikult ja läbipaistvalt, et oleks võimalik kahjusid vähendada.

Kahjuarvestus

- Tuleks läbi viia esmane, isiklikel kogemustel põhinev võimaliku kahju suuruse, selle tagajärjel tekkinud kahjude ja võimalike tagajärgede hindamine, samuti tuleb välja selgitada asutusesisene ja -väline personal, keda see turvaintsident võiks puudutada.
- Informatsiooni turvaintsidentide kohta ei tohi edasi anda selleks volitamata kolmandatele isikutele.

Käitumisreeglid tuleb teatavaks teha

Need üldised käitumisreeglid tuleb sobival viisil teatavaks teha kõigile asutuse või ettevõtte töötajatele, keda need potentsiaalselt puudutavad. Lisaks võib spetsiifilised käitumisreeglid edasi anda intsidentidest puudutatud osapooltele, eriti nendele, kes tegutsevad turvaintsidentide teatamiskohtades ja võtavad vastu esimesed otsused või rakendavad esimesi meetmeid. Nende hulka kuuluvad administraatorid, IT-rakenduste eest vastutavad isikud ja infoturbeosakond.

Nimetatud käitumisreeglite hulka kuuluvad järgmistes meetmetes kirjeldatud reeglid:

- M 6.23 Käitumisreeglid arvutiviiruste esinemisel
- M 6.31 Protseduurid süsteemi tervikluse kao puhuks
- M 6.48 Protseduurid andmebaasi tervikluse kao puhuks
- M 6.54 Protseduurid võrgu tervikluse kao puhuks
- M 6.102 Käitumisreeglid traadita kohtvõrkude turvaintsidentide puhul

Üks näide, kuidas suunistes kirjeldatud käitumisreegleid ja teatamisplaani kõigile intsidendiga seotud kaastöötajatele teatavaks teha, on asutuse või ettevõtte juhatuse allkirjastatud infoleht, kuhu on koondatud kõige tähtsam teave ja mida on võimalik hoida töökohas ning lisaks ka intranetis. Sellise infolehe näidis asub IT etalonturbe abimaterjalide hulgas. Selleks et vajalik informatsioon oleks vajaduse korral tõesti ka kättesaadav, ei ole otstarbekas levitada seda ainult elektroonilisel kujul. Kõik infolehed potentsiaalsete turvaintsidentide kohta tuleb iga olulise tähtsusega muutuse korral organisatsioonis, äriprotsessides või IT-s kohe uuendada, et selles kirjeldatud käitusreeglid veel kehtiksid ja et teatamisreeglid oleksid korrektsed.

Kontrollküsimused:

- Kas on olemas eri sihtgruppidele mõeldud suunised turvaintsidentide käsitlemiseks?
- Kas turvaintsidentide suunis on praktiliselt kasutatav ja kas iga asjaosaline loeb sellest välja oma ülesanded?
- Kas suunisega reguleeritakse kõiki turvaintsidentide käsitlemise aspekte?
- Kas suunis on kooskõlastatud IT-juhatuse või IT-süsteemiga? Kas asutuse või ettevõtte juhatus on selle vastu võtnud?
- Kas kõigi turvaintsidentide jaoks on olemas selgelt defineeritud protseduurid?
- Kas suunis on kõigile töötajatele (eriti IT ja esimese astme tugiteenuse töötajatele toekeskuses) tuttav?

- Kas toimub regulaarne suunisega kindlaks määratud protseduuride ajakohastamine?
- Kas on arvestatud teiste haldusvaldkondade liidestega, näiteks hädaolukordade haldamisega?

M 6.122 Turvaintsidendi defineerimine

Algatamise eest vastutavad: asutuse/ettevõtte juhatus, infoturbespetsialist
Rakendamise eest vastutavad: infoturbespetsialist

Sarnaselt hädaolukorra defineerimisega (vt M 6.110 Kehtivusala ja hädaolukorrahalduse strateegia määratlemine) on ka turvaintsidentide käsitlemisel vaja, et asutuses või ettevõttes valitseks selge arusaamine, mis on turvaintsident. Eelkõige peab selge olema, mille poolest erinevad turvaintsidendid igapäevatöös esinevatest tõrgetest. Ainult nii on võimalik igapäevase tõrgete ja vigade kõrvaldamise protsessis kindlaks määrata, millal on õige aeg alustada turvaintsidentide käsitlusprotsessi erimeetmetega. Üldine formaalne definitsioon ilma liiga suurte interpreteerimisvõimalusteta võib selle protsessi algust veelgi kergendada.

Turvaintsidentide defineerimine peaks toimuma asjassepuutuvate äriprotsesside kaitsevajaduse, IT-teenuste, IT-süsteemide või rakenduste alusel. Nii näiteks on otseselt ohustatud või kaudse ohupotentsiaaliga süsteemi kaitsevajaduse või BIA tulemuste põhjal võimalik defineerida lävi, millest alates on põhjust rääkida sündmusest kui turvaintsidendist. Lisaks sellele peaks infoturbeosakonnal olema võimalik olenemata definitsiooni piiridest välja kuulutada erakorraline turvaintsident.

Turvaintsidendi võimalik definitsioon võiks näiteks kõlada järgmiselt: „Turvaintsidendiks nimetatakse meie ettevõttes/asutuses sündmust, mis kahjustab meie kõrge või väga kõrge kaitsevajadusega teabe, äriprotsesside, IT-teenuste ja IT-süsteemide või -rakenduste konfidentsiaalsust, käideldavust ja terviklust sellisel määral, et võib meie ettevõttele/asutusele/klientidele/äripartneritele tekitada suurt kahju.”

Turvaintsidendi definitsioon peab olema kõigile turvaintsidentide haldusprotsessis osalevatele töötajatele teada. Otstarbekas oleks viia turvaintsidendi definitsioon vastavusse hädaolukorra definitsiooniga.

Kontrollküsimused:

- Kas on olemas selge definitsioon turvaintsidendi eraldamiseks tõrgetest?
- Kas turvaintsidendi definitsioon on viidud vastavusse hädaolukorra definitsiooniga?
- Kas turvaintsidendi definitsioon on teada kõigile turvaintsidentide käsitlemises osalevatele töötajatele?
- Kas turvaintsidentide defineerimisel on arvestatud asjassepuutuvate äriprotsesside, IT-teenuste, IT-süsteemide või -rakenduste kaitsevajadust?

- Kas turvaintsidentide definitsiooni abil on võimalik eristada neid tõrgetest igapäevatöös?

M 6.123z Ekspertmeeskonna moodustamine turvaintsidentide käsitlemiseks

Algatamise eest vastutavad: infoturbespetsialist, IT-juht
Rakendamise eest vastutavad: infoturbespetsialist

Selleks et turvaintsidentide käsitlemine oleks kogu nende käsitlusprotsessi jooksul asjatundlik, on otstarbekas moodustada selleks kogenud ja usaldusväärsetest spetsialistidest koosnev meeskond. Seda meeskonda võib vajaduse korral täiendada spetsialistidega väljastpoolt, et oleks võimalik sobivalt reageerida igat liiki turvaintsidentidele.

Kõigi ekspertmeeskonna liikmete usaldusväärsus peab olema kontrollitud (vt M 3.33z Personali taustakontroll). Seejuures tuleb tähelepanu pöörata ka asjaolule, et kõik meeskonna liikmed oleksid sobival moel eskalatsiooniprotsessi kaasatud. Lisaks ekspertmeeskonna moodustamisele tuleb tagada, et selle käsutusse antaks vajaduse korral viivitamata turvaintsidentide käitlemiseks vajalikud finantsilised ja tehnilised ressursid.

Enamik ekspertmeeskondi eksisteerib virtuaalselt ja need kutsutakse kokku vaid turvaintsidentide lahendamiseks ning töötavad kogenud juhtspetsialisti juhatusel.

Juhtspetsialisti rolli võtab enamasti enda kanda infoturbe eest vastutav töötaja. Kes meeskonna liikmetest konkreetsel juhul osaleb, sõltub reeglina turvaintsidendi liigist ja sellest puudutatud süsteemidest või asukohtadest. Olenevalt IT-kooslusest võivad meeskonda kuuluda näiteks SAP-süsteemi, Lotus Notesi, Windowsi, andmebaasi, Unixi või võrguspetsialistid. Ekspertmeeskonna liikmetel ei pea olema üksnes ulatuslikud teadmised kasutuses olevatest süsteemidest, vaid nad peavad olema välja õpetatud ka nende süsteemide turvaintsidentide analüüsi alal.

Selleks et alati üha uuenevatele ründevariantidele õigesti reageerida, peavad ekspertmeeskonna liikmed oma teadmisi regulaarselt täiendama.

Kontrollküsimused:

- Kas ekspertmeeskonna liikmed on kaasatud eskalatsiooni ja -teatamisprotsessi?
- Kas ekspertmeeskond on saanud väljaõppe kasutuses olevate süsteemide analüüsi alal?
- Kas ekspertmeeskonna käsutuses on finantsilised ja tehnilised ressursid turvaintsidendi kiireks ja diskreetseks käitlemiseks?

- Kas ekspertmeeskonna liikmete usaldusväärsus on kontrollitud?
- Kas ekspertmeeskonna liikmed osalevad regulaarselt täiendkoolitustel?

M 6.124z Turvaintsidentide käitlemise liideste kindlaksmääramine tõrgete ja vigade kõrvaldamiseks

Algatamise eest vastutavad: infoturbespetsialist, IT-juht
Rakendamise eest vastutavad: infoturbespetsialist

Tõrgete ja vigade kõrvaldamise (nimetatakse ka intsidentide halduseks) ülesanne on võtta kasutajatelt vastu kõik tõrgetega seonduvad sõnumid, päringud ja tellimused, et kasutajaid nende töös toetada ning tagada neile IT tõrgeteta kasutamine. Ka turvaintsidendid on selles mõttes tõrked, sest nende tõttu saab kahjustada IT abil töödeldavate andmete käideldavus, terviklus ja konfidentsiaalsus, mis omakorda võib kahjustada ärifunktsioone. Tõrked teenuste toimimises võivad tekkida ka tundmatute turvaintsidentide tagajärjel. See võib ette tulla juhul, kui turvaintsident on seotud rünnetega ning kasutatakse ära turvaauke, et IT-teenuseid ja selleks tarvilikke IT-süsteeme sihilikult destabiliseerida.

Mõnikord tuntakse turvaintsidendid ära alles nende põhjustatud tõrgete järgi. Intsidentide halduse põhieesmärk on tõrgete kõrvaldamine nii kiiresti kui võimalik ja kokkulepitud teenuse toimimise taastamine, et hoida äriprotsesside kahjustused nii väiksena kui võimalik. IT-tõrked võivad põhjustada ka uusi turvaauke, näiteks kui turvamehhanismid lülitatakse ebapüsivate süsteemide või IT vastukaalu tõttu välja.

Tõrked teenuste toimimises ja turvaintsidendid võivad seega olla nii põhjuseks kui ka tagajärjeks. Seetõttu tuleb neid vaadelda ja käsitleda koos. Seepärast tuleks analüüsida võimalikke intsidentide halduse, hädaolukorra halduse ja turvahalduse vahelisi liideseid ning määrata kindlaks koos kasutatavad ressursid.

Nii peaks intsidentide haldus vastama nii turvaintsidentide halduse kui ka hädaolukorra halduse vajadustele. Lisaks sellele peaks infoturbe haldusmeeskonnal olema lugemispääs intsidentide halduse tööriistadele, et vajaduse korral avastada kõrvalekalded või identifitseerida tõrked. Järgneva loetelu eesmärk on näitlikustada intsidentide haldusprotsessi olulise tähtsusega samme.

Infosüsteemide etalonturbe kataloogides soovitatud meetmetes kirjeldatakse, milliste integratsiooni aspektidega tuleb arvestada, et viia intsidentide halduse protsess vastavusse infoturbe halduse nõuetega.

- Äratundmine ja mõistmine (M 6.130 Turvaintsidentide äratundmine ja mõistmine)

- Kvalifitseerimine ja esmane katse leida lahendus (M 6.131 Turvaintsidentide kvalifitseerimine ja hindamine)
- Analüüs ja lahenduse pakkumine (M 6.64 Turvaintsidentide likvideerimine ja M 6.131 Turvaintsidentide kvalifitseerimine ja hindamine)
- Lahendus ja teenuse toimimise taastamine (M 6.64 Turvaintsidentide likvideerimine ja M 6.133 Töökeskkonna taastamine pärast turvaintsidente).
- Lahenduse kontroll ja juhtimine (M 6.133 Töökeskkonna taastamine pärast turvaintsidente ja M 6.134 Turvaintsidentide dokumenteerimine).
- Tõrke kõrvaldamine (M 6.133 Töökeskkonna taastamine pärast turvaintsidente)

Võimalused käsitleda tõrkeid ja turvaintsidente ulatusliku ja standardiseeritud intsidentide halduse osana suurenevad, kui arvestada ettenähtud integratsiooni aspektidega.

Kontrollküsimused:

- Kas on analüüsitud intsidentide halduse, hädaolukorra halduse ja infoturbe halduse vahelisi võimalikke liideseid? Kas on identifitseeritud teatud juhtudel koos kasutatavad ressursid?
- Kas intsidentide haldus on viidud vastavusse infoturbe halduse ja hädaolukorra halduse vajadustega?
- Kas infoturbe haldusmeeskonnal on olemas lugemispääs intsidentide halduse tööriistadele, et vajaduse korral avastada kõrvalekalded või identifitseerida tõrked?

M 6.125 Tsentraalse kontaktkoha sisseseadmine turvaintsidentide registreerimiseks

Algatamise eest vastutavad: infoturbespetsialist, IT-juht
Rakendamise eest vastutavad: infoturbespetsialist

Turvaintsidentide vastuvõtu efektiivsuse tõstmiseks tuleks mõelda, kas ei oleks otstarbekas sisse seada tsentraalne kontaktkoht, kuhu teatatakse turvaintsidentidest.

Praktikas on turvaintsidentidest teatamiseks kaks võimalust:

- Kõikidest tõrgetest (kaasa arvatud turvaintsidendid) antakse teada tsentraalse tõrgete vastuvõtukoha kaudu, niisiis tavaliselt intsidentide halduse esimese astme teenustoe kaudu.
- Turvaintsidentidest teatatakse eraldi kontaktkoha kaudu, mis paikneb infoturbe haldusmeeskonna kontaktisiku juures.

Tsentraalse tõrgetest teatamise eelised on järgmised:

- Kõik kasutajad ei ole võimelised turvalisuse seisukohalt olulisi tõrkeid ära tundma.
- Infoturbe haldusmeeskond võiks kasutada juba olemasolevat infrastruktuuri ja IT-teenustaseme haldusprotsesse.
- Teavet turvaintsidentide kohta võiks hallata koos teabega tõrgete kohta ühes keskses andmebaasis. Tsentraalne haldus ühises andmebaasis oleks võimalik, kui kasutatakse tugevat autentimist ja tööriist võimaldab piisavalt diferentseeritud volituste haldust. Tegelikkuses ei ole aga praegusel ajal kõik praktiliselt realiseeritav.

Nõuanne: otstarbekaks võib osutuda ka turvaeeskirjadele mittevastavate turvaintsidentide eraldi käsitlemine (näiteks asutusesisesed ründed).

Tsentraalse tõrgetest teatamise puuduseks on, et turvalisuse seisukohalt tähtsates küsimustes tuleb välja koolitada rohkem töötajaid ning kõikide tsentraalses teatamiskohas töötavate isikute usaldusväärsust tuleb kontrollida, et tundlikud andmed ei jõuaks soovimatult avalikkuse ette. Kui asutus või ettevõte otsustab sisse seada tsentraalse kontaktkoha turvaintsidentide registreerimiseks, tuleks seal tegevate töötajate käsutusse anda abivahendid ja meetodid turvaintsidentide äratundmiseks (näiteks ülevaade hooldatavate süsteemide kaitsevajaduste kohta). Samuti ei tohi alahinnata infoturbealaste koolituste vajadust (M 6.129 Teenustoe töötajate koolitamine turvaintsidentide käsitlemise alal). Kui seatakse sisse tsentraalne kontaktkoht, peab see olema kättesaadav tavapärasel tööajal. Kontaktkoha töötajad peavad turvaintsidente puudutava teabega konfidentsiaalselt ümber käima.

Kontrollküsimused:

- Kas kontaktkoha kättesaadavus turvaintsidentidest teatamiseks tavapärasel tööajal on tagatud?
- Kas tsentraalse tõrgetest teatamise koha töötajad on piisavalt koolitatud ja tunnevad infoturbe vajadusi?
- Kas turvaintsidente puudutava infoga ümberkäimine kontaktkohas on konfidentsiaalne?
- Kas kontaktandmed turvaintsidentidest teatamiseks on kõigile töötajatele teada?

M 6.126w Sissejuhatus arvutipõhisesse kohtulikku juurdlusesse

Algatamise eest vastutavad: asutuse/ettevõtte juhatus, infoturbespetsialist, IT-juht
Rakendamise eest vastutavad: infoturbespetsialist, audiitor

Arvutipõhise või digitaalse kohtuliku juurdluse korral kogutakse digitaalseid tõendeid ja analüüsitakse neid, et tõestada ja välja selgitada karistatavaid või teisi õigusvastaseid või sotsiaalselt kahjulikke tegusid. Sellise juurdluse eesmärgid on pärast süsteemi sissemurdmist või mõnda teist turvaintsidenti tavaliselt järgmised:

- meetodi või turvaaugu identifitseerimine, mis võis viia süsteemi sissemurdmiseni
- kahju väljaselgitamine pärast süsteemi sissemurdmist;
- ründaja identifitseerimine;
- tõendite kindlustamine edasiseks juriidiliseks tegevuseks.

Selleks on vaja koguda kõnealustest IT-süsteemidest intsidendi analüüsimiseks vajalikud andmed. Seejuures peab olema tagatud, et kompromiteeritud süsteemist oleks võimalik koguda nii palju teavet kui võimalik, ilma et muudetaks seejuures selle süsteemi hetkeseisundit või staatust. Efektiivse juurdluse läbiviimiseks on otstarbekas koostada eelnevalt juurdlusprotsessi läbiviimise juhis, milles on kirjeldatud kõiki teostatavaid samme.

Niinimetatud secure-analyse-present (S-A-P) mudeli järgi võib juurdlusprotsessi jagada kolme suurde etappi. Etapis secure registreeritakse kõik andmed hoolikalt. Sealjuures tuleb tähelepanu pöörata asjaolule, et uurimisvaldkond oleks hoolikalt turvatud. Selleks ajaks ei ole tihti veel teada, kas kurjategija on pärit oma asutusest. Kui ekspertmeeskonna liikmed tahavad ennetada võimalikke manipulatsioone, tuleb kasutusele võtta vastavad abinõud, et oma asutusest pärit kurjategijad ei saaks tõendeid kustutada.

Selles faasis pannakse sobivate meetodite abil alus sellele, et kogutud materjalid ei kaotaks hilisemas juriidilises kaalumises oma tõendusjõudu. Kuigi selles väga varases juurdlusfaasis ei ole tihti veel päris selge, kas taotletakse juriidilist arutlust, peab tõendusmaterjal olema kohtule esitamiseks valmis. Seetõttu peavad kõik tegevused olema hoolikalt dokumenteeritud ja protokollitud. Kogutud andmeid tuleb ka varakult kaitsta tahtmatu või tahtliku manipuleerimise eest. Seetõttu tuleks pidevalt rakendada vastavaid räsifunktsioone ja nelja silma printsiipi.

Analüüsifaasis toimub hoolikas jälgede analüüs ja tulemuste objektiivne hindamine. Järelduste tagamaid tuleb hoolikalt uurida, et identifitseerida iseseisvalt ja kindlalt argumentatsiooniketi lüngad.

Kui turva- ja analüüsifaasid on detailsusastme ja meetodi poolest tihti turvaintsidendi konkreetsest probleemist sõltumatud, sõltuvad tegevused etapis present

sellest, keda ja millisel kujul on vaja juurdluse tulemuste põhjal veenda. Lõpuks peab tulemus olema veenev isikutele, kes ei olnud algusest lõpuni juurdluse juures ja kellel ei ole tõenäoliselt nii palju tehnilisi teadmisi, et kõikidest üksikasjadest aru saada. See tähendab, et kõik otsused tuleb järjekindlalt ja ka tehnilistele võhikutele arusaadavalt dokumenteerida ning seejärel kõikidele sihtgruppidele veenvalt esitada. Kohtuliku juurdluse tulemused tuleb tavaliselt teatavaks teha kõigile asutusesisestele otsusetegijatele, aga ka asutusevälistele otsusetegijatele ja kriminaaljälitusorganitele.

Olenemata konkreetsest probleemist ja uuritavast IT-süsteemist (server, tööjaam, pihuarvuti, ruuter, sülearvuti jne) on üldjuhul võimalik identifitseerida mõningad tundlikud andmetüübid, mis pakuvad juurdluse läbiviijatele huvi:

- ebapüsivad andmed: info, mis võib IT-süsteemi korrapärasel mahalaadimisel ja väljalülitamisel kaduma minna (vahe- ja põhimälu sisu, võrguühenduste staatus, toimivad protsessid, registreeritud kasutajad jne).
- rabedad (fragile) andmed: info, mis on salvestatud IT-süsteemi kõvakettale, kuid mille seisund võib ebakompetentse juurdepääsu tõttu muutuda.
- ajutise juurdepääsuga andmed: info, mis paikneb kõvakettal, kuid millele on juurdepääs vaid teatud ajal, näiteks mingi rakenduse või kindla rakendusfunktsiooni kasutamise ajal.

Tähtis on teada nende andmete poolväärtusaega, kuna selle järgi määratakse kindlaks andmekogu järjekord secure faasis. Sellest tulenevad arvutipõhises kohtulikus juurdluses kasutatavad kaks põhilist juurdlusmeetodit, nimelt Live Response ja Post Mortem Analyse:

- Aktiivse, veel väljalülitamata süsteemi analüüs võimaldab koguda enamikku ebapüsivatest andmetest ning seda nimetatakse Live Response. See meetod on otstarbekas, kui väärtuslikud ebapüsivad andmed võivad kaduma minna ning ka süsteemi ei saa käideldavuse või sõltuvuse tõttu välja lülitada. Live Response analüüs on abiks ka juhul, kui on oht, et andmekandjale ei pääse süsteemi väljalülitamise korral enam ligi. Live Response analüüsi üks olulise tähtsusega eeliseid seisneb selles, et tihti on ainult selle meetodi abil võimalik kindlaks teha, kas süsteemi on tõepoolest rünnatud ning kas ja mil viisil on kahjulik kood aktiivne. Kõrvalekaldeid, mis viitavad juurkratile või mõnele muule kahjurvarale, ongi tihti võimalik märgata vaid süsteemi töötamise ajal. Eeliseks on tõik, et protsessi salvestit on võimalik struktureeritult varundada koos parajasti süsteemis toimuvate sündmustega. Üks põhiprobleeme Live Response analüüsi juures on, et ebapüsivate andmete varundamise järjekorda ei ole alati võimalik täpselt kindlaks määrata, kuna iga tegevus kahtlase süsteemi juures kutsub esile muutusi ka kahtlases süsteemis endas. Nii ilmuvad kahtlases IT-süsteemis toimuvate protsesside nimekirja varundamisel ka varundamisel kasutatavad käsud. Ebakompetentse tööriistade kasutamise korral on oht, et hävitatakse ka teisi andmeid või varjatakse süsteemile installeeritud juurkrati abil muud olulist informatsiooni.
- Teist uurimismeetodit nimetatakse tihti Post Mortem analüüsiks, kuna selle raames tegeletakse juba väljalülitatud süsteemide andmekandjate ja andmekandjakoopiate analüüsiga. Selle meetodi puhul viiakse läbi kompromiteeritud süsteemi andmekandja kohtuliku juurdluse koopia analüüs. Kohtu-

liku juurdluse jaoks tehtav koopia on ühebitine 1 : 1 koopia, mis on olemas kettapildifailina. Originaalandmekandja otsimisest tuleks ilma täiendavate turvamehhanismide rakendamiseta loobuda, kuna on olemas jälgede kustutamise oht. Post Mortem analüüs viiakse läbi, kui ebapüsivate andmetega salvesti ei ole uuritava intsidendi jaoks tähtis või intsidendi toimumisest on möödunud juba palju aega. Post Mortem analüüsi kasutamise eelised kohtuliku andmekandjakoopia analüüsimisel seisnevad selles, et ebapüsivaid andmeid ei ole võimalik kogemata hävitada ning kogu analüüsiprotsess või tööriista kasutamine on planeeritav, kuna teave ei saa kaduma minna. Kuid sellel on ka puudusi: süsteemi tööaja kohta on võimalik teha vaid väheseid järeldusi ning olulised jäljed võivad jääda varjatuks.

Kui turvaintsidendist arusaamiseks ja lahendamiseks on ebapüsivad andmed olulise tähtsusega, tuleks enne kahtlase süsteemi väljalülitamist püsivad andmed hoolega varundada. Kui see on hoolikalt ja kompetentselt läbi viidud, võib süsteemi vooluvõrgust eemaldada. Süsteemi tavapärast väljalülitamist tuleb võimaluse korral vältida, kuna seejuures hävitatakse palju rabedaid (fragile) andmeid, mida ei ole võimalik taastada.

Selleks et kõik ekspertrühma liikmed saaksid turvaintsidentide käsitlemisel arusaadavalt ja kainelt läbi viia kõik vajalikud analüüsid, peaksid spetsiaalses juhises olema kirjas kõik uuringu käigus tehtavad sammud. See juhis peaks sisaldama informatsiooni ka selle kohta, kuidas on võimalik varundada kahtlase süsteemi andmeid, analüüsiplaane tüüpilistele turvaintsidentidele ja analüüsimetoodikat. Lisaks peaks selles olema viiteid rakendatavate õiguslike aluste kohta. Kohtuliku juurdluse meetodite optimeerimisvõimalusi tuleks regulaarselt uurida.

Kontrollküsimused:

- Kas on olemas juhend, kuidas peab toimuma kahtlase süsteemi andmete varundamine?
- Kas ekspertmeeskonnale on turvaintsidentide käsitlemiseks juurdluse läbiviimise meetodite erinevused teada?
- Kas on tagatud, et turvaintsidentide esinemisel kogutakse informatsiooni, mis on tõendatav?
- Kas kõik juurdlusprotsessi tegevused dokumenteeritakse ja protokollitakse nii hoolikalt, et nendega ei oleks võimalik manipuleerida?
- Kas kõik järeldused dokumenteeritakse järjekindlalt ja arusaadavalt?

M 6.127z Tõendite varundusmeetmete kindlaksmääramine seoses turvaintsidendiga

Algatamise eest vastutavad: asutuse/ettevõtte juhatus, infoturbespetsialist, IT-juht
Rakendamise eest vastutavad: infoturbespetsialist

Enne turvaintsidentide käsitlemist tuleb planeerida ja kindlaks määrata meetodid digitaalsete tõendusmaterjalide tagamiseks. Tõendusmaterjalid on asjaolud või kindlakstehtavad asjaolud, mis aitavad kaasa tõe väljaselgitamisele arvutipõhise kohtuliku juurdluse või sellele järgneva juriidilise ekspertiisi käigus. Tõendusmaterjali ja protseduuri õigusjõu väljaselgitamiseks tuleks järele mõelda, kas selle teema puhul on vajalik juriidiline nõustamine. Lisaks vajalikele tehnilistele meetoditele (vt Live Response ja Post Mortem analüüsi M 2.64 Logifailide kontroll ja M 6.126w Sissejuhatus arvutipõhisesse kohtulikku juurdlusesse) tuleb tähelepanu pöörata ka tõendite varundamisele. Nende hulka kuuluvad näiteks ettevalmistatud formularid kindlakstehtud tõendite dokumenteerimiseks. Neid formulare võib kasutada ka digitaalsete tõendite analüüsi teostajate identifitseerimiseks.

Varundatud IT-süsteemide või andmekandjate hoidmiseks tuleb valida turvaline koht. See võib olla vastav hoiuruum või mõni teine ruum, millele on juurdepääs võimalikult väikesearvulisel ja usaldusväärsel töötajate ringil. Kui leitakse elektroonilisi tõendeid, tuleb analüüsi käigus tõestada igal sammul kontrollsumma meetodit kasutades tõendite puutumatus. Tõendid tuleks salvestada vaid eriti turvatud süsteemides, kus viiakse läbi ka nende analüüs. Selleks et tõendeid ei saaks muuta, peaksid need loomulikult olema eraldatud nii kompromiteeritud IT-süsteemidest kui ka ülejäänud produktiivsest võrgust.

Tõendite varundamise meetmete ja instrumentide puhul tuleb kontrollida, kas need sobivad tõendite usaldusväärseks ja manipulatsioonivabaks varundamiseks. Tõendite varundamise protseduur tuleb kooskõlastada infoturbe eest vastutava isiku ja turvaintsidentide käsitlemise ekspertmeeskonnaga. Selleks et tagada andmekaitsega seotud probleemidega arvestamine, tuleb kaasata ka andmekaitse eest vastutav töötaja. Kui on kahtlus, et kurjategija on keegi oma asutuse või ettevõtte töötajatest, peaks kaasama ka personali esinduse. Lisaks sellele tuleks kasutada asutusesiseste ja -väliste juristide abi, et anda hinnang kasutatud protseduuridele ja meetoditele.

Kontrollküsimused:

- Kas protseduurid leitud digitaalsete tõendite turvaliseks säilitamiseks on defineeritud ja testitud?
- Kas kindlaksmääratud meetmed ja instrumendid sobivad õigete tõendite usaldusväärseks ja manipulatsioonivabaks varundamiseks?
- Kas tõendite varundamiseks kasutatavad meetmed on kooskõlastatud infoturbe eest vastutava töötaja ja tema ekspertmeeskonnaga?
- Kas andmekaitse ja kaasarääkimise probleemid on eelnevalt lahendatud?

- Kas rakendatud protseduuride ja meetodite hindamiseks on kasutatud asutusesiseseid või -väliseid juriste?

M 6.128z Koolitus tõendusmaterjalide varundamise alal

Algatamise eest vastutavad: infoturbespetsialist, IT-juht
Rakendamise eest vastutavad: infoturbespetsialist

Turvaintsidentide käsitlemise ekspertmeeskonna liikmed peavad tundma digitaalsete tõendusmaterjalide varundamiseks ja analüüsiks kasutatavaid tööriistu ja oskama neid kasutada, kuna just Live Response analüüsi ajal võib tähtsaid andmeid tahtmatult hävitada. Mitme asukohaga asutustes ja ettevõtetes ei pruugi ekspertmeeskonna spetsialistid esimestel tundidel pärast turvaintsidendist teadasaamist alati kohal olla. Sellistel juhtudel võib usaldada tõendusmaterjali varundamise kohalikule usaldusväärsele IT-personalile või veel parem infoturbeosakonna personalile. Selleks tuleb neid isikuid vastavate instrumentide kasutamises koolitada. See puudutab ka serverite, turvalüüside või teiste IT-süsteemide administraatoreid, kui neil tuleb näiteks logifaile varundada. Seeläbi õpivad protsessis osalevad isikud tundma ka kasutatavate instrumentide võimalikke nõrkusi ja vigu, mis võivad mõjutada analüüsitulemusi.

Instrumentide valikul digitaalsete tõendite kogumiseks või analüüsiks on tähtis tunda nende instrumentide päritolu. Tarkvara instrumendid peavad pärinema usaldusväärsetest allikatest, näiteks otse tootjalt. Lisaks sellele tuleks näiteks kasutada kontrollsumma meetodit, et tunda varakult ära volitamata manipuleerimist instrumentidega. See on eriti tähtis, kui kasutatakse lähtekoodtarkvara instrumente, millest võivad ringluses olla erinevad variandid.

Kontrollküsimused:

- Kas administraatorid ja ekspertrühma liikmeid on koolitatud tõendusmaterjalide varundamisinstrumentide kasutamises?
- Kas tuntakse kasutatavate instrumentide vigu?
- Kas analüüsiinstrumentide päritolu on teada ja usaldusväärne?
- Kas kontrollitakse usaldusväärselt, et ei toimuks tarkvaraga manipuleerimist?

M 6.129 Teenustoe töötajate koolitamine turvaintsidentide käsitlemise alal

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Algatamise eest vastutavad: administraator, infoturbespetsialist, IT-juht

Kui asutus või ettevõte on otsustanud võtta teateid turvaintsidentide kohta vastu tsentraalse kasutajatoe, näiteks tsentraalse tõrgete vastuvõtukoha (intsidentide halduse tsentraalse teenustoe) kaudu, peavad sellega seotud töötajad olema infoturbe valdkonnas piisavalt teadlikud ja läbinud vajalikud koolitused. Selleks peavad nad muu hulgas tundma turvaintsidentide käsitlemist puudutavaid suuniseid ning kehtestatud käitumisreegleid, eskalatsiooni- ja teatamiskanaleid. Teenustoe töötajad peaksid regulaarselt osa võtma teabepäevadest ja koolitustest, mille käigus käsitletakse üldisi infoturbealaseid probleeme ja iseäranis turvaintsidentide äratundmist.

Nende läbiviimisega võivad tegelda infoturbe eest vastutavad või mittekooosseisulised töötajad ja nende sisu tuleb igal juhul kooskõlastada infoturbe eest vastutava spetsialistiga. Lisaks sellele peavad teenustoe töötajad juurde pääsema turvaintsidentide avastamiseks vajalikele abivahenditele ning olema nende kasutamise alal koolitatud. Selleks et turvaintsidente õigel ajal ja õigesti ära tunda, peavad teenustoe töötajad olema võimelised tegema kontrollnimekirjade abil kindlaks turvaintsidendi olemasolu. Õigete meetmete tarvitusele võtmiseks peavad teenustoe töötajad tundma ka nende süsteemide kaitsevajadust.

Kontrollküsimused:

- Kas teenustoe töötajad tunnevad turvaintsidentide või hädaolukorra käsitlemist puudutavaid suuniseid?
- Kas teenustoe töötajate käsutuses on abivahendid turvaintsidentide avastamiseks?
- Kas teenustugi tunneb ära selliste süsteemide kaitsevajaduse, milles esineb rohkem rikkeid?
- Kas teenustoe kontrollnimekirjad sisaldavad ka küsimusi turvaintsidentide avastamiseks?

M 6.130 Turvaintsidentide äratundmine ja mõistmine

Algatamise eest vastutavad: infoturbespetsialist
Rakendamise eest vastutavad: administraator, vastutav spetsialist, infoturbespetsialist, hädaolukorra lahendamise eest vastutav töötaja

Kõiki turvaintsidente ei ole võimalik kohe ära tunda. Paljusid turvaintsidente, eeskätt sihilikke ettekavatsetud ründeid IT-süsteemidele, on võimalik märgata alles tunde, päevi või nädalaid hiljem. Tihti esineb ka valehäireid, näiteks peetakse riist- või tarkvaraga seotud probleeme vahel ekslikult arvutiviirusega nakatumiseks. Selleks et turvalisuse seisukohalt olulisi ebareeglipärasusi oleks aga siiski võimalik uurida ja hinnata, tuleb juba eelnevalt läbi viia teatud kindlad analüüsid.

Nende hulka kuuluvad:

- olemasoleva IT-struktuuri ja IT-võrgustiku väljaselgitamine;
- IT-süsteemide kontaktisikute või kasutajate väljaselgitamine;
- IT-süsteemides kasutuses olevate rakenduste kindlakstegemine ning
- teabe, IT-süsteemide ja rakenduste kaitsevajaduse kindlaksmääramine.

Need uuringud viiakse läbi IT etalonturbe rakenduse esimese sammuna ning seetõttu peaksid nende tulemused olema infoturbeosakonna käsutuses.

Turvaintsidendid võivad teatavaks saada erineval moel:

- tuvastamine kasutajate kaudu: kasutajad annavad tavaliselt teada tõrgetest, näiteks arvatavast või tegelikust viirustega nakatumisest, andmekaost või info muutumisest
- tuvastamine süsteemi kaudu: süsteemi kontrolli korral (monitooring) genereeritakse kriitilise piirväärtuse ületamisel sündmus, mis saadetakse tõrkena edasi tugirühmale või edastatakse automaatselt intsidentide haldussüsteemile;
- sissetungi tuvastuse süsteem (intrusion detection system, IDS) registreerib näiteks ründekatse või sissemurdmise serverisse;
- tuvastamine IT-osakonna töötajate kaudu: kui töötajad avastavad tõrked, registreerivad nad need tavaliselt ise tõrgete analüüsi süsteemis;
- tuvastamine välise partneri poolt: teatud juhtudel võivad välised partnerid olla esimesed, kes turvaintsidendist teada annavad, näiteks kui nad on avastanud kõrvalekaldeid normaalselt toimivatest IT-teenustest. Sel juhul on eriti tähtis, et kõiki sõnumeid võetaks tõsiselt ning need edastataks õigesse kohta, kuna välised partnerid ei tea alati õigeid kontaktisikuid ega tunne asutusesiseselt kasutatavaid termineid;
- info õiguskaitseorganite või ajakirjanduse kaudu: kahjuks võib ka juhtuda, et asutus kuuleb turvaintsidentidest politsei või ajakirjanduse kaudu. Ka sel juhul on tähtis edastada need õigele kontaktisikule.

Selle informatsiooni põhjal saab saabuva turvaintsidendi teate korral kiiresti otsustada, millist IT-süsteemi milliste IT-rakendustega ja millise kaitsevajadusega see puudutab. Sellest selgub ka loomulikult, milline ärikriitiline teave ja äriprotsessid on puudutatud, ilma et seda iga kord täpselt välja toodaks. Ühtlasi saab ka

kindlaks teha, kes on määratud kontaktisikuks ja keda saab otsustamisprotsessi kiiresti kaasata. Kui seejuures selgub, et tõrge puudutab kõrge kaitsevajadusega IT-süsteemi või rakendust, on tegemist turvaintsidendiga ning sel juhul tuleb kasutusele võtta selleks kindlaksmääratud sammud. Kui tõrked puudutavad vaid tavapärase kaitsevajadusega IT-rakendusi või IT-süsteeme ning ei ole oodata, et puudutatud võiksid saada ka kõrgema kaitsevajadusega süsteemid, võib proovida turvaprobleemi lokaalselt kõrvaldada.

Seejuures tuleks aga arvestada ka võimaliku kumulatsiooniefektiga, kui on aru saada, et puudutatud võivad olla paljud tavapärase kaitsevajadusega IT-rakendused ja IT-süsteemid. Kui selgub, et turvaintsidendil võivad olla rasked tagajärjed ning see on piisavalt komplitseeritud, on otstarbekas kaasata selle lahendamisse lühiajaliselt ka turvaintsidentide käsitluse meeskond (vaata M 6.59 Turvaintsidentide käsitlemise eest vastutavate isikute määramine). Kui turvaintsidendi analüüsiks ja kõrvaldamiseks on vaja platvormi- või asukohaspetsiifilisi eriteadmisi, võib osutuda otstarbekaks kaasata turvaintsidentide käsitlemisse ekspertmeeskond (vt M 6.123z Ekspertmeeskonna moodustamine turvaintsidentide käsitlemiseks).

Turvaintsidendi uurimiseks ja hindamiseks tuleb välja selgitada järgmised mõjurid:

- Millised IT-süsteemid ja IT-rakendused võivad veel turvaintsidendist puudutatud olla?
- Kas kahjud võivad tekkida ka IT-süsteemide võrgu kaudu?
- Milliste IT-süsteemide ja IT-rakenduste puhul võib kahjustused ja kahjulikud tagajärjed välistada?
- Kui suur võib olla turvaintsidendi tekitatud otsene kahju või kahjulik tagajärg? Seejuures tuleb eelkõige silmas pidada erinevate IT-süsteemide ja IT-rakenduste sõltuvust.
- Mis käivitas turvaintsidendi (näiteks hooletus, ründaja või infrastruktuuri väljalangemine)?
- Millal ja millises kohas toimus turvaintsident? See võib olla väga kaugel turvaintsidendi esmase avastamise kohast. Ka selle uuringu juures on väärtuslikuks abiks hästi sisse seatud logifailid, kuid ainult juhul, kui võib kindel olla, et nendega pole manipuleeritud.
- Kas turvaintsidendist on puudutatud vaid asutusesisesed kasutajad või ka välised kolmandad isikud?
- Kui palju infot turvaintsidendi kohta on juba avalikkusele teada?

Kui selgub, et turvaintsidendil võivad olla rasked tagajärjed, tuleb kaasata vähemalt järgmine eskalatsioonitase. Pärast mõjurite väljaselgitamist tuleb koostada tegevusfunktsioonid, mis koosnevad viivitamata rakendatavatest meetmetest ja lisameetmetest. Siinjuures tuleb silmas pidada vastavaid prioriteete (M 6.62z Prioriteetide kindlaksmääramine turvaintsidentide käsitlemiseks). Selleks on vaja välja arvestada ka nende meetmete rakendamiseks vajalik aeg, vajalikud kulud ja ressursid probleemide kõrvaldamiseks ning süsteemi töö taastamiseks. Kui kahju suurus, aeg ja kulutused ületavad ettenähtud piiri, tuleb enne meetmete valikut arvestada suuruselt järgmise eskalatsiooni- ja otsustustasandiga.

Turvaintsidendi selliselt struktureeritud uurimise ja hindamise tulemusena esitatakse tegevusfunktsioonid. Kasutajatelt tulnud teated tõrgete kohta registreeri-

takse intsidentide halduse esimese astme teenustoe juures. Sellega on esimese astme kasutajatugi ja teenustugi kaasatud algusest peale tõrke käsitlemistsüklisse. IT-töös kindlaks tehtud tõrked registreerivad üldjuhul süsteemi administraatorid iseseisvalt probleemihalduse süsteemis või sarnaste instrumentidega. Tõrkeid võib erineval viisil ja moel ära tunda ja vastu võtta. See näitab selgesti, et tõrgete ja turvaintsidentide juhtimiseks on soovitatav kasutada selgeid protsessireegleid. Juba tõrke registreerimisel intsidentide halduse esimese astme teenustoe juures võivad märgid viidata asjaolule, et tegu on turvaintsidendiga, ilma et kasutajad sellest teaksid. Intsidentide haldus – sel juhul esimese astme kasutajatugi – peaks arvestama, et vajalikuks võib osutuda turvaintsidentide halduse kaasamine ja et teatavat isikut tuleks sellest informeerida.

Kontrollküsimused:

- Kas on olemas vajalikud eelnevalt läbiviidud analüüsid, näiteks kaitsevajaduse kindlaksmääramine ja struktuurianalüüs?
- Kas teatamiskohtadel (eriti intsidentide haldusel) ja nendele järgnevatel eskalatsioonitasanditel on olemas vajalik info kaitsevajaduse kindlaksmääramise kohta?
- Kas on olemas abivahendid turvaintsidentide tehniliseks toetamiseks, näiteks instrumendid logiandmete hindamiseks?

M 6.131 Turvaintsidentide kvalifitseerimine ja hindamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator, infoturbespetsialist, IT-juht

Mida diferentseeritumalt toimub turvaintsidendi või tõrke klassifitseerimine, seda täpsemalt on võimalik juhtida selle tõrke hindamis- ja käsitlemisprotsessi, aga seda töömahukam on klassifitseerimise kooskõlastamine ja rakendamine. Seetõttu tuleks klassifitseerimise struktuuri efektiivsust ja sobivust regulaarselt kontrollida. Igat liiki tõrgete ja turvaintsidentide käsitlemiseks peaks olema ühtne klassifitseerimismeetod.

See peaks olema infoturbe ja intsidentide haldusosakonna (niisiis tõrgete ja vigade kõrvaldamine) vahel kooskõlastatud. Lõplik klassifikatsioon võib erineda registreeritud klassifikatsioonist, kuna kasutajad nimetavad tõrke registreerimisel tavaliselt vaid sümptomid, mitte põhjused, või saadakse vastavate süsteemide kaitsevajadusest alles hiljem aru. Juhul kui turvaintsidendi mõjuala laieneb teiste süsteemide kaudu, võib see samuti kaasa tuua uue klassifikatsiooni.

Koos klassifitseerimisega tuleks tõrge siduda muu teabega, näiteks

- milliseid rakendusi, IT-süsteeme ja teenuseid tõrge puudutab;
- kellele töötajatest või töörühmadest on antud ülesandeks tõrke likvideerimine;
- kas teised, juba tuntud vead ja probleemid, näiteks IT-toodete ja konfiguratsioonide turvaaugud võivad olla tõrkega seotud.

Tõrgete registreerimiseks kasutatav instrument peaks võimaldama tõrgete registreerimist selliste klassifikatsioonide ja lisainfoga.

Kontrollküsimused:

- Kas turvaintsidentide ja tõrgete klassifitseerimiseks on kindlaks määratud ühtne klassifitseerimisprotseduur?
- Kas turvaintsidentide klassifitseerimisprotseduur on infoturbe ja turvaintsidentide haldusosakonna vahel kooskõlastatud?

M 6.132 Turvaintsidentide mõju tõkestamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht
Rakendamise eest vastutavad: administraator, infoturbespetsialist, IT-juht

Lisaks turvaintsidendi põhjuse efektiivsele analüüsile on oluline ka selle intsidendi tagajärjel tekkinud kahjustuste tõkestamine. Turvaintsidendi mõju tuleb otsekohe kindlaks teha, sellele tuleb anda hinnang ning selle mõju vähendada, et tekkiv kahju ei võtaks suurt ja väga suurt ulatust ega ületaks eksistentsi ähvardavat piiri.

Selleks on vajalik, et infoturbe haldusosakonnal oleks küllaldaselt informatsiooni ning ülevaade IT- ja äriprotsesside seostest, samuti selleks vajalikest IT-süsteemidest, IT-rakendustest ja teistest ressurssidest. See info võib pärineda näiteks struktuuranalüüsist, kaitsevajaduse kindlaksmääramisest ja BIA-st. Ainult nii on võimalik teha usaldusväärseid järeldusi mõju ulatuse ja kahju suuruse kohta.

Tihti on turvaintsidendi analüüsimine lihtsam, kui sellest puudutatud IT-süsteemid ja asukohad isoleeritakse ja vähendatakse sellega ohtu, et kahju ulatub intsidendist puutumata aladele. Aeg-ajalt tuleb ka vastu võtta otsus, et kahju tõkestamine on tähtsam kui selle likvideerimine. Sel põhjusel tuleks väljavalitud turvaintsidentide stsenaariumide jaoks välja töötada halvimad stsenaariumid.

Kontrollküsimused:

- Kas on olemas piisavalt informatsiooni, mille põhjal saab kindlaks määrata turvaintsidendi mõju?
- Kas väljavalitud turvaintsidentide stsenaariumide jaoks on välja töötatud halvimad stsenaariumid?

M 6.133 Töökeskkonna taastamine pärast turvaintsidente

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator, infoturbespetsialist, IT-juht

Turvaaukude kõrvaldamiseks tuleb võrgust eemaldada intsidendist puudutatud IT-süsteemid ja varundada kõik failid, mis võivad anda infot esinenud probleemide liigi ja põhjuse kohta. Nende hulka kuuluvad eelkõige kõik olulise tähtsusega logifailid. Kuna kõiki turvaintsidendist puudutatud IT-süsteeme tuleb vaadelda kui ebakindlaid või manipuleeritud süsteeme, peab uurima kõikide nende IT-süsteemide operatsioonisüsteeme ja rakenduste muutusi. Lisaks programmidele tuleb manipulatsioonide suhtes uurida ka konfiguratsiooni- ja kasutajafaile. Mõistlik oleks selleks kasutada kontrollsumma meetodit. See eeldab aga, et „turvalise" seisundi kontrollsummad tuleb eelnevalt kindlaks teha ja kirjutuskaitstud andmekandjatele välja saalida (M 4.93z Regulaarne tervikluse kontroll).

Paroolid tuleb muuta!

Selleks et olla kindel, et ründajapoolsed manipulatsioonid, näiteks Trooja hobused, on tõesti eemaldatud, tuleks originaalfailid installeerida uuesti kirjutuskaitstud andmekandjatelt. Seejuures tuleb tähelepanu pöörata asjaolule, et kõik olulise tähtsusega konfiguratsioonid ja paigad saaks samuti installeeritud. Kui varundatud failid installeeritakse uuesti, peab olema tagatud, et need ei oleks turvaintsidendist puudutatud, niisiis, et need ei oleks arvutiviirusesse nakatunud. Teisest küljest võib andmevarunduse uurimine olla abiks ründe või arvutiviirusega nakatumise alguse kindlaksmääramisel.

Pärast ründejärgset taaskäivitamist tuleb muuta intsidendist puudutatud IT-süsteemide kõik paroolid. Nende hulka kuuluvad ka IT-süsteemid, millega ei ole olnud vahetult manipuleeritud, kust aga ründaja on juba saanud infot kasutajate ja/või paroolide kohta. Pärast IT-süsteemi taastamist tuleks kontrollida, kas kõik funktsioonid on tõesti täielikult installeeritud. Sellesse võiks kaasata kasutajad, kellel on spetsiifilised teadmised rakenduste ja andmete alal. Tuleks arvestada asjaoluga, et ründaja proovib pärast „turvalise" seisundi taastamist uuesti rünnata. Seetõttu tuleks IT-süsteemide, eriti võrguülekäikude kontrollimiseks kasutada spetsiaalseid kontrollinstrumente. Lisaks laiendatud logifaili analüüsile võiks selleks kasutada ka näiteks sissetungi avastamise ja sissetungile reageerimise süsteemi (M 5.71z Sissetungi tuvastuse ja sellele reageerimise süsteemid).

Turvaintsidendi korral lahendab probleemi vastutav süsteemiadministraator, turvaintsidentide käsitlemise ekspertmeeskond, arvutiavariide tõrje rühm (computer emergency response team, CERT), IT-süsteemi tootja või turvaekspert. Selles faasis tuleks omistada suurt tähtsust sissejuhatavate meetmete dokumentatsioo-

nile (ümbersõit, lõplik lahendus, kes on meetmete oskusteabe kandja) ja teadmiste andmebaasi (probleemide ja lahenduste andmebaas) uute andmete alusel uuendada (M 6.134 Turvaintsidentide dokumenteerimine). Kui lahenduse rakendamiseks on vaja muutuste taotlust (change request), esitatakse see muudatuste haldusele (change management). Sellisel juhul jääb turvaintsident „lahtiseks", kuni muudatus on edukalt tehtud.

Üldiselt sobivad kriitiliste turvaintsidentide lahendamiseks erilised muudatuste halduse stsenaariumid (emergency changes), mis peavad võimaldama lahenduse viivitamata rakendamist. Kui tõrgete kõrvaldamisse saab kaasata väliseid teenuseosutajaid, tuleb kindlaks määrata, millisele teabele millise turvaintsidendi kohta ning kellele tohib juurdepääsu võimaldada.

Kontrollküsimused:

- Kas turvaaukude kõrvaldamiseks on võrgust eemaldatud intsidendist puudutatud IT-süsteemid ja varundatud kõik failid, mis võivad anda infot esinenud probleemide liigi ja põhjuse kohta?
- Kas kõikide intsidendist puudutatud IT-süsteemide operatsioonisüsteemide ja rakenduste muudatusi on uuritud?
- Kas turvalise operatsioonikeskkonna taastamisel kaasatakse kasutajad kasutusfunktsiooni testi läbiviimisse?
- Kas pärast taaskäivitamist kontrollitakse IT-süsteeme ja võrguülekäike, et uusi ründeid oleks võimalik tuvastada?

M 6.134 Turvaintsidentide dokumenteerimine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator, infoturbespetsialist, IT-juht

Turvaprobleemi kõrvaldamise ajal tuleks kõik läbiviidud toimingud võimalikult üksikasjalikult ning ideaalsel juhul standardiseeritult dokumenteerida selleks, et

- saada ülevaade põhjustest, tagajärgedest ja meetmetest,
- selgitada esinevaid probleeme,
- oleks võimalik kõrvaldada viga, mis võib ette tulla vastumeetmete kiire rakendamise korral,
- oleks võimalik juba tuntud probleeme nende korduval esinemisel kiiremini kõrvaldada,
- oleks võimalik turvaauke likvideerida ja ennetavaid meetmeid välja töötada,
- koguda võimaliku kriminaaljälituse jaoks tõendeid.

Sellise dokumentatsiooni hulka ei kuulu mitte ainult läbiviidud toimingute kirjeldus koos ajakava ja osalevate isikute nimedega, vaid ka intsidendist puudutatud IT-süsteemide logifailid. Turvaintsidentide dokumentide konfidentsiaalsust tuleb sobival viisil kaitsta. Turvaintsidentide haldusosakond peaks hoolitsema selle eest, et vajalik teave kantaks enne tõrke lõppu vastavatesse dokumentatsioonisüsteemidesse.

Selleks on vaja eelnevalt koostöös turvaintsidentide haldusosakonnaga defineerida kvaliteedinõuded. Turvaintsidendi standardiseeritud dokumenteerimiseks võib kasutada IT etalonturbe abivahendites olevat formulari, mille leiate RIA veebilehelt.

Kontrollküsimused:

- Kas kõik turvaintsidendid dokumenteeritakse standardiseeritud meetodi järgi?
- Kas raportite dokumenteerimisel ja arhiveerimisel on tagatud dokumentatsiooni konfidentsiaalsus?

M 6.135 Samba serveri tähtsate süsteemikomponentide regulaarne varundamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: andmevarunduse eest vastutavad töötajad

Samba serveri väljalangemine raskendab oluliselt asutuse või ettevõtte äriprotsesside toimumist. Planeerimata muudatused, näiteks valekonfiguratsioonid või riistvara vead, võivad nõuda olulise tähtsusega süsteemikomponentide taaskäivitamist. Olulise tähtsusega süsteemikomponentide hulka ei kuulu mitte ainult tegelikud süsteemifailid (näiteks Samba paketi smbd deemon), vaid ka konfiguratsioonifailid (näiteks smb.conf), staatuse info (näiteks TDB-failid TDB - Trivial Database - andmebaasis) ning logifailid (näiteks smbd deemoni logifail).

Andmete varundamine peab toimuma andmevarunduskontseptsiooni eeskirjade järgi (B 1.4 Andmevarunduspoliitika). Konfiguratsioonifailide, staatuse info ja süsteemifailide taaskäivitamisel tuleks tähelepanu pöörata asjaolule, et need ühilduvad üksteisega. Kui Samba serveri konfiguratsiooni taaskäivitamiseks kasutatakse näiteks konfiguratsiooniandmeid, mida esialgu kasutati Samba paketi uuema versiooniga, võib see tekitada probleeme.

Võimalik, et Samba vanem versioon ei suuda mõningaid parameetreid konfiguratsioonis läbi töödelda, kuna need on alles Samba hilisemas versioonis juurde tulnud. See asjaolu võib esile kutsuda soovimatuid (kõrval-)mõjusid või Samba funktsioneerimist täielikult takistada. Lisaks sellele tuleks enne taaskäivitamist tagada baasoperatsioonisüsteemi identne konfigureerimine (M 4.331 Samba serveri operatsioonisüsteemi turvaline konfiguratsioon). Vastavalt serverirollile ja käideldavuse nõuetele peaks serveri ootamatuseplaani raames toimuma serveri taaskäivitamise ja taasteaja regulaarne testimine ja parendamine.

Samba serveri seisundi taastamiseks peaks olema võimalik regulaarselt varundada järgmisi andmeid/ järgmist teavet:

- smb.conf fail (konfiguratsiooniandmed)
- olulise tähtsusega TDB-failid (konfiguratsiooniandmed ja staatuse info)
- konto info (staatuse info)
- logifailide kataloog (logiandmed).

Järgnevates lõikudes tutvustatakse meetmeid nimetatud andmete / info varundamiseks.

smb.conf (konfiguratsiooniandmed)

Fail smb.conf. on Samba tsentraalne konfiguratsioonifail. Selles failis toimub Samba teenuste seadistamine (nmbd , smbd ja winbindd). Selle faili salvestuskoht sõltub suvanditest, millega Samba on kompileeritud. “smbd -b | grep smb.conf” abil saab salvestuskoha teada.

TDB-failid (konfiguratsiooniandmed ja staatuse info)
Samba salvestab TDB-failidesse mitmesugust infot.

Mõned näited:

- Samba salvestab domeeni liikmena arvutikonto parooli failis secrets.tdb. Arvutikonto näol on tegemist tavalise kasutajakontoga domeenide kasutajate andmebaasis, mis on olemas igal liikmearvutil. Selle arvutikonto parooli abil toimub domeenide liikmete ja domeenikontrollerite vastastikune autentimine.

Kui arvutikonto parool läheb kaduma, peab Samba domeeniga uuesti liituma.

- Primaarse domeenikontrolleri (PDC) funktsioonis salvestab Samba secrets.tdb faili domeeni turvaidentifikaatori (SID). SID kadumine tähendab muu hulgas, et kõik kliendid peavad domeeniga uuesti liituma ja kõik kasutajaprofiilid tuleb uue domeeniga vastavusse viia.
- Teistesse TDB-failidesse salvestatakse reeglina vaid ajutist infot, mille kadu ei too endaga kaasa tagajärgi.

Samba salvestab TDB-failid kahte kataloogi. “smbd - b | grep PRIVATE_DIR” abil on võimalik välja selgitada PRIVATE_DIR kataloogi asukoht, välja arvatud juhul, kui smb.conf failis on kasutatud “private dir” suvandit. Sellesse kataloogi salvestatakse konfidentsiaalset infot sisaldavad TDB failid. Teise kataloogi näol on tegemist LOCKDIR-kataloogiga. Sellesse salvestatakse mittekonfidentsiaalset infot sisaldavad TDB-failid. “smbd - b | grep LOCKDIR” abil on võimalik välja selgitada LOCKDIR- kataloogi asukoht, välja arvatud juhul, kui smb.conf failis kasutatakse suvandit “lock directory”.

Soovitatav on teha regulaarselt kõikidest TDB-failidest mõlematesse kataloogidesse varunduskoopiad. TDB-faile, mis on salvestatud mõlema kataloogi alamkataloogidesse, ei ole vaja varundada. Need sisaldavad taaskäivitamiseks mittevajalikku informatsiooni. Tuleb tähelepanu pöörata asjaolule, et TDB-failide varundamine toimuks eeskirjadele vastavalt. (vaata lõiku „TDB-failide korrektne varundamine”).

Konto info (staatuse info)
Sõltuvalt sellest, millist Backend ’i (parameeter “passdb backend” smb.conf) Samba kontoinfo salvestamiseks kasutab, tuleb varundamiseks valida teine tee. Sambas 3.0.0 kuni 3.0.23 võis korraga kasutada mitut Backend’ i. Varasemad ja hilisemad versioonid ei toetanud seda funktsiooni. Taaskäivitamiseks on vajalik kõikide Backend’ ide kontoinfo regulaarselt varundada.

Olenevalt sellest, milliseid Backend’ e kasutatakse, soovitatakse kontoinfo varundamiseks järgmisi protseduure:

- smbpasswd - kui parameetri “passdb backend” kaudu smb.conf failis ei ole teisiti konfigureeritud (näiteks “passdb backend = smbpas-

swd:/etc/smb/ priv/datafile"), sõltub selle tekstifaili salvestuskoht sellest, milliste suvanditega on Samba kompileeritud. Kui ei ole kasutatud parameetrit "passdb backend", võib salvestuskoha välja selgitada „smbd -b | grep SMB_PASSWD_FILEäbil. Kuna see fail on lihtne tekstifail, ei ole varundamisel vajalik tähelepanu pöörata eripäradele.

- tdbsam - vastavalt standardile salvestatakse kontoinfo faili passdb.tdb kataloogis PRIVATE_DIR. Salvestuskohta on võimalik muuta parameetri "passdb backend" smb.conf kaudu (näiteks "passdb backend = tdbsam:/etc/smb/priv/datafile.tdb"). Tuleb silmas pidada asjaolu, et sellelt TDBfaililt toimub reeglitele vastav varundamine (vaata lõiku "TDB-failide õige varundamine").
- ldapsam - juhul kui asutuse või ettevõtte täieliku lihtsustatud kataloogisirvimise protokolli (LDAP) kataloogis puudub regulaarse varundamise protsess, tuleb Sambale olulise tähtsusega kontoinfo varundamiseks kindlaks määrata oma protsess.

Logifailide kataloog (logiandmed).

Sellesse kataloogi salvestavad nmbd, smbd ja winbindd oma logiandmed. Samba serveri seisundi taastamiseks ei ole andmed vajalikud. Kuid arvestades sellega, et hiljem tuleb leida tõrgete põhjused, tuleks neid andmeid regulaarselt varundada. Kui failis smb.conf ei ole teisiti konfigureeritud (suvand „log file"), sõltub kataloogi asukoht sellest, milliste suvanditega on Samba kompileeritud Sellisel juhul saab kataloogi asukoha kindlaks määrata "smbd –b | grep LOGFILEBASE" abil.

TDB-failide õige varundamine

TDB näol on tegemist binaarse andmebaasi formaadiga sarnaselt Berkeley DBle, mis toetab nii mitmete protsesside üheaegset kirjutusjuurdepääsu kui ka lukustamist. TDB-failide eripäraks on, et deemonid vahesalvestavad tihti andmebaaside sisu pikemaks ajaks ning nende kõvakettal olev sisu ei pea töötamise ajal enam alati aktuaalne olema. Lisaks sellele ei uuendata kirjutamise ajal TDBfailidesse failide ajatempleid. Kui TDB-failide varundamine töö käigus toimub ebasobivate programmidega (näiteks "cp"), ei arvesta need nende failide eripära. Loodud varukoopiad on teatud juhtudel mittevajalikud.

Varundusmehhanismidele nagu näiteks "rsync" valmistab normaalkäituse ajal probleeme see, et TDB-failide ajatemplid pärast varundusoperatsiooni ei muutu. Rsync ei ole nii võimeline kindlaks tegema, kas TDB-failide sisu on mingil määral muutunud. Andmebaaside konsistentsete varukoopiate loomiseks Samba käituse ajal tuleb kasutada rakendust "tdbbackup". "tdbbackup /etc/samba/passdb.tdb" käivitamine loob varufaili /etc/samba/ passdb. tdb.bak. "tdbbackup -v etc/samba/passdb.tdb" käivitamisega on võimalik kontrollida andmebaasi terviklust. Kui leitakse kahjustusi, kasutatakse andmebaasi taastamiseks olemasolevat varundusfaili. Parameetri –s kaudu saab tdbbackup-ile edastada, milliseid failide nimelaiendeid tuleb varundamisel ja kontrollimisel kasutada. Mõeldav oleks .bak asemel kasutada kuupäeva, näiteks 20080303.

Kontrollküsimused:

- Kas üleorganisatsioonilise andmevarunduskontseptsiooni raames toimub Samba serveri taaskäivitamiseks vajalike süsteemikomponentide varundamine?
- Kas varundamisel arvestatakse TDB-failide omapäraga?
- Kas konfiguratsioonifailide, staatuse info ja süsteemifailide taaskäivitamisel pööratakse tähelepanu asjaolule, et need peavad üksteisega ühilduma?
- Kas vastavalt serverirollile ja käideldavuse nõuetele toimub serveri ootamatuseplaani raames taastamise ja taasteaja testimine ja vajadusel parendamine?
- Kas kõikide kasutuses olevate Backend 'ide kontoinfo varundamine toimub regulaarselt ja reeglitekohaselt?

M 6.136 Hädaolukorraks valmisoleku plaani koostamine Samba serveri avarii puhuks

Algatamise eest vastutavad: infoturbespetsialist, IT-juht
Rakendamise eest vastutavad: administraator
Ootamatuseplaani koostamisel Samba serveri tõrke puhuks tuleks kõigepealt tähelepanu pöörata M 6.96 Serveri avariiplaan .

Lisaks tuleb arvestada järgmiste aspektidega:

- Installatsiooniallikad (näiteks lähteteksti- või binaarpaketid), millega Samba server on installeeritud, tuleks deponeerida kindlaksmääratud kohta (M 6.21 Kasutatava tarkvara varukoopia).
- Juhul kui Samba teenus installeeriti lähtekoodist, peaks dokumentatsioon sisaldama kõiki installeerimisel kasutatud optsioone (eriti optsioone, millega käivitati konfigureerimisskript).
- Juhul kui Samba teenus installeeriti binaarpaketist, tuleks dokumenteerida kõik etapid, mille järgi oleks installeerimise kulg arusaadav.
- Dokumenteerida tuleb kõik konfiguratsioonifaili muudatused, eriti smb.conf faili muudatused. Soovitatav on kasutada versioonihaldust. Lisaks sellele tuleb kõik konfiguratsioonifailid regulaarselt varundada. M 6.135 Samba serveri tähtsate süsteemikomponentide regulaarne varundamine annab täiendavat informatsiooni nimetatud teema kohta.

Kontrollküsimused:

- Kas on olemas vajalikud paketid ja info, et Samba serverit oleks hädaolukorras võimalik kiiresti uuesti installeerida?
- Kas konfiguratsiooni muutused dokumenteeritakse?
- Kas installatsioonipaketid, millest Samba server installeeriti, on deponeeritud kindlaksmääratud kohta?
- Kui Samba server installeeriti lähtetekstipaketist, kas on dokumenteeritud installeerimisel kasutatud suvandeid?
- Kas toimub regulaarne konfiguratsioonifailide varundamine?

M 6.138 Hädaolukorraks valmisoleku plaani koostamine virtualiseerimiskomponentide tõrke puhuks

Algatamise eest vastutavad: IT-juht, infoturbespetsialist
Rakendamise eest vastutavad: administraator

Virtualiseerimisserveri rivist väljalangemisel on infosüsteemile laialdane mõju. See tuleneb sellest, et rivist väljalangemine ei mõjuta mitte ainult virtualiseerimiskomponente, vaid ka kõik komponendil käitatavaid virtuaalsed IT-süsteeme. Seetõttu ei saa virtualiseerimiskomponendi rivist väljalangemist vaadelda kui eraldiseisvat juhtumit. Arvutisüsteemi IT-süsteemide virtualiseerimise kasutamise planeerimise raames tuleb arvestada, et soovitud konsolideerimisefektidega riistvara puhul tõuseb ka rivist väljalangemisega kaasneva kahju suurus.

Mida suurem on konsolideerimise mõju, seda suurem on potentsiaalne kahju. Seetõttu peab virtualiseerimiskomponentide turbevajadus peegeldama kõigi sellel paiknevate virtuaalsete IT-süsteemide turbevajadust. Siin tuleb jälgida maksimumipõhimõtet ja kumulatsioonipõhimõtet. Lisaks ei ole tihtipeale piisav jälgida ainult virtualiseerimisserverite rivist väljalangemist, millel virtuaalseid IT-süsteeme käitatakse. Kaasata tuleb ka teised, virtualiseerimisserveri käitamiseks vajalikud IT-süsteemid. Nende süsteemide rivist väljalangemine võib piirata virtualiseerimissüsteemide käideldavust.

Seetõttu tuleb alltoodud süsteemidele, kui need olemas on, kindlaks määrata tegutsemisviis nende rivist väljalangemisel:

- Virtualiseerimisserver
- Haldusserver (eelkõige Connection-Broker)
- Litsentsiserver

Sõltuvalt sellest, kuidas on virtualiseerimissüsteemid IT-taristusse integreeritud, tuleb vaadelda ka teisi süsteeme, nagu näiteks kataloogiteenuseid ja nimeteisendusteenuseid. Kuna taristuteenuseid nagu kataloogiteenused või nimeteisendusteenused on võimalik teostada ka virtuaalsetel IT-süsteemidel, võib ühe või mitme virtualiseerimiskomponendi rivist väljalangemisel tekkida väga keeruline olukord. Näiteks tuleb tugevalt virtualiseeritud andmekeskuse taaskäivitamist tihtipeale tekkivate teenusesõltuvuste tõttu detailselt planeerida.

Jälgida tuleb järgmisi aspekte:

- Virtualiseerimissüsteemide ootamatusplaan tuleb integreerida olemasolevasse ootamatusplaani (vt B 1.3 Hädaplaanimine).
- Virtualiseerimisserveri süsteemi rivist väljalangemine võib viia andmekaoni kõigil virtualiseerimisserveril paiknevatel virtuaalsetel IT-süsteemidel. Seepärast tuleb kõigi virtuaalsete IT-süsteemide jaoks kontrollida, kuivõrd on

võimalik olemas olevat andmevarunduskontsepti (B 1.4 Andmevarunduspoliitika) valitud virtualiseerimistehnikaga sobitada. Virtuaalsete IT-süsteemide puhul tuleb kontrollida, kas on võimalik uut andmevarundustehnikat (snapshot'id) kasutada ja millised võivad olla positiivsed ja negatiivsed mõjud. Andmevarundusse tuleb kaasata olulised süsteemikujutised.

- Kui üks virtualiseerimisserver langeb rivist välja, langevad välja ka kõik sellel käitatavad virtuaalsed IT-süsteemid. Tõenäosus, et vähemalt ühe kahjustatud virtuaalse IT-süsteemi juures tekib arvestatav andmekadu, tõuseb koos sellest puudutatud süsteemide arvuga. Ootamatusplaani korral tuleb seega arvestada, et võimalusel tuleks sisse planeerida laiaulatuslik taastusprotsess.
- Kui ühes farmis kasutatakse mitut virtualiseerimisserverit (virtuaalne taristu), tuleb jälgida, et valitakse virtuaalsete IT-süsteemide mõttekas gruppidesse jaotamine. Näiteks ei tohiks ühel virtualiseerimisserveril käitada koos kahte süsteemi, mis võivad teostada vastastiku üksteise ülesandeid.
- Tuleb kindlustada, et ootamatuste korral oleks kasutada virtuaalsete taristutega töötamiseks koolitatud personal.
- Virtualiseerimisserverite süsteemikonfiguratsioon (vt M 2.315 Serveri kasutuselevõtu planeerimine , M 2.318 Serveri turvaline installeerimine ja M 4.237 IT-süsteemi turvaline aluskonfiguratsioon) peab administraatoritele olema alati kättesaadav. See peab olema kujundatud nii, et ootamatuste korral suudaksid seda taastada ka töötajad, kes ei ole eelnevalt tehtud konfiguratsioonist detailselt teadlikud.
- Koostada tuleb taaskäivitusplaan, mis tagab virtualiseerimisserveri ja sellel paiknevate virtuaalsete IT-süsteemide reguleeritud taaskäivituse.
- Tuleb kindlustada, et virtualiseerimissüsteemide taaskäivitamine ei sõltuks ühestki andmekeskuse teenusest, mida pakub ainult üks virtuaalne IT-süsteem.
- Ootamatusplaani raames tuleks vaadelda erinevaid stsenaariume, mille korral on virtualiseerimissüsteemid kas täielikult või ainult osaliselt kompromiteeritud.

Nende stsenaariumite jaoks tuleb täpselt kirjeldada, kuidas sellele reageerida ja millised tegevused tuleb vastavalt teostada. Tegutsemist tuleks regulaarselt kontrollida.

Ootamatute asjaoludega toimetulemise õigeaegne planeerimine koos etteantud tegevusjuhistega, mida suudavad järgida ka isikud, kes ei ole virtualiseerimisserveri haldusega täpselt kursis, võib kahjujuhtumi tagajärgi vähendada. Dokumendid ootamatute situatsioonide kohta peavad volitatud isikutele kättesaadavad olema. Kuna nad sisaldavad tähtsat informatsiooni, tuleb neid turvaliselt säilitada. Eraldi tuleks vaadelda vähemalt järgmisi ootamatussituatsioone.

Rünne

Kui avastati ründed virtualiseerimisserverile, ei saa lähtuda sellest, et need olid suunatud virtualiseerimissüsteemil enda suhtes. Tuleb kontrollida, ega ei ole kompromiteeritud virtualiseerimissüsteemil paiknevaid virtuaalseid IT-süsteeme.

Seejuures tuleb arvestada võimalusega, et virtualiseerimisserveril aga ka virtuaalsetele IT-süsteemidele võib olla installeeritud kahjurvara (Backdoor , Trooja hobused). Peale selle on võimalik, et virtualiseerimisserveri võrgukonfiguratsiooni kaudu on avatud ebasoovitavad sideteed. Lisaks võib olla virtuaalseid IT-süsteeme kopeeritud. Kahjurvara usaldusväärseks eemaldamiseks on soovitatav virtualiseerimiskomponent täielikult taastada. Selleks võib kasutada eelnevalt loodud andmevarundusi aga ka süsteemikonfiguratsiooni dokumentatsiooni ja installeerimisjuhiseid.

Kui kasutatav virtualiseerimiskeskkonnas puudub kasutajahaldus administratiivsete ligipääsude juhtimiseks, tuleb kasutajakontosid ja eriti superkasutajate kontosid kontrollida korrektse gruppikuulumise suhtes. Järgnevate rünnakute edu vähendamiseks tuleb muuta kõik paroolid. Virtuaalsetele IT-süsteemidele, mida käitati kompromiteeritud virtualiseerimisserveril, tuleks läbi viia vastavas ootamatusplaanis kirjeldatud meetmed.

(Füüsiliste) virtualiseerimisserverit röövimine

Virtualiseerimisserverite varguse korral tuleb kõik kontaktid virtualiseerimisserveri haldamiseks varustada uute paroolidega. Tuleb arvestada, et virtualiseerimisserveriga koos varastati ka virtuaalseid IT-süsteeme, seda eelkõige siis, kui need olid salvestatud virtualiseerimisserveri lokaalsele kõvakettale. Isegi kui see nii ei ole, tuleb arvestada sellega, et varas on saanud oma käsutusse laialdased teadmised virtuaalse IT-süsteemi süsteemikonfiguratsioonist ja andmekeskuse virtualiseerimistaristust. Seetõttu tuleb kontrollida, kuivõrd võivad virtualiseerimistaristu parandused või muudatused kaasa aidata taristu paremale vastuseisule tulevaste rünnakute korral. Kahtluse korral tuleks kogu virtuaalne IT-süsteem taaskäivitada.

Virtuaalsete IT-süsteemide röövimine

Virtuaalse IT-süsteemi röövimine ei nõua reeglina füüsilist ligipääsu andmekeskusele. Ründaja saab virtuaalseid IT-süsteeme näiteks virtualiseerimisserveri funktsioonide kaudu kopeerida. Et pääseda ligi salvestusressurssidele, millel paiknevad virtuaalsed IT-süsteemid, vajab ründaja ainult ligipääsu võrgule. Ennetavalt tuleb välja töötada meetmed, mis seda võimalust raskendaksid (M 1.74z Virtuaalse taristu planeerimine ja M 4.349 Virtuaalse taristu turvaline kasutamine). Peale selle tuleb veel kontrollida, kuivõrd on võimalik selliseid rünnakuid avastada. Virtuaalsete IT-süsteemide ootamatusplaan peaks seega sisaldama regulatsioone, mis kirjeldaksid sellise röövi järgset tegevust.

Väärkonfiguratsioon

Virtualiseerimisserverite väärkonfiguratsioonil võivad andmekeskusele olla ulatuslikud negatiivsed tagajärjed. Seepärast tuleb hädaolukorraks valmisoleku raames virtualiseerimistarkvara regulaarselt väärkonfiguratsiooni suhtes kontrollida. Kui avastatakse väärkonfiguratsioon, tuleb hinnata selle mõju. Eelkõige tuleb siinjuures kontrollida, kas väärkonfiguratsioonist on mõjutatud virtuaalsed IT-süsteemid. Sõltuvalt väärkonfiguratsiooni tüübist võib mudatused konfiguratsioonivea kõrvaldamiseks teostada koheselt. Seejuures tuleb aga jälgida, et sellised muudatused võivad virtuaalseid IT-süsteeme mõjutada. Seepärast võib olla vajalik

enne konfiguratsioonimuudatuste läbiviimist virtualiseerimissüsteemid välja lülitada.

Rivist väljalangemine vääramatu jõu tõttu

Vääramatust jõust tulenevad ohud, näiteks maavärinad, üleujutused, tulekahjud, tormikahjud, kaablirikked, võivad virtualiseerimisserveri käideldavust negatiivselt mõjutada. Siinkohal tuleb kontrollida sobivaid meetmeid käideldavuse suurendamiseks, nagu näiteks IT-süsteemide liiased kommunikatsiooniühendused.

Kontrollküsimused:

- Kas kontrolliti virtuaalse taristuga kaasaskäiva konsolideerimisefekti mõju virtualiseerimisserveri käideldavusnõuetele?
- Kas määrati kindlaks toimimine virtualiseerimiskomponentide rivist väljalangemise korral?
- Kas ootamatusplaan on virtuaalse taristuga ühtlustatud?
- Kas andmevarunduskontseptsioon on virtuaalse taristuga ühtlustatud?
- Kas on kindlustatud, et ootamatuste korral on kasutada sobivad dokumendid ja personal?
- Kas koostati regulatsioonid, milles kirjeldatakse tegutsemist pärast virtuaalse IT-süsteemi röövi.
- Kas virtualiseerimisservereid kontrollitakse regulaarselt vigade suhtes?
- Kas kontrolliti meetmete vajadust, mis puudutavad käideldavust vääramatu jõu korral?

M 6.139 DNS-serveri avariiplaani koostamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht
Rakendamise eest vastutab: administraator
DNS-i avariil on tõsised tagajärjed kogu IT-infrastruktuuri tööle. Siinjuures pole probleemiks mitte niivõrd DNS-süsteemi avarii ise, kuivõrd sellest tulenev DNS-il põhinevate teenuste pärssimine. Veebiserveritele ei pääse enam ligi, kaughooldus ei tööta. Olenevalt DNS-serveri avariist ei tööta enam institutsioonisisene ja/või -väline nimeteisendus.

Kui väline nimeteisendus lakkab töötamast, märkab avalikkus seda tavaliselt kiiresti, aga kui katkestused muutuvad regulaarseks või pikaks, võib see kahjustada organisatsiooni mainet. Seega tuleb luua kontseptsioon, mis tegeleb avarii ja selle võimalike tagajärgede minimeerimisega.

Tegevuse kindlaksmääramisel tuleb arvestada järgnevaga:

- DNS-serveri avariiplaan tuleb integreerida olemasoleva avariiplaaniga (B 1.3 Hädaplaanimine).
- Süsteemi avarii tagajärjel võivad tekkida andmekaod. Seega tuleb tsoonifailide jaoks koostada andmevarunduse kontseptsioon. See tuleb integreerida olemasoleva andmete varundamise kontseptsiooniga (B 1.4 Andmevarunduspoliitika)
- Lisaks DNS-serveri avariiplaani peab olemas olema ka serveri operatsioonisüsteemi avariiplaan.
- Internetist tulevate päringute jaoks mõeldud DNS-serveri käitamiseks läheb tarvis töötavat internetiühendust.
- Süsteemi konfiguratsioon tuleb dokumenteerida (M 2.25 Süsteemi konfiguratsiooni dokumenteerimine). Olulisi ülesandeid tuleb kirjeldada nii, et IT-töötajad suudaksid avarii korral terviksüsteemi töökorda seada ka siis, kui nad ei tunne selle süsteemi konfiguratsiooni.
- Kui avarii põhjuseks oli rünne, tuleb turvaauk kõrvaldada ja dokumenteerida.
- Tuleb koostada taastamisplaan, et IT-süsteemi saaks uuesti nõuetekohaselt tööle panna.
- Avariiplaani tuleb katsetada, et veenduda selle praktilisuses.

Kontrollküsimused:

- Kas DNS-serverite jaoks on olemas avariiplaan?
- Kas DNS-serverite avariiplaan on integreeritud juba olemasolevate avariiplaanidega?
- Kas DNS-serveri avariiplaan on nõuetekohaselt dokumenteeritud?

M 6.140 Hädaolukorra plaani koostamine rühmatarkvarasüsteemide avarii puhuks

Algatamise eest vastutavad: infoturbespetsialist, IT-juht, hädaolukorra spetsialist
Rakendamise eest vastutavad: administraator

Rühmatarkvarasüsteemi osalise või täieliku rivist väljalangemisega kaasnevad kasutajate töövõimalustele enamasti tõsised tagajärjed, kuna mitte ühtegi serveril põhinevat ülesannet ei saa enam täita. Hädaolukorraks valmisoleku raames tuleb koostada kontseptsioon selle kohta, kuidas oleks võimalik väljalangemise kahjusid vähendada ja kuidas käituda rivist väljalangemise korral. Kasutatava rühmatarkvarasüsteemi hädaolukorraks valmisoleku planeerimisel peab arvestama asutuse hädaolukorra plaaniga (B 1.3 Hädaplaanimine).Kõigi rühmatarkvarakomponentide süsteemikonfiguratsioon tuleb dokumenteerida. Siia hulka kuuluvad kõvaketta partitsioonid ja nende kasutusala (süsteem, tegevusprotokoll, andmebaas jne) ning lisaks veel riistvara, rühmatarkvaraserveri operatsioonisüsteemi ja vajalike rühmatarkvara teenuste dokumentatsioon.

Rühmatarkvarasüsteemi töös hoidmiseks või selle taaskäivitamiseks vajalikke ülesandeid peab kirjeldama nii, et koolitatud personal saaks hädaolukorras need kohe ellu viia. Dokumentatsiooni detailsus sõltub hädaolukorras kasutatava personali teadmistest. Kui asutuses on näiteks grupp koolitatud administraatoreid, on võimalik hädaolukorra dokumentatsioonis teatud teadmisi juba eeldada. Kui asutuses tegutseb aga ainult üks koolitatud administraator, peaks hädaolukorra dokumentatsioonis sisalduvaid olulisi meetmeid kirjeldama nii, et neid saaks ellu viia mis tahes spetsialist.

Rühmatarkvarasüsteemi turvaliseks ja tõrgetevabaks käituseks peab rühmatarkvaraserver olema pidevalt kättesaadav. Serveri väljalangemise mõjude vähendamiseks saab rühmatarkvara andmeid partitsioonide loomisega jagada mitme serveri peale. Üksiku serveri väljalangemine mõjutab seejuures ainult osa andmetest. Partitsioonide loomist peavad planeerima spetsialistid, kes selle ka ellu viiksid. Hädaolukorras peab vähemalt osa rühmatarkvara klientidest olema töökorras või sellises seisus, et neid saaks kiiresti töökorda seada. Sellekohane tegevus tuleb dokumenteerida hädaolukorra plaanis.

Süsteemi väljalangemisega võib kaasneda ka andmekadu rühmatarkvaraserveril või -kliendil. Seetõttu tuleb rühmatarkvara jaoks luua andmevarunduskontseptsioon, mis tuleks paigutada juba olemasolevasse andmevarunduskontseptsioon (B 1.4 Andmevarunduspoliitika). Hädaolukorraks valmisoleku raames tuleks arvestada erinevate kompromiteerimisstsenaariumitega ja ette anda spetsiifilised tegutsemisviisid serveri, üksikute teenuste või kasutajakontode kompromiteerimise korral. Süsteemi taastamise kriisiõppusi on soovitatav regulaarselt läbi viia. Kriisi-

harjutustes tuleks arvestada kõiki süsteemi väljalangemise ja kompromiteerimise aspekte. Vastutavad isikud peaksid testkeskkonnas üksikud teenused välja lülitama (näiteks nagu kompromiteerimise korral) ja seejärel taaskäivitamist harjutama. Testsüsteem peaks tootmissüsteemiga võimalikult palju sarnanema.

Mõningatel juhtudel on andmete taastamiseks või rühmatarkvarasüsteemi parandamiseks vaja tundlikku ligipääsuinformatsiooni, nagu näiteks krüptograafilisi võtmeid või paroole. Tuleb jälgida, et ohutusplaan määraks sellisteks juhtudeks kindlaks konkreetse tegevusplaani. Lisaks tuleb andmevarunduse või teiste meetoditega kindlustada, et see teave on hädaolukorras kättesaadav. Koostada tuleb taaskäivitusplaan, mis tagaks pärast väljalangemist, et rühmatarkvarasüsteem käivitatakse taas reguleeritud moel.

Kontrollküsimused:

- Kas kasutatava rühmatarkvarasüsteemi jaoks on olemas hädaolukorra plaan?
- Kas kasutatava rühmatarkvarasüsteemi jaoks on olemas taaskäivitusplaan?
- Kas kriisiõppused toimuvad regulaarselt?

M 6.141 Interneti kasutamise asendusprotseduurid

Algatamise eest vastutavad: infoturbespetsialist, IT-juht, ülemused
Rakendamise eest vastutavad: infoturbespetsialist, personaliosakond

Põhjused, miks internetile ligi ei pääse või miks ligipääs on häiritud, võivad olla erinevad. Häiritud võivad olla ka ainult mõned üksikud veebiteenused ja -funktsioonid. Käituse tagamiseks kasutatakse tihti küll mitmetasandilisi meetmeid, kuid siiski võib juhtuda, et teatud veebiteenused pole kasutajatele kas ajutiselt kättesaadavad või ei tööta need õigesti. Kui interneti rike ei ole asutusele või ettevõttele vastuvõetav, on oluline kindlaks määrata vastavad asendusprotseduurid.

Neid protseduure kasutatakse seisakuaegade vältimiseks viisil, mis tagab ettenähtud tööprotsesside nõuetekohase jätkumise ka rikete korral või vähemalt vähendab rikke mõju. Avariihalduse raames tuleks seega välja töötada kontsept, kuidas vähendada asendusprotseduuridega võimalike rikete mõju ning mida on tarvis teha, kui tekib rike.

Näide:

Töötajatel seisab ees töölähetus ja nad broneerivad rongipiletid ise läbi interneti. Selleks, et interneti rikke korral ei tekiks tööprotsessis viivitusi, saab pileteid broneerida ka telefoni teel. Interneti kasutamise rikke asendusprotseduuride valimisel tuleks eristada vähemalt järgmisi stsenaariume:

1. rikked enda võrgu piires;
2. kommunikatsiooniühenduste rikked enda võrgu ja internetis kasutatavate IT-süsteemide vahel;
3. internetis kasutatavate IT-süsteemide rikked.

Enda võrgu rikkeid (1. stsenaariumi) käsitletakse B 1.3 Hädaplaanimine ja ka teistes IT etalonturbe kataloogi moodulites, mis kajastavad hädaolukorraks valmisoleku valdkonda. Kuna tehnilisi komponente käitavad tavaliselt kolmandad isikud, siis ei ole 2. ja 3. stsenaariumi institutsiooni sees peaaegu üldse võimalik mõjutada. Mõningast kaitset teatud liiki võrgurikete vastu pakub teise, st alternatiivse interneti teenusepakkuja ja vajaduse korral ka alternatiivse kommunikatsioonikanali kasutamine (vt M 6.75z Varu-sidekanalid). Kui rikke tõttu langevad rivist välja aga võrgu suuremad osad, võib juhtuda, et tegevuseks olulised veebilehed ei ole enam kättesaadavad või ei tööta. Seetõttu tuleks luua ülevaade range käideldavusnõudega veebiteenustest ja rakendustest. Seejärel tuleks nende jaoks välja töötada sobivad asendusprotseduurid. Ülevaadet tuleks regulaarselt värskendada.

Soovitatav on mõelda ka sellistele asendusprotseduuridele, mis saavad võimaluse korral hakkama ilma internetita. Tihti kasutatakse selleks telefonil või faksil põhinevat kommunikatsiooni. Tähelepanu tuleb pöörata sellele, et ka siin võivad valitud lahendused üksteist vastastikku mõjutada ning see võib omakorda pärssida ka asendusprotseduure. Näiteks tuleb internetitelefoni kasutamisel tagada, et interneti rike ei tooks endaga automaatselt kaasa telefoni- ja faksiteenuse riket.

Lisanäide sõltuvussuhete kohta on olukord, kus teenusepakkujate kõnekeskused sõltuvad oma töös organisatsiooni veebiserveri korrektsest toimimisest. Sellisel juhul ei ole internetiteenuse rikke korral teenusepakkuja infonumbrile helistamisest mingit kasu, sest arvatavasti on ka kõnekeskus töövõimetu. Põhimõtteliselt võib asendusprotseduurina vaadelda ka kommunikatsiooni ja andmetöötlust paberi teel. Enamasti langevad sellised meetodid aga valikust välja, sest ajaline viivitus on nende korral liiga pikk.

Kontrollküsimused:

- Kas range käideldavusnõudega veebiteenustest ja -rakendustest on olemas ülevaade?
- Kas kriitiliste veebiteenuste ja -rakenduste jaoks on kindlaks määratud asendusprotseduurid?

M 6.142z Redundantsete (ressurssi osaliselt või täielikult dubleerivate) terminaliserverite kasutamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht
Rakendamise eest vastutavad: administraator

Kuna terminaliserveri keskkonna rivist välja langemisest võib olla mõjutatud suur hulk kasutajaid, tuleb kasutusele võtta meetmed, et rivist väljalangemise korral oleks kahju nii väike kui võimalik. Lisaks on terminaliservereid võimalik ainult osaliselt laiendada, nii et tekkiv lisa süsteemikoormus tuleb jagada mitme serveri vahel (vt M 2.465 Terminaliserveri vajalike ressursside analüüs). Terminaliserveri gruppide kaudu on selliste juhtudel võimalik kindlustada nõuded selle kättesaadavusele. Selleks tuleb kasutajate seansid jagada sobivalt erinevate terminaliserverite vahel. Siinkohal tuleb arvestada, kuivõrd on terminaliserverid, millele terminaliserveri seansse üle kantakse, kättesaadavad ja kui suur on nende töökoormus.

Praktikas kasutatakse sellistel juhtudel kahte meetodit: võrgukoormusejagajaid (Loadbalancer) ja vastava terminaliserveri lahenduse süsteemiomaseid mehhanisme. Sisesed lahendused võrgukoormuse jaotamiseks võivad peale võrgukoormuse kontrollida ka protsesside ja mälu kasutamist. Nii välditakse, et väheste sisendite ja väljunditega aga samas jõudlust nõudvate protsessidega terminaliserveritele jagataks liiga palju kasutajaid. Kõrgete kättesaadavusnõuetega terminaliserveri keskkondades tuleks kasutada võrgukoormuse jaotamise mehhanisme, mis arvestavad ka nende faktoritega. Kui kasutatakse lahendusi automaatseks seansside jagamiseks, tuleks kasutusele võtta seansikataloog. Alles seeläbi saab võimalikuks, et kindla terminaliserveriga lõpetatud ühendus on võimalik hiljem uuesti luua ja kasutaja saab oma poolelijäänud seanssi jätkata.

Seansikataloog salvestatakse Citrix Presentation Server i ja Windows terminaliserveri all andmebaasides ja tuleks seega installeerida ainult spetsiaalsetele süsteemidele. Microsofti terminaliserverite korral kutsutakse seanssikataloogi Session Directory Citrix'i all salvestatakse seanssiiformatsioon nn IMA-s (Independent Management Architecture) ja osaliselt ZDC-s (Zone Data Collector). Selles andmebaasis sisalduv informatsioon on terminaliserveri farmi seisukohast infoturbeks olulise tähtsusega. Neid tuleks rivist väljalangemise, manipulatsiooni ja väärkasutuse vastu kaitsta (vt B 5.7 Andmebaasid). Nii Session Directory kui ka IMA Datastore vaikeseadistuse standardparoolid tuleb muuta. Kui terminaliserveril võimaldatakse rakenduste kasutamist, mis võimaldavad otsest ligipääsu andmebaasile või alluvad kõrgele turbevajadusele, tuleb andmebaasisüsteeme käitada eraldiseisvas võrgusegmendis. Sellisel juhul peaksid terminaliserveri farmi ja haldusteenuste vahelist ühendust kontrollima tulemüürid.

Kontrollküsimused:

- Kas terminaliserverite rivist väljalangemise kompenseerimiseks on need paigaldatud redundantselt?
- Kas kasutajaseansid jagatakse sobivalt erinevate terminaliserverite vahel?
- Kas terminaliserveri seansikataloogi andmebaasi standardparool on muudetud?

M 6.143 Terminaliserveri kliendi kasutuselevõtt katkestuse järgselt

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator

Kui terminaliserveri klient langeb rivist välja, ei ole vastaval kasutajal võimalik terminaliserveril paiknevatele rakendustele ligi pääseda. Seepärast peaks ilma oma operatsioonisüsteemita terminalide kasutamisel (*Thin Clients*) varuks hoidma asendus IT-süsteeme. Defektsete IT-süsteemide kiireks väljavahetamiseks võib vajaliku terminaltarkvara juba eelnevalt installeerida ja konfigureerida. Varusüsteemide vajaliku arvu hindamisel tuleks orienteeruda töökohtade arvust ja rivist väljalangemise tõenäosusest. Raskendatud tingimustes, näiteks suure mustuse ja tolmu käes ning kõrgete temperatuuride juures võib installeeritud klientide eluiga olla kordades väiksem. Sellised raamtingimused tuleb kalkulatsiooni sisse arvestada. Terminalide eemaldamine ning uute süsteemide kasutusele võtt tuleb dokumenteerida.

Täiendavad kontrollküsimused:

- Kas varusüsteemidena hoitakse valmis piisav kogus terminaliserveri kliente?
- Kas terminaliserveri klientide kasutamine varusüsteemidena on dokumenteeritud?

M 6.144z Terminaliserveri kliendi konfiguratsioon duaalseks kasutamiseks tava klient PC-na

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator

Kui keskne terminaliserveri teenus langeb rivist välja, saab terminaliserveril kasutatavate rakenduste ennetaval installeerimisel klient PC-le hädakäitust ajutiselt ülal hoida. Antud meetodi eelduseks on töökohaarvutid, millel on piisavalt ressursse ja iseseisev operatsioonisüsteem, mis on võimeline neid programme teostama. Selleks võib luua valikumenüü, mis lubab kasutajal arvuti käivitumisel eristada klientserver režiimi ja terminaliserveri konfiguratsiooni vahel. Tavalistel klient PC-del (*Fat Clients*), mis juba tavakäituses iseseisvalt rakendusi teostada suudavad ja ainult kindlad rakendused terminaliserverilt laeb, on lisaks võimalus mõlemad tarkvara paralleelselt installeerida. Kasutajatele tuleks läbi viia koolitus, mis näitab nende valikuvõimaluste õiget kasutamist. Terminaliserveri kasutamisel klient-PC-na tuleb järgida B 3.102 Server Unixi all .

Täiendav kontrollküsimus:

- Kas kasutajaid koolitati klient PC-de kasutamiseks terminaliserveri klientidena?

M 6.145 Kodukeskjaama (PBX) hädaolukorraks valmisolek

Algatamise eest vastutavad: infoturbespetsialist, IT-juht
Rakendamise eest vastutavad: IT-juht, administraator

Igas IT-käituses esineb häireid, mis võivad ulatuda komponentide juhuslikust väärkasutusest kuni mõne kindla seadme avariini. Turvalise käitamise eelduseks on häireolukorraks valmisolek. See puudutab riistvara ja tarkvara avariisid või kahjustusi, mis tulenevad kas defektidest, ohustatusest või kasutaja väärkasutusest. Selleks, et taolistele olukordadele oleks võimalik efektiivselt ja kiiresti reageerida, tuleb juba varem planeerida, kuidas võimalikke rikkeid kõrvaldada ja kriisisituatsioonideks valmis olla. Seepärast on otstarbekas määrata vastutajad ja kontaktisikud.

Tüüpiliste ja tõenäoliste kahjusituatsioonide kõrvaldamiseks tuleb koostada viivitamata rakendatavad meetmed ja juhised edasiseks tegevuseks. Üheks taoliseks tüüpiliseks viivitamata rakendamise meetmeks võib olla näiteks eraldi PSTNlülitusega otse ühendatud telefon, et hädaolukorras oleks võimalik kõnesid teha. Alternatiiviks või lisameetmeks võivad olla valmis pandud mobiiltelefonid, mida vajadusel saaks kasutada. Niinimetatud katastrooflülituse abil, mis kuulub varem rakendatavate abinõude hulka, võivad olemasolevad sissetulevad ja väljaminevad juhtmed olla suunatud varem kindlaksmääratud ühendustele. Sellega tagatakse, et katastroofi korral toimivad olulised üksused edasi.

Kodukeskjaama kindlatele elementidele võib olla mõttekas määrata asendusseadmed, mida tuleks ka töökorras hoida. Seda selleks, et oleks võimalik ettenägematult pikk ooteaeg samaväärse asendusriistvara abil üle elada. Asendusseadmed võivad hakata funktsioneerima niipea, kui neid vastavalt vajadusele vajalikul viisil konfigureeritakse. Selleks peavad kodukeskjaama konfiguratsiooniandmed olema varundatud (vt M 6.26 Kodukeskjaama (PBX) konfiguratsiooniandmete regulaarne varundus). Tavakäitusega võrreldes on taolisel varulahendusel tihti puudusi, eriti käitatavuse või liiasuse suhtes.

Üheks taolise varulahenduse tüüpiliseks näiteks on (ressursse nõrgestav) testsüsteem. Kõigile varulahendustele on tihti omane ühine asjaolu, et nende rakendamisel ei saavutata tavakäitust, vaid nende abil on võimalik tööd teha kuni tavaolukorra taastumiseni. Seepärast tuleks kodukeskjaama hädaolukorra plaanis kindlaks määrata, milliseid varulahendusi hädaolukorras rakendatakse ja millised sammud on vajalikud selleks, et need lahendused kasutusele võtta. Samuti tuleks kindlaks määrata, millises järjekorras millised kodukeskjaama komponendid taastatakse, kuna see aitab välja valida komponendid, mis tuleb kuni põhifunktsioonide täieliku taastumiseni kindlasti töös hoida. Mida olulisem on kodukeskjaama ühe osasüsteemi funktsioon kogu keskjaama töös, seda

varem tuleb see osasüsteem taastada või vähemalt ajutiselt asendada sarnaselt funktsioneeriva osaga.

Praktika on näidanud, et IT-kogulahendused on tihti liiga komplektsed selleks, et kõikvõimalike avariistsenaariume ettevalmistav läbimängimine ja igaühe jaoks sobilike taastamisvõimaluste määramine oleks võimalik. Seepärast oleks soovitatav lähtuda prioriteetidest.

Igale IT-süsteemidele määratakse selle prioriteetsusaste, mis tugineb järgmistele kriteeriumidele:

- sarnaste teenuste tehniline sõltumatus üksteisest,
- olulisus asutuse äriprotsessidele,
- nende kättesaadavusest kasu saava kasutajaskonna suurus.

Kõik abinõud, mis määratakse kindlaks selleks, et süsteemi oleks võimalik olulisuse järjekorras taastada, tuleb hädaolukorraks ettevalmistamise käigus dokumenteerida (nt IT-hädaolukorra käsiraamat). Just komplektsete süsteemide puhul on asutusele eripäraste ühenduste ja lahenduste kirjeldustel otsustav tähtsus, et osata riket hinnata ja võimalikult kiiresti ja turvaliselt tegutseda. Kui kogu asutust hõlmavas hädaolukorra käsiraamatus ei ole kodukeskjaamale konkreetseid tegevusi ette nähtud, tuleb need sätestada vastavas hädaolukorraplaanis. Nende tegevuste hulka kuuluvad kõik ettevalmistavad ja ettevaatavalt kindlaksmääratud viivitamata rakendatavad meetmed, varulahendused, käitamise viisid hädaolukorras ja teed nende saavutamiseks, aga ka tüüpilised toimingud tavakäituse taastamiseks. Samuti peab plaan sisaldama hädaolukorraks vajalikku kontaktinfot, kindlasti ka konkreetseid isikud, kes vastutavad hädaolukorra meetmete rakendamise eest. Samuti peab olema määratud isik, kellel on kohustus hädaolukord välja kuulutada. Hädaolukorra meetmete väljatöötamine ja nende vastavas olukorras rakendamine on väga tähtis. Tüüpmeetmete rakendamist tuleks regulaarselt harjutada. Kui seda ei tehta igapäevase rutiinse tegevuse käigus, tuleks selleks korraldada hädaolukorraõppusi.

Kontrollküsimused:

- Kas on olemas kodukeskjaama hädaolukorra kirjalik tegevusplaan?
- Kas kodukeskjaamaga seotult viiakse läbi hädaolukorraõppusi?
- Kas on nimetatud isikud, kes vastutavad hädaolukorras kodukeskjaama töö eest?

M 6.146 Andmete varundamine ja taastamine Mac OS X klientsüsteemides

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator, kasutaja

Mac OS X-s saab andmeid varundada süsteemi juurde kuuluva Time Machine'i teenusprogrammiga. Tarkvara on kasutusvalmis juba Mac OS X standardses installatsioonis. Time Machine'i teenusprogrammi saab ka kasutaja kergesti konfigureerida. Programm võimaldab kõvakettaid tervikuna või üksikuid katalooge varundada. Esmalt valmistab Time Machine varundatavast infost täieliku koopia, seejärel varundatakse veel ainult see info, mida on viimasest andmevarundusest saadik muudetud või mis on lisandunud (järkjärguline andmevarundus). Kui info varundatakse Time Machine'i teenusprogrammiga, tuleb silmas pidada järgmist:

- Varundusandmekandjal ei ole andmed krüpteeritud, seepärast tuleb neid hoida volitamata ligipääsu eest kaitstuna.
- Varundatud infot ei pakita kokku, mistõttu võib see hõivata kavandatust rohkem mäluruumi.
- Salvestatud andmete täielik taastamine võib olla aeganõudev.
- Kui teenusprogramm on sisse lülitatud, toimub andmevarundus automaatselt iga 30 minuti järel pärast IT-süsteemi käivitamist, kuid kasutajad võivad igal ajal teha ka käsitsi varunduse.
- Jooksvalt varundatakse ainult need andmed, mis ei ole File Vaultiga krüpteeritud. File Vaultiga krüpteeritud andmeid saab Time Machine'i abil varundada alles siis, kui kasutaja on end süsteemist välja loginud.
- Andmevõrgu kaudu varundamisel saab ilma täiendavate süsteemimuudatusteta kasutada ainult spetsiaalseid võrgumälusüsteeme (Network Attached Storage – NAS).
- Kogu süsteemi taastamisel peavad olemas olema Mac OS X installatsiooni DVD ning Mac OS X-ga klient tuleb sellest käivitada, sest taastamisprogrammid asuvad DVD-l.

Nende ja teiste piiravate tegurite tõttu on soovitatav kasutada Time Machine'i ainult piiratult. Time Machine'i kasutamine sõltub suuresti kohalikest asjaoludest. Heterogeense keskkonna jaoks andmevarundustarkvara valimisel on soovitatav kasutada andmevarunduseks selliseid programme, mis toetavad mitut platvormi, nt Mac OS X-t, Windowsit ja Linuxit. Time Machine'iga saab varundatud andmed salvestada välistele andmekandjatele, teistesse Mac OS X süsteemidesse või sisemisele andmekandjale, millelt süsteemi ei käivitata. Kui andmevarunduseks kasutatakse kohalikku ühendatud andmekandjat, siis tuleb see vormindada failisüsteemiga Mac OS Extended (Journaled). Teine võimalus on salvestada varundatud andmed lubatud kataloogi võrgus eemal asuvas süsteemis. See eeldab võrguprotokolli Apple Filing Protocols (AFP) kasutamist. SMB-/CIFS-protokolli saab konsoolis aktiveerida järgmise käsuga:

defaults write com.apple.systempreferences
TMShowUnsupportedNetworkVolumes 1

Muutuv „TMShowUnsupportedNetworkVolumes” on teiste võrguprotokollide töölelülitamise mitteametlik meetod. Sellega ei saa aga tagada veatut kasutust ning Apple ei toeta seda meetodit. Time Machine'i saab sisse lülitada süsteemiseadistustest punktis „Time Machine”. Seejärel tuleb varundatavate andmete salvestamiseks valida ühilduv kettaseade. Time Machine loob kõigist kõvakettal asuvatest andmetest koopia. Kui andmeid pole vaja andmevarundusse kaasata, saab suvandites määrata erandid. Kui olemasolevast mäluruumist andmevarunduseks enam ei piisa, antakse sellest kasutajale teada. Kasutaja peab kas vanemad varundatud andmed kustutama või kustutab programm need automaatselt, kuni on piisavalt mäluruumi. Andmevarundusel tuleb silmas pidada järgmisi punkte:

- Time Machine saab varundada kõiki süsteemifaile, mida ei ole kohaliku arvuti käivitamisel vaja. Andmeid tuleb varundada automaatselt regulaarse ajavahemiku tagant ja käsitsi konfiguratsiooni suuremate muudatuste korral.
- Andmevarunduse lõpus tuleb vastavast logifailist /var/log/system.log kontrollida, kas varunduse ajal on tekkinud vigu. Logifaili saab vaadata Mac OS-i teenusprogrammiga „Konsool”. Andmevarunduse loob protsess „backupd”, nii et tuleb otsida kõiki selle protsessinimega teateid. Kuna logifailis /var/log/system.log on muu hulgas ka konfidentsiaalset infot, võib seda näha ainult administraatoriõigustega kasutaja.
- Kui File Vault on aktiveeritud, peab kasutaja end kõigepealt süsteemist välja logima, et Time Machine saaks andmed varundada. Kui Mac OS X-ga klient on suletud või puhkeolekus, ei ole andmevarundus võimalik.

Süsteemi taastamine

Süsteemi täielikuks taastamiseks tuleb klient käivitada Mac OS X installatsiooni DVD-lt, sest taastamisprogrammid asuvad DVD-l. Selleks tuleb käivitumise ajal hoida all klahvi „C”. Pärast menüükeele valimist on teenusprogrammides andmete taastamise võimalus. Tuleb valida andmekandja, millel on varundatud andmed, ja kõvaketas, mida on vaja taastada. Time Machine suudab taastada ainult valitud failid. Selleks tuleb mitmes üksteise taga kuvatavas kronoloogiliselt järjestatud aknas valida soovitud versioonis objektid ja need nupu „Taasta” abil sihtkohta kopeerida.

Nõuded Mac OS X kliendi varundustarkvarale

Kui ulatuslikumate installatsioonide või suurte käideldavusnõuete korral kasutatakse andmevarunduseks lisatarkvara, siis tuleb varundustarkvara valimisel silmas pidada, et see täidaks järgnevatest nõuetest võimalikult paljusid:

- Varundamisel ja taastamisel peavad olema toetatud Mac OS X-s kasutatavad failisüsteemid HFS ja HFS+. Eeliseks on sellised täiendavad toetatud failisüsteemid nagu FAT ja NTFS.

- Varundusi peab saama teha vabalt määratud aegadel või seadistatavate intervallidega automaatselt, ilma et oleks vaja sekkuda rohkem, kui vajaliku varundusandmekandja valmispanek seda nõuab.
- Varundustarkvara peab toetama varundusandmekandja kaitsmist volitamata kasutamise eest kas parooli või, mis veelgi parem, krüpteerimise abil. Lisaks peaks see suutma varundatud andmeid pakitud kujul salvestada.
- Hea oleks, kui üht või mitut valitud kasutajat saaks varundustulemustest ja potentsiaalsetest veateadetest automaatselt meili teel või sarnaste mehhanismide abil teavitada.
- Kaasamis- ja välistamisnimekirjade loomine peab olema võimalik. Sobivate kaasamis- ja välistamisnimekirjade sisestamisel failide ja kataloogide valikult peab saama täpselt määrata, milliseid andmeid tuleb varundada ja millised võib vahele jätta. Neid nimekirju peaks olema võimalik varundusprofiilidesse koondada, salvestada ja edaspidistes varundustoimingutes kasutada.
- Varundatud andmeid peab saama salvestada mitmesugustele andmekandjatele, nt optilistele andmekandjatele (DVD-d, CD-d), kõvaketastele, magnetlintsalvestitele, USB-mäluseadmetele ja võrgudraividele.
- Varundatavaid andmeid peab saama valida nende loomise või viimase muutmise kuupäeva alusel.
- Varundustarkvara peab toetama nii täisandmevarundust kui ka järkjärguliste koopiate tegemist (muutuste varundamist).
- Varundustarkvara peab pärast varundamist võimaldama varundatud andmeid automaatselt originaaliga võrrelda ning pärast andmete taastamist võrrelda rekonstrueeritud andmeid ja varundusandmekandja sisu.
- Failide taastamisel peab saama valida, kas failid taastatakse algsesse või teise kohta. Samuti peab olema võimalik kontrollida tarkvara toimimist juhul, kui sihtkohas on juba sama nimega fail olemas. Seejuures peab saama seadistada, kas see fail kirjutatakse alati üle, seda ei kirjutata üldse üle või see kirjutatakse üle ainult juhul, kui see on vanem kui rekonstrueeritav fail, või kas sel juhul esitatakse kasutajale kindlasti päring.

Täiendavad kontrollküsimused:

- Kas Mac OS X andmete varundamiseks ja taastamiseks on olemas reeglid?
- Kas Mac OS X andmevarundusi, mis on tehtud Time Machine'i teenusprogrammiga, hoitakse volitamata ligipääsu eest kaitstult?
- Kas administraatorid näevad kohe varunduse vigu või tõrkeid, nt logifaili analüüsimisel või automaatsel teavitusel meilitsi?

M 6.147 Süsteemiparameetrite taastamine Mac OS X-s

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutavad: administraator, kasutaja

Juhul kui Mac OS X süsteem enam ei käivitu või tekib probleeme failide loetavusega, saab toimida mitmel viisil. Kasutajaid ja administraatoreid tuleb teavitada meetmetest, kuidas süsteemiparameetreid Mac OS X kasutamisel taastada. Time Machine'iga loodud varundatud andmete taastamiseks tuleb järgida M 6.146 Andmete varundamine ja taastamine Mac OS X klientsüsteemides esitatud juhiseid. Et tuvastada Mac OS X kliendi kasutamises esinevaid vigu, mis takistavad operatsioonisüsteemi tavalist käivitust, võib valida mitme käivitusrežiimi vahel. Kuna mõningaid neid käivitusrežiime saab kasutada ainult juhul, kui EFI püsivara parooli pole seatud, siis tuleb see kõigepealt ajutiselt eemaldada. Mac OS X installatsiooni DVD-l tuleb leida rakendus „Open Firmware Password", millega saab püsivara parooli lähtestada.

Single Useri režiim

Kui Mac OS X-ga klient käivitatakse, tuleb Single Useri režiimi saamiseks hoida all klahvikombinatsiooni „cmd + S". Single Useri režiim buudib ainult algelise operatsioonisüsteemi, ilma graafilise kasutajaliideseta. See režiim on väga lihtsakoeline ja enamasti kättesaadav ka siis, kui süsteem ebaõnnestunud installatsiooni või failisüsteemivea tõttu enam ei käivitu. Single Useri režiimis töötamiseks kasutatakse küll *root* -kontot, kuid alguses võib käivitusdraivile ligi pääseda ainult lugejaõigustega. Failisüsteemi kontrollimiseks võib sisestada käsu „ /sbin/fsck -fy". Single Useri režiimis kasutatakse Ameerika klaviatuuripaigutust, seega tuleb klahvisisestusi kohandada. Kui failisüsteem on kontrollitud ja vajaduse korral parandatud, võib käivitusdraivi kirjutamise ligipääsu käsuga „ / sbin mount -uw/" sisse lülitada. Nüüd on vigade kõrvaldamiseks veel muid võimalusi. Nii võib näiteks eemaldada vigased programmid, mis automaatselt koos süsteemiga käivituvad.

Verbose režiim

Sellesse režiimi jõudmiseks tuleb EFI-parool ajutiselt eemaldada. Verbose režiim pakub võimalust süsteemi lähemalt uurida. Režiimi pääsemiseks tuleb süsteemi käivitumise ajal hoida all klahvikombinatsiooni „cmd + V". Sellega käivitatakse süsteem tavalisel viisil, kuid ekraanipilti ei kata enam Apple'i logo. Selle asemel kuvab süsteem informatsiooni, mis annab teavet näiteks selle kohta, mis teenus just käivitati. Nii saab võimalikke veaallikaid täpsemalt piirata.

Safe Booti režiim

Kui käivitamise ajal hoitakse all klahvi „Shift", ei laadita kerneli laiendusi ega teiste tootjate käivitusobjekte. Seega välistatakse juba käivitamise ajal suur hulk veaallikaid. Kui tehakse kindlaks, et üks käivitusobjektidest takistab operatsiooni tavalist käivitamist, saab vastava käivitusobjekti süsteemiseadistustest kasutajakontode alt välja lülitada. Mittegraafilise liidese kaudu ligipääsetavad käivitusobjektid asuvad kataloogis „ /Library/StartupItems/" .

Käivitusobjektide kohandamine

Kui Safe Booti režiimis tehakse kindlaks, et käivitusobjekt põhjustab probleeme ja graafilist kasutajaliidest ei saa objekti eemaldamiseks kasutada, siis tuleb käivitusobjektiga tegelda käsitsi. Käivitusobjektid LaunchDaemons, mis vajavad *root* -õigusi, asuvad kaustas „/System/Library/LaunchDaemons" või „/Library/ LaunchDaemons". Käivitusobjektid, mille jaoks on vaja kasutajaõigusi, asuvad kaustas „ /System/Library/LaunchAgents" või „/ Library/LaunchAgents". Käivitusobjekti eemaldamiseks piisab faililõpu muutmisest.

Failide ligipääsuõiguste taastamine

Kui tehakse kindlaks, et pärast tarkvara installimist on failide ligipääsuõigusi tahtmatult muudetud, tuleb need tingimata taastada. Muidu võib halvimal juhul iga kasutaja süsteemifaile muuta. Failide ligipääsuõiguste lähtestamiseks standardväärtustele võib kasutada kõvaketta teenusprogrammi kaustas „Teenusprogrammid". Siin tuleb valida parandamist vajav partitsioon ja vajutada nuppu „Kõite pääsuõiguste parandamine". Teine võimalus on see toiming tööle panna käsurea käsuga, millega lähtestatakse failide ligipääsuõigused tootja määratud standardväärtusele. Kui failide ligipääsuõigused olid käsitsi kohalike asjaoludega kohandatud, siis lähevad need automaatse parandamise korral kaduma ja need tuleb turvaeeskirjade järgi uuesti luua.

Võtmekogu parandamine

Võtmekogu võib saada kahjustada näiteks kõvakettavea või rakenduste funktsioonivea tõttu. Võtmekogu teabe taastamiseks võib käivitada teenusprogrammidest rakenduse „Võtmekoguhaldus". Seejärel tuleb aktiveerida menüüpunkt „Võtmekoguhaldus I Võtmekogu I Esmaabi". Pärast kasutajanime ja selle juurde kuuluva parooli sisestamist saab kontrollida võtmekogu korrektsust. Kui tuvastatakse vead, tuleb võtmekogu enne edasist kasutamist parandada.

Parameetrimälu kustutamine

Püsimuutmälus (Permanent Random Access Memory – PRAM) salvestatakse süsteemiteave, nt kordussagedus, eraldusvõime ja värvisügavus, samuti teave käivitusdraivi kohta. Parameetrimälu kustutamiseks peab kõigepealt EFI-parooli ajutiselt välja lülitama. Seejärel tuleb arvuti käivitamisel hoida korraga all klahve „cmd" („Command"), „Alt", „p" ja „r", kuni käivitusheli on mitu korda kostnud.

Power Management Uniti lähtestamine

Kui süsteem pärast PRAM-i lähtestamist ikka veel ei käivitu, siis tuleb lähtestada Power Management Unit. Toimingud võivad erinevate toode puhul suuresti erineda, mistõttu tuleb otsida abi internetist Apple'i teabe andmebaasist.

Täiendav kontrollküsimus:

- Kas administraatoreid ja kasutajaid on teavitatud sellest, kuidas tuleks Mac OS X käivitusprobleemide korral toimida?

M 6.148 Mac OS X süsteemi kasutusest kõrvaldamine

Algatamise eest vastutavad: infoturbespetsialist, IT-juht

Rakendamise eest vastutab: administraator

Kasutusest kõrvaldatud töökohaarvutitest tuleb kogu konfidentsiaalne teave sobival viisil kustutada. See kehtib ka defektsetel andmekandjatel hoitava teabe kohta. Kui andmekandjale on salvestatud konfidentsiaalset teavet ja andmekandjale ei pääse enam riistvaravea tõttu ligi, siis tuleb andmekandja sobival viisil hävitada (vt B 1.15 Andmete kustutamine ja hävitamine). Mac OS X-st teabe kustutamiseks võib kasutada kõvaketta teenusprogrammi. Süsteemipartitsiooniga andmekandja korral tuleb arvuti Mac OS X installatsiooni DVD-lt käivitada ja avada seal „Kõvaketta teenusprogramm". Selle programmiga saab andmekandjal hoitavaid andmeid mitmel moel kustutada. Turvasuvandites peab olema seadistatud „Kirjuta andmed nullidega üle". Administraatorid peavad olema saanud kõvaketta teenusprogrammi käsitsemiseks ja Mac OS X andmekandjate turvaliseks kustutamiseks asjakohase väljaõppe. Enne IT-süsteemide või andmekandjate utiliseerimist tuleb need läbi vaadata ja veenduda, et neil ei oleks enam vajalikke andmeid. Andmed tuleb varundada või arhiveerida teistele andmekandjatele. Tuleb kontrollida, et tõepoolest kõik andmed on korrektselt varundatud (vt M 1.1 Vastavus normidele ja eeskirjadele).

Täiendav kontrollküsimus:

- Kas administraatoreid on teavitatud, kuidas toimida Mac OS X andmete kustutamisel ja hävitamisel?

M 6.149 Andmevarundus Exchange'is

Algatamise eest vastutavad: infoturbespetsialist, IT-juht
Rakendamise eest vastutab: administraator

Exchange'i jaoks tuleb luua andmevarunduspoliitika, mis integreeritakse institutsiooni olemasolevasse andmevarunduspoliitikasse (vt B 1.4 Andmevarunduspoliitika). Seejuures ei tule arvesse võtta mitte üksnes Exchange'i serverit, vaid ka Outlooki kliente.

Exchange'i serveriandmebaaside andmevarundus

Soovitatav on informatsioonimälu ehk Exchange'i postkastide serveriandmebaasid varundada. Tuleb kindlaks määrata varunduse tüüp (täielik või järkjärguline).

Kuna Microsoft Exchange'i süsteemid vajavad nõuetekohaseks töötamiseks Windows Active Directoryt, siis tuleb ka see varundada. Lisaks on soovitatav juba kustutatud Exchange'i objektid postkastidest ja avalikest kaustadest (serveripoolel) kustutada jäädavalt alles mõne päeva pärast ja seda alles siis, kui andmed on varundatud. Need seadistused saab teha iga informatsioonimälu jaoks eraldi. Peale selle on soovitatav kustutatud postkaste teatud ajavahemiku jooksul mitte jäädavalt kustutada (standardseadistus on 30 päeva). Need väärtused tuleb kohandada ettevõtte või asutuse asjakohaste nõuetega. Exchange'i serveriandmebaase tuleks varundada vähemalt kord päevas. Seepärast tuleb varundus ja taastamine võimaluse korral teha online -režiimis, s.t Microsoft Exchange'i teenuseid välja lülitamata. Varunduspoliitika, sh ka konkreetne toimimisviis, sõltub versioonist.

Microsoft Exchange'i serveri installatsiooni varundamiseks offline –režiimis tuleb Microsoft Exchange'i teenused välja lülitada. Seejärel tuleb varundada Exchange'i kataloog koos kõikide alamkataloogidega. Sellega on hõlmatud kõik Exchange'i serveri binaarandmed. See variant sobib harvemaks varundamiseks (nt kord nädalas).

Kohaliku Outlooki kausta andmevarundus

Meilide andmevarunduse korral tuleb arvesse võtta ka kliente. Kui Outlooki isiklikud kaustad salvestatakse kasutajasüsteemidesse, peab olema tagatud ka nende andmete varundamine, et vältida andmekadu. See kehtib ka offline –kaustade kohta. See, millised etapid tuleb andmevarunduses täpsemalt läbida, on erinevate Exchange'i/Outlooki variantide puhul erinev.

Kontrollküsimused:

- Kas kasutatavate Exchange'i ja Outlooki komponentide puhul varundatakse andmeid korrapäraselt?
- Kas Exchange'i/Outlooki jaoks on olemas andmevarunduspoliitika, milles võetakse arvesse kõiki olulisi komponente?

M 6.150 OpenLDAP andmevarundus

Algatamise eest vastutavad: spetsialistid, IT-juht

Rakendamise eest vastutab: administraator

OpenLDAP serveri andmevarundusi tuleb teha korrapäraselt. See on vigade korrigeerimise ja kustutatud andmete taaskuvamise oluline eeltingimus.

Ulatuslik andmevarundus

Andmevarunduse puhul mõeldakse sageli ainult tööandmete varundamisele. OpenLDAP korral on objektid kataloogis. Tegeliku edasi- ja taastöötamise tagamiseks tuleb lisaks varundada konfiguratsioonifailid. Olenevalt konfiguratsioonist (vt M 4.384 OpenLDAP turvaline konfiguratsioon) tuleb seega varundada kas konfiguratsioonifail slapd.conf või (*online* -konfiguratsiooni korral) sufiks CN=config. Peale selle ei tohi loodud varundus füüsiliselt samasse IT-süsteemi jääda, sest see pole siis IT-süsteemi rikke korral kättesaadav (vt M 6.20 Varukoopia andmekandjate õige ladustus).

Andmebaaside andmevarundus

OpenLDAP andmevarunduse järeleproovitud meetod on kasutada slap*-tööriista *slapcat* , millega eksporditakse andmeid LDIF-vormingus sel ajal, kui slapd-serveri töö on katkestatud. Loodud ekspordi saab salvestusest kokku pakkida, sest LDIF-failide avatekstistruktuur moodustab tarbetult suuri faile. Kui kataloogiteenuse andmeid eksporditakse töötava slapd-serveri ajal *slapcat* iga, siis võib see kaasa tuua andmevarunduse ebakõlasid, sest andmeid muudetakse eksportimise ajal. Varundatavaid andmebaase on võimalik üle viia ka kirjutuskaitsega olekusse. Sel juhul tuleb aga arvestada, et server ei ole siis kirjutatava ligipääsu jaoks avatud ja sel viisil ei saa ka *online* -konfiguratsiooni varundada. Sufiksit CN=config saab küll kirjutamiskaitsega olekus muuta, kuid sellest olekust ei vabane see enne taaskäivitust. Seepärast ei ole ühtne ja täielik varundamine ilma slapd-serveri seiskamiseta võimalik.

Varundamine

Andmekogude varundamiseks tuleb alati kasutada tööriista slapadd. Põhimõtteliselt on ka tööriist ldapadd või mõni sobiv klientrakendus võimeline objekte LDIF-failidest kataloogiteenusesse lisama. Sellel on siiski järgnevad puudused:

- Tööriist slapcat loob LDIF-ekspordi vastavalt objektide füüsilisele järjekorrale andmebaasis. Kui see fail lisatakse klientrakenduse ldapadd vms abil kataloogiteenusesse, võib juhtuda, et objekte ei looda, kui neist kõrgemal astmel asuvaid objekte ei ole veel loetud (sest need salvestati varundatud andmebaasis füüsiliselt alles pärast madalamal astmel asuvaid objekte).
- Klientrakendused, nt ldapadd, suhtlevad töötava slapd-serveriga potentsiaalselt krüpteeritud olemasoleva võrguühenduse kaudu. Andmevarunduse algne importimine sel viisil nõuab tarbetult palju aega, ribalaiust ja ressursse.
- Importimine klientrakenduse ldapadd vms kaudu nõuab töötavat slapd-serverit, millele on tagatud kirjutamisõigusega ligipääs. On oht, et importimise ajal pääsetakse teiste klientide kaudu ligi mittetäielikele andmetele või luuakse või muudetakse objekte viisil, mis on veel varundatavate andmekogudega konfliktis.

Replikatsiooni varundamine suurte käideldavusnõuete korral

Kui slapd-serveri käideldavusnõuded ei luba serveri töö katkestamist (*downtime*) või kirjutamisõiguse ligipääsu piiramist varundamise ajaks, siis on replikatsiooni kaudu varundamine hea variant. Selle jaoks tuleb eelkirjeldatud toimimisviisi kasutada tarbijal. Teenusepakkuja on edasi kättesaadav, kui tarbija on peatatud. Pärast andmevarunduse lõppu tehakse slapd-serveri taaskäivitusel tarbijale synrepl-mehhanismi abil automaatselt kõik need muudatused, mida teenusepakkuja on vahepeal tarbijale teinud. Tuleb arvesse võtta erinevusi teenusepakkuja ja tarbija varundatud konfiguratsioonis.

Muud kasutusvõimalused

Siin kirjeldatud andmevarundus sobib hästi ka selleks, et täita sellega algselt kataloogiteenuse replikatsioon (vt M 4.389 OpenLDAP partitsioonid ja replikatsioonid), ajakohastada OpenLDAP-d (vt M 4.390 OpenLDAP turvaline ajakohastamine) või juhtida üleviimist teise kataloogiteenusesse. Neil juhtudel tuleb siiski olla ettevaatlik, kui konfiguratsiooni laaditakse kataloogiteenusesse kataloogipuu osana. Näiteks võib teenusepakkuja konfiguratsiooni tähelepanematu ülekandmine luua identse teenusepakkuja (tarbija asemel), millega kaasneksid kahest vastuolulisest teenusepakkujast tingitud võrguprobleemid lühikese aja jooksul.

Täiendavad kontrollküsimused:

- Kas luuakse regulaarselt andmevarundusi OpenLDAP-serverist koos selle kataloogiteenuse objektide ja konfiguratsiooniseadistustega?
- Kas andmevarunduses on arvesse võetud kõik OpenLDAP serveri partitsioonid?
- Kas andmed taastatakse andmekao korral üksnes sobivate tööriistadega?

M 6.151 Logimise häirepoliitika

Algatamise eest vastutab: asutuse/ettevõtte juhtkond

Rakendamise eest vastutavad: IT-juht, infoturbespetsialist, organisatsiooni juht

Et infokoosluse turvaintsidentidele adekvaatselt reageerida, peab olema välja töötatud häirepoliitika. Häirepoliitikas kirjeldatakse teavituskanalit, mille kaudu informeeritakse pädevaid isikuid turvaintsidendist, samuti sisaldab see häireprotsessi üksikasjalikku kirjeldust.

Mitmesugused teavitusmoodused

IT-turvaintsidentide korral tuleb häire anda võimalikult paljude erinevate teavitusmehhanismide kaudu. Nii tagatakse, et turvalisusega seotud sündmus ei jää tähelepanuta. Valitud teavitusvormidest tuleb häirepoliitikas kinni pidada. Ideaalne on järgmist tüüpi teavitustugi:

- Pärast turvaintsidendi tuvastamist saab IT-eelhoiatussüsteemi korral halduskonsooli häire väljastada.
- Vastutavat isikut saab sündmustest teavitada meili teel. See on väga populaarne suhtlusvorm, kuid selle puhul ei saa kindel olla, et teatatud intsidendiga kohe tegeldakse.
- Turvaintsidente võib saata ka SMS-teatena pädeva administraatori mobiiltelefonile või piiparile. Seejuures tuleb siiski arvestada, et teade võib raadioleviaukude tõttu liiga hilja või üldsegi mitte kohale jõuda.
- Kui saadetakse SNMP-teateid, võib IT-eelhoiatussüsteem olla seotud Ticketi süsteemiga. Sel juhul saadetakse teave turvaintsidentide kohta otse Ticketi süsteemidesse edasi.
- Kui on olemas avatud ja hästi dokumenteeritud programmeerimisliidesed, pakuvad need väliste levitamissüsteemidega ühendamisel suurt paindlikkust.

Vastutavad isikud

Häirepoliitikasse tuleb kirja panna isikud, keda tuleb IT-turvaintsidendi korral teavitada. Enamasti on need infokoosluse administraatorid. Sel otstarbel peavad olema koostatud kontaktide nimekirjad kontaktisikute aadressi ja telefoninumbriga. Nimetatud isikutele tuleb teada anda nende ülesanne häirepoliitikas ning kontrollida regulaarselt kontaktide nimekirjade, nt esitatud telefoninumbri õigsust.

Häireprotsessi kindlaksmääramine

Oluline punkt häirepoliitikas on häireprotsessi kindlaksmääramine. See peab hõlmama loetelu kõikidest toimingutest alates turvaintsidendi esinemisest kuni intsidendi täieliku kõrvaldamiseni. Kõikide häireprotsessi etappide kohta peavad olemas olema üksikasjalikud kirjeldused, et võimalikke valetõlgendusi juba eos ära hoida. Siin tuleb määrata, keda, millal, kuidas ja kelle kaudu häirest teavitada ning kuidas probleemi lahendada. Peale selle tuleb häirepoliitikas kindlaks määrata, millal häire genereeritakse. Selleks võib keskses logimissüsteemis seadistada läviväärtused. Kohe, kui väärtus ületab seatud piiri, vallandatakse häire. Kui väärtus on piirväärtusele väga lähedal, on võimalik väljastada hoiatusteateid, mis tõmbavad tähelepanu võimalikule probleemile. Häirepoliitikat tuleb regulaarselt kontrollida ja ajakohastada. Ainult nii on võimalik selles loetletud abinõusid tõsise juhtumi korral õigesti ja praktiliselt rakendada.

Täiendavad kontrollküsimused:

- Kas häirepoliitika on välja töötatud?
- Kas häire antakse erinevate teavitusvormide abil?
- Kas IT-turvaintsidendist teavitatavad isikud on koos aadressi ja telefoninumbriga häirepoliitikasse kirja pandud?
- Kas häirepoliitikas nimetatud isikutele on nende ülesannetest teada antud?
- Kas häirepoliitikas on üksikasjalikult kirjeldatud kõiki häireprotsessi etappe?
- Kas häirepoliitikat kontrollitakse ja ajakohastatakse regulaarselt?

M 6.152 XXX

M 6.153 XXX

M 6.154 Veebiteenuste hädaolukordade haldamine

Algatamise eest vastutavad: IT-rakenduste eest vastutavad töötajad, IT-juht

Rakendamise eest vastutab: administraator

Veebiteenused kujutavad endast paindlikku, kuid samal ajal ka keerulist lahendust, et toetada IT-süsteemide kaudu äriprotsesse. Tõrke või jõudlusekaol võivad olla olulised tagajärjed toetatavatele äriprotsessidele. Seepärast on oluline, et järgides üldist hädaolukorra haldust (vt moodul B 1.3 Hädaplaanimine) ja andmevarunduse kontseptsiooni (vt moodul B 1.4 Andmevarunduspoliitika), võetaks vastavad meetmed, millega ennetada hädaolukordi ja neid asjakohaselt käsitleda.

Aluseks on siinjuures hädaolukorra planeerimine, mis võtab riskianalüüsis arvesse erinevaid sündmusi.

Need võivad olla alljärgnevad.

Veebiteenuse tõrge

Veebiteenustel ja üksikutel komponentidel on tõrked ja nende poolt toetatavad äriprotsessid ei tööta.

Jõudluse langused

Veebiteenus või üksikud komponendid ei taga nõutavat jõudlust (nt vastuste ajad) ja sellega kahjustatakse äriprotsesse. Põhjuseks võivad olla näiteks Denial-of-Service-tüüpi ründed või tähtajast tingitud ülekoormused (nt aasta lõpus).

Loogilised vead veebiteenuses

Veebiteenus ise on kasutatav väljapoole. Selle sisemine andmetöötlus toimub siiski vigaselt. Seetõttu on terviklusega seotud andmed ohustatud ja tööprotsesside tulemused kahjustatud. Veebiteenus ei ole enam oma tõelises tähenduses kasutatav. Lisaks tuleb arvesse võtta, et ilmselt ka veebiteenuse andmebaas on terviklust puudutavate valede andmete tõttu kahjustatud.

Kahjustamine sõltuvuse tõttu

Muud komponendid, mis sõltuvad veebiteenusest, on oma kättesaadavuse või jõudluse osas kahjustatud. Siinjuures võivad komponendid olla näiteks muud veebiteenused, autentimisteenused, salvestisüsteemid või ka vastavad võrgud ja võrgujuurdepääsud. Nende komponentide kahjustamine võib ühelt poolt tähendada seda, et veebiteenus ise ei ole kättesaadav. Teiselt poolt võivad kõik vastavad veebiteenuse funktsiooni osad olla kahjustatud. Sellistel olukordadel on tagajärjed selliste äriprotsesside jõudlusele, milles kasutatakse veebiteenuseid. Neid tagajärgi tuleb analüüsida ja võtta vastavaid sõltuvusi arvesse Business Impact Analyse'is (BIA). Seejuures tuleb arvestada ka vahetute sõltuvustega muude veebiteenuste kaudu, mis töötavad koos kahjustatud veebiteenusega.

Sündmuste ja nendega seotud tagajärgede põhjal tuleb hädaolukordade plaanis välja arendada ennetavad ja reageerimise meetmed. Hädaolukorra enne-

tamise kontseptsioonis tuleb järgida sobivaid ennetusmeetmeid veebiteenuste jaoks.

- Krüptograafiliste funktsioonide jaoks peavad vajalikud võtmed olema taastatavad. Uued võtmed ja sertifikaadid, nt edastuskrüpteering, peavad olema genereeritud või soetatud piisavalt lühikese ajaga. Teatud tingimustel võiksid turvalises kohas olemas olla varuvõtmed.
- Veebiteenuses vajalikud konfigureerimis- ja metaandmed peavad olema dokumenteeritud ja varundatud, et võimaldada nende taastamist.
- Dokumentatsiooni tuleb hoida sobivas kohas, et see oleks hädaolukorras kiiresti kättesaadav. Dokumentatsiooni kvaliteet peab võimaldama, et asjatundlik kolmas isik saab end sellega sobiva aja jooksul keskkonnas sisse töötada.
- Kui veebiteenuse kättesaadavusele on kõrged või väga kõrged nõudmised, tuleks kontrollida, kas ehitada veebiteenus üles liiasusega ja jaotatult erinevatesse asukohtadesse.

Konkreetsed meetmed veebiteenuse taaskäivitamiseks peavad olema kirjas taaskäivitamise plaanis.

Seejuures tuleb tähele panna järgmist.

- Taaskäivitamine peab vastama äriprotsesside ajalistele nõudmistele.
- Ka hädaolukorra ja taaskäivitamise korral peavad olema turbenõuded nii palju kui võimalik täidetud (nt Policy Management).
- Plaanid peavad arvesse võtma veebiteenuse komponentide järjekorda taaskäivitamisel.
- Arvestada tuleb ka sõltuvustega teistest veebiteenustest. See võib eriti mõjutada taaskäivitamise järjekorda.

Kui veebiteenuseid osutatakse kolmandale isikule, tuleb kontrollida, millised on teenuse kasutaja nõudmised hädaolukorra planeerimisele ning kuidas kooskõlastada üksteisega mõlema poole ennetus- ja reageerimismeetmeid.

Hädaolukorra plaani tuleb ka regulaarselt praktiliselt testida. Ainult nii saab tagada, et taaskäivitamisplaanides kirjeldatud meetmed on ka tegelikult teostatavad. Samal ajal õpivad töötajad harjutuste abil kirjeldatud protsesse tundma ja treenivad nende rakendamist. Lõpuks vahendab harjutus teadmised tegelikesse taastus- ja taaskäivitusprotsessidesse ning võimaldab nii kontrollida BIA-s toodud nõuetest kinnipidamist.

Kontrollküsimused:

- Kas veebiteenuste kui äriprotsesside ressurssidega on Business Impact Analyse'is piisavalt arvestatud? Kas seejuures on tähelepanu pööratud ka veebiteenuste omavahelistele sõltuvustele?
- Kas on võimalik veebiteenuse piisavalt kiire taastamine, võttes arvesse vajalikke krüptograafilisi võtmeid, konfigureerimis- ja metaandmeid?

- Kas dokumentatsioon on hädaolukorras kättesaadav ja põhjalik?
- Kas välja on töötatud veebiteenuse taaskäivitusplaan? Kas arvesse on võetud veebiteenuse komponentide omavahelisi sõltuvusi ja sõltuvusi teistest veebiteenustest?
- Kas veebiteenuse hädaolukorrad mõjutavad kolmandaid isikuid ja kas hädaolukorra meetmed arvestavad nendega?
- Kas hädaolukorra meetmeid testitakse regulaarselt?

M 6.155 Pilvteenuse hädaolukorra kontseptsiooni koostamine

Algatamise eest vastutavad: IT-juht, infoturbeametnik

Rakendamise eest vastutavad: administraator, infoturbeametnik, IT-juht

IT hädaolukorra kontseptsiooni koostamine pilvteenuste kasutamise sisemiste protsesside jaoks on hädaolukorra ennetamise oluline meede. Hädaolukorra kontseptsiooni raames tuleb käsitleda nii töökorralduslikke kui ka tehnilisi aspekte.

Pilvteenuste kasutamise hädaolukorra ennetamise töökorralduslikud aspektid

Hädaolukorra kontseptsioon peab sisaldama kõiki vajalikke ülesandeid vastutusaladele ja kontaktisikutele, et hädaolukorras oleks võimalik kiiresti reageerida. Kõik ettenähtud protseduurid peavad olema täpselt reguleeritud ja täies mahus dokumenteeritud.

Tuleb koostada üksikasjalikud reeglid andmevarunduse jaoks, sest sellele langeb hädaolukorras eriline tähendus. Siin on mõeldavad näiteks nõuded, mis puudutavad eraldatud varunduse andmekandjaid iga pilvteenuse kasutaja jaoks, nõudeid kättesaadavusele, esindamisreeglitele, eskaleerimisstrateegiatele ja viirusetõrjele. Samuti tuleb töökorralduslike seisukohtade all näha vajadust üksikasjalike tööjuhiste koostamiseks. Need peaksid sisaldama konkreetseid korraldusi kindlateks veaolukordadeks. Seetõttu peab asutus välja töötama kontseptsiooni regulaarselt läbiviidavate hädaolukorra harjutuste jaoks. Kui kasutatav pilvteenus või selle abil loodud äriprotsess seda nõuavad, tuleb teha otsus, mil määral tuleb ette näha hädaolukorra harjutused koos pilvteenuseosutajaga.

Pilvteenuste kasutamise hädaolukorra ennetamise tehnilised aspektid

Hädaolukorra ennetamise raames tuleb lisaks töökorralduslikele aspektidele dokumenteerida ka tehnilised nõudmised. Vajalike haldustööriistade kättesaadavus on pilvteenuse kasutamisel eriti suure tähtsusega (vt ka G 4.98 Pilvteenuste haldustööriistade tõrked pilvteenuste kasutamisel). Seetõttu tuleb need üldjuhul luua liiasusega või üles ehitada liiasusega taristule. Ka vajalikud liidesesüsteemid peavad olema liiasusega. Seetõttu peaks hädaolukorra kontseptsioon sisaldama andmeid selle kohta, kuidas tagada tõrkekindel ühendus pilvteenuseosutajaga.

Pilvteenuse kasutamiseks hädaolukorra kontseptsiooni koostamisel tuleb tähele panna, et ühenduse kaitsevajadus ja liidesesüsteemid peavad olema võrreldes asutuse seniste nõudmistega kõrgemad. Põhjus on selles, et pilvteenuseid kasutatakse kriitiliste äriprotsesside jaoks.

Kontrollküsimused:

- Kas kasutatavate pilvteenuste jaoks on olemas hädaolukorra kontseptsioon, mis sisaldab nii töökorralduslikke kui ka tehnilisi aspekte?
- Kas hädaolukorra kontseptsioon sisaldab kõiki vajalikke andmeid vastutusalade ja kontaktisikute kohta?

- Kas on vastu võetud andmevarundust puudutavad üksikasjalikud eeskirjad?
- Kas on kinni peetud nõuetest haldustööriistade loomisele liiasusega?

M 6.156 Organisatsioonisiseste andmevarunduste tegemine

Algatamise eest vastutab: infoturbeametnik

Rakendamise eest vastutavad: administraator, spetsialist, infoturbeametnik

Kui asutus teeb pilvteenuste kasutamise planeerimismeetmete koostamise jooksul või hiljem kindlaks, et erilised asjaolud muudavad vajalikuks oma andmevarunduse, tuleb tähelepanu pöörata mõningatele olulistele aspektidele. Tuvastatud vajadus oma andmevarunduse jaoks tuleb põhjendada ja dokumenteerida.

Põhimõtteliselt on organisatsioonil kaks erinevat võimalust täiendava andmevarunduse läbiviimiseks. Ühelt poolt võib asutus andmevarunduse loomise ise ette võtta, teisalt on see rakendatav täiendava teenuse kasutamisega (varundus teenusena, backup as a service). Sellisel juhul võtab ülesande enda peale väline teenuseosutaja.

Eriti välise teenuseosutaja kaasamise korral peaksid asutuse nõuded varundusteenusele olema üksikasjalikult välja töötatud ja hoolikalt dokumenteeritud. Neid tuleb võrrelda eriliste asjaoludega, millest on tekkinud oma andmevarunduse vajadus. Varundusteenus on siis kas teine pilvteenus või väljasttellimise ettevõte, millele tuleb rakendada vastavate moodulite turvameetmeid. Põhimõtteliselt soovitatakse oma andmevarunduse õigus valitud pilvteenuseosutajaga lepinguliselt kokku leppida. Sellisel juhul tuleb lepingu koostamise meedet (vt M 2.541 Pilvteenuseosutajaga sõlmitava lepingu koostamine) täiendada vastava aspekti sisseviimisega.

Kontrollküsimused:

- Kas otsus oma andmevarunduse läbiviimiseks on põhjendatud ja dokumenteeritud?
- Kas varundusteenuse jaoks on olemas üksikasjalikud nõudmiseks?

M 6.157z Rakenduste liiasuse kontseptsiooni koostamine

Algatamise eest vastutavad: IT-juht, infoturbeametnik
Rakendamise eest vastutavad: vastutav spetsialist, IT-juht

Kui äriprotsessil või teatud andmetel on kõrge kaitsevajadus kättesaadavuse põhiväärtuse osas, võib siin olla kasulik koostada ja rakendada liiasuse kontseptsiooni (üldised andmed liiasuse kohta on olemas meetmes M 1.52z Tehnilise infrastruktuuri varud). Liiasuse kontseptsiooni jaoks tehakse täiendava turvaanalüüsi ja riskianalüüsi (vt standard 100-3) alusel kindlaks, milliseid ruumi- ja hoonetaristuid, süsteeme, võrgukomponente ja liine äriprotsessi või andmeid kõrge kaitsevajadus mõjutab? Sellele põhinedes määratakse liiasuse kontseptsioonis kindlaks, milliste tehniliste ja töökorralduslike meetmetega tuleb tagada vajalik kättesaadavus.

Liiasuse kontseptsiooni loogilisust tuleb kontrollida, võrreldes seda üldise hädaolukorra kontseptsiooniga (vt M 6.114 Hädaolukorraks valmisoleku kontseptsiooni koostamine) ja sobitada see vajaduse korral üldiste nõudmistega. Liiasuse kontseptsiooni meetmeid tuleb testida ja harjutada. Need testid ja harjutused tuleb kooskõlastada asutuse hädaolukorra kontseptsiooniga (vt M 6.117 Testid ja valmisoleku harjutused). Vastavalt infokoosluse kõikide elementide kättesaadavuse nõudele võib arvesse võtta järgmisi tegureid, et vältida nende tõrkeid.

Meetod

- Hädaolukorra jaoks tuleb koostada töökorralduslikud eeskirjad. Need eeskirjad võivad mõnede rakenduste jaoks ette näha tagasipöördumist paberipõhistele töödele. Lisaks tuleks rakendused seada tähtsuse järjekorda ja mõelda, kas rakendused, millel on vähene prioriteet, võiks välja lülitada ja anda sellest vabaks jäänud ressursid kõrgema prioriteediga rakenduste kasutusse.
- Tuleb kontrollida, kas kasutatakse ruume, IT-süsteeme ja muid andmetöötlusseadmete taristuid muudes asutustes, kellega tehakse koostööd.
- Kõrgema prioriteediga rakenduste korral tuleb kontrollida, kas rakendused on võimelised kasutama liiasust süsteemitasandil. Siia alla kuuluvad nt Load-Balancing-, klastrifunktsioonid. Neid võib vastavalt kasutada, teatud juhtudel tuleb need ka kõigepealt valmistada.
- Kõrgema prioriteediga rakenduste puhul tuleb kontrollida, kas need rakendused on võimelised kasutama liiasust teenusetasandil, nt lühiajalised üleminekud alternatiivsele andmebaasile jne. Neid võib vastavalt kasutada, teatud juhtudel tuleb need ka kõigepealt valmistada.

Süsteemid

- Osaline või täielik liiasus komponentide tasandil. Rakendused vajavad töötamiseks rida komponente. Kättesaadavuse tõstmiseks võivad need olla loo-

dud osalise või täieliku liiasusega, näiteks kõvaketta-RAID-de, liiasusega võrgukaartide, võrguosade jne kasutamisega.

- Tuleks kontrollida, kas varusüsteeme tuleks käitada Cold-, Warm- või Hot-Standby-süsteemis või tuleks rakendada süsteemi klastrit. Cold-Standbysüsteemide korral on varusüsteemid eelnevalt konfigureeritud, kuid välja lülitatud ja neile ei edastata ajakohaseid andmeid.Warm-Standby-süsteemide korral on varusüsteemid eelnevalt konfigureeritud ja varustatud andmehulgaga viimasest varundamisest, kuid on välja lülitatud. Hot-Standbysüsteemid käitavad varusüsteeme ja võtavad funktsiooni tõrke korral üle põhisüsteemi funktsiooni. Lisaks saavad Hot-Standby varusüsteemid kõik vajalikud andmed sünkroonse peegelduse kaudu ja võivad ideaaljuhul kohe üle võtta väljalangenud süsteemi töö, ilma et tekiks andmekadu või et kasutaja märkaks tõrget. Süsteemi klastrite korral jaotatakse rakendus üle mitmete süsteemide, kusjuures üks või mitu süsteemi teostavad koormuse jaotamise ja ülejäänud töötlevad ülesandeid. See eeldab kõnealuse rakenduse klastrifunktsiooni M 2.314z Kõrgkäideldava serveriarhitektuuri kasutamine). Klastrilahendusi võib rakendada ka kombineeritult masinate virtualiseerimisega (Hardware-Emulation või Hardware-virtualiseerimine) (vt B 3.204 Klient Unixi all).

Sideühendused

Kui rakendus vajab oma tööks sideühendusi, võib kättesaadavuse tõstmiseks _ näha täiendavalt ette sideühendused nagu faks, telefon, mobiiltelefon ja kõnesideühendused (vt M 6.75z Varu-sidekanalid):

- mis luuakse sideühenduste jaoks kasutatavate füüsiliste või virtuaalsete liinide liiasusega (vt M 6.18z Varuliinid),
- luua liisasusega kasutatavad tsentraalsed võrgukomponendid (vt M 6.53z Võrgukomponentide liiasus).

Kontrollküsimused

- Kas liiasuse kontseptsioonis kindlaksmääratud meetmed on sobivad, et tagada rakenduse nõutav kättesaadavus?
- Kas liiasuse kontseptsiooni kontrolliti kohandatavuse osas hädaolukorra kontseptsiooniga ja kohandati vastavalt?
- Kas liiasuse kontseptsiooni meetmeid testitakse ja harjutatakse?

M 6.158 Ettevalmistumine rakenduste hädaolukorraks

Algatamise eest vastutab: hädaolukorra ametnik

Rakendamise eest vastutavad: vastutav spetsialist, IT-juht, infoturbeametnik

Kõik rakendused tuleb hõlmata hädaolukorra ennetamise planeerimisse ja hädaolukorra haldusse (vt moodul B 1.3 Hädaplaanimine).

- Rakenduse tähendus asutuse äri- ja haldusprotsesside raames tuleb kindlaks määrata ja dokumenteerida. Selle põhjal tuleb rakendus seada võrreldes muude rakendustega tähtsuse järjekorda.
- Kasutatud tehnilised ja töökorralduslikud meetmed hädaolukorra ennetamiseks tuleb kirja panna ja neid tuleb kirjeldada hädaolukorra kontseptsioonis.
- Tuleb planeerida, kuidas käituda piiratud IT-süsteemi korral (kes, kus ja milliseid ülesandeid rakendusega eelistatult täidab? Millised ülesanded tuleb edasi lükata?).
- Tuleb planeerida reguleeritud rakenduse töö taastamist (vt ka M 6.114 Hädaolukorraks valmisoleku kontseptsiooni koostamine).

Kontrollküsimused:

- Kas rakendused on hõlmatud hädaolukorra plaanidesse ja hädaolukorra haldusesse?

M 6.159 Nutitelefonide ning tahvel- ja pihuarvutite kaotuste ja varguste ennetamine

Algatamise eest vastutab: infoturbeametnik
Rakendamise eest vastutab: IT-juht

Selleks, et nutitelefonide, tahvel- või pihuarvutite varguse või kaotuse korral ei läheks samaaegselt kaduma ka kõik kontaktandmed, juurdepääsuandmed asutuse võrgule ja muud kaitset vajavad andmed lõppseadmel või et neid ei kuritarvitataks, tuleb rakendada vastavaid soovitusi.

Kasutada tuleks ainult lõppseadmeid, mis toetavad täielikku andmete krüpteerimist. Kui lõppseade kasutab välist mälukaarti, tuleks ka see võimalikult täielikult krüpteerida. Selleks tuleb valida turvaline parool (vt M 2.11 Paroolide kasutamise reeglid). Andmevarunduse jaoks tuleks kaasata M 6.56 Andmevarundus krüptoprotseduuride kasutamisel .

Nutitelefonide, tahvel- või pihuarvutite kaotuse või varguse korral peaks olema võimalik suunata eemalt meetmeid kaasaskantava lõppseadme lukustamiseks, väljalülitamiseks ja positsioneerimiseks. Selleks on olemas rakendused, mis tuleb välja otsida ja seadmetele installeerida. Kuna suurem osa Mobile Device Management'i (MDM) lahendusi või viirusetõrjeprogramme (vt M 4.230z Nutitelefonide, tahvel- ja pihuarvutite tsentraalne haldamine ja M 4.466 Viirusetõrjeprogrammide kasutamine nutitelefonides ning tahvel- ja pihuarvutites) pakub neid funktsioone kaasa, tuleks kontrollida, kas juba kasutatavad lahendused sisaldavad kõiki vajalikke funktsioone. Kui ostetakse sisse uued MDM-lahendused või viirusevastased kaitseprogrammid, tuleb kindlaks teha, et need sisaldavad kõiki funktsioone, mis on vajalikud, et reageerida vargusele või kaotusele. Tööalaselt kasutatavate nutitelefonide, tahvel- või pihuarvutite varguse või kaotuse korral peab olema määratletud selge toimingute järgnevus. Kõik puudutatud töötajad peavad teadma vastavaid protseduure, kontaktandmeid ja muid andmeid.

Nutitelefonide, tahvel- või pihuarvutite kaotamise või varguse korral tuleb viivitamata teavitada asutuse osakonda, kes algatab kõik järgmised sammud. Kõigepealt tuleb välja lülitada selle lõppseadme igasugune juurdepääs infokooslusele, näiteks e-posti või VPN-i kaudu. Seejärel tuleks eemalt kõik kaitset vajavad andmed lõppseadmelt kustutada ja seade lukustada. Lukustuskuva võib varustada vabalt valitud sõnumiga. Siin peaksid ausa leidja jaoks olema kõik vajalikud kontaktandmed, et ta saaks seadme asutusele tagasi anda.

Varas püüab tavaliselt takistada lõppseadme positsioneerimist, eemaldades SIM-kaardi. Seetõttu soovitatakse kasutada seadme positsioneerimiseks, väljalülitamiseks ja lukustamiseks selliseid rakendusi, mis võivad neid tegevusi teostada sündmuste põhiselt. Nii tuleks kõik kaitset vajavad andmed lõppseadmelt kustutada, kui sisestatakse teine SIM-kaart või kui SIM-kaart eemaldatakse.

Varga paremaks tuvastamiseks on kasulik, kui rakendus edastab automaatselt uue SIM-kaardi telefoninumbri GPS-koordinaadid asutusele. Kui saabuvad sellised automaatsed sõnumid, tuleks selle seadme jaoks täiendavalt lukustada juurdepääs asutuse andmetele. Selline teade ei asenda siiski kasutaja isiklikku teadaannet kaotuse kohta.

Kui kaotatud seadmed jälle välja ilmuvad, tuleks need üle kontrollida, et tuvastada võimalikud manipulatsioonid riist- ja tarkvaral, nt kruvide avamine, turvakleebise eemaldamine või seadme kaalu erinemine seadme väljastamishetke kaalust. Kahtluste korral tuleks vastav seade kas kohe utiliseerida või toimetada täiendavaks kontrollimiseks mõne spetsialisti kätte. Et kindlaks teha, ega uuesti üles leitud nutitelefonides, tahvel- või pihuarvutites ei ole manipuleeritud programme, tuleb seadmelt kustutada kõik andmed ja see täiesti uuesti installeerida.

Kontrollküsimused:

- Kas nutitelefonide, tahvel- või pihuarvutite kaotuse või varguse korral on olemas protseduuriskeem?
- Kas lõppseadmele on installeeritud ja konfigureeritud programm, mis võimaldab seadet eemalt lukustada, välja lülitada ja positsioneerida?
- Kas see programm on konfigureeritud nii, et SIM-kaardi vahetamisel seade lukustub, lülitub välja ja positsioneeritakse ning saadetaks asutusele uus telefoninumber?
- Kas on määratletud, millisel moel kontrollida tagasi saadud seadet manipulatsioonide suhtes riist- ja tarkvaral, enne kui seda jälle kasutama hakatakse?

M 6.160 Hädaolukorra ennetamise kava SOA-keskkondade jaoks

Algatamise eest vastutavad: IT-turbespetsialist, IT-juht

Rakendamise eest vastutavad: IT-turbespetsialist, IT-juht

Kui teenusele orienteeritud arhitektuuris (SOA) langeb näiteks üks teenuseosutaja rivist välja, võivad sellel olla tõsised tagajärjed asutuse äriprotsessidele. Seejärel tuleb nii kiiresti kui võimalik alustada uuesti korrapärast tööd ja võtta asjakohased turvameetmed. Järgides üldist hädaolukorra kontseptsiooni (vt B 1.3 Hädaplaanimine ja M 6.83 Väljasttellimise avariiplaan), tuleb SOA-keskkondade jaoks koostada asjakohane hädaolukorra ennetamise kava. Selleks tuleks kõigepealt analüüsida ja hinnata võimalikke ohte ning need koos vastavate turvameetmetega dokumenteerida.

Et SOA-keskkondades on mõnikord eritingimused, tuleb neid ka kontseptsioonis arvesse võtta. Nii ei tule näiteks üksnes tagada käideldavust, vaid aeg-ajalt ka kontrollida, kas teenused on ikka õigustatult registreeritud. Volitusteta teenused tuleb kataloogist kustutada.

Peale selle tuleks välja töötada käitamisraamat, mis reguleerib hädaolukorda talitluspidevuse plaanis (ingl Business Continuity Plan). See võtab arvesse SOA-keskkonna eripärasid, analüüsib ohtusid, mis on seotud tõsiste kahjude tekkimisega ning sisaldab soovitusi hädaolukorra meetmete võtmiseks.

Kontrollküsimused:

- Kas SOA-keskkondade jaoks on olemas hädaolukorra ennetamise kava?

M 6.161 Liiasusega riistvarakomponendid teenustele suunatud arhitektuurides

Algatamise eest vastutavad: IT-turbespetsialist, IT-juht
Rakendamise eest vastutavad: administraator, IT-juht

Kui teostatakse SOA-platvorm, tuleb tähelepanu pöörata sellele, et oluliste teenuste jaoks oleksid olemas liiasusega riistvarakomponendid, mida võib aktiveerida vastuvõetava ajavahemiku jooksul. Nii tagatakse töö jätkamine ka siis, kui mõni teenus peaks rivist välja langema.

Lisaks tuleks teenuseid korrapäraselt varundada, et neid oleks pärast riket võimalik kiiresti uuesti teisele riistvarale juurutada ja seal käitada. Infoturbekontseptsioonis tuleb määratleda meetmed riistvara rikke puhuks ja nimetada selle jaoks näiteks kontaktisik ja asendusriistvara allikad (vt M 6.160 Hädaolukorra ennetamise kava SOA-keskkondade jaoks).

Rikke saab siiski ainult sel juhul kompenseerida, kui alternatiivne teenus tehakse teatavaks ka teenusekasutajatele. SOA-platvormi raames võib see toimuda näiteks WS-Discovery abil. Ilma selleta laseb automaatne signalisatsioon rikke kõrvaldada üksnes küllaltki mahuka käsitsi tööga.

Kontrollküsimused:

- Kas on olemas liiasusega riistvarakomponendid?
- Kas olemasolevad komponendid on aktiveeritavad vastuvõetava ajavahemiku jooksul?

M 6.162z Reageerimine krüpteerimismeetodi praktilise nõrgenemise korral

Algatamise eest vastutavad: IT turbespetsialist, IT-juht, organisatsiooni juht
Rakendamise eest vastutavad: administraator

Nõrgestatud krüpteerimismeetodi korral tuleb võimalikult kiiresti analüüsida, kuidas protseduuri sobiva alternatiivi abil lõpuni viia, et tagada asutuse infoturve.

Kui katkestatud või rünnatav krüpteerimismeetod inaktiveeritakse, tuleb eristada kaht võimalust: kui IT-süsteemis on valida mitme krüpteerimisalgoritmi vahel ja üks neist muutub tõendatult ebaturvaliseks, tuleb tagada, et katkestatud algoritmi rohkem ei kasutataks. Kui alternatiivset algoritmi ei ole, tuleb olenevalt kaitsevajadusest võtta asjakohased meetmed. Näiteks tuleks kaaluda IT-süsteemi vastavate osade väljalülitamist või võrgust eraldamist.

Ohtu, mis katkestatud krüptograafilise protseduuri tõttu tekib, tuleks hinnata igal üksikjuhul eraldi. Sageli on ründed krüptograafilistele protseduuridele pigem teoreetilised ja praktikas üksnes äärmiselt suure kuluga teostatavad. Kui ohtu on uuesti hinnatud, tuleks kavandada sobiv migratsioonistrateegia.

Nõrgestatud krüptograafilist protseduuri võib pärast ohu hindamist vajaduse korral piiratud ajavahemiku jooksul edasi kasutada, kui ei ole võimalik mõistlike kulutustega viivitamata üle minna alternatiivsele protseduurile. Mingil juhul ei tohi nõrgestatud protseduuri püsivalt edasi kasutada. Sama kehtib ka juhul, kui krüptograafilise protseduuri rakendamisel avastatakse turvaaugud. Siin tuleb nii kiiresti kui võimalik paigaldada vajalikud turvapaigad või võtta kasutusele vastavad abinõud.

Kontrollküsimused:

- Kas juhuks, kui kasutatav krüptograafiline protseduur on rünnatav, on olemas kindlaksmääratud protsess?

M 6.163 Integreeritud süsteemide taastamine

Algatamise eest vastutavad: IT juht
Rakendamise eest vastutavad: hankija, administraator, planeerija, arendaja

Kui integreeritud süsteemi laaditakse tarkvara uus versioon, peab olema võimalik täielikult taastada süsteemi olek enne muudatuse algust. Kui seda ei ole võimalik teha süsteemil põhinevate mehhanismidega, tuleb eelnevalt tagada, et selle ajani kasutatud tarkvaraversioon jääks kättesaadavaks ja selle võib ebaõnnestunud värskenduse korral käsitsi uuesti paigaldada. Tavapärasest suuremate käideldavuse nõuete korral peaksid olemas olema mehhanismid, et taastada viimast töökonfiguratsiooni ja tarneolekut. Selleks tuleb enne iga muudatust salvestada täielik konfiguratsiooni olek. Samuti on mõeldav, et viimase töökonfiguratsiooniga valmis konfigureeritud tagasipöörde süsteemid hoitakse alles. Need võivad rikke korral muudetud ja uue versiooniga korralikult mittetöötavaid süsteeme kiiresti asendada.

Kontrollküsimused:

- Kas süsteemil on tagasipöörde võimalus?
- Kas on võimalik taastada viimast töökonfiguratsiooni?
- Kas on võimalik taastada tarneolekut?

M 6.164 Valmisolek hädaolukorraks tarkvaraarenduses

Algatamise eest vastutavad: arendusjuht
Rakendamise eest vastutavad: arendaja, erialaosakond

Tavaliselt töötatakse lihtsate komponentide piiridest väljuv tarkvara välja keeruliste tööriistadega. Seetõttu on arendusega seotud paljud projekti- ja süsteemiandmed, nii et ainuüksi selle üpris keerulise struktuuri ühe väikese osa kaotamine võib kaasa tuua märkimisväärsed kahjud ja isegi ajakohase arendusstandardi kaotuse.

Sel põhjusel on vajalik kõikide tarkvaraarenduses kasutatavate dokumentide, tööriistade ja komponentide hästi struktureeritud haldus ja andmete varundamine.

See tähendab, et tarkvaraarenduse jaoks tuleb kindlaks määrata üksikasjalik andmevarundus- ja taastamise kontseptsioon.

See peab lisaks programmikoodile sisaldama vähemalt järgmisi elemente:

- nõuete kataloog ja tarkvara spetsifikatsiooni dokumendid,
- süsteemi arhitektuuri ja liideste määratluste dokumendid,
- arenduskeskkond, kompilaator, raamatukogud,
- konfiguratsioonihaldussüsteem,
- testimisandmed, -tulemused ja -dokumendid,
- varasemad versioonid.

Andmevarundus- ja taastamise kontseptsiooni tuleb testida (vt M 6.71 Mobiilse IT-süsteemi andmevarundus). Testide tulemused tuleb dokumenteerida. Ka arendus- või testsüsteemide rikke puhuks tuleks kehtestada adekvaatsed hädaolukorra ennetamise meetmed.

Tarkvaraarenduse juurde ei kuulu üksnes dokumendid, programmid ja süsteemid, vaid ka inimeste oskusteave. Kui teadmised, mis on vajalikud rakenduse väljatöötamiseks, hooldamiseks või edasiarenduseks, on koondunud ühe isiku kätte, võivad selle suure sõltuvusega kaasneda väga tõsised probleemid.

Selliste hädaolukordade vältimiseks tuleks tähelepanu pöörata järgmistele punktidele:

- Kogu tarkvaraarenduse hea struktuur on vältimatu: sageli eelistatakse arendusprobleemi struktureeritud ja dokumenteeritud lahendusele kiiret lahen-

dust. Selle puudus on, et seetõttu mõistavad tarkvaras olevaid seoseid üksnes arendajad. Kui nad ei ole enam kättesaadavad, on tarkvara igasugune edasiarendus väga kulukas või isegi võimatu.
- Tarkvaraarendust puudutavate teadmiste teemadel tuleks arendusmeeskonna sees piisavalt suhelda, nii et igaüks võiks teatud juhtudel teise meeskonnaliikme ülesande üle võtta. See hoiab ära sõltuvuse ühest isikust ja muudab arenduse paindlikumaks, sest ajahädas on võimalik ülesandeid paremini jaotada.
- Tarkvaraarendus peab olema nii dokumenteeritud, et selle ala spetsialist saaks seda dokumentide abil kontrollida ja tarkvara edasi arendada. Selleks on vajalikud dokumendid ja protseduurid, mis kehtestatakse kvaliteedihalduse ning muudatuste ja konfiguratsioonihalduse kaudu. Hädaolukorra ennetamise raames tuleks kontrollida, kas peetakse kinni protseduuridest ja poliitikatest ning kas nendega seotud dokumendid on ajakohased ja täielikud.

Pärast arenduse lõpetamist tuleks lähtekoodi, arendusdokumentide koopiad ja arenduskeskkonna kirjeldus hoiustada turvalises kohas, et tekkivate probleemide korral oleks igal ajal võimalik kontrollida arendatud tarkvara õigsust ja manipulatsioonikindlust.

Kui tarkvaraarendust tehti tellimustööna, tuleks mõelda, kas teenuseosutajaga tuleks kokku leppida koodi hoiustamise suhtes.

Kontrollküsimused:

- Kas tarkvaraarenduse jaoks on koostatud andmevarundus- ja taastamise kontseptsioon?
- Kas andmete taastamist on juba testitud?

M 6.165 Hädaolukorra plaani koostamine kohaliku võrgu tõrke puhuks

Algatamise eest vastutavad: IT-turbespetsialist, IT-juht
Rakendamise eest vastutavad: administraator

Kohaliku võrgu osaline või täielik rike avaldab tavaliselt suurt mõju IT-keskkonnale, sest kasutajad ei pääse enam võrgu funktsioonidele ligi. Nad ei pääse siis ligi näiteks oma e-postile ega ka failiserverile, ei saa enam trükkida ja võib-olla isegi mitte helistada.

Hädaolukorra ennetamise raames tuleb seega luua kontseptsioon, mis aitaks hoida avarii tagajärgi võimalikult minimaalsetena ja määraks, millised sammud on avarii korral kohustuslikud.

Siinkohal tuleb arvestada järgmiste aspektidega:

Üldised aspektid
Kohaliku võrgu hädaolukorra plaan tuleb integreerida olemasolevasse hädaolukorra plaani (vt moodulit B 1.3 Hädaplaanimine). See peab olema kooskõlas aktiivsete võrgukomponentide (M 6.92 Marsruuterite ja kommutaatorite hädaolukorraks valmisoleku plaan), turvalüüside (M 6.94 Turvalüüside hädaolukorraks valmisoleku plaan), serveri (M 6.96 Serveri avariiplaan), võrguhalduse (M 6.57 Avariiplaani koostamine haldussüsteemi avarii puhuks) jne hädaolukorraks valmisoleku plaanidega.

Andmevarundus
LAN-i rike võib põhjustada andmekadu. Seetõttu tuleb üldise andmete varundamise kontseptsiooni raames (vt moodulit B 1.4 Andmevarunduspoliitika) koostada eeskirjad LAN-i jaoks. Selleks, et pärast riket saaks tööga alustada nii kiiresti kui võimalik, tuleb tähtsaimad konfigureerimisfailid (nt aktiivse võrgukomponendi, turvalüüsi, haldussüsteemi jne konfigureerimisandmed) varundada elektroonilisel kujul (vt ka M 6.32 Regulaarne andmevarundus). Nende seadistuste kiireks juurutamiseks pärast riket tuleb konfiguratsioone süstemaatiliselt dokumenteerida (vt ka M 2.25 Süsteemi konfiguratsiooni dokumenteerimine).

Dokumentatsioon
Et LAN-i saaks pärast riket jälle kiiresti rakendada, peab olemas olema LAN-iajakohane dokumentatsioon (süsteemidokumentatsioon), sh kõik võrguplaanid (võrgu loogiline ja füüsiline topoloogia). Tähtsaid ülesandeid tuleb kirjeldada nii, et LAN-i saaks hädaolukorras taastada ka ilma eelnevate teadmisteta üksikute IT-süsteemide konfiguratsioonist. Oluliste konfiguratsioonimuudatuste korral tuleb dokumentatsiooni ajakohastada. Tähelepanu tuleb pöörata sellele, et hädaolukorra vastavad dokumendid sisaldavad olulist ja kaitsmist vajavat teavet, nii et neid tuleb säilitada kaitstud kohas. Vaatamata sellele, peavad volitatud isikud sellele hädaolukorras ligi pääsema.

Varuvõrk

Käideldavusele esitatavate kõrgendatud nõudmiste korral peaksid olulised võrgukomponendid olema loodud liiasusega ja vajaduse korral tuleks mõelda ka alternatiivsete võimaluste kasutamisele, nt varuvõrgule ümberlülitumisele.

Personal

Hädaolukorraks valmisoleku plaaniga tuleb tagada, et hädaolukorras oleks kasutada vastava koolituse saanud töötajad.

Taasteplaan

Tuleb luua taasteplaan, mis tagaks kohaliku võrgu korrakohase taaskäivitamise. Kõiki vajalikke nõuete kirjeldusi tuleb korrapäraselt kontrollida ja katsetada. Arvesse tuleb võtta varieeruvaid tegevusviise erinevate operatsioonisüsteemide korral.

Hädaolukorra harjutused

Ka parimast taasteplaanist pole eriti kasu, kui see ei ole praktikas kasutatav. Seetõttu on erilise tähtsusega korrapäraste hädaolukorra harjutuste läbiviimine, et tunda ära nõrgad kohad ja osata neid parandada. Ainult nii saab tagada, et taasteplaanides kirjeldatud meetmeid on ka tegelikult võimalik ellu viia. Samal ajal õpivad töötajad õppuste käigus kirjeldatud protsesse tundma ja treenivad nende rakendamist. Lõpuks saadakse õppustega teadmisi tegelikest taastus- ja taaskäivitusprotsessidest ning seeläbi saab kontrollida kinnipidamist toime analüüsis (ingl Business Impact Analyse, BIA) toodud nõuetest.

Kontrollküsimused:

- Kas kohaliku võrgu hädaolukorra plaan integreeriti olemasolevasse hädaolukorra plaani ja kooskõlastati muude hädaolukorraplaanidega?
- Kas dokumendid on ajakohased ja kas neid ajakohastatakse oluliste muudatuste korral? Kas dokumendid on kaitstud loata juurdepääsu eest, kuid on vastutavate isikute jaoks hädaolukorras siiski igal ajal kättesaadavad?
- Kas üldise andmevarunduse kontspetsiooni raames koostati eeskirjad LAN-i jaoks?
- Kas tähtsaimaid konfigureerimisfaile varundatakse elektroonilisel kujul?
- Kas hädaolukorras saab kasutada koolitatud töötajaid?
- Kas on olemas taasteplaan?
- Kas viiakse läbi hädaolukorra õppusi hädaolukorra ennetamiseks LAN-i rikke korral?

M 6.166 Valmisolek hädaolukorraks identiteedi- ja volituste halduse süsteemi puhul

Algatamise eest vastutavad: IT turbespetsialist, IT-juht

Rakendamise eest vastutavad: IT turbespetsialist, administraator

Kui identiteedi- ja volituste halduse süsteem langeb rivist välja, ei saa kasutajaprofiile muuta, uusi määrata ega neid kustutada. Tuleb kontrollida, kui suured on selle turbekriitilised mõjud äriprotsessidele. Samuti tuleb uurida, kuidas mõjutab rünne õigusi, mida ei saanud identiteedi- ja volituste halduse süsteemi rikkega seoses kustutada.

Et kõik identiteedi- ja volituste halduse süsteemis salvestatud andmed oleksid ka riistvara rikete, tõrgete või (sihilike või mittesihilike) muudatuste korral jätkuvalt kasutatavad, on vaja korrapäraseid ja põhjalikke andmevarundusi. Vajalikke meetmeid on kirjeldatud moodulis B 1.4 Andmevarunduspoliitika .

Kui identiteedi- ja volituste halduse jaoks kasutatakse asutuses tsentraalset tööriista, on selle korrakohane kasutamine oluline kõikide sellega seotud protsesside ja rakenduste säilitamiseks. Seetõttu tuleb hädaolukorra ennetamise raames täpsustada, millised on tööriistade rikke mõjud identiteedi- ja volituste haldusele ja kuidas need hädaolukorras kiiresti uuesti töökorda saadakse (vt ka moodulit B 1.3 Hädaplaanimine).

Hädaolukordades võib osutuda vajalikuks ulatuslike lühiajaliste volituste andmine spetsialistidele (nt kriisistaabist), et kõrvaldada hädaolukord ja taastada töörežiim. Volituste andmise, dokumenteerimise ja äravõtmise protsess peab olema kirjeldatud hädaolukorra kontseptsioonis. Peale selle tuleb hädaolukorra kontseptsioonis kontrollida, kas selles hädaolukordade jaoks ettenähtud volituste kontseptsioonid on identiteedi- ja volituste halduse süsteemi tõrke esinemise korral veel kasutatavad.

Kontrollküsimused:

- Kas teostatakse korrapäraseid identiteedi- ja volituste halduse tööriistade andmevarundusi?
- Kas hädaolukordade jaoks on olemas volituste kontseptsioonid?
- Kas hädaolukordade volitused on identiteedi- ja volituste halduse süsteemi tõrke korral veel kasutatavad, et rakendada hädaolukorra meetmeid?

ISKE kataloogid

HG: Kohustuslikud üldmeetmed

Meetmete nimekiri

HG.1 Lisanõuded juhtmestuse kohandamisele

M 1.3 J uhtmestuse kohandamine parametriseering

Lisaks M 1.3 Juhtmestuse kohandamine nõuetele kehtivad lisanõuded juhtmestuse kohandamise sageduse osas. Juhtmestik tuleb üle vaadata ning vajadusel kohandada iga kord, kui:

- ruumide funktsioone muudetakse (nt kabinet antakse ühe allüksuse töötajalt teisele, kabineti asemel tehakse nõupidamisruum vms);
- ruume kasutavate töötajate tööülesandeid muudetakse;
- installeeritakse uut süsteemset riistvara;
- muudetakse võrgu topoloogiat;
- toimus kaablirikkega seotud intsident.
- turvainspekteerimisel avastati tegeliku juhtmestiku lahknevus dokumentatsioonis kirjeldatust;
- muudetakse asutuse turvapoliitikat või riistvara puudutavaid turvaplaane.

Juhtmestik tuleb üle vaadata ka juhtudel, kui asutuses muudetakse füüsilisi turvatsoone või võrgu eralduslüüse (tulemüürid, VPN-id jms), samuti ka turvatsoonidega seotud pääsuõigusi.

HG.2 Tuletõrje-eeskirjade täitmise seire

Unikaalmeede

Tuletõrje-eeskirjade (M 1.6 Tuletõrje-eeskirjade täitmine) täitmist tuleb kontrollida:

- vähemalt kaks korda aastas, pistelise kontrollina juhuslikel aegadel, ilma etteteatamiseta;
- kui asutuses on avastatud juhuslikult (st ilma eriseireta) vähemalt üks tuletõrje- eeskirjade rikkumine;
- kui tuletõrjesignalisatsioon on rakendunud üle nelja korra aastas.

Lisaks eeltoodule tuleb juhinduda tuleohutuse seaduses sätestatust.
Kõik eeltoodu on hoone haldusjuhi kohustus.

HG.3 Tõrgete kaugindikatsiooni vastuvõtmiskohustus

Unikaalmeede

Kui töötajale on loodud tõrgete kaugindikatsiooni võimalus (mobiiltelefoni, spetsiaalse raadiosaatja vms abil, vt M 1.31 Tõrgete kaugindikatsioon), peab töötaja olema 24 tundi ööpäevas selle seadme signaaliulatuses. See tähendab telefonihelina kuuldeulatuses olemist või signaali tuvastamist hiljemalt 15 minuti jooksul pärast signaali.

Töötaja ei tohi kaugindikatsiooni võimaldavat seadet üle anda teistele isikutele, kuna teave kaugindikatsiooni kohta võib sisaldada konfidentsiaalset informatsiooni infosüsteemi turvaseisundi või -intsidentide kohta.

Eelnev tuleb teha töötajale kohustuslikuks töötaja töölepingus, ametijuhendis või asutuse sisese korraga.

HG.4 Võrguhaldussüsteemi turbe regulaarseire

Unikaalmeede

Võrguhaldussüsteemi turvalisust (vt M 2.146 Võrguhaldussüsteemi turvaline kasutamine) tuleb kontrollida:

- pistelise kontrollina vähemalt kaks korda aastas, juhuslikel aegadel, ilma etteteatamiseta;
- pärast igat suuremat muutust võrguhaldussüsteemis (tarkvara ja/või riistvara muutus, kaabelduse paigutuse muutus, püsikonsooli asukoha muutus jms);
- haldussüsteemi turvalisuse kahtluse ilmnemisel logidest või muudest andmetest;
- pärast igat võrguhaldussüsteemi puudutavat turvaintsidenti;
- üldtunnustatud turvalistidesse teadete laekumisel sarnaste süsteemide haldamise turbe probleemide kohta.

HG.5 Lisanõuded viiruseskänneri värskendamisele

M 2.159 Viiruseskanneri värskendamine parametriseering

Lisaks viiruseskänneri värskendamise nõuetele peab lähtuma alljärgnevast:

- Viiruseskänner peab üldjuhul kord päevas viirusedefinitsiooni automaatselt uuendama. Erandiks on offlines töötavad seadmed, mille seaded ja viirusetõrje korralduse määrab turvajuht eranditena hinnates turvapoliitika olukorda arvestades(vt M 2.380 Erandite kooskõlastamine).
- Automaatse uuendamise funktsionaalsus peab olema sisse lülitatud. Arvuti kasutaja ja/või administraator peavad teadvustama signaale, mis kaasnevad automaatuuenduse või aktiveerituse väljalülitamistega. Neil juhtumeil tuleb viivitamatult teavitada turvajuhti.
- Turvajuht või tema poolt volitatud isik peab pidevalt jälgima viirusetõrjeprogrammide võrdlusi ja sellealaseid eksperthinnanguid. Kui selgub, et kasutatav viirusetõrjeprogramm ei uuenda ennast enam piisavalt kiiresti, ei suuda kahjurkoodi piisavalt kohe ja efektiivselt avastada jne, tuleb viirusetõrjeprogramm viivitamatult teise vastu välja vahetada. Vt ka M 2.157 Sobiva viiruseskanneri valimine .

HG.6 Arvuti paroolkaitse rangemad reeglid

M 4.1 IT-süsteemide paroolkaitse parametriseering

Lisaks IT-süsteemide paroolkaitse nõuetele peab kasutaja poolt arvutisse sisestatav parool vastama järgmistele tingimustele:

- olema vähemalt 15 märki pikk või kasutada kahe-faktorist (2FA) autentimist;
- sisaldama vähemalt kaht suur- ja kaht väiketähte;
- sisaldama vähemalt kaht numbrit või erimärki;
- olema kontrollitud parooliskänneriga nõrkade paroolide otsinguks.

Kolmest esimesest omadusest (eelnimetatud nelja hulgast) võib loobuda juhul, kui parooli töödeldakse niisuguse autentimissüsteemi, mille ülesehitus välistab parooli ammendava otsingu (sõnastikründe realiseerimise) ning kus teatud arv kordi paroole proovides (soovitatavalt mitte üle viie korra) läheb seade lukku, st edaspidiseid paroolipro ovimisi enam läbi viia ei saa. Selline paroolipoliitika kehtib näiteks Eesti ID-kaardi puhul (selles paroolina toimivad PIN- ja PUK-koodid).

Nimetatud turvameede kehtib kõikide seadmete kohta, mida võib vaadelda arvutite või selle lisaseadmetena – serverid, lauaarvutid, sülearvutid, pihuarvutid, GPSid jne (kaasajal on turul palju hübriidseadmeid, mida on raske kindlasse lahtrisse liigitada).

Turvameede kehtib lisaks ka parooliga toimivate koodlukkude kohta, mida kasutatakse füüsilise pääsu reguleerimiseks (ruumid, territooriumid jms) ilma inimese juuresolekuta.

HG.7 Ekraaniluku lühem ooteaeg

M 4.2 Ekraanilukk parametriseering

Rakendajal on õigus hinnata, kui pika aja pärast aktiveerub automaatne ekraanilukk, kuid kindlasti ei tohi see aktiviseeruda hiljem kui 15 minutit. (M 4.2 Ekraanilukk soovitab 15 minuti jooksul). Lisaks peab kasutaja töökohalt lahkudes alati iseseisvalt ekraani lukustama.

HG.13 Lisanõuded andmete kaugedastuse hädaolukorraplaanile

- andmeside kaugedastuse hädaolukorraplaanid tuleb pistelise kontrolli käigus läbi vaadata vähemalt kaks korda aastas;
- andmeside kaugedastuse hädaolukorraplaanid tuleb läbi vaadata kahe nädala jooksul pärast andmeside konfiguratsiooni (liinid, teenusepakkujad, riistvaraplatvorm vm) muutumist;
- andmeside kaugedastuse hädaolukorraplaanid tuleb läbi vaadata kahe nädala jooksul pärast kriitilise turvaaugu ilmsikstulekut (vaata üldkasutatavad turvafoorumid), mis andmeside kaugedastust puudutab;
- andmeside kaugedastuse hädaolukorraplaanid tuleb läbi vaadata kuu jooksul pärast turvaintsidente (või nende uurimise lõpetamist), mis andmete kaugedastusega seotud olid.

Kõik eeltoodu on turvajuhi kohustus.

HG.14 Lisanõuded hädaolukorrajärgsele taasteplaanile

Hädaolukorrajärgsed taasteplaanid tuleb läbi vaadata

- pistelise kontrolli käigus vähemalt kaks korda aastas;
- kahe nädala jooksul pärast süsteemi puudutava kriitilise turvaaugu ilmsikstulekut (vt üldlevinud turvafoorumid);
- kuu jooksul pärast turvaintsidendi toimumist (või selle uurimise lõpetamist);
- kuu jooksul pärast süsteemi olulist modifitseerimist (uus riistvara, tarkvara, kasutajad, muutunud ärireeglid).

Turvajuhi kohustus on otsustada, milline muutus on eeltoodud loetelu mõttes oluline.

HG.15 Tihendatud perioodiga hädaolukorraõppused

Hädaolukorraõppusi tuleb läbi viia:

- vähemalt kord aastas;
- pärast igat suuremat muutust, millega muutub olulistes osades ka vastava ressursi taasteprotsess;
- pärast igat turvaintsidenti, kui selle järel tuvastati ühe põhjusena taasteplaani ebakorrektset järgimist.

HG.16 Andmevarundusplaani perioodiline läbivaatus

Unikaalmeede

Andmevarundusplaanid tuleb pistelise kontrollina läbi vaadata kaks korda aastas. Samuti tuleb need läbi vaadata ja vajadusel korrigeerida nädala jooksul, juhul kui:

- andmete varunduse tehnilisi põhimõtteid on oluliselt muudetud;
- andmevarundamise alast vastutust (organisatsioonilist korraldust) on oluliselt muudetud;
- muudetud on asutuse turvapoliitikat ja/või turvaplaani ja muutused puudutavad olulisel määral andmevarundust.

Eelmainitu on asutuse turvajuhi kohustus.

HG.17 Asendushankeplaani perioodiline läbivaatus

Unikaalmeede

Asendushankeplaanid tuleb pistelise kontrollina läbi vaadata vähemalt kaks korda aastas. Samuti tuleb need läbi vaadata ja vajadusel modifitseerida nädala jooksul, juhul kui:

- muudetud on asendushanke instantse/partnereid;
- asendushanke alast vastutust (organisatsioonilist korraldust, lepinguid hankijatega) on oluliselt muudetud;
- turvaintsidendi uurimisel selgus, et selle üheks põhjuseks olid muuhulgas ka puudused asendushankeplaanis või selle täitmatajätmine;
- muudetud on asutuse turvapoliitikat ja/või turvaplaani ja muutused puudutavad olulisel määral asendushanget.

Eelmainitu on asutuse turvajuhi kohustus.

HG.18 Leppetrahvid tarnijatega tehtavatesse lepingutesse

Unikaalmeede

Leppetrahvid tarnijatega tehtavatesse lepingutesse peavad kehtima järgmiste olukordade puhuks:

- tarne ei ole õigeks ajaks kohale jõudnud;
- tarnitud on nõuetest erinevaid tooteid/teenuseid;
- tarnes ettenähtud toote või teenuse tugi ei vasta lepingutingimustele.

HG.19 Lisanõuded andmetaaste harjutamisele

Unikaalmeede

Andmete taastamise harjutamise nõuetele vastavalt tuleb andmete varukoopiatelt taastamise harjutamine läbi viia:

- vähemalt üks kord aastas;
- pärast andmekoosseisu olulist muutumist;
- pärast igat turvaintsidenti, kui sellele järgnevalt tuvastati ühe põhjusena taasteplaani halb järgimine.

HG.20 Taustauuring personali palkamisel

M 3.33 Personali taustakontroll parametriseering seadmine

Lisaks personali taustakontrolli nõuetele personali taustauuringul tuleb lähtuda järgnevast:

- Taustauuringus tuleb selleks kasutada globaalotsinguid veebis ning otsingut Eesti temaatilistes veebifoorumites ja vestlusgruppides (Facebook, muud suhtluskeskkonnad, isiklikud tutvused).
- Taustakontrolli peab kindlasti olema kaasatud asutuse turvajuht.

Kui kasutatakse väljasttellimist, tuleb käesoleva meetme ja personali taustakontrolli nõudeid rakendada ka selle organisatsiooni võtmeisikute suhtes, kellelt töö tellitakse. Nimetatud isikute nimekirja määrab ja uuringu teeb turvajuht koostöös asutuse personalijuhiga.

HG.21 Personali perioodiline turva-alane atasteerimine

Unikaalmeede

Atesteerimist korraldab turvajuht koostöös personalijuhiga. Atesteerimisse tuleb võimalusel kaasata väljastpoolt oma asutust vähemalt üks turvaekspert, kes tunneb töötajasse puutuva valdkonna turvateemat piisavalt põhjalikult.

Atesteerimisel peab töötaja teadma asutuse turbe üldisi eesmärke ja tema konkreetsete töökohustuste kõiki turvatahke ja –aspekte, mida tal praktikas vaja läheb. Atesteerimine tuleb läbi viia töötajate hulgas, kes puutuvad oma töökohustuste põhjal kokku kõrge turbeastmega andmetega. Üheks võimalikuks atesteerimise meetodiks võiks olla näiteks asjakohase testi täitmine.

HG.22 Ööpäevaringne intsidentidest teatamise võimalus

Unikaalmeede

See võimalus tuleb luua turvalise sidekanali abil (mobiiltelefon, turvaline e-post). Lubamatu on selleks kasutada turvamata avalikke teenusekanaleid (tavaline e-post, avalikud uudisegrupid ja foorumid vms).

Intsidentidest teavitatakse turvajuhti või tema poolt määratud isikut (isikuid).

HG.23 Kahe erineva tootja kahjurvara- ja ründetuvastusprogrammi kasutamine

Unikaalmeede

Kõikide kõrgastme turbega seotud infosüsteemi viirusetõrje ülesehitus peab tagama olukorra, kus kasutatakse kaht erinevat pahavara tuvastusprogrammi. Soovitavalt tuleks siin eelistada olukorda, kus ühe tootja toodet kasutatakse serveril, teist tööjaamades. Ebasoovitav on kahe enam-vähem ühesuguse funktsioonidega toote kasutamine, mis erinevad ainult tootjate poolest.

HG.24 Paroolide regulaarkontroll parooliskänneriga

Unikaalmeede

Paroolide regulaarne perioodiline kontroll parooliskänneriga tuleb läbi viia:

- pisteliselt vähemalt neli korda aastas;
- pärast igat turvaintsidenti, mille on põhjustanud nõrga parooli kasutamine.

Kontrollimiseks on soovitatav kasutada vähemalt kahte erinevat üldtunnustatud parooliskännerit.

HG.25 Kaugpöörduste kohustuslik logimine

M 5.9 Serveri logi parametriseering

Lisaks serveri logidele esitatavatele nõuetele tuleb kõik kaugpöördused alati kohustuslikus korras serverisse logida. Konkreetsete andmete koosseis, mida konkreetsel juhumil logitakse, määratakse turvajuhi ja IT juhi koostöös.

Nimetatud logisid tuleb säilitada sellises keskkonnas, kus andmeid ei saa kaugpöördusvahenditega muuta, vaid üksnes (vajadusel) lugeda. Asutuses tuleb kirjalikult fikseeritult määrata isik (tavaliselt süsteemiadministraator), kelle tööülesannetesse tuleb kirjalikult lisada nende logide pisteline või automatiseeritud läbivaatamine kohustus. Soovitatav on teha logide läbivaatus vähemalt korra tööpäeva jooksul.

HG.26 Andmekandjate vahetuse dokumenteerimine

Unikaalmeede

Andmekandjate vahetus tuleb dokumenteerida. Dokumenteerida tuleb järgmised parameetrid:

- millal andmekandja saadi;
- andmekandja liik;
- kes andmekandja üle andis ja kes vastu võttis;
- millisesse süsteemi andmed andmekandjalt sisestati.

Kui andmekandjate vahetus dokumenteeritakse digitaalselt, ei tohi seda dokumentatsiooni saada kaugpöördustehnikaga muuta, vaid üksnes (vajadusel) lugeda.

Vt ka M 2.3 Andmekandjate haldus ja M 2.45 Andmekandjate üleandmine

Ülalmainitu on IT juhi või tema poolt määratud töötaja kohustus.

HG.27 Tulemüüri ründekatsete kaugindikatsioon

Unikaalmeede

Tulemüüri ründe katsete kaugindikatsioon tuleb realiseerida ning selle käigus on vajalik:

- spetsifitseerida pöördumised tulemüüridesse, mille korral kaugindikatsioon rakendub;
- kaugindikatsioon logida (vt HG.25 Kaugpöörduste kohustuslik logimine);
- kaugindikatsiooni teabe edastamise juures tuleb teave krüpteerida turvameetme HT.52 Lisanõuded krüptovahenditele nõuete kohaselt, juhul kui sõnumis sisaldab konfidentsiaalset informatsiooni.

Mainitu on IT juhi või tema poolt määratud töötaja kohustus.

HG.28 Kõrge turbeteaseme serveri kettatäitumise kaugindikatsioon

M 5.54 Meili ülekoormuse ja spämmi tõrje parameetrite seadmine

Lisaks meili ülekoormuse ja spämmi tõrje nõuetele tuleb realiseerida meiliserveri ketta täitumise kaugindikatsioon, mis:

- rakendub asutuse poolt kriitiliseks määratud mahu juures;
- suudab edastatava teabe logida (vt HG.25 Kaugpöörduste kohustuslik logimine);
- teabe edastamise juures tuleb teave krüpteerida turvameetme HT.52 Lisanõuded krüptovahenditele nõuete kohaselt.

Lisaks eelmainitule tuleb garanteerida tõrketeabe jõudmine meiliserveri administraatorini.

HG.30 VPNi kasutamise kohustus, kui raadiovõrku kasutatakse magistraalvõrguna

M 2.384 Sobiva traadita kohtvõrgu krüpteerimisviisi valik parametriseering

Juhul kui raadioühendust (WiFi vms) on kasutatud magistraalvõrguna, on kogu liikluse konfidentsiaalsuse ja tervikluse tagamise täiendav turve kohustuslik. Soovitavalt tuleb turve tagada VPNi vahenditega - mitte mingil juhul ei tohi turvet teostada WiFi (IEEE 802.11i) enda vahenditega (vt M 4.224 Virtuaalsete privaatvõrkude integreerimine turvalüüsidesse). VPNi juures kasutatavad krüptoalgoritmid peavad vastama HT.52 Lisanõuded krüptovahenditele nõuetele. Vt ka M 5.60 Sobiva magistraalvõrgutehnika valimine .

Lisaks tuleb kaaluda, kas kõrgastme turbe korral on üldse mõistlik kasutada traadita lahendusi või jääda siiski traditsiooniliste traadiga võrkude juurde. Nimetatud turvariskide kaalumine on turvajuhi kohustus.

HG.31 Traadita kohtvõrgu väline turvaaudit

M 5.141 Regulaarsed traadita kohtvõrgu turvakontrollid parametriseering

Lisaks regulaarsetele traadita kohtvõrgu turvakontrolli nõuetele tuleb soovitavalt kord kahe aasta jooksul viia läbi kohustuslik väline turvaaudit, sest WiFi lahendused muutuvad kiiresti ning enamik uusi lahendusi on osutunud ebaturvaliseks. Esimene turvaaudit tuleb läbi viia enne WiFi-põhise süsteemi kasutusele võtmist.

Selline audit tuleb lasta sooritada pikaajalise kvalifikatsiooni ja praktikaga Wi-Fi spetsialistil. Soovitav on niisugune auditeerimine läbi viia vähemalt kord kahe aasta jooksul.

HG.33 Meiliaadresside asenduskorra regulaarseire

M 2.274 Asendamise korraldamine meilivahetuse alal parameetrite seadmine

Lisaks meilivahetuse alase asendamise korraldamise nõuetele tuleb olemasolevad meiliaadressid, nende moodustamise kord, asendamise kord jm, läbi vaadata regulaarselt kaks korda aastas. Eelkõige tuleb selle käigus kontrollida, kas asutuse üldised meiliaadressid ja siselistid, millele saadetud meil saadetakse laiali mitmetele töötajatele, vastavad töötajate praeguse hetke töökohustustele ega pole vahepeal aegunud.

Turvaintsidendi ilmnemisel, mille üheks osaks oli meilivahetuse puudulik korraldus, tuleb teha erakorraline läbivaatus hiljemalt kaks nädalat pärast nimetatud turvaintsidendi uurimise ja põhjuse selgitamise lõppu.

HG.34 Sülearvutite kasutuse regulaarseire

M 2.36 Sülearvuti väljaandmise ja tagastamise reeglid parameetrite seadmine

Lisaks sülearvuti väljaandmise ja tagastamise nõuetele tuleb asutuses vähemalt kaks korda aastas läbi vaadata sülearvutite kasutamise kord ning olemasolevad sülearvutid ja nende praktiline kasutamine töötajate ja nende poolt tehtavate tööde raames. Nimetatud läbivaatuse juures peavad kindlasti osalema IT juht (või IT infrastruktuuri juht) ja turvajuht.

Nimetatud seire käigus tuleks eelkõige kontrollida viiruse- ja pahavaratõrje vahendite ajakohasust ja toimivust ning kasutatava tarkvara turvapaikade installeeritust. Kui võimalik, siis võiks see tegevus olla osaliselt või täis mahus automatiseeritud.

Kui ilmneb turvaintsident, mille oluliseks osaks on sülearvutite puudulikult reguleeritud kasutamine või kasutusreeglite eiramine, tuleb teha sülearvutite kasutamise erakorraline läbivaatus vastavalt turvaintsidentide käsitlemise korrale (M 6.64 Turvaintsidentide likvideerimine , M 6.65 Asjassepuutuvate isikute teavitamine turvaintsidentidest , M 6.66 Turvaintsidentide järelhindamine , M 6.67 Turvaintsidentide avastamismeetmete rakendamine ja M 6.68 Turvaintsidentide käsitluse süsteemi tõhususe testimine).

HG.35 Pihuarvutite kasutuse regulaarseire

M 2.304 Pihuarvutite turvapoliitika ja kasutamise reeglid parametriseering

Lisaks pihuarvutite turvapoliitika ja kasutamise reeglitele tuleb vähemalt kaks korda aastas pisteliselt läbi vaadata pihuarvutite kasutamise kord ning olemasolevad pihuarvutid ja nende praktiline kasutamine. Turvaintsidendi ilmnemisel, mille üheks osaks oli pihuarvutite puudulikult reguleeritud kasutamine või kasutusreeglite eiramine, tuleb teha erakorraline läbivaatus hiljemalt kaks nädalat pärast nimetatud turvaintsidendi uurimise lõppu.

Nimetatud läbivaatuse/seire korraldamine on asutuse turvajuhi pädevuses. Kuna pihuarvutid kujutavad oma mobiilsusega paljudel juhtudel täiendavaid turvariske, peavad kõik pihuarvutite kasutusjuhtumid kõrgastme turbega andmete töötlemiseks olema alati väga tõsiselt läbi kaalutud. Soovitav on neid kasutada vaid juhtudel, kui nende kasutamine annab väga olulist ergonoomilist või käideldavuskasu võrreldes paiksete arvutitega. Samuti peab mobiilsusega kaasnevat täiendavat turvariski on võimalik efektiivselt maandada. Lõpliku otsuse tegemine igal konkreetsel juhtumil jääb siin turvajuhi pädevusse. Vt ka M 4.230 Pihuarvutite tsentraalne haldus .

HG.36 Väljasttellimise avariiplaani regulaarne läbivaatus

Unikaalmeede

Vähemalt kaks korda aastas tuleb väljasttellimise avariiplaan (M 6.83 Väljasttellimise avariiplaan) pisteliselt läbi vaadata. Juhul kui toimub turvaintsident, mille üheks osaks on väljasttellimise väär korraldus või reeglite eiramine, tuleb teha erakorraline läbivaatus hiljemalt kaks nädalat pärast nimetatud turvaintsidendi uurimise lõppu.

Nimetatu on turvajuhi töökohustus.

HG.37 Tarkvara tervikluskontroll igal installeerimisel

M 4.177 Tarkvarapakettide tervikluse ja autentsuse tagamine parameetrite seadmine

Lisaks tarkvarapakettide tervikluse ja autentsuse tagamise nõuetele tuleb igal tarkvara installeerimisel, uuestiinstalleerimisel, turvapaikade lisamisel jms juhtudel enne installeerimist kontrollida tarkvara terviklust krüptograafilise räsifunktsiooni abil. See toiming tuleb kirjalikult dokumenteerida ja tarkvara installeerija peab oma allkirjaga (või sellega võrdsustatud digiallkirjaga) kinnitama, et on installeeritava tarkvaratoote ehtsust räside põhjal kontrollinud.

Eelpool kasutatavad räsifunktsioonid peavad vastama HT.52 Lisanõuded krüptovahenditele nõuetele (st keelatud on MD-perekonna räsid).

Lisaks käsitsi teostatavale kontrollile sobib siin ka automaatkontroll, kui selle põhikäik ja protsessid vastavad eeltoodule (nt Microsofti tarkvara automaatuuendusel tehtu).

HG.38 Turvapaikade paigaldatuse regulaarseire

M 2.273 Turvalisust mõjutavate paikade ja värskenduste kiire paigaldamine parameetrite seadmine

Lisaks turvalisust mõjutavate paikade ja värskenduste kiire paigaldamise nõuetele tuleb vähemalt kaks korda aastas kogu kasutatavat tarkvara valikuliselt ja pisteliselt testida turvapaikade ja -uuenduste installeerituse osas.

Turvaintsidendi ilmnemisel, mille üheks põhjuseks osutuvad puudused turvapaikade paigalduses, tuleb läbi viia erakorraline seire ning uurida eranditult kogu kasutatavat tarkvara. Nimetatud erakorraline seire tuleb läbi viia hiljemalt kaks nädalat pärast nimetatud turvaintsidendi uurimise lõppu ja tulemuste ilmnemist.

HG.39 Lisanõuded tarkvara vastuvõtuprotseduuridele

M 2.62 Tarkvara vastuvõtuprotseduurid parameetrite seadmine

Lisaks tarkvara vastuvõtuprotseduuride nõuetele tuleb lähtuda järgmistest aspektidest:

- vastuvõturühmas peab olema kindlasti üks turbespetsialist;
- tarkvaras kasutatavad krüptoalgoritmid, -protokollid ning nende üksikasjad ja parameetrid peavad dokumentatsioonist üheselt selguma ja vastama HT.52 Lisanõuded krüptovahenditele nõuetele;
- tarkvaras kasutatavaid krüptoalgoritme, -protokolle ning nende üksikasju tuleb vastuvõtmisel valikuliselt testida, veendumaks nende dokumentatsioonile vastavuses;
- testimis- ja vastuvõturühm peab olema vähemalt kolmeliikmeline;
- soovitatav on lasta test sooritada isikutel ja/või organisatsioonil, kellel on pikaajalised kogemused turvaomadustega tarkvara auditeerimise alal;
- soovitav on lisaks tellida ka läbistustest ja/või koodiaudit.

HG.40 CERT-EE teavitamine välismõjuga turvaintsidendist

M 6.65 Asjassepuutuvate isikute teavitamine turvaintsidentidest parameetrite seadmine

Suändmus, millega kaasneb andmete voõi muude infovarade kaäideldavuse, tervikluse voõi konfidentsiaalsuse kadu voõi tekib oht nende kadumiseks, siis tuleb lisaks asjassepuutuvate isikute turvaintsidendist teavitamise nõuetele sellest teavitada ka Eesti riigi rahvuslikku CERT'i vastavalt Riigi Infosüsteemi Ameti (RIA) poolt antud juhisetele. Oluline turvaintsident voõib lisaks oma infosuästeemile moõjutada teiste asutuste teenuste osutamiseks vajalike infosuästeemide toimimist.

RIA on oma veebilehel avaldanud täpsemad juhised ja raportite vormid kuidas ja millal CERT EE-d teavitama peab. https://www.ria.ee/et/kuberturvalisus/kuberintsidendist-teavitamine.html

Sisemistest faktoritest poõhjustatud turvaintsidentidest, mis ei vii asutuste toäoä voõi elutaähtsate teenuste katkestuse ohuni ega moõjuta teisi suästeeme ega voõrgupoõhiseid lahendusi, CERT-EE-d teavitama ei pea.

Kontakteerumine ja teabe edastamine CERT-EE-le on infoturbejuhi, IT juhi voõi infoturbe eest vastutava inimese kohustus.

HG.41 Windows Server 2003 laiendatud turvaaspektid

M 4.279 Windows Server 2003 laiendatud turvaaspektid parametriseering

Windows Server 2003 laiendatud turvaaspektide loetelus kirjeldatud soovituslikud meetmed on siin kõik kohustuslikuks rakendamiseks. Lisaks tuleks tähelepanu pöörata järgmistele nüanssidele:

- installeerimise faasis peab Windows olema võrgust eraldatud või paiknema kõrgema kaitstus kategooriaga võrgus;
- kõik kasutamata ja põhjendamata teenused tuleb välja lülitada;
- mittevajalikud välisliidesed tuleb deaktiveerida (nt BIOS'i ja Windows'i *device manager*) ning teisaldatavad andmekandjad tuleb eemaldada või lukustada instalatsiooni järgselt;
- standardsed volitused süsteemikataloogidele ja süsteemiobjektidele on niigi piiravad, kuid kõrge turbeastme korral tuleb neid veelgi karmistada - selleks eemaldatakse standardgruppide volitused ja omistatakse volitused igale kasutajale eraldi.

HG.42 Nõuded traadita kohtvõrgu migratsioonietappide planeerimisele

M 2.386 Traadita kohtvõrgu migratsioonietappide hoolikas planeerimine parametriseering

Ülaltoodud meetmes välja toodud soovituslikud meetmed on käesoleval juhul kõik kohustuslikuks täitmiseks. Eriti hoolikalt tuleb jälgida turvaseadeid, nt seda, et igal pool kasutataks WEPi asemel WPA2.

Lisaks tuleb tõsiselt kaaluda, kas kõrge turbeastme korral on WiFi kasutamine üldse õigustatud, st kas sellest tulenevad riskid ei kaalu üles siit saadavaid eeliseid. Võimaluse korral (st riskide maandatuse ebakindluse korral) tuleks kõrge turbeastme korral alati eelistada traditsioonilisi traadiga võrke. Nimetatud riskide kaalumine ja WiFi lubamise/mittelubamise otsuse tegemine on turvajuhi pädevuses.

HG.43 Lisanõuded traadita kohtvõrgu tööde väljasttellimisele

M 2.387 Kolmandate osapoolte kasutamine traadita kohtvõrgu paigaldamisel, konfigureerimisel ja nõustamisel parametriseering

Ülaltoodud meetmes välja toodud soovituslikud meetmed on käesoleval juhul kõik kohustuslikuks täitmiseks. Lisaks tuleb lähtuda veel järgnevatest nõuetest, mis ülaltoodud meetmes pole piisava konkreetsusega välja toodud:

- Turvasuunised ja -strateegia koostamine on tellija (tellija turvajuhi) ülesanne, mida ei tohi mingil juhul jätta töö tegija rolliks. See tuleb fikseerida kirjalikult ja selle peab ka töö tegija kinnitama.
- Tellija peab töö tegemise ajal tehtavat – eriti turvaomadusi – pidevalt jälgima. See on tellija turvajuhi kohustus (mille ta võib edasi delegeerida, aga mitte töö tegijale või tööd teostava asutuse töötajatele).
- Tellija kohuseks on hoolitseda, et väljasttellitava töö lõppedes likvideeritakse kõik töö tegijale antud ajutised pääsud, muudetaks vastavad paroolid jms. Vt ka HT.57 Algparoolide muutmise regulaarkontroll nõuded.

HG.44 Avalike pääsupunktide turvaline opereerimine ja kasutus

M 4.293 Avalike pääsupunktide turvaline käitamine parametriseering

Ülaltoodud meetmes välja toodud soovituslikud meetmed on käesoleval juhul kõik kohustuslikuks täitmiseks. Turvalise autentimise praktilisel korraldamisel tuleks lisaks juhinduda HT.59 Lisanõuded turvalisele sisselogimisele nõuetest.

HG.46 SAP rakenduslüüside kasutamine

Unikaalmeede

Kõrge turbeastme korral tuleks kasutada välisvõrkudest SAP süsteemidele ligipääsuks rakenduslüüse. SAP rakenduslüüside näideteks on SAP Router ja SAP Web dispatcher. Esimest neist kasutatakse dialoog ning RFC ühenduste jaoks, teist aga HTTP(S) ühenduste jaoks.

SAP Router võimaldab:

- filtreerida sissetulevaid pöördumisi IP aadressi ja protokolli baasil;
- nõuda parooli saatmist pöördumiste puhul;
- nõuda turvalist autentimist ja krüpteerimist võrgukihis.

Kasutades SAP Router'it tuleb avada välisvõrgust SAP protokollide jaoks vaid üks rakenduslüüsi kommunikatsiooniport, mis vastab SAP Router 'is konfigureeritud pordile. Sellisel juhul peavad kõik sissetulevad ühendused kasutama seda sihtporti (vaikimisi 3299). Tuleb arvestada, et SAP Router täiendab, kuid ei asenda turvalüüsi. SAP Router üksi ei ole piisavalt turvaline kõrge turbeastme jaoks, seega tuleb seda kasutada alati koos turvalüüsiga.

SAP Web dispatcher'it saab kasutada koormuse jagamiseks ja HTTP või HTTPS protokollil põhinevate pöördumiste filtreerimiseks. Filtreerimise reeglid on määratud konfiguratsioonifailis, mis asub SAP Web dispatcher arvutis. SAP Web dispatcher toetab transpordikihi turvalisust SSL protokolli kaudu.

Eriti kõrge turbevajaduse korral tuleks rakenduslüüside ja SAP Web Application Serveri kaasabil koostada sisemise ja välimise DMZ-ga võrgutopoloogia. Sellisel juhul asub SAP Router või SAP Web dispatcher välimises DMZ-is ja *SAP Web Application Server* sisemises DMZ-is. Kõrgete turvanõuetega SAP rakendusserverid, sisemine DMZ, välimine DMZ ja välisvõrk on omavahel eraldatud turvalüüsidega.

HG.48 Võrdõigusteenuse keeld IP-kõne puhul

Unikaalmeede

Erinevad võrdõigusteenuse *(peer-to-peer* , p2p) programmid (*skype, google-talk*) võimaldavad kasutada IP-kõne teenust üle avaliku võrgu (Interneti). Asutustes kiputakse neid programme kasutama ka kiirsõnumivahetuse eesmärgil. Üha enam kasutatakse neid programme ka IP-kõne jaoks, seda eriti kaugkõnede puhul. Kui sidekanalina kasutatakse Interneti eri harusid p2p tehnika põhjal, kus erinevad liinid on erinevate asutuste ja instantside hallata, on väga raske tagada kindlat sidekvaliteeti, st käideldavust ja terviklust.

Mis puudutab konfidentsiaalsust, siis sageli kasutavad need IP-kõne ja kiirsõnumi programmid firmakohaseid protokolle, mille krüpteerimisalgoritmid ei ole avalikud ja seetõttu ei saa selles veenduda (st seda ei ole võimalik objektiivselt hinnata). Lisaks sellele võimaldab selline tarkvara sageli tekitada tunneli Internetti, mis võimaldab minna mööda asutuse turvalüüsidest ja teistest turvameetmetest.

Sellest tulenevalt tuleb sellise tarkvara installeerimine ja kasutamine keelata organisatsiooniliste ning blokeerida tehniliste turvameetmetega. Interneti võrdõigusteenuse tarkvara keelustamine tuleb sätestada organisatsiooni turvapoliitikas. Tehniliselt saab neid IP-kõne programme blokeerida vastava turvalüüsi konfiguratsiooniga. Vahel on selliste IP-kõne programmide blokeerimine seotud raskustega, kuna nende programmide poolt kasutatavad protokollid on koostatud turvalüüside läbimise eesmärgiga, st ei ole muudest protokollidest tihti selgelt eristatavad.

HG.49 IP-kõne protokollistiku funktsionaaltestimine

Unikaalmeede

Selleks, et veenduda IP-kõne protokollistiku turvalises konfiguratsioonis tuleb seda regulaarselt testida funktsionaalsete protokolli testeritega (*fuzzing tools*). Funktsionaalne protokollistiku testimine *(fuzzing, black-box-testing)* aitab leida vigu ja haavatavusi protokollistiku rakenduses. Häkkerite poolt kasutatakse samu tööriistu teenustõkestusrünnete ja puhvri ületäitumise rünnete sooritamiseks. Funktsionaalse testimise käigus genereeritakse ja saadetakse suurel hulgal erinevat tüüpi pakette, mis võivad põhjustada protokollistiku murdumise. Need paketid saadetakse rakendustele, operatsioonisüsteemidele, või ka riistvaralisele seadmele *(appliance, hardphone*) mis töötlevad kõne all olevat protokolli. Jälgitakse võimalikku seadme ebanormaalset käitumist (kinni jooksmine, ebatavaline ressursikulu jne).

Funktsionaalsete testimiste käigus on avastatud erinevate tootjate seadmetel erinevaid haavatavusi. Enamasti püüavad tootjad vigu parandada turvapaikadega.

Üheks võimalikuks IP-kõne protokollide funktsionaalse testimise tööriistaks on Oulu ülikooli poolt arendatud PROTOS testimiskeskkond, mis võimaldab nii H.323, kui ka SIP protokollistiku testimist. Tester on saadaval Oulu Ülikooli kodulehelt tasuta ja seda saab ka kohandada, et sooritada spetsiifilisemaid teste vastavalt asutuse vajadustele ja IP-kõne installatsiooni eripärale. Testimisel tuleks jälgida järgmisi asjaolusid:

- Tuleks testida kõiki seadmeid, mis saadavad, võtavad vastu või loevad IP-kõne protokolle: riistvaralisi telefone, tarkvaralisi telefone, SIP proxysid, H.323 lüüse, kõnekeskusi (*call manager*) ja turvalüüse, mis on IP-kõne pakettide teel.
- Haavatavuste avastamisel tuleb otsida ja installeerida turvapaigad, nende puudumisel teatada probleemist tootjale.
- Testimist tuleb korrata, et veenduda turvapaikade eesmärgipärasuses ja selles, et turvapaigad ei toonud kaasa uusi haavatavusi. Samuti tuleb testimist korrata peale versiooniuuenduste ja värskenduste installeerimist.
- Suure IP-kõne investeeringu puhul tuleks jälgida, et osa investeeringust oleks suunatud testimiskeskkonna arendusse.
- IP-kõne funktsionaalsed testid tuleks lülitada asutuse koormustestide kavasse, mida sooritatakse auditite käigus.

HG.50 Virtuaalsed salvestivõrgud ja pordipõhine tsoneerimine

M 5.130 Salvestisvõrgu (SAN-i) kaitse segmenteerimise abil parametriseering

Salvestivõrkudes on võimalik piirata volitamata ligipääsu transporditavatele andmetele võrgu segmenteerimise teel. Lisaks ülaltoodud meetme nõuetele tuleb arvestada, et *Fibre Channel* tehnoloogial põhinevaid salvestivõrke on võimalik tsoneerida põhiliselt kolmel erineval viisil:

- Tarkvaraline tsoneerimine (*soft-zoning*). Filtreerimine *Fibre Channel* kommutaatorites *World Wide Name* (WWN) alusel. Meetodi nõrkuseks on asjaolu, et juhul, kui ründaja suudab ära arvata *Fibre Channel* aadressi, on siiski võimalik tsooni piiridest üle hüpata. Põhimõtteliselt on tarkvaralise tsoneerimise eeliseks lihtne võrgustruktuuri muutmise võimalus ja puuduseks (lisaks meetodi haavatavusele) on see, et võrguadapteri (HBA) vahetamisel tuleb *Fibre Channel* kommutaator ümber konfigureerida.
- Riistvaraline ehk pordipõhine tsoneerimine (*hard-zoning, port zoning*). *Fibre Channel* kommutaatori liidesed jagatakse erinevatesse tsoonidesse pordipõhiselt. Pordipõhine tsoneerimine teeb võrgustruktuuri muudatused keerukamaks, kuna iga struktuuri muudatuse käigus tuleb *Fibre Channel* kommutaator ümber konfigureerida. Samas on riistvaraline tsoneerimine turvalisem, kuna füüsilisi pordinumbreid ei ole võimalik loogiliselt petta.
- LUN (*Logical Unit Number*) maskeerimine on võrguadapteri baasil teostatud meetod, mis teeb LUNi nähtavaks ainult teatud masinatele. LUN maskeerimise nõrkuseks on võrguadapteri suhteliselt lihtne manipuleerimise võimalus.
- Kõrge turbeastme korral tuleb kasutada pordipõhist tsoneerimist. Tsoonid tuleb plaanida nii väikesed, kui võimalik vastavalt kommunikatsioonimaatriksile.
- Kui kommutaatorid seda võimaldavad, tuleks suuremate võrkude puhul rakendada ka virtuaalsete salvestivõrkude tehnoloogial (VSAN) põhinevat segmenteerimist. VSAN võib hõlmata mitut kommutaatorit ning vastupidiselt iga kommutaator võib kuuluda ka mitmesse VSAN-i.
- Nii tarkvaralise, kui ka pordipõhise tsoneerimise korral kuuluvad erinevad *Fibre Channel* tsoonid ühte turvadomeeni (ehk turvatsooni). VSAN võimaldab erinevate turvadomeenide (ehk turvatsoonide) formeerimist, mida võib siis omakorda jagada pordipõhiselt *Fibre Channel* tsoonideks.

HG.51 Traadita kohtvõrgu IP-adresseerimine

Unikaalmeede

Reeglina on traadita kohtvõrkudes võrguprotokollina kasutusel IP-protokoll. Kõrge turbeastme korral tuleks IP protokollistiku konfigureerimisel rakendada mõningaid turvameetmeid, millest igaüks eraldi ei ole kuigi efektiivne, kuid mida tuleks käsitleda lisaturvameetmetena.

- Tuleks kasutada staatilist IP-adresseeringut. See võimaldab paremini seirata traadita kohtvõrkude autoriseeritud seadmete tegevust. Staatilised IP-aadressid võimaldavad ka võrguadministraatoritel paremini konfigureerida turvalüüsi pääsuks kaabeldatud võrku. Lisaks sellele on paljud ründetuvastussüsteemid tõhusamad staatilise IP-adresseeringuga võrkudes. Kõrge turbeastmega võrgus tuleks aktiveerida ainult hädavajalikud teenused – staatilise IP-adresseeringu kasutamisel tuleb DHCP protokoll välja lülitada.
- Traadita kohtvõrgu kliendiseadmetes ja pääsupunktides tuleks kasutada staatilisi ARP (*Address Resolution Protocol*) kirjeid. ARP on võrguprotokoll, mis võimaldab seadmetel leida MAC aadressi, teades IP aadressi. ARP kirjeid hoitakse vahemälus kuni nad aeguvad või kirjutatakse üle. Dünaamiline ARP protokoll on haavatav *ARP poisoning* ründega, mille käigus ründaja üritab illegaalsete ARP vastuspakettidega muuta dünaamilisi ARP kirjeid, eesmärgiga suunata teatud IP aadressile saadetud paketid enda MAC aadressile. Staatilised ARP kirjed välistavad seda tüüpi ründe võimaluse. Staatiline ARP konfigureerimine on küll töömahukam, kuid kuna kliendilt-kliendile kommunikatsioon peaks olema traadita kohtvõrgus nagunii keelatud, ei ole ARP kirjete arv seadmetes väga suur.
- Traadita kohtvõrgus tuleks kasutada privaatseid IP-aadresse. Privaatsete IP- aadresside kasutamine tagab teatud anonüümsuse juhul, kui ründajal õnnestub tuvastada kasutatav IP-aadressruum. Privaatsete IP-aadresside kasutamine tagab ka võrkude eraldatuse nii sisse kui ka väljapoole.
- Alati tuleb tagada, et *ARP broadcast* ei leviks kaabeldatud kohtvõrgust traadita kohtvõrku, kuna võimaliku ründe korral võib see paljastada sisevõrgu MAC aadresse.

HG.52 Traadita ründetuvastus- ja -tõkestussüsteemid

Unikaalmeede

Viimasel ajal on lisaks tavalistele kohtvõrkude ründetuvastussüsteemidele turule jõudnud ka traadita kohtvõrkude ründetuvastussüsteemid (*Wireless Intrusion Detection Systems*, WIDS). Need seadmed kasutavad anduritena kas eraldiseisvaid raadioandureid või kasutavad traadita kohtvõrkude pääsupunkte selleks, et spektrit seirata ja anomaaliaid avastada (nt võõraid pääsupunkte ja kliente). Kõrge turbeastme korral tuleb sellised ründetuvastussüsteemid võrguseireks töösse rakendada.

Traadita ründetuvastussüsteemide rakendamine algab hoolikast plaanimisest, mille käigus määratakse andurite asukoht ja arv. Kui anduritena kasutatakse võrgu pääsupunkte, tuleb arvestada, et see võib mõjuda negatiivselt võrgu läbilaskevõimele. Edasise plaanimise käigus tuleb määrata logimise regulatsioonid, intsidentide definitsioonid ja tegutsemine turvaintsidentide korral.

Selleks, et traadita kohtvõrgu ründetuvastussüsteeme soodsamalt soetada, võib juba traadita kohtvõrgu seadmete valimisel üheks kriteeriumiks seada nende koostöövõime traadita kohtvõrgu ründetuvastussüsteemidega.

HG.53 Avalike pääsupunktide kasutamise piiramine

Unikaalmeede

Soovitavalt tuleks kõrge turbeastme korral keelata avalike pääsupunktide kasutamine. Kui see ei osutu võimalikuks, tuleks seada avalike pääsupunktide kasutamisele järgmised regulatsioonid:

- Kasutada tohib vaid usaldusväärseid operaatoreid, kes suudavad garanteerida andmete turvalisuse ja andmekaitse nõuetest kinnipidamise.
- Ühendus on lubatud vaid VPN-tunneli kaudu.
- Kliendiarvutile peab olema installeeritud personaalne turvalüüs mis tuleb konfigureerida piirangutega – st seest välja tohib lubada vaid teatud pordid
- Vahetatavate andmekandjate kasutamine tuleb keelata või piirata.
- Kombineeritud autentimise kasutamine (vt HT.59 Lisanõuded turvalisele sisselogimisele)

HG.54 Regulaarse turvaauditi kohustus

Unikaalmeede

Süsteemi väline turvaaudit tuleb läbi viia iga kahe aasta tagant. Esmane audit peab toimuma maksimaalselt kuus kuud pärast süsteemi reaalset käivitumist.

Turvaaudit peab vastama ISKE määrusele ning ISKE auditi juhendile – nende mõlema viimased, toimivad versioonid asuvad RIA veebilehel https://www.ria.ee/et/kuberturvalisus/infosusteemide-turvameetmete-susteem-iske.html). Audit tuleb läbi viia tervikuna kogu infosüsteemis (kui kasutatakse turvatsoneerimist, siis vastava turbetasemega alamsüsteemis).

Kui süsteemis on toimunud ohtlik turvaintsident, võib vastutav töötleja (vastutava töötleja turvajuht kooskõlastatult juhtkonnaga) nõuda erakorralist turvaauditit.

HG.55 Esemete tõstetud hoidmine serveri- ja arhiiviruumides

Unikaalmeede

Kõik seadmed, andmekandjad ja arhivaalid, samuti kõik toite- ja andmesidevõrkude osad ning komponendid tuleb serveri- ja arhiiviruumides hoida vähemalt 50 cm kõrgusel põrandast riiulitel, kappidel, seinale kinnitatuna või muudel tarinditel.

Nõue on vajalik ootamatu uputuse korral, mis võib seadmeid ja esemeid rikkuda. Lähemal kui 50 cm põrandast on lubatud hoida vaid mööbli, kinnitustarindite, hoonekonstruktsioonide jms osi ning selliseid detaile, mis vett ei karda. Erandina on lubatud allpool eelnimetatud 50 cm piiri hoida ka kaableid, juhtumeil kui kõik harundseadmed ja ühenduskohad (sh ka parandatud kohad) asuvad ülalpool 50 cm piiri.

Nõue ei kehti juhtumeil, kui ruumides on kasutatud spetsiaalseid tõstetud põrandaid (*raised floor*), mis tavaliselt lasevad uputusvee endast läbi. Samuti ei kehti nõue nendes andmearhiivides, kus arhivaalid asuvad veekindlas (vastava sertifikaadiga) seifis, mis vastab IP67 veekindlusnõuetele (vastavalt IEC 60529:2001 sätestatule).

HG.56 Lisanõuded muudatuste haldusele

M 2.221 Muudatuste haldus parameetrite seadmine

Lisaks muudatuse halduse nõuetele tuleb kindlaks määrata, millist laadi muudatused vajavad turvajuhi poolset aktsepteeringut ja millist laadi muudatused mitte. See üldpõhimõte tuleks kokku leppida IT korralduskomitee ja turvajuhi poolt ning sätestada põhilistes selle valdkonna raamdokumentides (muudatuste üldpõhimõtted, turvapoliitika jt).

Vt ka HT.23 Muudatuste eelnev turvajuhi poolne kinnitamine .

HG.57 Muudatuste haldusinstrumentide pääsuõiguste määramine

M 2.424 Paikade ja muudatuste haldamise tööriistade turvapoliitika parameetrite seadmine

Lisaks paikade ja muudatuste haldamise tööriistade turvapoliitika nõuetele peab muudatuste ja turvapaikade haldusinstrumentide pääsud kinnitama turvajuht.

Tehniliselt võib nende pääsude reguleerimist teostada kas turvajuht või tema poolt määratud isik, kuid siin tuleb lähtuda rollide lahususe printsiibist - see isik, kel on pääsuõiguste muutmise õigus, ei tohi üldjuhul ise tegeleda muudatuste ja turvapaikade registreerimisega selles instrumendis.

Väga väikeses asutuses võib viimasest (rollide lahususe) pritsiibist turvajuhi eriloal loobuda, kuid siis tuleb seda käsitleda erandina (vt M 2.380 Erandite kooskõlastamine).

HG.58 Lisanõuded turvakoolitusele

M 3.5 Turvameetmete koolitus parameetrite seadmine

Lisaks turvameetmete koolitusele sätestatud soovituslikele meetmetele tuleb lisaks juhinduda alljärgnevast:

- Turbe baasteadmiste (nii üldisi kui infosüsteemi/inimese spetsiifikat puudutavaid) alal tuleb töötajaid koolitada iga kahe aasta tagant. Inimeste korral, keda on varem sel teemal koolitatud, tuleb lisakoolitamisel põhitähelepanu suunata viimase kahe aasta tehnoloogilistele jm uuendustele. Koolituse korraldab (või viib isiklikult läbi) turvajuht.
- Kriitiliste alade töötajaid tuleb soovitavalt saata kord-kaks aastas majavälisele turvakoolitusele.
- Asutuse (kriitiliste valdkonna töötajate) üldkoosolekul peab turvajuht vähemalt neli korda aastas kajastama piiratud mahus aktuaalseid turvateemasid.

Vt ka M 3.45 IT-turbealaste koolituste sisu kavandamine .

HG.59 Sagedasem turvameetmete läbivaatus

M 2.182 IT-turvameetmete regulaarne läbivaatus parameetrite seadmine

Lisaks IT-turvameetmete regulaarse läbivaatuse nõuetele tuleb seda teha pideva pistelise protsessina arvestusega, et kõik turvameetmed saaksid vähemalt kaks korda aastas üle vaadatud. Kui mõne komponendi/meetme sedavõrd sage testimine ei osutu mõjuvatel põhjustel võimalikuks, tuleb see lahendada turvajuhi poolt spetsiaalselt kinnitatud eranditega (vt M 2.380 Erandite kooskõlastamine).

HG.60 Lisanõuded automaatsete uuendusmehhanismide konfigureerimisele

M 4.342 Last Access ajatempli aktiveerimine parameetrite seadmine

Ülalmainitud meetmes mainitud automaatsete uuendusmehhanismide seadete muutmine tuleb kooskõlastada turvajuhiga, juhul kui nimetatud muudatused kuuluvad meetmes HG.56 Lisanõuded muudatuste haldusele kirjeldatuna selliste meetmete hulka, mis vajavad turvajuhi kinnitust.

HG.61 Nõuded kodutööarvutile

Unikaalmeede

Kodutöökohas kasutatav arvuti peab vastama järgmistele tingimustele:

- arvuti peab olema varustatud (BIOS-i) paroolkaitsega ja/või ketta krüpteerimisega, mis välistab ta kasutamise võõraste poolt;
- arvuti igapäevakasutus ei tohi toimuda süsteemihalduri õigustes, vaid piiratud kasutaja õigustes;
- soovitavalt võiksid ka kodutööarvutid olla asutuse ühtse administreerimise all, kui see on võimalik.

HG.62 Lisanõuded nõupidamisruumide võrguühendusele

M 5.124 Võrgupääsu korraldus nõupidamis-, ürituse- ja koolitusruumides parameetrite seadmine

Kui üht ja sama nõupidamisruumi kasutatakse nii sisemisteks üritusteks kui ka väljastpoolt oma asutust pärinevaid inimesi hõlmavateks üritusteks, siis on mõistlik luua ruumis kaks eraldiseisvat traadita võrku – üks sisemiste ürituste, teine avatud ürituste tarbeks.

HG.63 Lisanõuded võrguteenuste inventuurile

M 5.16 Võrguteenuste inventuur parametriseering

Lisaks võrguteenuste inventuurile kehtestatud nõuetele tuleb võrguteenuste inventuur ja sellega seotud turvakontroll viia läbi pisteliselt vähemalt neli korda aastas. Seda peab läbi viima turvajuht või tema määratud isik, vajadusel tuleb protsessi kaasata süsteemiadministraatoreid.

HG.64 Lisanõuded kaabelduse dokumenteerimisele ja märgistusele

M 5.4 Kaabelduse dokumenteerimine ja märgistus parametriseering

Lisaks kaabelduse dokumenteerimise ja märgistuse nõuetele tuleb lähtuda alljärgnevast:

- Kõik muudatused kaabelduses ja/või jaotusseadmetes peavad olema dokumenteeritud tööpäeva lõpuks; puhkepäevadel ja pühadel 24 tunni jooksul.
- Kui asutuses on kasutatud ruumide tsoneerimist selliselt, et leidub nii kõrgkonfidentsiaalsusnõuetele (turvaosaklassiga S3) vastavaid ruume kui ka madalamate konfidentsiaalsusnõuetega tsoone, tuleb kõrgkonfidentsiaalsusnõuetega tsoonide kaabelduse skeemid koostada ja hoida ülejäänud tsoonide kaabelduse skeemidest eraldi.

HG.65 Mitmekordse nurjunud logimise automaatteavitus

M 6.67 Turvaintsidentide avastamismeetmete rakendamine parameetrite seadmine

Lisaks turvaintsidentide avastamismeetmete rakendamise nõuetele peab mitmekordne nurjunud logimiskatse käivitama automaatteavituse, mis peab vastama HG.3 Tõrgete kaugindikatsiooni vastuvõtmiskohustus ja HG.22 Ööpäevaringne intsidentidest teatamise võimalus nõuetele. Kaugindikatsioon peab soovitavalt rakenduma kolmandal nurjunud logimiskatsel, kohustuslik on selle rakendumine viiendal nurjunud logimiskatsel.

HG.66 Tulekustutite nõue serveri- ja arhiiviruumides

M 1.7 Tulekustutid parametriseering

Lisaks tulekustutile kehtestatud nõuetes kirjeldatule peab tulekustuti asuma igas arhiivi- ja serveriruumis. Nõue kehtib ka siis, kui üldtsooni tulekustuti asub nimetatud ruumide ukse taga selle vahetus läheduses.

HG.67 Veetorude keeld serveri- ja arhiiviruumides

M 1.24 Veetorude vältimine IT-ruumis parametriseering

Lisaks veetorude vältimise nõuetele IT-ruumis on veetorude (sh reoveetorude) paiknemine arhiivi- ja/või serveriruumides keelatud.

Juhul kui seda nõuet ei ole võimalik täita, tuleb:

- torud ekraneerida veekindla ekraaniga alates laest kuni 40 sentimeetri kõrguseni põrandast, selleks et vältida toru lekkimahakkamisel või purunemisel vee sattumist ruumis asuvatele esemetele ja/või seadmetele;
- põrandapinnale paigutada niiskusandur, mis rakendumise korral teavitab süsteemiadministraatorit kaugindikatsiooni teel (vt HG.3 Tõrgete kaugindikatsiooni vastuvõtmiskohustus);
- käsitleda juhtumit erandina, mida reguleerib meede M 2.380 Erandite kooskõlastamine .
- Lisaks veetorudele kehtib keeld ka igasuguste muude vedelike jaoks mõeldud torude osas (õli, kütus, gaas, freoon või muu kliimaseadmete külmakandevedelik jms) ja nendel juhtumitel ilma igasuguste eranditeta.

HG.68 Valvesignalisatsiooni kohustus

M 1.44 Kodutöökoha sobiv konfiguratsioon parametriseering

Lisaks kodutöökoha sobiva konfiguratsiooni nõuetele peab kodutöökohas olema valvesignalisatsioon, mille alarmid peavad jõudma turvafirmasse, kellega on sõlmitud kirjalik valveleping.

Nõudest võib loobuda, kui kodutöökohta käsitletakse mobiilse töökoha funktsionaalsuses (vt B 2.10 Mobiilne töökoht), kuid sel juhul lisanduvad arvutile mitmed rangemad nõudmised (peamiselt HT.56 Lisanõuded mobiilsele kaugtööarvutile).

HG.69 Ruumide turvatsoneerimise korraldamine

Unikaalmeede

Sagedasti on asutuse tööruumidest vaid osa seotud infosüsteemiga. Samuti on tüüpiline selline olukord, kus ruumid on jaotatud tsoonideks, milledele rakenduvad ISKE kohaselt erinevad turvaklassid.

Kõikidel niisugustel juhtumitel tuleb lähtuda alljärgnevast:

- Tsoneerimine tuleb viia läbi mõistlikult, st tsoonidevaheliste pääsude hulka minimeerides, enam kaitset vajavaid tsoone sissepääsust ja külaliste tsoonidest kaugemale paigutades jms. Tsoneerimise juures peab kindlasti osalema turvajuht, kes peab tulemuse ka kirjalikult kinnitama.
- Kõik tsoonidevahelised pääsud peavad sisaldama autentimist. Vastavalt olukorrale ja vajadustele võib autentimisvahendiks olla magenetkaartlukk, kiipkaartlukk, RFID-kaardiga lukk, tavaline võtmega lukk, valvuriga pääsla vms.
- Lubamatu on jätta tsoonidevahelisi pääsusid lahti ilma inimvalveta ka lühikeseks ajaks ning remontide ja ümberkorralduste ajaks. Kui see on siiski hädavajalik, peab tsoonide taasloomisel kõik muutunu turvajuht spetsiaalselt üle kontrollima.

HG.70 Piiratud õigustega personaalne kasutajakonto

M 2.63 Pääsuvolituste kehtestamine parametriseering

Kõikides arvutites, mida kasutatakse lõppkasutaja töökohana (kliendina), tuleb lisaks pääsuvolituste kehtestamise nõuetele luua igale kasutajale personaalne kasutajakonto, mis võimaldab süsteemil tuvastada, kes parajasti arvutiga töötab. Nimetatud kasutajakonto (või kasutajakontod) peavad omama piiratud õigusi, sh tarkvara installeerimine ja konfiguratsiooni muutmine nende alt peab olema keelatud. Ühe piiratud õigustega kasutajakonto alt ei tohi saada ligi teise piiratud õigustega kasutajakonto andmetele ega konfiguratsioonile.

Süsteemiadministraatori õigusi omava kasutajakonto alt ei tohi teha igapäevatööd, vaid üksnes tarkvara installeerimist ja konfiguratsiooni muutumisi.

Vahel on vaja eeltoodud nõuetest teha erandeid, mille peamisteks põhjusteks on:

- lõppkasutaja tarkvara vajab kasutamiseks administraatori õigusi;
- opsüsteem või arvuti konfiguratsioon ei võimalda piiratud õigustega kasutajakontode loomist või nende eraldamist üksteisest.

Neid juhtumeid tuleb vaadelda eranditena, mida võib teha turvajuhi eriloal ja vastavalt meetmes M 2.380 Erandite kooskõlastamine kirjeldatule.

HG.71 Lisanõuded mobiiltelefoni/pihuarvuti soetusele ja käitlusele

M 2.188 Mobiiltelefonide kasutamise eeskirjad ja turvasuunised ja M 2.304 Pihuarvutite turvapoliitika ja kasutamise reeglid parametriseering

Lisaks pihuarvutite turvapoliitika ja kasutamise nõuetele on vajalik rakendada lisanõudeid ka mobiiltelefonide ning pihuarvutite (edaspidi – PDAde) soetusele ja käitlusele. Põhjuseks on asjaolu, et pruugituna või kahtlasest allikast ostetud mobiiltelefon või PDA võib endas sisaldada dokumenteerimata omadusi, mis halvimal juhul võivad olla troojalased, mis on suutelised salvestama/edastama kõnesid/paroole, tungima PDA poolt kasutatavatesse arvutivõrkudesse, tegema seal kasutaja teadmata mitmeid tegevusi jne.

Üldjuhul tuleb kõrgastmel turvet sisaldavate andmete töötlemisel kasutatav mobiiltelefon või PDA osta uuena sellelt edasimüüjalt või esinduselt, mille asutuse turvajuht on aktsepteerinud. Sama kehtib mobiiltelefoni või PDA remondi, hoolduse või tarkvarauuenduse korral, mis peab toimuma samuti asutuse turvajuhi poolt aktsepteeritud kohtades.

Mobiiltelefoni või PDA korral on keelatud:

nende soetamine pruugituna tundmatust allikast;

- kasvõi lühiajaline üleandmine teisele isikule, kui see pole asutuse töökorralduse kooskõlas või selleks pole turvajuhi eriluba;
- nende jätmine järelevalveta üldkasutatavasse kohta kasvõi lühimakski ajaks (üleriiete taskusse garderoobi, koju lukustamata tuppa lauanurgale vms).

Asutuse konkreetsed, ärivajaduste eripära arvestavad nõuded kõrgastmel turbega andmete töötluseks kasutatavate mobiiltelefonide ja/või PDAde soetuse ja käitluse kohta tuleb lisada nende kasutamise korrale/kordadele või luua selleks eraldi kord (vt M 2.188 Mobiiltelefonide kasutamise eeskirjad ja turvasuunised , M 2.190 Mobiilikogu sisseseadmine , M 2.303 Pihuarvutite kasutamise strateegia määramine ja M 2.304 Pihuarvutite turvapoliitika ja kasutamise reeglid), mille korraldamise eest vastutab asutuse turvajuht. Vt ka HG.35 Pihuarvutite kasutuse regulaarseire .

HG.72 Lisanõuded lepingutele SAN teenusepakkujatega

M 2.356 Lepingud SAN teenusepakkujatega parametriseering

Lisaks SAN teenusepakkujatega sõlmitavatele nõuetele sätestatule peavad lepingutes sisalduma niisugused leppetrahvid, mis vastavad SAN süsteemiga haldavate andmete turvariskidele (peamiselt käideldavus- ja konfidentsiaalsuskaoriskidele), mis on hinnatud nii tellija kui andmete haldaja poolt.

HG.73 Võrgu aktiivkomponentide turvalise paigutuse regulaarseire

Unikaalmeede

Meetmes M 1.43 Võrgu aktiivkomponentide turvaline paigutus kirjeldatud turvalise paigutuse tingimuste täidetust tuleb pisteliselt kontrollida kõikide aktiivkomponentide (marsruuterid, kommutaatorid jms) korral vähemalt kaks korda aastas. Selline kontroll on turvajuhi kohustuseks.

Meede kehtib ka tulemüüride jm turvalüüside korral, kus tuleb juhinduda lisaks meetmetest M 2.70 Turvalüüsi (tulemüüri) kontseptsiooni väljatöötamine ja M 2.71 Turvalüüsi (tulemüüri) turvapoliitika . Kaasajal on piir marsruuterite ja tulemüüride ja muude turvalüüside vahel seoses multifunktsionaalsete seadmete ilmumisega hägustunud.

HG.74 Modemi kaudu sooritatava kaughoolduse keeld

M 5.33 Kaughoolduse turve parametriseering

Kõrgastme (H) turbe korral ei tohi üldjuhul modemi kaudu seadmete kaughooldust teha. Põhjuseks on asjaolu, et modemi kaudu sissehelistamisel ei pruugi (seadme poolelt) olla tagatud turvaline autentimine, mida standardsete VPN- ja muude TLS-(SSL-)tehnikatega sinna lisada on ülikeeruline võrreldes kaugpääsuga üle üldkasutatava interneti (TCP/IP võrgu). Lisaks on modemi kaudu kaughooldus arhailine, mida kaasaja seadmed reeglina ei kasuta.

Äärmisel erijuhul võib siin teha erandi turvajuhi kirjalikul loal vastavalt erandeid sätestava meetme M 2.380 Erandite kooskõlastamine tingimustele.

HG.75 Lisanõuded SAP-süsteemi väljasttellimisele

M 2.345 SAP süsteemi väljasttellimine parametriseering

Lisaks SAP süsteemi väljasttellimise nõuetele peab SAP-süsteemi väljasttellimisel arvestama järgmisi aspekte:

- Töö tegijal olema pikaajaline praktiline kogemus ISKE kõrget turbeastet (H) omavate infosüsteemide arendamisega.
- Kuna reeglina saab tegija SAPi andmete üle täieliku kontrolli, tuleb temaga enne tööde teostamist koostada selline konfidentsiaalsuskohustuse leping, milles sisalduvad leppetrahvid vastavad SAPiga haldavate andmete turvariskidele (peamiselt käideldavus- ja konfidentsiaalsuskaoriskidele)

HG.76 Traadita kohtvõrgu nimevalikunõuded

M 2.381 Traadita kohtvõrgu kasutamise strateegia väljatöötamine parametriseering

Traadita kohtvõrgu nimi peab kõrgastmega (H) turvet omavates süsteemides olema neutraalne (nt Juku, Mari, Vork16 vms), ta ei tohi mingil kujul viidata ei firma ega ka teenuse nimele, et võrgu levialas olija ei saaks seda kindla asutuse/instantsiga seostada. Vt ka HG.62 Lisanõuded nõupidamisruumide võrguühendusele .

HG.77 Traadita kohtvõrgu nimevalikunõuded

Lisake tavapäraste penetratsioonitestidele (vt M 5.150 Penetratsioonitestide läbiviimine) tuleb läbi viia ka turvatestid, mis puudutavad ID-kaardi/PKI lahenduste kõiki eriomadusi. Testid peavad kindlasti hõlmama järgmisi valdkondi:

- Soovitavalt tuleks PIN-kood sisestada pin-pad 'i abil – vt HG.80zPin-pad'i kasutamine "Pin-pad' i kasutamine".
- PIN- ja PUK-koodide käitlemise korral tuleb veenduda, et vahetult peale seda, kui PIN- või PUK-kood on edastatud pöördkonstrueerimatusse seadmesse, ta mälust, ketastelt vm paikadest kustutatakse, kusjuures kustutamine peab toimuma turvameetme M 2.13 Tundlike ressursside jäljetu hävitamine nõudeid arvestades. Digiallkirjastamist võimaldavate lahenduste korral tuleb testida kõiki allkirja andmise võimalusi – mitu allkirja ühel dokumendil, erinevate vahenditega (ID-kaart, mobiil-ID vms) antud allkirjade andmise võimalus samale dokumendile jms.
- Digiallkirju j a/või digitempleid verifitseerivate lahen duste korral tuleb testida kõikide DDOC-alamvormingute (põlvkondade) toetamist.
- Turvalist autentimist võimaldavate lahenduste korral tuleb testida sessiooni de lõpetatuse tingimuste täidetust meetme M 4.E5 Nõuded ID-kaardi/PKI lahendusi kasutavale turvalisele autentimisele nõuetele. Kui autentimiskeskkonnale ei ole rakenduse poolt esitatud kitsendusi kasutatavale brauseritüübile, tuleb neid testida kolme kasutatavaima brauseri – Internet Exploreri, Mozilla Firefoxi ja Google Chrome'i – keskkonnas.
- Turvalist autentimist võimaldavate lahenduste korral tuleb testida, et peale sessiooni lõppemist oleks kogu sessiooni vältel brauseriaknas vahetatav teave kustutatud meetme M 2.13 Tundlike ressursside jäljetu hävitamine nõudeid arvestades.

Turvatestide läbiviimise korraldab turvajuht või IT-juht koostöös turvajuhiga.

HG.78 Halduslike meetmete rakendamine korporatiivsete ja riiklike PKI-lahenduste jätkusuutlikuks kasutuseks

Vastutav algatuse eest: turvajuht

Vastutav elluviimise eest: IT-juht, IT rakenduste loojad

Kõrge turveastme korral tuleb asutuses tagada, et kõik PKI vahenditega realiseeritud allkirjastamise, signeerimise ja transpordikrüpto teenused oleksid kaetud vähemalt kahe erineva vahendiga, mis tagab nende teenuste jätkusuutlikkuse mingi vahendi tõrke korral.

Selle olukorra tagamiseks on asutuses mõistlik koostada maatriks, mille ridadeks on signeerimise, autentimise ja transpordikrüpto teenused ning veergudeks võimalikud vahendid, millega neid teenuseid on võimalik realiseerida. Halduslike meetmetega tuleks tagada, et selle maatriksi igas reas oleks vähemalt kaks lahtrit täidetud.

HG.79z ID-kaardi või sarnase seadme perioodiline loendurikontroll

Vastutav algatuse eest: turvajuht
Vastutav elluviimise eest: kasutajad

Fakultatiivne (vabatahtlik) meede

Kui kasutaja ID-kaart on arvutiga liidestatud, võib keerulisemate ründejuhtumitel ning ebapiisaval pahavara tõrjel anda pahavara digiallkirju, dešifreerida transpordikrüpto vormingus faile ning autentida kasutaja nimel ilma kasutaja teadmata. Täpsemalt vt - G 5.E6 PIN koodi ja ID-kaardi (või sarnase seadme) üheaegne vargus või röövimine.

Selle ohu minimeerimiseks oleks mõistlik heita aeg-ajalt pilk peale ID-kaardi (või sarnase seadme) loenduritele, mis näitavad, mitu korda on nii autentimisvõtmepaari kui ka signeerimisvõtmepaari kasutatud. ID-kaardi korral pääseb nendele loenduritele ligi ID-kaardi haldustarkvara kaudu, slängis nimetatakse neid ka sertifikaatide loenduriteks

ID-kaardi, mobiil-ID, digi-ID ja/või sarnase seadme kasutaja kohustusteks on vaadata võtmepaaride loendurid üle vähemalt neli korda aastas. Kui loendurid on eelmise vaatamisega võrreldes märgatavalt suurenenud (st kasutaja on üsna kindel, et ta ei ole nii palju kordi end turvaliselt autentinud ega digiallkirja andnud) tuleb sertifikaat kohaselt peatada (vt - M 5.E1 Sertifikaatide õigeaegne peatamine). Lisaks peab ta informeerima juhtunust asutuse turvajuhti.

Kui arvutist, kus on kasutatud ID-kaarti või muud analoogilist seadet, leitakse troojalane, mis võis kasutada PKI lahendusi ilma kasutaja teadmata, tuleb teha erakorraline loendurikontroll. Selle olukorra üle otsustamine, erakorralise loendurikontrolli algatamine ning võimalike turbetaasteliste järeltegevuste vajaduse (nt sertifikaatide peatamise) üle otsustamine on sel juhtumil turvajuhi vastutusalas.

Nimetatud loendurite vaatamise võimalust tuleb käsitleda ka töötajate koolitamisel – vt M 3.E2 Töötajate koolitus ID-kaardi/PKI lahenduste kasutamise osas .

Kontrollküsimused:

- Kas ja kuidas saab asutuse turvajuht veenduda, et kõik ID-kaarti või analoogilisi seadmeid kasutavad töötajad loendureid regulaarselt kontrollivad?

HG.80z Pin-pad ’i kasutamine

Vastutav algatuse eest: IT juht
Vastutav elluviimise eest: administraatorid, IT töötajad

Fakultatiivne (vabatahtlik) meede

Kõrgastme turbe korral tuleks tõsiselt kaaluda nii autentimisel kui ka signeerimisel kasutatavate PIN-koodide sisestamist mitte üldkasutatavalt klaviatuurilt (mis teeks need tihti pahavarale kättesaadavaks) vaid eraldiseiva *pin-pad* ’i kaudu.

HG.81 Krüptograafilisi detaile peitva vaheteegi kasutamine

Algatamise eest vastutavad: IT-juht
Rakendamise eest vastutavad: IT-turvaosakond

Krüptograafilised algoritmid vananevad varem voõi hiljem ja muutuvad loõpuks ebaturvaliseks. Osades IT-komponentides saab vananenud algoritmi asendada lihtsa ümberseadistamisega, kuid see ei ole alati voõimalik näiteks kasvoõi seetoõttu, et ka koõik kasutatavas krüptoteegis pakutud alternatiivsed algoritmid, millega vananenud algoritmi saab asendada, on juba ebaturvalised.

Et vananenud krüptoteeki saaks hoõlpsamini uuega asendada, rakenduskoodi muutmata, tuleb loodavates IT-lahendustes kasutada vaheteeki rakenduskoodi ja krüptograafilisi funktsioone sisaldava teegi vahel, mis peidaksid rakendusprogrammi eest krüpteerimise detailid. Naäiteks ei tohiks krüptograafiat kasutav rakenduskood nimeliselt vaälja kutsuda krüptograafilisi algoritme, vaid peaksid seda tegema vahendavate programmeerimisliideste kaudu uäldiste funktsioonide järgi (krüpteerimine, dekrüpteerimine, signeerimine, signatuuri verifitseerimine jne).

Kontrollküsimused:

- Kas organisatsioonis kasutatavad tarkvaraarenduse suunised reguleerivad ka krüptograafiliste teekide kasutamist?
- Kas organisatsioonis loodav rakendustarkvara peab voõimaldama krüptoteegi vahetust?

HK: Teabe käideldavuse turvameetmed

Meetmete nimekiri

HK.1 Varu-elektrigeneraatori nõue

Unikaalmeede

Kõrgkäideldavusnõuetega (käideldavusosaklassiga K3) süsteemidel on nõutav varu-toitegeneraatori olemasolu, mis peab vastama järgmistele nõuetele:

- Varugeneraator peab asetsema eraldi ruumis, mis vastab Eestis kehtivatele tuleohutusnõuetele.
- Varugeneraator peab olema suuteline koostoimima katkematu toiteallikaga (vt M 1.28 Puhvertoiteallikas) – viimase akude jõudmisel kriitilise mahtuvuspiirini peab generaator käivituma.
- Lahendatud peab olema varugeneraatori regulaarne hooldus, mis peab olema dokumenteeritud vastava töötaja töölepingus, ametijuhendis, viimaste lisas või välise partneriga sõlmitavas lepingus.
- Varugeneraatoril peab olema kütusevaru 48 tunniks (kaheks ööpäevaks).
- Varugeneraatori käivitamisest tuleb süsteemiadministraatorile teatada kaugindikatsiooni teel (vt HG.3 Tõrgete kaugindikatsiooni vastuvõtmiskohustus).

HK.5 Mobiilseadme aku regulaarvahetus

M 4.115 Mobiiltelefonide toite tagamine parametriseering

Lisaks mobiiltelefonide toite tagamise nõuetele tuleb mobiiltelefonide, pihuarvutite, GPS-navigaatorite, raadiojaamade jm mobiilseadmete akud vahetada enne töökõlbmatuks muutumist. Võimalikud on kaks tegutsemisvarianti:

- mobiilseadmel toimib aku eluea arvestus ning aku vahetatakse siis, kui ta prognoositavast tööajast on järel alla poole;
- tuleb hinnata mingite meetoditega ligikaudselt aku tööaega, ning vahetada aku, kui sellest tööajast on 75% läbi.

Konkreetsete juhtumite tegevuskavad töötatakse välja koostöös turvajuhiga, kes need kirjalikult kinnitab.

HK.6 Edastmiseks genereeritud andmete kahes eksemplaris varukopeerimine

M 6.38 Edastatud andmete varukoopiad parameetrite seadmine

Lisaks edastatud andmete varukoopiate nõuetele tuleb edastatud andmete varukoopiaid hoida kahes eksemplaris. Eri eksemplarid tuleb hoida võimaluse piires eri hoonetes või sama hoone erinevates tulekindlates sektsioonides. Nende võimaluste puudumisel tuleb eksemplarid hoida üksteisest võimalikult kaugel, seda tuleb arvestada tööruumide planeerimisel ja ümberplaneerimisel.

HK.7 Kahes eksemplaris varukopeerimine kodutööl

M 6.47 Kaugtöö andmevarundus parameetrite seadmine

Lisaks kaugtöö andmevarunduse nõuetele tuleb kodus ilma asutuse sisevõrguga ühenduses olemata töötamisel (nt. ilma kaugtöö VPN ühenduseta töötamisel) tulemandmete üks eksemplar viia töökohta esimesel võimalusel, nt esimesel töökoha külastamisel pärast kodus töötamist. Alternatiiv on luua vastav kuumarhiveerimissüsteem, mis töötab võrgu kaudu ja kasutab turvalist kaugpöördusprotokolli.

HK.8 Andmebaasi tervikliku varundamise nõue

M 6.49 Andmebaasi varundamine parameetrite seadmine

Lisaks andmebaasi varundamise nõuetele tuleb varundada kogu andmebaasi sisu. Olenevalt tehnoloogiast võib staatilisi või vähemuutuvaid andmeid varundada harvemini, kuid sel juhul peab olema koostatud üksikasjalik taasteplaan, mis võimaldab eri aegadel varundatud andmete põhjal taastada kogu baasi sisu.

Kui varundamisel kasutatavad sideliinid väljuvad kasvõi ühes kohas füüsiliselt turvatud alast, on rangelt soovitav turvalist kaugpöördusprotokolli, mille krüptovõtted peavad vastama meetme HT.52 nõuetele. Erandeid sellist tavast võib teha vaid turvajuhi eriloal, kes peab hindama sealtkaudu tekkivaid jääkriske.

HK.9 Varusidekanali nõue

M 6.75 Varu-sidekanalid parameetrite seadmine

Lisaks varu-sidekanali nõuetele peab olema kasutusse võetud varusidekanal mis kasutab erinevaid infrastruktuuri osi. Keelatud on rakendada kaht sidekanalit (põhi- ja varusidekanalit) niiviisi, et neil oleks ühiseid osi (ühine kaabeldus, ühine ruuter, ühine kandesagedus traadita levis vms).

HK.10 Lisanõuded personali asendamisele

M 3.3 Asendamise korraldamine parameetrite seadmine

Lisaks asendamise korraldamise soovituslikes meetmetes sätestatule tuleb arvestada järgmisi nõudeid:

- personali tagamine asendajatega peab olema kirjalikult dokumenteeritud ning vastavad sätted peavad sisalduma ka töötajate töölepingutes, ametijuhendites ja/või nende kirjalikes lisades;
- töötajate lisandumisel ja/või nende rollide muutmisel tuleb kriitiliste valdkondade personali dubleeritus/asendamine läbi vaadata nädala jooksul pärast iga muudatuse tegemist;
- asendusplaanid ja nende muutmised kuuluvad turvajuhi poolsele kirjalikule kinnitamisele.

HK.11 Serveriruumide ja kaitsekappide temperatuuriseire

Unikaalmeede

Kõikide serveriruumide ja kaitsekappide korral tuleb kindlaks määrata kaks piirtemperatuuri – hoiatuslävi ja kriitiline lävi. Hoiatusläveks tuleb valida selline temperatuur, mis jääb veel seadmete normaalsete töötingimuste piiresse, kuid mille edasisel tõusmisel võib see normaalsete tingimuste alt väljuda. Kriitiline lävi on temperatuur, mis asub juba kindlalt ülalpool seadmete normaalseid töötingimusi, mistõttu seadmete riknemine sellel temperatuuril on tõenäoline.

Temperatuuri tõusmise nii hoiatusläveni kui ka kriitilise läveni jõudmise peab seiresüsteem fikseerima ning edastama vastava teatise süsteemiadministraatorile kaugindikatsiooni teel (vt HG.3 Tõrgete kaugindikatsiooni vastuvõtmiskohustus .

Temperatuuri mõõtepunktid peavad asuma serveriruumis piisava paigutusega tagamaks tõest lugemit, kinniste isoleeritud kaitsekappide puhul peavad nad asuma igas kapis. igas kaitsekapis (moodul B 2.7 Kaitsekapid) nende ülaosas, kus tõenäoliselt temperatuur on kõrgeim. Kui serveriruumis asub osa seadmeid kaitsekapis, osa aga väljaspool kappe, piisab temperatuuri mõõtepunktide olemasolust kaitsekappides. Kui serveriruumis kaitsekappe ei asu, peab sealne temperatuuri mõõtepunkt asuma suurema hulga seadmete kohal ruumi lae all, kus tõenäoliselt on temperatuur kõrgeim.

HK.12 Arhiveerimisel kasutatavate andmekandjate taustauuring

M 4.169 Sobiva arhiveerimis-andmekandja valimine parameetrite seadmine

Lisaks sobiva arhiveerimis-andmekandja valimise nõuetele tuleb enne varundamiseks kasutatavate andmekandjate soetamist teha andmekandja tüübi taustauuring. Lubatud on kasutada andmekandjaid, mille puhul eksperdid hindavad andmete säilivusajaks vähemalt kümme aastat.

Keelatud on kasutada selliseid andmekandjaid, mis on välja töötatud ja turule tulnud hiljem kui aasta tagasi, sest nende tegelikud omadused ei ole veel selgunud.

HK.13 Arhiveerimisel kasutatavate andmekandjate regulaarkontroll

M 1.60 Arhiivi-andmekandjate asjakohane säilitus parameetrite seadmine

Lisaks arhiivi-andmekandjate asjakohase säilituse soovituslikele meetmetele sätestatule tuleb vähemalt kord kahe aasta tagant läbi vaadata arhiveerimiseks kasutatavate andmekandjate sobivus andmete pikaajaliseks säilitamiseks.

Kui ilmneb turvaintsident, mille üheks osaks osutub arhiveerimiseks ebasobivate andmekandjate kasutamine või sellega seotud muud tõrked, tuleb läbi viia erakorraline läbivaatus hiljemalt kaks nädalat pärast nimetatud turvaintsidendi uurimise lõppu.

HK.14 Arhiivketta salvestusressursside kaugindikatsioon

M 2.257 Arhiveerimis-andmekandja salvestusressursside seire parameetrite seadmine

Lisaks arhiveerimis-andmekandja salvestusressursside seire nõuetele tuleb evitada salvestusressursside kaugindikatsioon.

Kaugindikatsioon peab rakenduma, kui täidetud on asutuse (turvajuhi) poolt määratud protsent serveri salvestusmahust.

Teabe vastuvõtmisel tuleb juhinduda HG.3 Tõrgete kaugindikatsiooni vastuvõtmiskohustus nõuetest. Teabe edastamine peab toimuma krüpteeritult, kui teabes sisaldub konfidentsiaalseid osi. Krüpteerimise kasutamisel peavad selleks kasutatavad vahendid vastama HT.52 Lisanõuded krüptovahenditele nõuetele.

HK.15 Lisanõuded arhiveerimisprotsessi auditeerimisele

M 2.260 Arhiveerimisprotseduuri regulaarne auditeerimine parameetrite seadmine

Lisaks arhiveerimisprotseduuri regulaarse auditeerimise nõuetele tuleb arhiveerimisprotseduuri auditeerida vähemalt kord kahe aasta jooksul (soovitatavalt kord aastas). Kui ilmneb turvaintsident, mille üheks osaks on tõrge arhiveerimise korralduses või protsessis, tuleb läbi viia erakorraline läbivaatus hiljemalt kaks nädalat pärast nimetatud turvaintsidendi uurimise lõppu.

HK.16 Veebipääsu dokumenteerimine

Unikaalmeede

Kogu veebipääs, täpsemalt kõik antud pääsuõigused andmekogusse (nii asutuse sees kui ka väljaspool asutust), tuleb alati ilma eranditeta dokumenteerida. Kui dokumenteeritakse digitaalselt, tuleb IT ja/või füüsiliste vahenditega tagada, et kandeid ei saaks kustutada, vaid neid saaks üksnes lisada.

HK.17 Lisanõuded kõrgkäideldavusega salvestivõrkudele

M 2.354 Kõrge käideldavusega SAN-konfiguratsiooni kasutamine parametriseering

Ülaltoodud meetmes mainitud kahes füüsilises asukohas andmeid hoidva süsteemi kasutamine on siin kohustuslik (seal oli ta soovituslik).

Lisaks tuleb arvestada järgmisi nõudeid:

- Kahte andmete instantsi (koopiat) hoida üksteisest vähemalt 500 meetri kaugusel.
- Maksimaalne taaskäivitusaeg (RTO, *recovery time objective*) ei tohi olla pikem kui 2 minutit.

HK.18 Windows Server 2003 klasterdamine

Unikaalmeede

Kõrgete käideldavusnõuete korral tuleb *Windows Server 2003* klasterdada. *Windows Server 2003 Enterprise Edition* ja *Datacenter Edition* operatsioonisüsteemil põhinevaid servereid saab klasterdada kasutades kahte erinevat tehnoloogiat: serverite klaster (*Server cluster*) ja võrgukoormuse tasakaalustamine (*Network Load Balancing, NLB*). Neid tehnoloogiaid kasutatakse erinevat tüüpi teenuste kõrge käideldavuse tagamiseks. Serverite klastrit tuleks kasutada kriitiliste rakenduste ümberlülitamiseks. Andmebaasi-, ERP, CRM, OLTP, faili-, prindi- ja meiliteenuste käideldavuse tõstmiseks kasutatakse enamasti serverite klastrit. Kui klientide pöördumisi tuleb jaotada serverite vahel (veebiserver, proksiserver, turvalüüs) tuleks võimalusel kasutada võrgukoormuse tasakaalustamist.

Serverite klaster	Võrgukoormuse tasakaalustamine
On *Windows Server 2003 Enterprise Edition* ja *Windows Server 2003 Datacenter Edition* koostisosa	Kasutatav kõikide *Windows Server 2003* versioonidega
Sõlmed võivad olla geograafiliselt eraldatud	On hästi laiendatav ehk skaleeritav
Kuni kaheksa sõlme	Kuni 32 sõlme
Nõuab jagatud või tiražeeritud salvestusseadmeid	Ei nõua spetsiaalset riist- või tarkvara, töötab kohe.

Mõlema lahenduse korral on võimalik täielikult elimineerida hoolduseks, tarkvara paikade installeerimiseks ja versiooniuuendusteks vajalik seisuaeg.

HK.19 Liiasuse nõue salvestivõrkudes

M 2.362 Sobiva salvestisüsteemi valik parametriseering

Lisaks sobiva salvestissüsteemi valiku nõuetele tuleb kõrge käideldavusnõude korral salvestisüsteemid plaanida ja ehitada ilma kriitiliste tõrkekohtadeta. See tähendab, et kõik salvestid ja salvestite kommunikatsiooniteed peavad olema ehitatud liiasusega, ning vajadusel automaatse ümberlülitamisega, mis siinkohal on rakendamiseks kohustuslik.

Väga kõrgete käideldavuse nõuete korral võib osutuda vajalikuks geograafiliselt eraldatud sõlmedega salvestivõrk. Geograafiliselt eraldatud süsteemide plaanimisele peab alati eelnema põhjalik turvaanalüüs.

Kõrge käideldavusnõude korral tuleb plaanimisfaasis eelistada salvestivõrke (*Fibre Channel* tehnoloogial põhinevaid) *Ethernet* kohtvõrgul põhinevatele võrgusalvestitele. *Fibre Channel* salvestivõrgud on tänapäeval võtmetehnoloogia liiasusega kriitiliste tõrkepunktideta salvestisüsteemide ehitamisel.

Kõrge käideldavusnõude korral tuleb kõik versiooniuuendused, värskendused ning turvapaigad eelnevalt testida. Mitte kunagi ei tohi muudatusi teostada töösüsteemidel vaid kõik konfiguratsioonimuudatused tuleb eelnevalt testida testsüsteemil. Seega on vajalik testsüsteemi soetamine, mida tuleb juba salvestisüsteemide eelarve koostamisel arvestada. Testimata muudatuste keeld ja testimisprotseduurid tuleb sätestada ka asutuse vastavates infoturbe juhendites.

HK.20 SAP'i klasterlahenduse kasutamine

Unikaalmeede

Kõrge käideldavusnõude korral tuleb SAP süsteemi rakenduste ja andmebaasi töökindlust suurendada klasterlahenduse kasutamise teel. Klaster koosneb kahest või enamast masinast, mida nimetatakse klastri sõlmedeks. Klastri sõlmed jagavad ühist salvestusseadet ja koordineerivad oma tööd klastri tarkvara ja klastriühenduse kaudu (*heartbeat*).

Windows operatsioonisüsteemi jaoks toetab *SAP Microsoft Cluster Services* (MSCS) klastri tarkvara, mis on operatsioonisüsteemi koosseisus. Muude operatsioonisüsteemide jaoks tuleb kasutada eraldi klastri tarkvara, mis on operatsioonisüsteemiga tihedalt integreeritud. Siia alla kuuluvad näiteks alljärgnevad erinevate tootjate klastritarkvara.

Iga salvestusseade ühendatakse sel juhul klastri kõikide sõlmedega. Kui kasutatakse *Fibre Channel* (FC) tehnikat, tuleb salvestite tõrkekindlaks ühendamiseks kasutada kas *Fibre Channel* jaoturit või kommutaatorit. Klastri kasutamisel tuleb vältida kriitilisi tõrkepunkte kogu infrastruktuuris (toide, andmesidevõrk, salvestivõrk). Väga kõrgete käideldavusnõuete puhul tuleb kaaluda klastrisõlmede eraldamist tulekindla seinaga eraldatud ruumidesse või ka erinevatesse hoonetesse.

HK.25 Puhvertoiteallika kasutamine IP kõne puhul

Unikaalmeede

Reeglina on telefonisüsteemi kasutajad harjunud, et isegi kui arvuti võrguühendus ei ole töökorras on telefon alati kasutatav. Sageli on äriprotsessid üles ehitatud selliselt, et telefonisüsteemi välja langemine võib põhjustada olulisi tagajärgi asutuse praegusele ja edasisele tegevusele.

IP-kõne süsteem koosneb erinevatest osadest, milleks võivad olla telefonid, SIP proksid, H.323 lüüsid, kõnekeskused (*call manager*), turvalüüsid, võrguseadmed jne.

IP-kõne teenuse toimimiseks on vajalik kogu IP-kõne infrastruktuuri toimimine. Tuleb jälgida, et nii sõlmseadmete toiteks (vahendussüsteem, registrar, SIP lüüs jm), kui ka kogu infrastruktuuri toiteks (kommutaatorid, marsruuterid, lüüsid jm) oleks kasutatud puhvertoiteallikat. Puhvertoiteallika patareidelt toitmise tööiga peab olema kooskõlas IP-kõne avariiplaaniga (vt M 6.100). See on sõltuvuses alternatiivsete sidevahendite (nt mobiiltelefonide) kasutamise võimalusest ja nendele üleminemise kiirusest. Näiteks tuleb otsustada, kas puhvertoiteallikas peab seadmeid toitma ainult vajalike üleminekuoperatsioonide sooritamiseks (kõnede ümbersuunamine) või peab puhvertoiteallikas tagama IP-kõne kasutatavuse teatud aja jooksul.

IP-kõne telefonide toiteks tuleks kasutada toidet kohtvõrgu kaudu (*power over Ethernet*), mis lihtsustab oluliselt terminalide katkematu toite tagamist avariiolukorras.

HK.26 IP-kõne kestseadmete dubleeritus

Unikaalmeede

Reeglina on telefonisüsteemi kasutajad harjunud, et isegi kui arvuti võrguühendus ei ole töökorras on telefon alati kasutatav. Sageli on äriprotsessid üles ehitatud selliselt, et telefonisüsteemi välja langemine võib põhjustada olulisi tagajärgi asutuse praegusele ja edasisele tegevusele.

Ohtudest tuleb arvestada, et IP-kõnes kasutatavad protokollid ja erinevate tootjate tõlgendused ning realiseeringud on valminud alles viimaste aastate jooksul. Seetõttu ei ole IP-kõne protokollide realiseeringud seadmetes alati nii väljapeetud ja küpsed, kui seda on mõne aastakümneid kasutusel olnud protokolli puhul, millest tuleneb suurenenud tehnilise tõrke oht. Samuti võib protokollidel esineda erinevaid nõrkusi, mida teatud tingimustel on võimalik kasutada teenustõkestusrünnete sooritamiseks.

Kõrge käideldavuse nõude korral tuleks IP kõne kestseadmed ehitada liiasusega nii, et ühe seadme väljalangemise korral oleks võimalik edasine IP-kõne teenuse kasutamine. Liiasusega tuleks ehitada nii kestseadmed (vahendussüsteem, lüüsid, jne) ja ka võrguseadmed (kommutaatorid, marsruuterid, turvalüüsid). Liiasuse nõe ei ole kohustuslik terminalidele.

IP-kõne serverkomponentide korral saab liiasusnõude realiseerida kas koormusjaoturite või klasterlahendusega. IP-kõne võrk tuleb kõrge käideldavusnõude korral kindlasti eraldada andmeside võrgust ja samuti tuleb rakendada erinevaid meetodeid võrgu käideldavuse tõstmiseks. Võrgu topoloogia plaanimisel tuleb otsustada, kuidas toimub automaatne ümberlülitamine võrgukomponendi tõrke korral (*Spannig Tree* , HSRP, VRRP, *Routing Protocol*). IP-kõne võrgu dokumentatsioon peab kajastama ka ümberlülitusmehhanisme.

HK.27 Puhvertoiteallikas serveri sulgemise tagamiseks

Unikaalmeede

Reeglina toidetakse servereid läbi puhvertoiteallika, mis tagab serveri toite akudelt juhul, kui väline elektrivarustus peaks mingil põhjusel katkema. Sageli paigutatakse serverid serveriruumi, kuhu on juba infrastruktuuri ehitamise käigus installeeritud piisavalt võimsad puhvertoiteallikad, mis varustavad mitmeid serveriruumi seadmeid. Kui sellist võimalust ei ole, tuleb serveri toiteks kasutada eraldi puhvertoiteallikat.

Mõlemal juhul tuleb plaanimisfaasis otsustada, kui pika aja jooksul peab puhvertoiteallikas avariiolukorras serveri toite tagama. Tuleb arvestada olukorraga, mil puhvertoiteallika aku saab tühjaks ja serveri toitevarustus katkeb.

Serveri ootamatu toite kadumine võib aga põhjustada andmete tervikluse kadumise nii, et ainus võimalus serveri töö taastamiseks on taastamine varukoopiatelt, mis põhjustab reeglina teatud andmekao ja töö seisakule lisandub veel andmetaastele kuluv aeg.

Sellise olukorra vältimiseks tuleb kõrge turbeastmega serverite toide plaanida selliselt, et enne puhvertoiteallika aku tühjaks saamist suletakse server tarkvaraliselt. Praktika näitab, et serveri sulgemiseks võib kuluda rohkem kui 15 minutit. Põhimõtteliselt on avariiolukorras automaatse sulgemise ajal serveri toite tagamiseks kaks võimalust:

- Serveri puhvertoiteallikas mõõdab koormust ja aku mahtuvust, ning teatud aeg enne aku lõplikku tühjenemist antakse serverile signaal automaatseks sulgemiseks.
- Teisel juhul kasutatakse puhvertoiteallikat, mis on arvestatud serverit toitma vaid serveri sulgemiseks vajamineva perioodi jooksul. Sellisel juhul antakse signaal serveri sulgemiseks kohe, kui toide on puhvertoiteallika sisendist kadunud. Sageli kasutatakse kõrge turbeastmega serverite puhul sellist lühikese tööajaga puhvertoiteallikat lisaks serveriruumi üldisele puhvertoiteallikale. Sellisel juhul jätkub avariiolukorras serveri tavapärane töö kuni serveriruumi puhvertoiteallika aku tühjenemiseni. Seejärel, toite kadumisel lühikese tööajaga puhvertoiteallika sisendis, käivitatakse serveri automaatse sulgemise protsess, mille jooksul toidetakse serverit väiksemast puhvertoiteallikast.

Enamasti toimub andmeside serveri ja puhvertoiteallika vahel kas järjestikliidese või kohtvõrgu kaudu kasutades SNMP protokolli. Reeglina tuleb automaatse sulgemise korraldamiseks installeerida serverisse vastav tarkvara.

Kõrge käideldavusnõude korral tuleks kasutada serveri automaatse sulgemise juhtimist isegi siis kui lisaks serveriruumi puhvertoiteallikale kasutatakse varugeneraatorit.

Veel on oluline silmas pidada, et kasutades ühte puhvertoiteallikat klasterlahenduse toiteks osutuks see kriitiliseks tõrkepunktiks. Seega tuleks klasterlahenduse puhul kasutada vähemalt kahte puhvertoiteallikat, kahesõlmelise klastri puhul mõlemale sõlmele oma.

HK.28 Nõuded toitevõrgu varukoormusele

Unikaalmeede

Kõikide kõrgkäideldavustsoonis (turvaosaklass K3) asuvate elektrivõrgu komponentide (liinid ja harundseadmed) projekteerimisel ja ehitamisel tuleb lähtuda pooleteisekordsest võimsusvarust. Selleks tuleb ruumide elektriinstallatsiooni ehitamisel või rekonstrueerimisel hinnata nende kaudu toidetavate seadmete (sh ka lambid, soojapuhurid, ventilaatorid, kohvimasinad, tolmuimejad, veekeedukannud jms) koguvõimsust ja ehitada võrk välja sellest poolteist korda suuremale võimsusele.

Kord aastas peab turvajuht korraldama elektriinstallatsiooni reaalset võimsuskoormuse kontrolli ning hindama, kas poolteisekordne varu on jätkuvalt tagatud või mitte. Kui toimus reaalne võrguülekoormus, on turvajuhil soovitav teha järgmise poole aasta jooksul veel pistelisi võimsusvaru kontrolle.

Vt lisaks ka M 1.21 Liinide õige dimensioneerimine liinide füüsilise paiknemise kohta.

HK.29 Kaabelduse minimaalsuse nõue andmearhiivides

M 1.3 Juhtmestuse kohandamine parameetrite seadmine

Andmearhiivides tuleb toitejuhtmestuse ja võrgukaabelduse ehitamisel ning kohandamisel, mida reguleerib meede juhtmestuse kohandamine, lähtuda lisaks kaabelduse minimaalsuse nõudest.

Andmearhiivid on tavaliselt paigad, kus asuvad seadmed elektrit ei tarbi, v.a. ruumi valgustus, signalisatsioon(id) ja vajadusel ka konditsioneer ning küte. Kõik ülejäänud elektriinstallatsioon, mis ei ole nende seadmetega seotud, tuleb andmearhiividest välja viia. Andmearhiivides on keelatud kogu transiitkaabeldus ja selle harundseadmed, mis on mõeldud teiste ruumide elektritoite tarbeks.

Ka andmearhiive läbivaid võrgu- ja andmekaableid tuleb võimalusel vältida.

Nõue ei kehti juhtumeil, kui andmearhiivis on arhivaalid vee- ja tulekindlas seifis, mille turve vastab EN 1143/1 nõuetele.

HK.30 Serveriruumi ja andmearhiivi eraldatuse nõue

M 1.13 Kaitset vajavate ruumide paigutus parametriseering

Kõrgtasemel käideldavuse ja terviklusega infosüsteemides (turvaosaklass K3 või T3) peab ruumide paigutamisel lisaks kaitset vajavate ruumide paigutuse nõuetele sätestatule lähtuma nõudest, et serveriruum ja andmearhiiv peavad asuma eraldi ning üksteisest võimalikult kaugel (olemasoleva kontoripinna võimaluste piires). Nõue on vajalik juhtumeiks, kui ühes neist ruumidest toimub tulekahju või uputus, mis nõuete täitmisel säästab teist ruumi. Eraldiseisva andmearhiivi korral kehtib seal kaabelduse minimaalsuse nõue (vt HK.29 Kaabelduse minimaalsuse nõue andmearhiivides), st kõik elektrit tarbivad (*online*)seadmed tuleb koondada serveriruumi ja vältida nende olemasolu andmearhiivis.

Tehnilise infrastruktuuri ruumi (moodul B 2.6 Tehnilise infrastruktuuri ruum) võib ühitada serveriruumiga, kuid ei tohi üldjuhul ühitada andmearhiiviga.

Kui serveriruumist ja/või tehnilise infrastruktuuri ruumist eraldiseisvat andmearhiivi ei õnnestu olemasoleva kontoripinna baasil luua, tuleb kasutada kaugarhiveerimise (kaugvarundamise) teenuseid.

HK.31 Kõrgkäideldavuse lisanõuded kaabelduse paigaldusele

M 1.68 Nõuetele vastav installatsioon parametriseering

Lisaks nõuetele vastava installatsiooni nõuetele tuleb käideldavusosaklassiga K3 süsteemides paigutada kõik kaablid (sh arvuti sisendkaablid, printerijuhtmed, samuti ka kõik elektrotehnilised kaablid) põrandapinnast vähemalt 10 cm kõrgusele, et vältida nende võimalikku vigastamist tallamisel. Nõue kehtib olenemata tõstetud põranda olemasolust või puudumisest.

Nõue ei kehti kohtades, kuhu inimene käima ei mahu – kitsad kapivahed, kapitagused, riiulialused jms –, kuna seal ei saa ta kaableid vigastada.

HK.33 Kõrgkäideldavuse lisanõuded mobiilsetele andmetekandjatele

M 2.3 Andmekandjate haldus parametriseering

Kõrgtasemel käideldavusanõuete (turvaosaklassi K3) korral tuleb lisaks andmekandjate halduse nõuetele viia kõikide kasutatavate mobiilsete andmekandjate korral läbi eelnev taustauuring. Sellise taustauuringu korraldamine on turvajuhi kohustus ning see peaks minimeerima andmekandjate tehnilistest rikestest põhjustatud käideldavuskadusid infosüsteemis.

Olenevalt andmekandjate kasutamise kohast ja rollist infosüsteemis otsustab turvajuht taustauuringu põhjalikkuse, samuti selleks kasutatavate spetsialistide (vajadusel väliste ekspertide) kaasamise. Taustauuring peab alati lõppema andmekandja kirjaliku tüübikinnituse koostamisega, millede loomine ja hoidmine on turvajuhi kohustus.

HK.34 IP-kõne võrgu eraldatusnõue

M 2.376 Andmeside ja IP-kõne (VOIP) võrgu eraldamine parametriseering

Kui asutuses ei ole rakendatud sideliinide paralleliseerimise võtet (kus ühe liini riknemine ei halva side toimimist), siis tuleb andmeside ja IP-kõne võrk eraldada, kui IP-kõned on kõrgkäideldava (turvaosaklass K3) süsteemi osa. Ülaltoodud meetmes on selle teostamine soovituslik, kuid siinkohas kohustuslik.

HK.35 Lisanõuded elektriseadmete kontrollimisele

M 2.394 Elektriseadmete kontrollimine parametriseering

Turvaosaklassiga K3 teabe korral tuleb lisaks elektriseadmete kontrollimise nõuetele arvestada alljärgnevaga:

- Lisaks regulaarsele kontrollile võib turvajuht nõuda erakorralist elektriseadmete kontrolli, kui talle laekunud andmete põhjal on alust arvata, et käideldavuskadu või käideldavuskao oht tekkis rikkis seadmetest.
- Elektriseadmete kontrollimisakti peab igal juhul kinnitama ka turvajuht.

HK.36 Käideldavusnõuete täidetuse regulaarseire

M 6.1 Käideldavusnõuete inventuur parameetrite seadmine

Käideldavusnõuete seire (inventuur) tuleb infoturbejuhi poolt läbi lisaks käideldavusnõuete inventuuri nõuetele sooritada vähemalt kaks korda aastas. Samuti tuleb see sooritada nädala jooksul, kui:

- infosüsteemi on oluliselt modifitseeritud
- on installeeritud uusi tark- või riistvarakomponente, mis võivad olulisel määral muuta käideldavust

HK.37 Usaldusele toetuv deponeerimine (Escrow)

Unikaalmeede

Algatamise eest vastutavad: infoturbespetsialist, hädaolukorra lahendamise eest vastutav töötaja

Vastutav elluviimise eest: üksikute IT rakenduste eest vastutavad isikud

Mida ärikriitilisem protsess on, seda tähtsam on kindlustada seda väljalangemise eest. Paljude äriprotsesse toetavate toodete tarnimisel (tarkvara, masinad, automaadid jne), ei saa ostja kõiki osi, mis on vajalikud toote hoolduseks. Hooldustööde teostamise eest vastutab sel juhul tihti tarnija. Kui tootja või tarnija ära langeb, ei ole toode enam hooldatav. Tuleks kontrollida, kas selline oht oleks vähendatav puuduvate osade deponeerimisega (Escrow).

Escrow on tarne hulka mitte kuuluvate toote hooldamiseks vajalike materjalide usaldusele toetuv deponeerimine kolmanda isiku juures (Escrow agentuur). Nimetatud materjalide näol võib olla tegu tarkvara (käivitatav või lähtekoodina), käsiraamatute, konstruktsiooniplaanide, konfiguratsiooniseisundite, testimisandmete, võtmete, paroolide või teiste osadega.

Olenevalt toote liigist võivad ettevõtted või asutused selle instrumendiga kindlustada ennast järgmiste riskide vastu:

- Teenuste äralangemine tellimuse täitja poolt seoses toote valmimise, hoolduse ja edasiarendamisega;
- komponentide ja elementidega varustamise katkemine.
- Spetsiaalselt tarkvara osas: Lähte ja / või objektikoodide kadumine suurte kahjustuste korral IT-valdkonnas;
- Puuduvad võimalused tõendada, millal milline versioon olemas oli, näiteks seoses autoriõiguse, vastutuse või maksejõuetusega.

Funktsionaalne kirjeldus

Toote kasutaja kindlustab Escrow abil ühe või mitme ärikriitilise protsessi järjepideva kulgemise. Selleks saab ta õiguse omada kindlaks määratud tingimustel juurdepääsu deponeeritud materjalile ning seda toote hooldamiseks kasutada, näiteks kui tarnija ei täida kasutaja suhtes kokkulepitud kohustusi. Teiselt poolt kaitseb tarnija oma konkursieeliseid ja ärisaladusi, seni kuni ta oma kohustusi täidab. Escrow agentuur kontrollib ja säilitab materjali mõlemale poolele.

Kasutaja ja tarnija sõlmivad Escrow agentuuriga lepingu, milles on defineeritud vähemalt järgmised aspektid:

- Õiguste ja tingimuste kindlustamine deponeeritud materjali väljaandmiseks;
- materjali verifitseerimine;

- materjali nõuetekohasuse tagamine ja sobiv varundamine;
- materjali uuendamine.

Deponeerimistingimused ja eriti Escrow agentuuri kohustused seoses verifitseerimise ja väljaandmisega tuleb Escrow lepingus täpselt kirjeldada. Lepingu üksikasjad sõltuvad nii riskide hindamisest, mille vastu deponeerija tahab end kindlustada, kui ka õigusruumist.

Escrow lepingu sõnastamisel ja sõlmimisel tuleks järgida järgmisi nõuandeid:

- Tuleb vältida kasutuslepingu ja Escrow lepingu vahelisi lahknevusi.
- Kasulik on sõlmida kasutusleping ja Escrow leping paralleelselt. Ajaline edasilükkumine võib osutuda kasutaja jaoks puuduseks.
- Olenevalt õigusruumist võib Escrow leping ohtu sattuda, kui see sõlmitakse liiga hilja, näiteks vahetult enne tarnija maksejõuetuks muutumist.
- Materjali väljastamine peaks olema selgelt defineeritud. Escrow leping peaks sisaldama täpset protseduuri kirjeldust, kuidas väljaandmist tuleb alustada ja läbi viia.
- Escrow agentuur peab mõlemate poolte silmis olema usaldusväärne ning pakkuma kindlaid ja sobivaid säilitamisvõimalusi deponeeritavale materjalile.
- Tuleb määrata kindlaks deponeerimise tehnilised aspektid. Escrow agentuuril peaks olema vajalik tehniline kompetents, et oleks võimalik kontrollida materjali edasise kasutamise võimalust ning teostada värskenduste järelhooldust.
- Materjali kasutatavust pärast väljaandmist tuleb sobival viisil kontrollida juba kättetoimetamisel. Kontrollimise sügavus sõltub riskide hindamisest ja kasutatavast tehnikast. Kontrollimise näideteks on tarkvara kompileerimine deponeeritud lähtekoodist või montaažijuhendi läbimängimine.
- Sobivate värskendustsüklite kindlaksmääramisega tuleb materjal aktuaalsena hoida. See, millised tsüklid on vajalikud, sõltub eelkõige riskide hindamisest ja kasutaja tootmisprotsessidest.

Hindamisküsimused

- Kas on kontrollitud, kas usaldusel põhineva deponeerimise (Escrow) abil on võimalik vähendada turvariske?
- Kas Escrow lepingus on üksikasjaliselt kindlaks määratud kõik deponeerimise, aktualiseerimise ja väljaandmise tingimused, samuti osalevate poolte õigused ja kohustused?
- Kas on tagatud, et Escrow leping on kooskõlas vastava kasutuslepinguga?
- Kas Escrow agentuuril on olemas vastavad kvalifikatsioonid?
- Kas usaldusele toetuva deponeerimise korral kontrollitakse, kas materjal on väljastamise korral tulevikus kasutatav?

Digi-ID omamise kohustus varuseadmena

HK.38 Krüptograafiliste algoritmide kasutuskataloog

Kui ID-kaardi/PKI lahendused kasutavad ID-kaardi põhist turvalist autentimist, on vastavatel töötajatel kohustus muretseda digi-ID. Digi-ID toimib sel juhul ID-kaardi varuseadmena, kui viimasega midagi juhtub (või vastupidi).

Kohustus tagada autentimine nii ID-kaardi kui ka digi-ID-ga

Kui infosüsteemis kasutatakse turvalist autentimist, peab rakenduse poolt olema tagatud autentisvõimalus nii ID-kaardiga kui ka digi -ID-ga vastavalt kasutajate soovile.

Lisanõuded juurdepääsutõendiga määratud signeerimisressursi seirele

M 4.E4 Juurdepääsutõendiga määratud signeerimisressursi seire ja uuendamine parameetrite seadmine

Lisaks ülaltoodud meetme nõuetele tuleb juurdepääsutõendiga määratud signeerimisressursi igakuise seire andmed edastada ka asutuse turvajuhile või tema poolt määratud isikule. Turvajuht võib vajadusel kehtestada jooksvalt lisanõudeid juurdepääsutõendi uuendamiseks (pikem periood vms).

Transpordikrüpto vormingus faili koostamine nii ID-kaardi kui ka digi-ID jaoks

Juhtumeil, kui transpordikrüpto adressaadil on olemas nii ID-kaart kui ka mobiil-ID ning mõlema seadme sertifikaadid on aktiivsed, tuleb krüpteerimisel alati krüpteerida mõlema sertifikaadiga. Sel korral on võimalik saadetist dešifreerida ja juhtumeil, kui adressaadi üks seadmetest pole mingil põhjusel kasutatav.

HK.38 Krüptograafiliste algoritmide kasutuskataloog

Algatamise eest vastutavad: IT-juht
Rakendamise eest vastutavad: IT-turvaosakond

Koõik krüptograafilised algoritmid muutuvad varem voõi hiljem ebaturvaliseks kas struktuursete noõrkuste ilmnemise toõttu voõi lihtsalt vananevad inimkonna käsutuses olevate arvutiressursside olulise kasvu toõttu. Ehkki algoritmide vananemist saab arvutustehnika arengut jälgides mingi täpsusega prognoosida, on struktuursete noõrkuste avastamine prognoosimatu ja soõltub krüptograafia kui teaduse arengust.

Kriitilise tähtsusega infosüsteemides kasutatavate krüptograafiliste algoritmide vananemine on toõsine oht, mis voõib poõhjustada toõsist kahju. Et institutsioonid suudaksid oõigeaegselt reageerida informatsioonile mingi krüptograafilise algoritmi vananemisest ja vajadusel vastavad IT-komponendid väälja vahetada voõi ümber seadistada, peab organisatsioonil olema teave IT-komponentides kasutatavatest krüptograafilistest algoritmidest.

Et see teave oleks oõigeaegselt kättesaadav, on vajalik organisatsioonisisese krüptograafiliste algoritmide kataloogi pidamine, millest saaks mis tahes algoritmi nimetuse järgi kohe tuvastada need IT-lahendused, kus seda algoritmi kasutatakse ja mis vajavad muutmist voõi ümberseadistamist.

Tuleb arvet pidada ka IT-komponentide kohta, kus ei ole enam voõimalik kasutatavat vananenud krüptograafilist algoritmi lihtsa ümberseadistamisega muuta ja turvalisemaga asendada, st kas selline voõimalus puudus kohe algul voõi on koõik voõimalikud asendusalgoritmid juba ise vananenud.

Kontrollküsimused:

- Kas IT-komponentide dokumentatsioon kajastab koõikides IT-komponentides kasutatavaid krüptograafilisi algoritme?
- Kuidas toimitakse, kui organisatsiooni teavitatakse mingi krüptograafilise algoritmi vananemisest voõi ebaturvaliseks muutumisest?

HT: Teabe tervikluse turvameetmed

Meetmete nimekiri

HT.2 Süsteemi ja võrgu pääsuõiguste perioodiline seire

Unikaalmeede

Süsteemi ja võrgu pääsuõiguste (vt M 2.7 Süsteemi ja võrgu pääsuõiguste andmine) perioodiline seire tuleb läbi viia:

- pistelise kontrollina vähemalt neli korda aastas;
- pärast iga juhtumit, kus leiti töötajatele töökohustuste täitmiseks mittevajalikke pääsuõigusi;
- pärast süsteemi või töökohustuste iga suuremat ümberkorraldust, millega kaasneb olulisi pääsuõiguste muudatusi;
- pärast iga turvaintsidenti, mille ühe põhjusena tuvastati pääsuõiguste puudulik korraldus;
- pärast asutuse turvapoliitika ja/või turvaplaani muutusi, mis puudutavad olulisel määral pääsuõigusi ja nende tähtsust turbes.

Seire teostamine on turvajuhi või tema poolt määratud töötaja kohustus

HT.3 Rakenduste ja andmete pääsuõiguste perioodiline seire

Unikaalmeede

Rakenduste ja andmete pääsuõiguste (vt M 2.8 IT-rakendustele ja andmetele pääsuõiguste andmine) perioodiline seire tuleb läbi viia:

- pistelise kontrollina vähemalt neli korda aastas;
- pärast iga juhtumit, kus leiti töötajatele töökohustuste täitmiseks mittevajalikke pääsuõigusi;
- pärast süsteemi või töökohustuste iga suuremat ümberkorraldust, millega kaasneb olulisi pääsuõiguste muudatusi;
- pärast iga turvaintsidenti, mille ühe põhjusena tuvastati pääsuõiguste puudulik korraldus;
- pärast asutuse turvapoliitika ja/või turvaplaani muutusi, mis puudutavad olulisel määral pääsuõigusi ja nende tähtsust turbes.

Seire tegemine on turvajuhi või tema poolt määratud töötaja kohustus

HT.4 Sagedasem tarkvara inventuur

M 2.10 Riistvara ja tarkvara inventuur parameetrite seadmine

Lisaks riistvara ja tarkvara inventuuri nõuetele tuleb tarkvara inventuur kindlasti läbi viia:

- pistelise kontrollina vähemalt kaks korda aastas;
- pärast iga juhtu, kus leiti dokumenteerimata ja/või kinnitamata tarkvara kasutamist;
- pärast süsteemi iga suuremat ümberkorraldust, millega kaasneb olulisi muutusi kasutatavas tarkvaras;
- pärast asutuse turvapoliitika ja/või turvaplaani muutusi, mis puudutavad olulisel määral tarkvarainventuuri rolli ja/või korraldust.

HT.6 Esemeliste pääsuvahendite halduse seire

Unikaalmeede

Esemeliste pääsuvahendite all mõeldakse siin võtmeid, magnetkaarte, kiipkaarte, kontaktivabu kaarte jt esemeid, mis võimaldavad pääsu arvutitesse/infosüsteemidesse või kaitsekappidesse/ruumidesse/territooriumitele. Nende halduse üldnõuded vt M 2.14 Võtmete (ja kaartide) haldus .

Esemeliste pääsuvahendite halduse seire tuleb läbi viia:

- pistelise kontrollina vähemalt kaks korda aastas;
- pärast iga turvaintsidenti, mille üheks põhjuseks olid puudused võtmete ja kaartide halduses;
- pärast süsteemi iga suuremat ümberkorraldust, millega kaasneb oluline muudatus ka kasutajate õigustes ning seetõttu ulatuslik võtmete ja kaartide vahetus/ümberprogrammeerimine;
- kui kuu jooksul on lahkunud töölt üle 20% töötajatest;
- pärast asutuse turvapoliitika ja/või turvaplaani muutusi, mis puudutavad olulisel määral pääsuvahendite haldust ja korraldust;
- peale kolimist või olulist ressursside muutmist (nt töötajate ümberpaigutamist hoones või ruumide lõikes).

Seire teostamine on turvajuhi või tema poolt määratud töötaja kohustus.

HT.7 Kasutajate ja nende profiilide perioodiline seire

Unikaalmeede

Kasutajate ja nende profiilide (vt M 2.31) perioodiline seire tuleb läbi viia

- pistelise kontrollina vähemalt kaks korda aastas;
- peale üleminekut kasutajaid (profiile) haldava tarkvara uuele platvormile või versioonile
- pärast iga turvaintsidenti, mille üheks põhjuseks oli puudulik kasutajaõiguste haldus;
- pärast süsteemi iga suuremat ümberkorraldust, millega kaasneb oluline muutus ka kasutajate õigustes.
- pärast asutuse turvapoliitika ja/või turvaplaani muutusi, mis puudutavad olulisel määral kasutajaprofiilide rolli;
- peale kolimist või olulist ressursside muutmist (nt töötajate ümberpaigutamist hoones või ruumide lõikes).

Ressursside kokkuhoiu mõttes on mõistlik koos kasutajaprofiilide perioodilise seirega viia läbi ka esemeliste pääsuvahendite halduse (vt M 2.14) seire (vt HT.6).

Seire tegemine on turvajuhi või tema poolt määratud töötaja kohustus.

HT.9 Andmebaasi pääsuõiguste perioodiline seire

M 2.129 Andmebaasiinfo pääsu reguleerimine parametriseering

Lisaks andmebaasiinfo pääsu reguleerimise nõuetele tuleb andmebaasi pääsuõiguste perioodiline seire läbi viia:

- pistelise kontrollina vähemalt kaks korda aastas;
- pärast iga turvaintsidenti, mille üheks põhjuseks oli andmebaasi pääsuõiguste puudulik haldus;
- pärast süsteemi iga ümberkorraldust, millega kaasneb oluline muutus andmebaasi kasutajate õigustes;
- pärast andmebaasitarkvara või selle versiooni vahetamist;
- pärast asutuse turvapoliitika ja/või turvaplaani muutusi, mis puudutavad olulisel määral andmebaasi pääsuõiguste diferentseerimist.

Seire tegemine on turvajuhi või tema poolt määratud töötaja kohustus

HT.10 Andmebaasi kannete krüptoaheldamine

M 2.130 Andmebaasi tervikluse tagamine parameetrite seadmine

Lisaks andmebaasi tervikluse tagamise nõuetele tuleb andmebaasi ja selle kannete terviklus tagada krüptoaheldamise meetodiga alljärgnevaid põhimõtteid arvestades:

- Andmebaasi kanded tuleb kronoloogilises järjestuses siduda omavahel krüptograafilise ahelaga (lokaalse ajatempliga), mille juures tuleb kasutada krüptoräside pööramatuse omadust.
- Kasutatud aheldamise võte peab välistama andmete märkamatu vahelt kustutamise.
- Kasutatud krüptovahendid peavad vastama HT.52 Lisanõuded krüptovahenditele nõuetele.
- Kindlaksmääratud töötajale tuleb teha kohustuseks nimetatud ahela tervikluse perioodiline kontroll. See nõue peab olema dokumenteeritud tema töölepingus, ametijuhendis või nende lisades.

Kui eelnimetatud krüptoaheldamist ei ole mingil põhjusel võimalik läbi viia, saab turvajuht teha siin erandi ja asendada selle piisaval tasemel organisatoorsete ja tehniliste turvameetmete kogumiga. Sel juhul peab turvajuht läbi viima põhjaliku riskianalüüsi ja veenduma, et sellega ei tekitataks äripoole jaoks talumatuid turvariske.

HT.11 Infoturbe regulaararuanded juhtkonnale

M 2.200 Infoturbearuanded juhtkonnale ja hinnangud infoturbele parameetrite seadmine

Lisaks infoturbeanuanded juhtkonnale ja hinnangud infoturbele soovituslikes meetmetes sätestatule peab infoturbe aruanne sisaldama:

- teavet kõigi turvaintsidentide kohta ning olulisimat rünnete avastamise ja intsidentide uurimise kohta;
- teavet (statistikat) olulisimate ja ohtlikemate ründekatsete kohta;
- teavet süsteemi turva-alaste üldiste muutmisvajaduste kohta tulevikus;
- teavet vajalike eelseisvate turvakoolituste pidamise kohta (nii sisemine kui ka väline koolitus, vt M 2.197 Töötajate kaasamine turbeprotsessi).

Lisaks korralistele aruannetele tuleb pärast turvaintsidenti koostada erakorraline aruanne hiljemalt nädal pärast viimaste taastemeetmete rakendamist.

Aruandeid tuleb esitada regulaarselt kord kvartalis.

HT.13 Tulemüüri konfiguratsioonimuudatuste krüptoaheldamine

M 4.47 Turvalüüsi operatsioonide logimine parameetrite seadmine

Lisaks turvalüüsi operatsioonide logimise nõuetele tuleb tulemüüri konfiguratsioonimuudatuste logikirjete terviklus tagada krüptoaheldamise meetodiga:

- Tulemüüri konfiguratsioonimuudatuste logikirjed tuleb kronoloogilises järjestuses siduda omavahel krüptograafilise ahelaga (lokaalse ajatempliga), mille juures tuleb kasutada krüptoräside pööramatuse omadust.
- Kasutatud aheldamise võte peab välistama andmete märkamatu vahelt kustutamise.
- Kasutatud krüptovahendid peavad vastama HT.52 Lisanõuded krüptovahenditele nõuetele.
- Kindlaksmääratud töötajale tuleb teha kohustuseks kontrollida perioodiliselt nimetatud ahela terviklust ning see peab olema dokumenteeritud tema töölepingus, ametijuhendis või nende lisades.

HT.14 Süsteemi tegevuslogide krüptoaheldamine

M 4.93 Regulaarne tervikluse kontroll parameetrite seadmine

Lisaks regulaarse tervikluse kontrolli nõuetele tuleb süsteemi operatsioonide kirjete logide terviklus tagada krüptoaheldamise meetodiga:

- Süsteemi operatsioonide kirjed tuleb kronoloogilises järjestuses siduda omavahel krüptograafilise ahelaga (lokaalse ajatempliga), mille juures tuleb kasutada krüptoräside pööramatuse omadust.
- Kasutatud aheldamise võte peab välistama andmete märkamatu vahelt kustutamise.
- Kasutatud krüptovahendid peavad vastama HT.52 Lisanõuded krüptovahenditele nõuetele.
- Kindlaksmääratud töötajale tuleb teha kohustuseks kontrollida perioodiliselt nimetatud ahela terviklust ning see peab olema dokumenteeritud tema töölepingus, ametijuhendis või nende lisades.

Meetme M 5.25 Saate- ja vastuvõtulogide kasutamine juures on eeltoodud nõuded soovituslikud, kui need pole tagatud organisatsiooniliste ja füüsiliste turvameetmete koosmõjuga.

Vt ka M 4.34 Krüpteerimise, kontrollsummade ja digitaalallkirjade rakendamine , kus antud soovituslikud nõuded on siin kohustuslikud.

HT.16 Serverilogi krüptoaheldamine

M 5.9 Serveri logi parametriseering

Lisaks serveri logile esitatavatele nõuetele tuleb:

- Serveri krüptoaheldatud logi kirjed kronoloogilises järjestuses siduda omavahel krüptograafilise ahelaga (lokaalse ajatempliga), mille juures tuleb kasutada krüptoräside pööratamatuse omadust (kasutatavad algoritmid peavad vastama HT.52 Lisanõuded krüptovahenditele nõuetele)
- Kasutatud aheldamise võte peab välistama andmete märkamatu vahelt kustutamise.
- Kellelegi töötajatest tuleb teha kohustuseks kontrollida perioodiliselt nimetatud ahela terviklust ning see peab olema dokumenteeritud tema töölepingus, ametijuhendis või nende lisades.

HT.17 Krüptoaheldatud saate- ja vastuvõtulogid

M 5.25 Saate- ja vastuvõtulogide kasutamine parametriseering

Andmete saate- ja vastuvõtulogide kirjed tuleb kronoloogilises järjestuses siduda omavahel krüptograafilise ahelaga (lokaalse ajatempliga), mille juures tuleb kasutada krüptoräside pööratamatuse omadust. Kasutatavad krüptoalgoritmid ja -protokollid peavad vastama HT.58 Lisanõuded tarbetute kontode ja terminalide blokeerimisele nõuetele.
Kasutatud aheldamise võte peab välistama andmete märkamatu vahelt kustutamise võimaluse.

Kindlaksmääratud töötajale tuleb kohustuseks teha kontrollida perioodiliselt nimetatud ahela terviklust ning see peab olema dokumenteeritud tema töölepingus, ametijuhendis või nende lisades.

HT.23 Muudatuste eelnev turvajuhi poolne kinnitamine

M 2.427 Muudatustaotluste kooskõlastamine parameetrite seadmine

Muudatustaotluste kooskõlastamise meetmes käsitletud muudatustest tuleb arvestada asutuse suurust ja võimalust lisada turvajuhile kinnitamise kohustusi järgnevates valdkondades:

- tark- ja riistvara muudatused (uuendused, modifikatsioonid jms);
- võrkude topoloogia muutmine, kokku- ja lahkuühendamine, seadmete väljavahetamine;
- tööruumide funktsioonide muutmine.

Vajaduse korral võib turvajuht pidada nõu juhtkonnaga (juhul kui modifikatsioon puudutab asutuse mitut valdkonda).

HT.26 Serveriruumi ja andmearhiivi külastajate logiraamatu pidamine

Unikaalmeede

Sisse tuleb viia serveriruumi ja andmearhiivi külastajaid ja külastusi kajastav logiraamat.

Selles tuleb dokumenteerida:

- iga külastusaja algus ja lõpp;
- iga külastaja nimi;
- külastaja vastuvõtnud töötaja nimi;
- külastuse põhjus (vajadusel);
- külastatud ruumide loetelu.

Kui nimetatud logiraamatut peetakse digitaalselt, tuleb halduslike, infotehnoloogiliste või füüsiliste vahenditega tagada, et raamatusse kantud kirjeid ei saaks hiljem muuta ega kustutada.

HT.29 Kombineeritud autentimise nõue

M 4.133 Sobivate autentimismehhanismide valimine parameetrite seadmine

Lisaks sobivate autentimismehhanismide valimisele esitatavatele nõuetele on keelatud autentimine viisil, mis kasutab ainult teadmuslikku pääsutõendit (parooli) või biomeetrilist vahendit (nt sõrmejälge) ja ei kasuta teisi autentimisviise (ese, MAC-aadress vms).

Soovitavaks autentimisevahendiks on Eesti ID kaart, mobiil-ID kaart või muu sellega funktsioonidelt ja ülesehituselt (kahefaktoriline autentimine) sarnane vahend. Selle all mõeldakse eelkõige parooliga käivitatavat seadet, mis sisaldab avaliku võtmega krüptoalgoritmi ning mis on eelnevalt genereerinud avaliku võtmega krüptoalgoritmi võtmepaari nii, et privaatvõtit ei saa seadmest välja lugeda, vaid üksnes kasutada seadme sees.

Seadmes kasutatavad krüptovahendid peavad vastama HT.52 Lisanõuded krüptovahenditele nõuetele.

HT.31 Arhiveerimisel kasutatavate andmekandjate regulaarkontroll

M 1.60 Arhiivi-andmekandjate asjakohane säilitus parameetrite seadmine

Lisaks arhiivi-andmekandjate asjakohasele säilitusele esitatavatele nõuetele, tuleb vähemalt kord kahe aasta tagant läbi vaadata arhiveerimiseks kasutatavate andmekandjate sobivus andmete pikaajaliseks säilitamiseks.

Turvaintsidendi ilmnemisel, mille üheks osaks osutub arhiveerimiseks ebasobivate andmekandjate kasutamine või sellega seotud muud tõrked, tuleb läbi viia erakorraline läbivaatus hiljemalt kaks nädalat pärast nimetatud turvaintsidendi uurimise lõppu.

HT.34 Digiallkirja kasutamine

M 2.265 Digitaalallkirjade õige kasutamine arhiveerimisel ja M 4.34 Krüpteerimise, kontrollsummade ja digitaalallkirjade rakendamine parameetrite seadmine

Lisaks ülaltoodud meetmetele esitatavatele nõuetele tuleb lähtuda alljärgnevast:

- Iga asutus peab ise hindama, millist tõestusväärtust tema andmed omama peavad ning sellest lähtuvalt otsustama, kas tuleb kasutada inimese enda digitaalset allkirja või digitaalset templit.
- Tõestusväärtuslike (turvaosaklassiga T3) andmete ja dokumentide juures on keelatud kasutada digitaalsignatuuri mehhanisme, mis ei vasta (eriti infrastruktuuri osas) Eesti Vabariigi digitaalallkirja seaduse nõuetele (siia klassifitseeruvad nt PGP- ja GnuPG-signatuurid).
- Digiallkirjastamata võib jätta tehnilisi ja –tugiandmeid. Kui soovitakse jätta digiallkirjastamata jätta osa andmebaasi või infosüsteemi põhiandmeid, siis tuleb luua ISKE mõttes mitu turvatsooni ning digiallkirjastamata andmed viia madalamasse tsooni, mille terviklusosaklass on T2 või väiksem.

HT.35 Tavalise faksiteenuse kasutuskeeld

Unikaalmeede

Keelatud on kasutada tavalist faksiteenust läbi turvamata telefonivõrgu, st läbi võrgu, mille korral ei ole välistatud andmete pealtkuulamine ja/või aktiivse salaharundi tekitamine. Erandiks on olukorrad, kus kogu faksiteenuse telefoniliin on krüpteeritud (vastavalt HT.52 Lisanõuded krüptovahenditele nõuetele) ja autenditav (nt faks VoIP lahenduse kaudu, kui kasutatakse VPN vahendeid või muud turvalist kaugpöördusprotokolli TCP/IP kaudu).

Vt lisaks M 3.15 Kõigi töötajate juhendamine faksi kasutamise alal ja M 6.69 Faksiserverite avariiplaan ja rikkekindluse tagamine .

HT.36 Tavalise automaatvastaja kasutuskeeld

Unikaalmeede

Keelatud on süsteemis kasutada automaatvastajaid läbi turvamata telefonivõrgu, st läbi võrgu, mille korral ei ole välistatud andmete pealtkuulamine ja/või aktiivse salaharundi tekitamine. Erandiks on olukorrad, kus kogu telefoniliin on krüpteeritud (vastavalt HT.52 Lisanõuded krüptovahenditele nõuetele) ja autenditav (nt faks VoIP lahenduse kaudu, kui kasutatakse VPN vahendeid või muud turvalist kaugpöördusprotokolli TCP/IP kaudu).

HT.37 Andmete krüpteerimise nõue transpordil ja salvestamisel

Unikaalmeede

Kõrge konfidentsiaalsus- või terviklusnõude (juhul, kui andmed ei ole digitaalselt allkirjastatud/tembeldatud) korral tuleb nii kohtvõrgu salvestite, kui ka salvestivõrkude puhul kasutada andmete krüpteerimist. Põhimõtteliselt tuleb tagada andmete krüpteerimine nii edastamisel (*data in flight*) kui ka salvestatuna (*data at rest*).

Salvestatud andmete krüpteerimisel peaksid andmed olema enne krüpteerimist tihendatud. Eksponeeritud on vaid meta-andmed, nii on tagatud andmebaasi halduss üsteemidele ja salvestisüsteemidele vajalik info andmete halduseks, kuigi failid ise ei ole nähtaval. Pääsukontrolli mehhanismid peavad tagama volitatud ligipääsu andmetele, ning logima kõik andmete edastamise juhud.

Samuti tuleb andmed krüpteerida edastamisel salvestisüsteemist rakenduse või kliendini ja vastupidi. See eeldab krüpteerimistarkvara olemasolu nii salvestisüsteemis ja ka serveris või kliendiarvutis. Kohtvõrgu salvestite ja IP-põhise andmeülekande puhul saab reeglina rakendada IPSec tunnelit ning sageli on võimalik kasutada ka TLSi (SSLi). *Fibre Channel* salvestivõrgu puhul tuleb kasutada teisi protokolle, näiteks FC-SP protokolli. Kõrge turbeastme korral tuleb kasutada alati avalikke krüpteerimisalgoritme.

Lisaks tarkvaralise krüpteerimisele võib kasutada ka erinevaid riistvaralisi krüpteerimisseadmeid. Sellised seadmeid on võimalik kasutada nii salvestatud salvestiste kui ka andmeedastuse krüpteerimiseks. Krüpteerimisseadmed ja -algoritmid peavad vastama HT.52 Lisanõuded krüptovahenditele nõuetele.

HT.38 Windows Server 2003 krüpteeritud failisüsteemi kasutus

M 4.278 EFS-i turvaline kasutamine Windows Server 2003 keskkonnas parametriseering

Ülaltoodud meetmes toodud soovituslikud nõuded on siin kohustuslikuks täitmiseks. Lisaks tuleb arvestada kolme järgmist aspekti:

- Backup'i konto ei tohi olla Data Recoveri Agent;
- EFS-i kasutamisel tuleb DRA -le korraliku võtme halduse ja protseduuridega võtmed määrata;
- DRA privaatvõtit ei tohi hoida arvutite kõvaketastel, selle hoidmiseks ja kasutamiseks tuleb ette näha põhjalik protseduur.

HT.39 SAP'i parooli tugevdamine

Unikaalmeede

Alates SAP'i versioonidest *Web AS ABAP 7.00* või *Netweaver 2004s* on võimalik kasutada tugevamaid kasutajaparoole. SAP süsteem eristab alates nimetatud versioonist paroolide suur- ja väiketähti ja parooli pikkus on 40 tähemärki endise 8 asemel. Uute kasutuselevõetud SAP süsteemide puhul on uued paroolireeglid automaatselt rakendatud. Selleks, et vältida SAP versiooni uuendamisest tingitud probleeme, on uuendatud süsteemis tagatud ka vanade paroolide jätkuv kasutamine, mille maksimaalpikkus on 8 tähemärki ning kus suur- ja väiketähti ei eristata. Kasutaja põhiandmetes on kirje, mis määrab, kas kasutatakse uut või vana tüüpi parooli. Seda informatsiooni analüüsitakse parooli kontrollimisel. Vana tüüpi parooli puhul konverteeritakse esimesed kaheksa märki suurtähtedeks ja ülejäänud 32 märki täidetakse tühikutega. Uut tüüpi parooli kasutamise korral analüüsitakse kogu parooli ilma konverteerimata.

Uuteks parooli seadistuse parameetriteks on:

- *login/min_password_lowercase*
- *login/min_password uppercase*
- *login/password_downwards_compatibility*

Kui kasutuses on varasem SAP süsteemi versioon, mis ei võimalda uute tugevate paroolide kasutamist, tuleks kõrge konfidentsiaalsus või terviklusnõude korral kaaluda SAP süsteemi versiooni uuendamise võimalust. Kui sooritatakse versiooniuuendus, tuleb konfigureerida parooli reeglid, mis tagaksid, et järgmise paroolivahetuse käigus vastaksid paroolid meetme HG.6 Arvuti paroolkaitse rangemad reeglid nõuetele

Sättega login/password_compliance_to_current_policy = 1 saab sundida paroolivahetuse kasutajatele, kelle parool ei vasta uuendatud nõuetele.

HT.42 VPNi kasutuskohustus traadita võrgus

Unikaalmeede

Kõrge terviklusastme (T3) ja/või konfidentsiaalsusastme (S3) korral tuleb traadita võrgu kasutamisel alati kohustuslikus korras kasutada turvalist VPN-ühendust. Loodav või kasutatav VPN-lahendus peab vastama M 2.415 VPN vajaduste analüüs , M 2.416 VPNi kasutamise planeerimine , M 2.417 VPNi tehnilise teostuse planeerimine , M 2.418 VPNi kasutamise turvapoliitika koostamine , M 2.419 Sobivate VPN-toodete valimine , M 2.420 Trusted VPN teenusepakkuja valimine .

HT.43 Keskse autentimisserveri kasutamine

M 5.138 RADIUS serverite kasutamine parametriseering

RADIUS serverite kasutamisele toodud soovituslikud nõuded on siin kohustuslikuks täitmiseks. Keskse autentimisserveri (RADIUS või analoogne) kasutamine on siin kohustuslik ja see peab vastama meetme M 4.250 Keskse võrgupõhise autentimisteenuse valimine tingimustele ja nõuetele.

HT.44 Lisanõuded turvaustele ja -akendele

M 1.10 Turvauksed ja -aknad parametriseering

Lisaks turvaustele ja -akendele kehtivatele nõuetele peavad:

- turvauksed (standardi EVS-EN 1627:2011 RC 1 N, RC 2N, RC 3N, . . . kohaselt 1. klassi nõuetele vastavad) olema igal turvaosaklassiga T3 või S3 serveriruumil või andmearhiivil;
- turvaaknad (standardi EVS-EN 1627:2011 RC 1 N, RC 2N, RC 3N, . . . kohaselt 1. klassi nõuetele vastavad vastavad) olema igal turvaosaklassiga T3 või S3 serveriruumil või andmearhiivil;
- turvaaknad olema varustatud valgust hajutava klaasi või spetsiaalse hajutiga, mis ei võimalda väljastpoolt näha ruumi sisse.

Nõuded ei kehti nende andmearhiivide korral, kus arhivaalid on seifis, millel on EVS-EN 1627:2011 RC 1 N, RC 2N, RC 3N, . . . järgi 1. klassi murdmiskindlus ning mis on spetsiaalselt hoonekonstruktsioonide külge kinnitatud, et oleks välistatud nende äraviimine.

HT.47 Lisanõuded hooldustöödele ja remondile

M 2.4 Hooldus- ja remonditööde reeglid parameetrite seadmine

Lisaks hooldus- ja remonditööde reeglitele kehtestatud nõuetele peab iga hooldus- ja remonditööde tegijaga olema sõlmitud konfidentsiaalsuskohustusleping, mis sisaldab muuhulgas ka asutuse turvapoliitikas määratud tasemele vastavaid leppetrahve. Lisaks konfidentsiaalsuskohustusele tuleb lepinguliselt reguleerida ka volitamata (sh kuritahtlike) modifitseeringute ärahoidmine, mis tuleb terviklusosklassi T3 korral samuti reguleerida turvapoliitikas sätestatud turvaeesmärkidega kooskõlas olevas mahus leppetrahvidega.

HT.48 Lisanõuded krüptolahenduste võtmehaldusele

M 2.161 Krüptokontseptsiooni väljatöötamine parametriseering

Krüpteerimist sisaldavate süsteemide kavandamisel peab lisaks krüptokontseptsiooni väljatöötamise nõuetele lähtuma lisapiirangutest, mis puudutavad tervikluse ja/või konfidentsiaalsuse kaitseks kasutatavate krüptolahenduste võtmete haldust

Soovitatavalt tuleb võtmeid hoida pöördkonstrueerimatutes (*non-reverse engineerable*) riistvaraseadmetes (nagu Eesti ID-kaart, üldkasutatav riistvaraline turvamoodul HSM vms), kus neid saab kasutada, kuid millest ei saa neid välja lugeda.

Kui pöördkonstrueerimatut riistvaraseadet ei saa mingil põhjusel kasutada, siis võib võtmeid hoida sümmeetrilise algoritmiga krüpteeritult, kus dešifreerimisvõti arvutatakse kasutaja paroolist. Kasutatavad paroolid peavad siin vastama HG.6 Arvuti paroolkaitse rangemad reeglid nõuetele ja kasutatavad krüptoalgoritmid HT.52 Lisanõuded krüptovahenditele nõuetele.

Deponeeritud võtmed – varuvõtmed, mida iga päev ei kasutata – tuleb hoida turvajuhi vastutusalas seifis või spetsiaalses lukustatavas ruumis teisaldataval andmekandjal või paberkujul pitseeritud ümbrikus.

Võtmehalduse kinnitab turvajuht (kas eraldiseiseva dokumendina või olemasoleva(te) dokumendi(-tide) osana).

HT.49 Lisanõuded arhiveeritud andmete krüptoatribuutide regenereerimisele

M 2.264 Krüpteeritud andmete regulaarne regenereerimine arhiveerimisel parameetrite seadmine

Kui arhiveeritud andmete tõestusväärtus on kaitstud looja/esitaja digiallkirja või -signatuuriga, tuleb lisaks ülaltoodud meetme soovituslikele nõuetele arvestada sellega, et digiallkirja aluseks olevad krüptovahendid aja möödudes nõrgenevad ning ühel hetkel tuleb hakata arhiveeritud andmeid tõestusväärtuse taastamiseks arhiveeriva instantsi poolt ülesigneerima.

Probleem tõstatub tõenäoliselt siis, kui andmeid on tõestusväärtuslikuna (turvaosaklassi T3 nõuetele vastavalt) vaja säilitada üle kümne aasta. Sel juhul tuleb turvajuhi initsiatiivil luua kontseptsioon andmete ülesigneerimiseks (digiallkirja krüptoatribuutide regenereerimiseks) ja olla edaspidi, krüptoalgoritmide kriitilist nõrgenemist puudutava esimese signaali korral, valmis reaalseks ülesigneerimiseks.

Nõrgeneva krüptograafilise algoritmiga moodustatud digitaalallkirju on loomulikum kaitsta ajatemplitega, mitte aga ülesigneerimisega.

Nõrgeneva räsifunktsiooni abil moodustatud ajatempliga andmete (sh digitaalallkirjade) regenereerimiseks piisab, kui nii andmetele kui ka nende vananevatele ajatemplitele võetakse uued turvalisemal räsifunktsioonil põhinevad ajatemplid.

Täiendavat teavet vt Eesti Rahvusarhiivi tellimisel koostatud dokumentide pikaajalise tõestusväärtuse tagamise juhendist ning meetmest M 2.265 Digitaalallkirjade õige kasutamine arhiveerimisel .

HT.50 Andmete turvaline haldamine kodu- ja kaugtööl

M 2.112 Kodutööjaamade ja asutuse vahelise dokumentide ja andmekandjate transportimise reguleerimine parametriseering

Kodu- ja kaugtööl tuleb lisaks ülaltoodud meetme soovituslikele nõuetele lähtuda alljärgnevast.

Kodu- või kaugtööl on turvaosaklassidega S3 või K3 andmete töötlemine keelatud.

Juhul kui kodu- või kaugtööl töödeldakse terviklusosaklassiga T3 andmeid, tuleb:

- andmete transporti teostada ainult krüpteeritud kujul (nii nende transportimisel teisaldatava andmekandjaga, süle- ja/või pihuarvutiga kui ka üle võrgu);
- tagada, et eelpoolkasutatavad krüpteerimisvahendid peavad vastama HT.52 Lisanõuded krüptovahenditele nõuetele;
- saada töötlusprotsessile ja kasutatavatele tavadele, seadmetele ja protsessidele turvajuhi kirjalik nõusolek, mille ta annab peale protsessi vastavuse kontrollimist asutuse turvapoliitikaga.

Kõige mugavam variant digiteabe töötlemiseks kodu- ja/või kaugtööl on turvalise VPNi loomine koos tavaga, et töötlusarvutit käsitletakse vaid nn “õhukese” kliendina, kuhu andmeid ja/või dokumente ei salvestata ja mis toimib faktiliselt vaid targa (*smart*) terminalina.

Avalike pääsupunktide kasutamisel (vt M 2.389 Avalike pääsupunktide turvaline kasutus) tuleb arvestada, et kasutada ei tohi võõrast arvutit (nt avalikus internetipunktis) ega kasutajaliideseid (laenatud väline hiir, klaviatuur vms), vaid üksnes avaliku pääsupunkti poolt pakutavat standardprotokolset (reeglina WiFi) välisühendust.

HT.51 Lisanõuded teabe hankimisele turvaaukude kohta

M 2.35 Teabe hankimine turvaaukude kohta parametriseering

Lisaks teabe hankimisel turvaaukude kohta sätestatud nõuetele tuleb alati kohustuslikus korras hankida teavet kolmest erinevast allikast:

- suhtluskanalid tarnijate/tootjatega;
- kaks erinevat üldist turvaaukude teavitamisele orienteeritud süsteemi (turvaportaali), mis ei ole seotud ühegi konkreetse tootjaga.

Nimetatud teabe hankimine on süsteemiadministraatorite ülesanne, millega nad peavad tegelema isiklikult, seda kohustust üleandmata.

HT.52 Lisanõuded krüptovahenditele

M 2.164 Sobiva krüptoprotseduuri valimine Digiarhiiv

Lisaks sobiva krüptsoprotseduuri valimise nõuetele tuleb krüptovahendite valikul lähtuda alljärgnevast:

- Krüptoalgoritm- ja/või protokoll peab olema avalikustatud – või tehtud kättesaadavaks krüptoanalüütikutele selle turvalisuse hindamiseks – vähemalt kaks aastat tagasi. Suletud kirjeldusega krüptovahendid peavad olema läbinud turvaauditi, mille käigus on veendutud nende murdmatuses. Viimasel juhul peab asutuse turvajuht veenduma niisuguse suletud turvaauditi usaldusväärsuses ja seda aktsepteerima.
- Sümmeetrilise krüptoalgoritmi (efektiivne) võtmepikkus peab olema vähemalt 192 bitti ja algoritmil ei tohi olla teada olulist võitu (enam kui 8-16 korda ajalist võitu) andvaid krüptoanalüütilisi võtteid.
- Räsifunktsioonide MD2, MD4 ja MD5 kasutamine on täielikult (ilma igasuguste eranditeta) keelatud olenemata nende kasutuskohast, -otstarbest ja -viisist.
- Kui krüptoräsisid kasutatakse andmete tõestusväärtuse (tervikluse) tagamiseks enamaks kui kümneks aastaks, peab kasutatavate räsifunktsioonide väljund (räsi pikkus) olema vähemalt 256 bitti. Seega on sel juhul räsifunktsioonide RIPEMD- 160 ja SHA-1 kasutamine keelatud. Soovitav on sel juhul kasutada SHA-2 perekonda kuuluvad räsifunktsioone või RIPEMD pikema räsiga variante.
- Kui avaliku võtmega krüptoalgoritmi kasutatakse niisuguse digisignatuuri koosseisus, mis peab tagama andmete tõestusväärtuse enamaks kui kümneks aastaks, peab RSA võtmepikkus olema vähemalt 1536 bitti. Kaasajal tavalise 1024se RSA kasutamine neil juhtumeil on keelatud.
- Kui avaliku võtmega krüptoalgoritmi kasutatakse niisuguse digisignatuuri koosseisus, mis peab tagama andmete tõestusväärtuse enamaks kui 15 aastaks, peab RSA võtmepikkus olema vähemalt 4096 bitti. Kaasajal tavalise 1024se RSA kasutamine neil juhtumeil on keelatud.

HT.53 Lisanõuded paroolisalvestusvahenditele

M 4.306 Paroolisalvestusvahenditega ümberkäimine parameetrite seadmine

Lisaks paroolisalvestusvahenditega ümberkäimise nõuetele tuleb paroolisalvestusvahendite kasutamisel arvestada alljärgnevaga:

- Kui paroolisalvestusvahend ei põhine pöördkonstrueerimatul riistvaraseadmel, vaid krüpteerituna salvestamisel, peavad kasutatavad krüptovahendid vastama HT.52 Lisanõuded krüptovahenditele nõuetele ning krüpteerimiseks kasutatav *master* -parool HG.6 Arvuti paroolkaitse rangemad reeglid nõuetele.
- Paroolisalvestusvahend (selle kasutatav versioon) peab olema olnud turul vähemalt ühe aasta, et eksperdid oleksid saanud veenduda turvaaukude puudumises.
- Paroolisalvestusvahend ja selle kasutuskord peavad saama turvajuhi kirjaliku heakskiidu.

HT.54 Lisanõuded turvafunktsioonide rakendamisel

M 4.42 Turvafunktsioonide rakendamine IT-rakenduses parameetrite seadmine

Lisaks turvafunktsioonide rakendamisele IT-rakenduses nõuetele tuleb veenduda, et tüüptarkvara dokumentatsioonis mainitud turvafunktsioonid oleksid ka tegelikult realiseeritud ja toimiksid vastavalt kirjeldustele. Selleks on üldjuhul piisav kasutada üldkasutatavates tarkvara- ja turvafoorumites (nt *www.securityfocus.com*) olevat aktuaalteavet. Turvajuhi erinõudmisel võib rakendada lisa-turvatestimisi, kui süsteemi turvapoliitika ja tarkvaratoote turvakriitilisus seda nõuavad.

HT.55 Värske tarkvara kasutuskeeld

Unikaalmeede

Turvaosaklassiga T3 andmete töötlemisel kasutatav tüüptarkvara (selle versioon) ei tohi olla olnud kasutuses vähem kui poolteist aastat. Uuema tarkvara kasutamisel ei ole kriitilised turvaaugud ja - puudused sealt veel piisava põhjalikkusega üles leitud ning ära paigatud.

Keeld ei kehti juhul kui:

- uus versioon on välja antud spetsiaalselt turvaaugu parandamiseks ning algne versioon on vanem kui poolteist aastat;
- vastava funktsionaalsusega vanem tarkvara turul puudub - sel juhul tuleb korraldada spetsiaalne turvatestimine ning turvajuht peab kasutamise kui erandi (vt M 2.380 Erandite kooskõlastamine) aktsepteerima ja kinnitama.

HT.56 Lisanõuded mobiilsele kaugtööarvutile

M 4.63 Kaugtöökohaarvutite turvanõuded parametriseering

Juhul kui väljaspool kodutöökohta kasutatava mobiilse kaugtööarvutiga töödeldakse turvaosaklassi T3 andmeid, tuleb lisaks kaugtöökohaarvutite turvanõuetes kirjeldatule juhinduda veel järgmistest nõuetest:

- Arvuti kogu kettasisu peab olema krüpteeritud vastavalt HT.63 Sülearvutite krüpteerimine ja HT.67 Pihuarvutite krüpteerimine nõuetele. Šifreerimiseks/dešifreerimiseks kasutatav võti peab olema arvutatav arvuti käivitamisel sisestatavast paroolist, mis peab vastama HG.6 Arvuti paroolkaitse rangemad reeglid nõuetele.
- Töö lõpetamisel turvaosaklassiga S3 või T3 andmetega tuleb arvuti alati välja lülitada, seda ei tohi viia säästurežiimile (*stand-by*). Kui talveunne (*hibernating*) viimisel kirjutatakse andmed kettale krüpteeritult, on selline tegevus lubatud, kui mitte, siis pole ka talveune kasutamine lubatud.
- Mobiilse kaugtööarvuti kasutamine koos kasutatavate tavade ja konfiguratsiooniga tuleb turvajuhiga kokku leppida, kes sätestab kirjalikult kinnitatud reeglid.

Ülaltoodud nõuded kehtivad kõikide mobiilkasutuses seadmete (sülearvuti, pihuarvuti/PDA, nutitelefon, lisavõimalustega GPS-navigaator, programmeeritav raadiojaam vms) korral. Kaasajal on turul arvukalt hübriidseadmeid, millede lahterdamine ühte või teise eelnimetatud kategooriatest on väga raske.

Siinjuures tuleks tõsiselt kaaluda mobiilkasutuses olevate seadmete kasutamist ka turvaosaklassiga T3 andmete töötlemiseks, kuna vastavalt heale tavale hoitakse niisugused seadmed (eelkõige mobiiltelefonist väljaarenenud pihuarvutid) pidevalt sisselülitatuna, siin lisandub aga väljalülitamisnõue. Lõpliku otsuse niisuguste seadmete kasutamiseks teeb asutuse turvajuht, kaaludes käideldavusest saadavaid lisaväärtusi lisanduvate turvariskidega.

HT.57 Algparoolide muutmise regulaarkontroll

Unikaalmeede

Juhul kui süsteem ei ole võimeline automaatselt nõuda algparoolide vahetamist, siis tuleb pisteliselt kontrollida algparoolide muutmist (meetme M 4.7 Algparoolide muutmine nõuded) vähemalt kaks korda aastas. Kontrolli peab teostama turvajuht või tema määratud isik või isikud.

HT.58 Lisanõuded tarbetute kontode ja terminalide blokeerimisele

M 4.17 Tarbetute kontode ja terminalide blokeerimine parametriseering

Lisaks tarbetute kontode ja terminalide blokeerimise nõuetele tuleb pisteliselt, vähemalt kaks korda aastas kõiki kontosid ja terminale nende kasutatavuse seisukohalt kontrollida, millele peab järgnema tarbetute blokeerimine. Nimetatud regulaarkontrolli peab teostama turvajuht või tema määratud isik(ud).

HT.59 Lisanõuded turvalisele sisselogimisele

M 4.15 Turvaline sisselogimine parametriseering

Lisaks turvalise sisselogimise nõuetele tuleb sisselogimisel kasutada lisaks paroolipõhisele autentimisele ka kombineeritud autentimist – parool + kiipkaart (nt ID-kaardi tehnika), parool + biomeetria vms.

Nõuet ei ole vaja rakendada juhtumitel, kui autentimine on murdmatu tehnika abil piiritletud vaid kindlas füüsilises paigas asuva arvutiga/terminaliga (nt MAC-aadress + arvuti paiknemine suletud tsoonis), millele on ligipääs füüsiliste või halduslike turvameetmetega piiratud. Viimasel juhul on mõistlik kasutada nt VPN-tehnikat.

HT.60 Lisanõuded tarbetute liinide kõrvaldamisele

M 5.1 Tarbetute liinide kõrvaldamine või lühistamine ja maandamine parameetrite seadmine

Lisaks tarbetute liinide kõrvaldamise, lühistamise või maandamise nõuetele tuleb kõrgtasemel tervikluse ja konfidentsiaalsusega tsoonides:

- ühe tööpäeva jooksul peale andmekaabelduse modifitseerimist kõrvaldada sellised tarbetud liinid, mis viivad kõrgastme tsoonist mingisse teise turvatsooni (kui asutuses on kasutuses mitu turvatsooni):
- neli korda aastas teha tarbetute andmekaablite pistelist seiret, kusjuures põhitähelepanu tuleb pühendada nendele liinidele, mis võivad viia kõrgastmel turbega tsoonist mingisse madalamate nõuetega tsooni.

Erinevalt M 5.1 Tarbetute liinide kõrvaldamine või lühistamine ja maandamine kirjeldatud tegevustest korraldab eelnimetatud seiret turvajuht. Vt ka meede M 5.144 IT-kaabelduse demonteerimine .

HT.61 Kataloogiteenuse sidumine rahvusliku PKIga

M 2.404 Kataloogiteenuse turvakontseptsiooni koostamine parametriseering

Lisaks kataloogiteenuse turvakontseptsiooni koostamise nõuetele tuleb loodav kataloogiteenus kohustuslikus korras sertifikaatide kaudu siduda Eesti rahvusliku avaliku võtme infrastruktuuriga (PKI), mis omakorda vastab Eesti Vabariigi digitaalallkirja seaduse esitatud nõuetele

HT.63 Sülearvutite krüpteerimine

M 4.29 Kaasaskantavatele IT-süsteemidele mõeldud krüpteerimistoote kasutamine parameetrite seadmine

Lisaks ülaltoodud meetmes välja toodud nõuetele tuleb juhinduda alljärgnevast:

- Kõigil füüsiliselt turvatud tsoonist välja viidavatel (nt kodus töötamiseks kasutatavatel) sülearvutitel on kohustuslik kasutada kogu kettasisu krüpteerimist.
- Kasutatavad krüptovahendid peavad vastama HT.52 Lisanõuded krüptovahenditele nõuetele.
- Krüpteerimistarkvaral ei tohi olla turvaauke, mis võimaldavad parooli teadmata ja/või autentimisseadet omamata juurdepääsu mistahes andmetele sülearvuti kettal.

HT.65 Lisanõuded teisaldatavate andmekandjate kasutusele

M 2.3 Andmekandjate haldus ja M 4.32 Andmekandjate füüsiline kustutamine enne ja pärast nende kasutamist parameetrite seadmine

Lisaks ülaltoodud meetmete nõuetele tuleb teisaldatavate andmekandjate (välkmälud/mälupulgad/mälukaardid, välised kõvakettad jms) käitlemisel pidada nende üle arvestust, dokumenteerides:

- andmekandja tüübi;
- töötaja nime, kelle valduses on see andmekandja;
- andmete liigid, mida selle kandjaga edastatakse;
- kõigi selle andmekandja kasutamise kontrollimise ajad;
- andmekandja andmise/äravõtmise aja.

Kõigil füüsiliselt turvatud tsoonist välja viidavate väliste teisaldatavate korduvkirjutatavate andmekandjatel on kohustuslik kasutada kõigi kandjal olevate andmete krüpteerimist, mis peab vastama HT.52 Lisanõuded krüptovahenditele nõuetele. Kasutataval krüpteerimistarkvaral ei tohi olla turvaauke, mis võimaldavad parooli teadmata ja/või autentimisseadet omamata juurdepääsu mistahes andmetele korduvkirjutataval andmekandjal.

Kaks korda aastas tuleb pisteliselt kontrollida asutuses olevate teisaldatavate korduvkirjutatavate andmekandjate (mälupulgad, välised kõvakettad jms) kasutusreegleid ning nendest kinnipidamist. Kui ilmneb turvaintsident, mille üheks osaks oli teisaldatavate korduvkirjutatavate andmekandjate kasutuse väär korraldus või kasutamisreeglite eiramine, tuleb läbi viia erakorraline läbivaatus hiljemalt kaks nädalat pärast nimetatud turvaintsidendi uurimise lõppu. Niisuguse kontrolli organiseerimine on turvajuhi kohustus.

HT.67 Pihuarvutite krüpteerimine

M 4.228 Pihuarvutite turvamehhanismide rakendamine parameetrite seadmine

Lisaks pihuarvutite turvamehhanismide rakendamise nõuetele tuleb juhinduda alljärgnevast:

- Kõigil füüsiliselt turvatud tsoonist välja viidavatel (nt kodus töötamiseks kasutatavatel) pihuarvutitel (PDA) on kohustuslik kasutada kõikide andmete krüpteerimist.
- Kasutatavad krüptovahendid peavad vastama HT.52 Lisanõuded krüptovahenditele nõuetele.
- Krüpteerimistarkvaral ei tohi olla turvaauke, mis võimaldavad parooli teadmata ja/või autentimisseadet omamata juurdepääsu mistahes andmetele sülearvuti kettal

Juhul kui pihuarvuti ehitus ei võimalda eeltoodud tingimustele vastavat krüpteerimist, ei tohi seda väljaspool turvatsooni T3 ega S3 turvaosaklassiga andmete töötlusel kasutada.

HT.68 OWASP rünnete vastased lisakaitsemeetodid

M 2.363 SQL-injektsiooni kaitse parametriseering

Lisaks SQL-injektsiooni kaitse nõuetes sätestatule tuleb juhinduda järgmistest nõuetest:

- OWASP ründemeetodite edetabeli 10 esimese meetodi vastu (SQL Injection jt) tuleb rakendada lisakaitsemeetodeid.
- Vähemalt kaks korda aastas tuleb pisteliselt kontrollida kõikide andmebaasisisestuste parameetrite filtreerimist. Vastav kontroll on turvajuhi vastutusalas.
- Uued või oluliselt modifitseeritud andmebaasisüsteemid tuleb enne nende evitamist praktikasse lasta spetsiaalselt kontrollida SQL-injektsiooni vastu pikaaegset kogemust omavate praktikute poolt (soovitavalt väljastpoolt oma asutust). Soovitav on sarnaseid tegevusi teha ka teiste OWASP edetabelisse kuuluvate ründemeetodite korral.
- Äärmiselt soovitav on andmebaasisisestuste parameetrite filtreerimisel kasutada põhisüsteemist eraldatud valideerimissüsteemi.

HT.69 Lisanõuded salvestivõrgu administreerimiskonfiguratsiooni seirele

M 2.359 Salvestisüsteemide seire ja haldamine parametriseering

Lisaks salvestissüsteemide seire ja haldamise nõuetes sätestatule peab turvajuht kaks korda aastas pisteliselt seirama salvestivõrgu konfiguratsioone, mille järel peab turvajuht kirjalikult kinnitama, et tegelikult realiseeritu vastab asutuse turvapoliitikale (juhul kui realiseeritu on vastuolus asutuse turvapoliitikaga, siis loetleb turvajuht üles konkreetsed puudused). Kui kasutatakse tsentraliseeritud kontrolli, peab ka selle seire kuuluma eeltoodu skoopi.

HT.70 Lisanõuded salvestisüsteemide haldusvõrgule

M 2.357 Salvestisüsteemide haldusvõrgu ehitus parametriseering

Lisaks salvestissüsteemide haldusvõrgu ehituse nõuetes sätestatule peab juhinduma järgmistest nõuetest:

- Käitamistarkvara ja rakenduste haldusjuurdepääsud tuleb serverites alati (ilma eranditeta) siduda eraldi haldusvõrgu võrguaadressiga.
- Kasutamisfaasis võib tugineda ainult turvalistele teenustele, milles kasutatavad krüpteerimisalgoritmid peavad vastama turvameetme HT.52 Lisanõuded krüptovahenditele nõuetele.
- Haldusvõrk peab tootmisvõrgust ilma eranditeta olema füüsiliselt eraldatud (lubatud on tootmisvõrgu ahelate kasutamine haldusvõrgu poolt turvaliste kaugpöördusprotokollide või VPNide poolt, kui need teenused vastavad eelmises punktis toodud nõuetele.

HT.71 Lisanõuded võrguhaldusprotokolli valimisele

M 2.144 Sobiva võrguhaldusprotokolli valimine parametriseering

Lisaks sobiva võrguhaldusprotokolli valimise nõuetele ja soovitustele tuleb siin SNMP kasutamise korral alati lähtuda versioonist 3 (SNMPv3), SNMP vanemate ebaturvaliste ja ebapiisava pääsupoliitikaga versioonide kasutamine on käesoleval juhul keelatud.

HT.72 Turvatunneldamise protokolli kasutuskohustus

M 5.66 TLS-i/SSL-i kasutamine parametriseering

Ülaltoodud meetmes antud soovitus turvatunneldamisprotokolli (SSL ja selle järglane TLS, samuti analoogid) kasutamisele on käesoleval juhul – turvaosaklasside T3 ja S3 puhul – asendatud selle kasutamiskohustusega.

Kohustus rakendub kahel alljärgneval juhtul:

- Kui võrgu, veebiliidese vms kaudu edastatakse konfidentsiaalseid materjale, millest kasvõi osa ei ole eelnevalt, rakenduse tasemel krüpteeritud (vastavalt HT.52 Lisanõuded krüptovahenditele nõuetele).
- Kui võrgu, veebiliidese vms kaudu edastatakse tõestusväärtust vajavaid materjale, millest kasvõi osa ei ole alati sajaprotsendiliselt kaitstud Eesti Vabariigi digitaalallkirja seaduse nõuetele vastava digiallkirja või digitempliga (meetmele HT.34 Digiallkirja kasutamine vastavalt).

Kõigil muudel juhtudel jääb turvatunneldamise protokolli (TLS, analoogid) kasutamine soovituslikuks, mitte kohustuslikuks.

HT.73 Välise sertifikaadi kasutuskohustus

Unikaalmeede

Veebiserveril on kohustuslik kasutada mingi välise osapoole väljaantud sertifikaati, mis peab vastama järgmistele nõuetele:

- Sertifikaadi peab välja andma selline usaldatav kolmas osapool, kes kas osutab nimetatud teenust üldkasutatavalt või temaga on sõlmitud leping, mis kohustab sertifikaatide väljaandmisel tegema seda usaldusväärselt.
- Sertifikaati ei tohi välja anda oma asutuse või kontserni teine haru, kes on sertifikaadi kasutajaga samade omanike käes või juhtimise all.
- Soovitatavalt tuleks võtta sertifikaat firmalt või asutuselt, kellel on sertifitseerimisteenuse osutamise luba digitaalallkirja seaduse mõttes.
- Aegunud sertifikaat tuleb koheselt uuendada, äärmiselt soovitav on seda teha veidi aega enne aegumist.

Vt ka M 4.176 Autentimismeetodite valimine veebilehtede jaoks (mitmed seal soovitatud meetmed on siin kohustuslikud).

HT.74 SAP'i konfiguratsiooni regulaarseire

M 4.269 SAP süsteemi andmebaasi turvaline konfiguratsioon parametriseering

Lisaks meetmes M 2.347 SAP süsteemi regulaarsed turvakontrollid sätestatud turvakontrollidele tuleb lisaks veel SAP süsteemi andmebaasi turvalise konfiguratsiooni nõuetes kirjeldatud kõiki ülejäänud konfiguratsiooni aspekte regulaarselt kontrollida. Nende kontrollimise/ülevaatamise eest vastutab turvajuht ja seda peab tegema pisteliselt vähemalt neli korda aastas. Siia peavad lisanduma veel erakorralised kontrollid, mis tuleb viia läbi järgnevatel juhtumitel (nädala jooksul pärast juhtumit):

- SAP'i tarkvara või serverit uuendatakse;
- toimub turvaintsident, mis on seotud SAP'iga;
- avastatakse turvaauk SAP'is mille kõrvaldamine (paikamine) muudab olemasolevaid seadeid

M 2.E19 ID-kaardi või digi-ID edasiandmiskeeld teisele isikule parametriseering

Kui madala või keskmise turbeastme korral on ülaltoodud turvameetme täitmine vabatahtlik, siis turvaosaklassi T3 või S3 korral on selle meetme täitmine kohustuslik. Lisaks tuleb rõhutada, et ID-kaart tuleb arvutist eemaldada ka töökohast lühiajalisel või lühiajalisena planeeritud lahkumisel – WCsse, kööki kohvi järele, kolleegiga teise tuppa vestlema vms.

M 2.E14 Digitempli turvaline evitamine asutuses parametriseering

Lisaks digitempli turvalise evitamise nõuetele asutuses tuleb arvestada sellise lisanõudega, et ühte peidetud kujul deponeeritud PUK koodi tuleb kindlasti hoida kusagil põhitöökohal. See on vajalik käideldavuskadude ärahoidmiseks PIN/PUK koodi unustamise korral.

Asutuse turvajuht või tema poolt määratud isik peab vähemalt kaks korda aastas tegema digitembeldussüsteemide seiret. Selle käigus tuleb kontrollida järgnevat:

- Tutvuda digitembeldussüsteemide füüsilise asukohaga ja selle vastavusega dokumentides kirjeldatuga.
- Tutvuda digitembeldussüsteemi võtmepaari kasutamise loenduriga.
- Võrrelda digitembeldussüsteemi tegelikke pääsu- ja kasutusõigusi dokumenteerituga.

M 2.E20 ID-kaardi või digi-ID edasiandmiskeeld teisele isikule parametriseering

Lisaks ülaltoodud meetmes väljatoodud nõuetele tuleb arvestada järgmiste nõuetega:

- DOC-, DOCX, XLS- ja XLSX-vormingus dokumentide digiallkirjastamine on ilma igasuguste eranditeta keelatud.

- Võimaluse piires võiks allkirjastatavad dokumendid olla PDF-vormingus.
- Kui infosüsteemi spetsiifika nõuab mingi PDF-vormingust erinevas vormingus dokumentide allkirjastamist, tuleb see kirjalikult kooskõlastada asutuse turvajuhiga. Turvajuht peab enne kooskõlastamist veenduma kasutatava failivormingu turvalisuses, täpsemalt võimatuses tekitada selle vormingu baasil asutuses kasutatavatel juhtudel mitmetähenduslikke dokumente.

Fakultatiivne (vabatahtlik) meede

Enne süsteemide testimist reaalsete ID-kaartidega (või sarnaste vahenditega) tuleb vastavad testid läbi viia test-ID-kaartidega (või sarnaste vahendite testvahenditega). Testvahendite soetamise kohta leiab täpsemat teavet aadressilt http://www. id .ee/index.php? id =30276 .

Lisaks tuleb testkaartide kasutamisel arvestada, et nende kõik funktsionaalsused ei pruugi olla samad päris ID-kaartide funktsionaalsusega – osad teenused võivad olla testkaartidega keelatud.

ISKE tulevastes versioonides on plaanis praegu fakultatiivne (vabatahtlik) nõue teha kohustuslikuks nõudeks.

HS: Teabe konfidentsiaalsuse turvameetmed

Meetmete nimekiri

HS.11 Lisanõuded andmekandjate turvalisele kasutamisele

M 2.167 Andmete kustutamine või hävitamine parameetrite seadmine

Juhul kui kustutamise dokumenteerimine toimub digikujul, siis tuleb lisaks andmete kustutamise või hävitamise nõuetele arvestada veel nõudega, et kustutamist kajastavat logi ei tohi olla võimalik kaugpöördusmeetoditel muuta, vaid üksnes (vajadusel) lugeda.

HS.17 Lisanõuded külastajate saatmisele

M 2.16 Välispersonali ja külastajate valve ja saatmine parameetrite seadmine

Lisaks välispersonali ja külastajate valve ja saatmise nõuetele peab külalise vastuvõtjal külastajaga olema kogu külastusperioodi vältel silmside ning ta peab jälgima külalise kõiki toiminguid. Erandiks on WC, vannitubade, köökide jm selliste ruumide külastamine, kus ei asu infosüsteeme ega -turbe seisukohalt olulisi seadmeid. Sel juhul peab külalise vastuvõtja ootama külalist nimetatud ruumi ukse taga ning eelnimetatud ruumidel ei tohi olla teisi väljapääse.

HS.31 Lisanõuded ruumide paigutusele

M 1.13 Kaitset vajavate ruumide paigutus parametriseering

Kõrgkonfidendtsiaalsustsoonide (turvaosaklass S3) ruumid peavad lisaks kaitset vajavate ruumide paigutusele esitatavatele nõuetele vastama veel alljärgnevatele nõuetele:

- Esimese korruse ruumide aknad peavad olema varustatud trellide, turvaruloode või turvaklaasidega. Sama nõue kehtib kõrgemate korruse korral, kui akende taga väljaspool on katus, karniis vm ehitustarind, mida mööda saab sissetungija hõlpsalt akendeni liikuda.
- Kui kõrgkonfidentsiaalsustsooni ruumidega külgnevad avatud tsooni ruumid (kuhu pääsu ei kontrollita), siis ei tohi eraldusvaheseinad olla valmistatud kipsplaadist, puitkiudplaadist vm kergesti purustatavast materjalist. Kui nimetatud vaheseinte taga on kontoriruumid, kuhu võõrad vabalt ei pääse ja kus kehtib külastajate saatmise nõue (vt M 2.16 Välispersonali ja külastajate valve ja saatmine), siis nimetatud nõuded ei kehti.
- Kõik ehitustööd kõrgkonfidentsiaalsustsooni ruumides tuleb eelnevalt kooskõlastada turvajuhiga, samuti peab turvajuht olema ehitustööde tellijapoolses vastuvõtukomisjonis.
- Kõrgkonfidentsiaalsustsooni(de) ruumid tuleb ülejäänud ruumidest helikindlalt isoleerida, juhul kui nendes ruumides arendatakse turvaosaklassi S3 kuuluvaid vestlusi või kuulatakse läbi vastava konfidentsiaalsusosaklassiga fonogramme.

HS.34 Lisanõuded kolimise turbele

M 2.177 Kolimise turve parameetrite seadmine

Lisaks kolimise turbe nõuetele peab lähtuma järgnevast:

- turvajuht peab osalema logistiliste kolimisplaanide koostamises nende algusest peale
- kõiki konfidentsiaalseid dokumente, andmekandjaid, arvuteid jm teavet sisaldava materjali kolimise plaani peab turvajuht kinnitama
- deponeeritud paroolide, pääsuvahendite jm kolimise juures peab olema turvajuht isiklikult või tema poolt spetsiaalselt selleks volitatud isik.

HS.39 Lisanõuded andmebaaside krüpteerimisele

M 4.72 Andmebaasi krüpteerimine parameetrite seadmine

Kui infosüsteemi äriloogika nõuab andmebaasi krüpteerimisel *offline* -krüpteerimise asemel kindlasti *online* -krüpteerimist, tuleb lisaks andmebaasi krüpteerimise nõuetele juhinduda alljärgnevast:

- Andmehaldus ja andmebaasi kasutajate haldus peavad olema andmebaasitarkvara vahenditega eraldatud ning volitatud erinevatele füüsilistele isikutele vastavalt rollide lahutamise põhimõtetele.
- Andmed peavad ketastel olema salvestatud krüpteeritud kujul; selleks kasutatavad krüptovahendid peavad vastama HT.52 Lisanõuded krüptovahenditele nõuetele.
- Andmebaasiga peab olema liidestatud niisugune riistvaraline turvamoodul (HSM, *hardware security module*), mille põhirolliks on andmete krüpteerimine/dešifreerimine ja mille võtmehaldus põhineb kopeerimatuse ja pöördkonstrueerimatuse põhimõttel. Turvamooduli füüsiline keskkond peab vastama meetme M 4.87 Krüptomoodulite füüsiline turve nõuetele.

HS.40 Juhtmeta klaviatuuri kasutuskeeld

M 4.254 Juhtmeta klaviatuuri ja hiire turvaline kasutuselevõtt parameetrite seadmine

Turvaosaklassiga S3 andmete töötlemisel ei tohi kasutada juhtmeta klaviatuure.

Keeld ei kehti kahe erandjuhu korral:

- kui ruum on varustatud sertifitseeritud ja testitud kiirguskaitsega, mis garanteerib, et klaviatuuri sidesignaalid väljapoole ruumi (kiirguskaitse ala) ei levi;
- kui traadita klaviatuuri liides kasutab turvalist sideprotokolli, mis kaitseb autentsust, terviklust ja konfidentsiaalsust ning mille poolt kasutatavad krüptovahendid vastavad HT.52 Lisanõuded krüptovahenditele nõuetele.

HS.48 Kõrgkonfidentsiaalsuse lisanõuded IT kaabelduse paigaldusele

M 1.68 Nõuetele vastav installatsioon parameetrite seadmine

Lisaks nõuetele vastava installatsiooni nõuetele tuleb kaabliutre paigutusel arvestada järgnevaga:

Kui lähestikku asetsevad konfidentsiaalsusosaklassiga S3 andmeid krüpteerimata kujul edastavad andmesidekaablid ning kaablid, mille üks ots väljub turvatsoonist, siis tuleb need kaablid asetada montaažil üksteisest vähemalt 10 cm kaugusele. Nimetatud nõue kehtib kaablite paralleelse asetuse korral, kus üksteisele lähemal asuvad paralleelsed kaablid võivad tekitada omavahelist läbikostvust, seega võimaldada pealtkuulamist väljaspool turvatsooni.

Nõue ei kehti kaablite ristumisel ning muudes kohtades, kus kaablid kulgevad vähem kui 10 cm läheduses lühemalt kui 20 cm pikkuselt.

HS.51 Lisanõuded tundlike ressursside hävitamisele

M 2.13 Tundlike ressursside jäljetu hävitamine ja M 4.32 Andmekandjate füüsiline kustutamine enne ja pärast nende kasutamist parameetrite seadmine

Lisaks ülaltoodud meedetes väljatoodud nõuetele peab järgima Eesti Rahvusarhiivi vastavaid soovitusi, mis on saadaval arhiivi soovituste rubriigis veebiaadressil http://www.ra.ee/public/Juhised/digiinfo_havitamine.pdf

Lisaks tuleb lisatähelepanu pühendada välkmäluseadmete (mälupulgad, mälukaardid jms) hävitamisele, mida tuleb teha ühel kahest alljärgnevast meetodist:

- seade põletatakse tulekoldes (hävitatakse vähemalt 200 C temperatuuri juures);
- seadme kiip purustatakse mehaaniliselt (nt haamriga alasil).

HS.54 Lisanõuded turvalisele kustutamisele

M 4.56 Turvaline kustutus Windows operatsioonisüsteemides parametriseering

Lisaks turvalise kustutamise nõuetele Windows operatsioonisüsteemides tuleb andmed kõikidelt korduvkirjutatavatelt andmekandjatelt kustutada sellise tarkvaraga, mis tagab andmete vähemalt kolmekordse ülekirjutamise pseudojuhusliku bitijada ehk valge müraga. Niisuguse bitijada saab genereerida kahel viisil:

- Riistvaral (füüsikalistel protsessidel) põhineva juhuarvugeneraatoriga.
- Sümmeetrilise krüptoalgoritmi käimalaskmisel tagasiside režiimis, mis tagab piisavalt pseudojuhusliku bitijada, mis statistiliste ja muude testidega ei ole eristatav tõelisest juhuslikust bitijadast. Siin kasutatavad krüpteerimisalgoritmid peavad vastama HT.52 Lisanõuded krüptovahenditele nõuetele.

Turvaliseks kustutamiseks kasutatav tarkvara peab olema aktsepteeritud asutuse turvajuhi poolt, kes peab tagama selle vastavuse eelkirjeldatud nõuetele.

Lisateavet vt Rahvusarhiivi turvalise kustutamise/hävitamise soovitustest http://www.ra.ee/public/Juhised/digiinfo_havitamine.pdf

HS.56 Paroolide taastamise/uuendamise lisanõuded

M 2.402 Paroolide uuendamine parameetrite seadmine

Konfidentsiaalsusosaklassiga S3 andmetele ligipääsul tuleb lisaks paroolide uuendamise nõuetele lähtuda lisaks järgmistest nõuetest:

- Paroolide edastamine posti, faksi ja telefoni teel, samuti usaldusisiku kaudu on keelatud. Erandjuhtusid võib siin teha turvajuhi eriotsusel, kes peab hindama tegevuse jääkriske turvapoliitika valguses (nt parooli üks osa saata postiga, teine GSM-mobiilivõrgu SMS-ga vms). Kõiki nimetatud erandeid tuleb käsitleda meetme M 2.380 Erandite kooskõlastamine kohaselt.
- Paroolipõhine autentimine paroolide uuendamisel/taastamisel on lubatud vaid neil juhtudel, kui seda kasutatatakse kombineeritud autentimismeetodi (ID-kaart, MAC-aadress vms) ühe komponendina.

HS.59 Eraldi printer kõrgkonfidentsiaalsetele andmetele

Unikaalmeede

Kui asutuses on vajadus konfidentsiaalsusosaklassiga S3 andmete printimiseks ühiskasutuses oleva võrguprinteriga, tuleb selleks kasutada spetsiaalses turvatsoonis asuvat spetsiaalset printerit, millega muid printimistöid (mitte-S3 andmete printimistöid) ei tehta.

Nõue ei kehti juhtumitel, kui S3 andmete printimiseks kasutatav printer asub arvutiga samas ruumis, st arvutilt pintimiskäsku andval töötajal on printer kogu aeg silma all.

Vt ka M 2.397 Printerite, koopiamasinate ja multifunktsionaalsete seadmete kasutamise planeerimine ja M 2.398 Printerite, koopiamasinate ja multifunktsionaalsete seadmete kasutusjuhised .

HS.60 Juuresolekunõue kõrgkonfidentsiaalsete dokumentide paljundamisel

Unikaalmeede

Konfidentsiaalsusosaklassiga S3 andmete kopeerimisel koopiamasinaga ei tohi masinat kopeerimisprotsessis (kuni kopeeritavate ja kopeeritud dokumentide eemaldamiseni) jätte järelevalveta. Kui niisuguseks kopeerimiseks kasutatakse ühiskasutuses olevaid koopiamasinaid (mis ei asu töötaja kabinetis), siis ei tohi töötaja enne kopeerimisprotsessi lõppu masina juurest lahkuda.

Kui kopeerimiseks ja/või paljundamiseks kasutatav teade jätab paljundamisteabe alles oma sisemisele andmekandjale, võib selliseid seadmeid installeerida ainult turvaosaklassiga S3 turvatsooni.

Vt ka M 2.398 Printerite, koopiamasinate ja multifunktsionaalsete seadmete kasutusjuhised .

HS.61 Lisanõuded printerite, koopiamasinate ja multifunktsionaalsete seadmete ja nende komponentide kasutuselt kõrvaldamisele

M 2.400 Printerite, koopiamasinate ja multifunktsionaalsete seadmete turvaline kasutuselt kõrvaldamine parametriseering

Lisaks ülaltoodud meetmes väljatoodud nõuetele tuleb kõik niisugused printerid, koopiamasinad ja nende lisaseadmed ning kulumaterjalid, milledele võib töö käigus olla salvestatud konfidentsiaalseid andmeid, mis on seal hiljem loetavalt säilinud, hävitada samadel alustel konfidentsiaalsete dokumentide ja andmekandjatega. Soovitav on hävitustöö tellida spetsiaalselt dokumentide ja seadmete hävitamise firmalt, kellega tuleb sõlmida vastav konfidentsiaalsusleping.

Millised seadmed ja komponendid nimetatud loetelu alla kuuluvad, on turvajuhi otsustada, kes vastutab selle eest, et kogu konfidentsiaalne jääkteave saaks jälgi jätmata hävitatud. Turvajuht korraldab ka hävitusprotsessi.

Vt ka M 2.13 Tundlike ressursside jäljetu hävitamine .

HS.62 Infrapunaliidese ja bluetooth ’i kasutuskeeld

M 4.255 Infrapunaliidese kasutamine parametriseering

Kõrgkonfidentsiaalsuse (turvaosaklass S3) korral tuleb lisaksinfrapunaliidese kasutamise nõuetele lähtuda alljärgnevast:

- Infrapunaliidese ja *bluetooth* ’i kasutamine andmeedastuseks on keelatud, see tuleb asendada kaablipõhise andmeedastusega.
- Nendel aegadel, mil mobiilseadmes (mobiiltelefon, PDA, analoogid) töödeldakse turvaosaklassiga S3 andmeid krüpteerimata kujul (vt HT.56 Lisanõuded mobiilsele kaugtööarvutile nõuded) peavad infrapunaliides ja *bluetooth* olema deaktiveeritud.
- Enne infrapunaliidese ja *bluetooth* i aktiveerimist peab kasutaja veenduma, et kõrgkonfidentsiaalseid andmeid töötlenud rakendus oleks töö lõpetanud ning sellised andmed esineksid seadmes ainult krüpteeritud kujul.

HS.63 Häälteabe kõnepõhine edastuskeeld

Unikaalmeede

Kõrgkonfidentsiaalset (turvaosaklass S3) teavet ei tohi GSM-põhises mobiiltelefonivõrgus tavarežiimis edastada, kuna kasutatavad krüptoalgoritmid ja protokollid ei taga selleks piisavat turvet.

Keeld ei kehti juhtumeil, kui kõne krüpteeritakse lisaks GSMi enda vahenditele ka mobiiltelefoni, PDA (või muu seadme) põhiselt ja kasutatavad krüptovahendid vastavad HT.52 Lisanõuded krüptovahenditele nõuetele. Sel juhul peab kasutatava tarkvara ja konfiguratsiooni turvajuht kirjalikult kinnitama, veendudes eelnevalt selle turvalisuses.

Vt ka M 5.80 Kaitse mobiiltelefonidega pealtkuulamise eest

HS.65 Tarkvaratelefonide kasutuskeeld

Unikaalmeede

Põhimõtteliselt võib jagada IP-kõne terminalid kahte rühma:

- Tarkvaralahendused, mis installeeritakse töökoha arvutisse või siis eraldiseisvasse arvutisse ning mis vajavad oma tööks laiatarbe operatsioonisüsteemi (nt Windows, *Linux* jne.). Audioseadmena kasutatakse neil juhtumeil reeglina mikrofoniga kõrvaklappe. Sellist tüüpi terminale nimetatakse inglise keeles *softphones*.
- Eraldiseisvad telefonid, mis on väliselt sarnased telefonivõrgus kasutatavate süsteemitelefonidega, kuid, millel on telefonivõrgu ühenduse asemel kohtvõrgu ühendus. Ka telefoniadapterid, mis võimaldavad ühendada olemasoleva tavatelefoni (sh ka traadita telefoni) IP-kõne võrguga, kuuluvad siia.

Tarkvaratelefonid, mis on installeeritud rakendusena arvutisse, on eraldiseisvatest telefonidest tunduvalt suurema haavatavusega (kuigi ka IP telefonid aparaadina võivad olla üsna haavatavad), kuna nii operatsioonisüsteem, kui ka arvutisse installeeritud muud rakendused ja teenused võivad omada mitmeid turvaauke ja nende algset funktsionaalsust saab süsteemiülema õigusi omades lihtsalt muuta. Seetõttu ei tohi kõrge konfidentsiaalsusastme (S3) korral kasutada tarkvaralisi telefone, vaid peaks hankima eraldiseisvad, reeglina riistvaral põhinevad IP-telefonid.

Omaette klassi terminale moodustavad traadita IP-kõne terminalid. Ka need võivad olla realiseeritud tarkvaralahendusena, mis installeeritakse näiteks mobiiltelefoni või pihuarvuti rakendusena, kuid on ka spetsiaalseid traadita IP-kõne terminale. Traadita IP-kõne terminalid kasutavad ühenduseks traadita kohtvõrku. Erinevate käideldavuse ja konfidentsiaalsuse piirangute tõttu ei tohiks kõrge konfidentsiaalsusastme korral kasutada ka traadita IP-kõne terminale.

Erandina võib tarkvaratelefone kasutada juhtumeil, kui side on turvatud/krüpteeritud võrgu tasemel (tavaliselt VPN-tehnikaga) ja seal kasutatavad krüpteerimisvahendid vastavat HT.52 Lisanõuded krüptovahenditele nõuetele.

HS.69 Exchange/Outlook 2000 turbesuuniste regulaarseire

M 2.248 Exchange/Outlook 2000 turvapoliitika määratlemine parametriseering

Lisaks ülaltoodud meetmes sätestatule tuleb seal kirjeldatud turbesuuniseid regulaarselt kontrollida. Nende kontrollimise/ülevaatamise eest vastutab turvajuht ja seda peab tegema pisteliselt vähemalt neli korda aastas. Neile peavad lisanduma veel erakorralised kontrollid, mis tuleb viia läbi järgnevatel juhtudel (nädala jooksul pärast juhtumi toimumist):

- Exchange'i/Outlook'i tarkvara või serverit uuendatakse;
- toimub turvaintsident, mis on seotud Exchange'i või Outlook'iga;
- avastatakse turvaauk Exchange'is/Outlook'is mille kõrvaldamine (paikamine) muudab olemasolevaid seadeid

HS.72 IP-kõne täismahus krüpteerimise nõue

Unikaalmeede

Kõrgtasemel konfidentsiaalsusnõuete (turvaosaklassi S3) korral tuleb süsteemi skoopi kuuluvad IP kõned kõik ilma eranditeta krüpteerida. Kasutatavad krüpteerimisalgoritmid peavad vastama turvameetme HT.52 Lisanõuded krüptovahenditele nõuetele. Vt ka M 2.374 IP-kõne krüpteerimise ulatus .

HS.73 Traadita kohtvõrgu kasutuskeeld

Unikaalmeede

Nendes infosüsteemi komponentides, kus konfidentsiaalsusosaklass on kõrgtasemel (S3), ei tohi üle avaliku traadita kohtvõrku kasutades andmeid öödelda. - need tuleb asendada kas traadipõhiste lahendustega või kasutada sisemist ja turvatud asutuse traadita kohtvõrku. Vt ka M 2.381 Traadita kohtvõrgu kasutamise strateegia väljatöötamine .

HS.74 Piirangud IT süsteemide virtualiseerimisele

M 2.392 Virtualiseerimisserverite ja virtuaalsete IT-süsteemide modelleerimine parameetrite seadistamine

Turvaosaklassidega S3 süsteemides tuleb süsteemide virtualiseerimisega olla äärmiselt ettevaatlik ja tagasihoidlik, sest tark- või riistvaraviga (leitud turvaauk) virtualiseeritud süsteemides võib viia selleni, et üks virtuaalne süsteem võib seda turvaauku ärakasutades (*exploit*) pääseda ligi teise süsteemi andmetele ja halvemal juhul ka äriloogikale.

Seepärast tuleb lisaks virtualiseerimisserverite ja virtuaalsete IT-süsteemide modelleerimise sätetele juhinduda alljärgnevast:

- Kõiki virtualiseerimisi tuleb vaadelda kui reeglist hälbivaid erandeid, mida reguleerib meede M 2.380 Erandite kooskõlastamine
- Kõik virtualiseerimised tuleb kooskõlastada turvajuhiga, kes peavad enne selle lubamist igal konkreetsel juhtumil korraldama spetsiaalse turvaanalüüsi. Sellise analüüsi eesmärgiks on välja selgitada, kas virtualiseerimisega kaasnevad konfidentsiaalsuskaoriskid on konkreetses situatsioonis talutavad ning milliste täiendavate turvameetmete rakendamist nad tingivad.
- Kõik juba lubatud virtualiseerimisjuhtumite virtualiseerimiskonfiguratsioonide muudatused (uue alamsüsteemi lisamine, vana eemaldamine, administreerimissüsteemi muutmine vms) peavad saama turvajuhi täiendava heakskiidu ja neid tuleb vaadelda ja käsitleda samuti nagu erandeid (vt M 2.380 Erandite kooskõlastamine).

HS.75 Lisanõuded infovahetuse reguleerimisele

M 2.393 Infovahetuse reguleerimine parameetrite seadmine

Turvaosaklassiga S3 teabe infovahetuse korral tuleb lisaks infovahetuse reguleerimise nõuetele arvestada alljärgnevaga:

- Turvajuht peab turvaosaklassiga S3 andmete vahetuse üle pidama eriarvet.
- Igasugused muudatused infovahetuse põhimõtetest (äriloogikas) ja kasutatavates tehnilistes vahendites tuleb kooskõlastada turvajuhiga.

Eeltoodud lisanõudeid ei ole vaja rakendada juhtumitel, kui teave on vahetusfaasis krüpteeritud kujul (vastavalt HT.52 Lisanõuded krüptovahenditele nõuetele) ning dešifreerimist võimaldavad andmed/vahendid asuvad turvaosaklassiga S3 tsoonis. Täpsemalt – dešifreerimisvahend peab andmete töötlemise ajal asuma turvatsoonis (muul ajal pole see kohustuslik, nt ID kaardiga dešifreerimise korral).

HS.76 Mobiilsete andmekandjate võimalik vältimine

Unikaalmeede

Konfidentsiaalsusosaklassiga S3 andmete hoidmisel ja edastamisel tuleb mobiilsete andmekandjate kasutamist andmehõived võimalikult vältida. Kõiki sellest reeglist eiramisi tuleb vaadelda eranditena (vt M 2.380 Erandite kooskõlastamine), mida võib teha vaid turvajuhi eriloal, kes peab hindama sellega kaasnevaid riske ja nende talutavust vastavalt kehtivale infoturbepoliitkale.

Juhul kui turvajuht on S3 andmete käitlemiseks mobiilsel andmekandjal eriloa andnud, peab kasutusjuhtum vastama järgmistele tingimustele:

- Käibelt kõrvaldamisel tuleb andmekandja hävitada (vastavalt HS.51 Lisanõuded tundlike ressursside hävitamisele nõuetele), keelatud (ilma eranditeta) on selle sisu turvaline kustutamine ja andmekandja kasutselevõtt mingis teises valdkonnas.
- Kui andmekandja viiakse väljapoole turvaosaklassiga S3 turvatsooni (kas- või lühiajaliselt), peab selle sisu olema alati ja ilma eranditeta krüpteeritud (vastavalt HT.52 Lisanõuded krüptovahenditele nõuetele).

HS.77 Kiirgusturve

Algatamise eest vastutavad: IT-turbespetsialist
Rakendamise eest vastutavad: IT-turbespetsialist

Iga elektrooniline seade kiirgab rohkemal või vähemal määral tugevaid elektromagnetilisi laineid. See kiirgus on tuntud kui elektromagnetiline koormus ning selle maksimaalselt lubatud tugevus on üldjuhul seaduses reguleeritud. Eestis on selleks kiirgusseadus (RT I 2009, 48, 322). Infotöötlusseadmete puhul (PC, printer, faksiaparaat, modem jne), võib see elektromagnetiline kiirgus endas kanda ka hetkel töödeldavat infot. Sellist infot kandvat kiirgust nimetatakse paljastavaks kiirguseks. Kui paljastav kiirgus püütakse kinni teatud kauguses, nt naabermajas või lähedusesasuvas sõidukis, saab selle abil infot taastada. See ohustab andmete konfidentsiaalsust. Reeglina tuleb sellise tegevuse takistamiseks tarvitusele võtta lisameetmed.

Paljastav kiirgus võib ruumist lahkuda mitmel erineval moel:

- Elektromagnetiliste lainetena, mis levivad vabas ruumis nagu raadiolained.
- Juhtmaterjaliga seotud kiirgusena mööda metalljuhte (kaabeleid, kliimašahte, küttetorusid).
- Andmekaabli ja paralleelselt jooksva kaabli kattumisel. Kiirgus levib paralleelkaablil pikalt edasi ja on veel kaugel pealtkuulatav.
- Akustilise kiirgusena, nt printeritel. Printimise detailinfo levib heli või ultraheli kaudu ja on mikrofonidega salvestatav.
- Akustilisel kattuvusel teiste seadmetega. Heli muutmine elektrisignaalideks toimub heli suhtes tundlike seadmedetailidega, mis võivad teatud eeldustel töötada nagu „mikrofon“. Edasi toimub levimine mööda metalljuhti või elektromagnetilise ruumikiirguse kujul.
- Paljastavat kiirgust võib tekitada ka seadmete väline manipulatsioon. Kui nt kiiritada seadet kõrgsagedusliku energiaga, võivad seadmes toimuvad elektrilised protseduurid saabuvaid laineid selliselt mõjutada, et need kannavad endas nüüd töödeldud infot.

Igal juhul mõjutab seadmete installatsioon ehk nende omavahelised kaablid ja ühendus vooluvõrguga olulisel määral kiirguse levikut ja seega ka ulatust.

Järgnevalt on välja toodud mõningad kaitsemeetmed mis vähendavad ohtu ilma et sellega kaasneks olulisi lisakulusid:

Tsoonimudel

Tsoonimudel arvestab paljastava kiirguse levimistingimustega seoses vastavate hoone –ja maastikutingimustega. Seejuures mõõdetakse põhjustavast ITseadmest potentsiaalse vastuvõtjani leviva kiirguse nõrgenemist. Sõltuvalt kasutuskoha omadustest võib kasutada ka seadmeid, milles on võetud tarvitusele ainult vähesed häirevähendamise meetmed või siis selliseid, millel need üldse puuduvad.

Häire piiramine allikas

Häire piiramine allikas on eriti tõhus uute IT-toodete arendamisel. Antud juhul vähendatakse või muudetakse paljastavat kiirgust juba tekkekohas seadme sees selliselt, et seda ei saaks enam kasutada. Tänu sellele meetodile on nt võimalik kasutada ka soodsamat plastikkorpust, mis tõstab toote hinda vaid tühisel määral.

Lühimõõtmise meetod

Lühimõõtmise meetodi ja manipulatsiooni kontrollmeetodi väljatöötamine võimaldab tagada kiirgusturvalisust vähese vaevaga ka pärast hooldust, parandamist või võimalikke volitamatuid juurdepääse.

Vähese kiirgusega või varjestatud seadmete kasutamine

PC-monitoride tootjad reklaamivad sageli mõistega „vähese kiirgusega“ vastavalt normidele MPR II, TCO või SSI. Need direktiivid arvestavad eranditult seadmete kiirguse võimalike tervist kahjustavate mõjudega. Seega ei sobi kiirguse mõõtmismeetodid ja piiväärtused paljastava kiirguse tõendamiseks ja sarnaselt elektromagnetilise ühilduvuse (EMC) mõõtmistele ei võimalda hinnata andmete volitamatu pealtkuulamise ohtu.

See, kas tootja pakub varjestatud seadmeid, mis vastavad nn TEMPEST-kriteeriumitele, tuleb kindlaks teha küsides tootja käest, või uurides Kinnituse juurde, et seadmel on olemas TEMPEST-luba, kuulub alati ka loaastme info.

Asutuse turvajuht peab vähemalt kaks korda aastas tutvuma asutuses kasutatavate tarnspordikrüpto (nt CDOC-vormingus krüpteerimise) lahendustega. Peamiselt seisneb see kontroll vastavate töötajatega vestlemises, kes transpordikrüpto vorminguskrüpteerimist või krüpteeritud failide dešifreerimist oma igapäevatöös kasutavad.

Kui asutuses ilmneb turvaintsident, mille osaks on transpordikrüpto vahendite väär kasutamine või vajalike failide krüpteerimata jätmine, tuleb turvaintsidendi järgselt läbi viia erakorraline kontroll.